USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Descomposición primaria de ideales

Irene Macías Tarrío

2020/2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Descomposición primaria de ideales

Irene Macías Tarrío

Xullo, 2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Descomposición primaria de ideais
Breve descrición do contido
Unha das ferramentas fundamentais da álxebra conmutativa é a descomposición primaria dun ideal, non só polo seu alcance teórico, senón tamén pola parte práctica, pola información que proporciona sobre o ideal e, en consecuencia, sobre a variedade alxébrica que define. O obxectivo do traballo é estudar esta descomposición para entender mellor a estrutura dos aneis e ideais co fin de poñer en relevo o papel dos ideais primarios e primos inmersos.
Recomendacións
É recomendable cursar a materia "Álxebra, Números e Xeometría".
Outras observacións
Bibliografía: R. Y. Sharp, *Steps in Commutative Algebra*, 2nd ed. LMS, Student Texts 51, Cambridge University Press, 2000. I. Swanson, *Primary decompositions*, `https://www.math.purdue.edu/~iswanso/primdec.pdf`

Índice general

Resumen

En este trabajo trataremos en profundidad la idea de descomposición primaria de un ideal en un anillo Noetheriano, probando la existencia de la misma, dando ejemplos, y aplicaciones en geometría.

En primer lugar, recordaremos conceptos básicos de ideales, y distintos tipos de estos, así como propiedades de los mismos. Luego demostraremos paso a paso la existencia de una descomposición primaria de un ideal en un anillo Noetheriano, y, como consecuencia, obtendremos una descomposición primaria minimal. Hablaremos también de la unicidad de estas descomposiciones y aclararemos todas estas ideas con ejemplos.

Por último, veremos la relación entre ideales y variedades estableciendo el diccionario álgebra–geometría, y traduciremos esta descomposición primaria a la geometría, viendo así una aplicación de la misma. Terminaremos el trabajo exponiendo ejemplos de cómo podemos hacer cálculos efectivos de la descomposición primaria de un ideal en el anillo de polinomios usando el software SageMath.

Abstract

In this work, we will deal in depth with the idea of the primary decomposition of an ideal in a Noetherian ring, proving the existence of this one and giving examples and applications in geometry.

First of all, we shall recall some basic notions of ideals and different types of them and some of their properties. After this, we will prove step by step the existence of a primary decomposition of an ideal in a Noetherian ring and, consequently, we will obtain a minimal primary decomposition. We will also talk about the uniqueness of these decompositions, and we will clear up all these ideas by giving examples.

Finally, we will see the relationship among ideals and varieties by establishing the algebra–geometry dictionary, and we will translate this primary decomposition to geometry, going over one of its applications. We will end the work by showing examples of how we can make effective calculus of primary decomposition of an ideal in the polynomial ring using SageMath software.

Introducción

El teorema de descomposición primaria es un resultado bien conocido en álgebra conmutativa, que afirma que todo ideal en un anillo Noetheriano es intersección finita de ideales primarios. El teorema fue probado, en el año 1905, por Emanuel Lasker (1868–1941, ajedrecista, matemático y filósofo alemán, y campeón del mundo de ajedrez de 1894 a 1921) para los anillos de polinomios y series de potencias, y en el año 1921, por Emmy Noether (1882–1935, matemática alemana, especialista en la teoría de invariantes y conocida por sus contribuciones de importancia fundamental en los campos de la física teórica y del álgebra abstracta) para anillos Noetherianos.

El teorema de Lasker–Noether es una extensión del teorema fundamental de la aritmética que establece que todo número entero se puede descomponer de manera única, salvo unidades, como producto de números primos.

Los ideales primarios fueron definidos por primera vez por Lasker, como generalizaciones de los ideales primos. Los ideales primarios son a los primos lo que las potencias son a los primos en el anillo de los números enteros. Traducido al lenguaje de la geometría algebraica, el resultado dice que toda variedad es unión finita de variedades irreducibles, es decir, aquellas que no pueden descomponerse de forma no trivial como uniones finitas de otras variedades.

Francis Macaulay (1862–1937, matemático inglés que hizo grandes contribuciones a la geometría algebraica) demostró la unicidad de la descomposición primaria, lo cual implica que toda variedad puede expresarse de forma única como unión de variedades irreducibles, una especie de teorema fundamental de la aritmética de las variedades. También hay que mencionar las importantes contribuciones de David Hilbert (1862–1943, matemático alemán que más impactó en el desarrollo de las matemáticas durante los siglos XIX y XX) a este tema, que luego influyeron en su trabajo sobre los invariantes.

La prueba de Lasker del teorema de descomposición primaria fue un cálculo largo y complicado. Como veremos en este trabajo, una perspectiva más amplia da mucho más con mucho menos esfuerzo. El Teorema de Lasker es una consecuencia inmediata del Teorema de Noether junto con el Teorema de la Base de Hilbert (si R es un anillo Noetheriano,

entonces los anillos $R[x]$ y $R[[x]]$ son Noetherianos, donde $R[[x]]$ es el anillo de series de potencias formales), que se demostró en 1888 y cuya prueba, notablemente corta y simple, generó primero controversia y luego una profunda admiración. Lo mismo ocurre con el teorema de Noether. Es a partir de este teorema, y la extraña sencillez de su demostración, que los anillos Noetherianos reciben su nombre.

Noether, en su artículo trascendental de 1921, extendió la teoría de descomposición en los anillos de polinomios a anillos conmutativos abstractos con la condición de cadena ascendente, ahora llamados anillos Noetherianos. Más concretamente, Noether demostró en dicho artículo, titulado "Idealtheorie in Ringbereichen" ("Teoría de ideales en anillos"; una versión traducida al inglés en el año 2014 puede verse en [7]), que los resultados de Hilbert, Lasker y Macaulay sobre la descomposición primaria en los anillos de polinomios eran válidos para cualquier anillo (abstracto) con la condición de cadena ascendente. Así, resultados que parecían intrincadamente relacionados con propiedades de los anillos de polinomios, ¡¡se demostraron que se deducen de un único axioma!!

Noether también comenzó a desarrollar, en su artículo de 1921, una teoría general de ideales para anillos conmutativos. Las nociones de ideal primo, primario e irreducible, intersección y producto de ideales aparecen en este artículo; en resumen, gran parte de la maquinaria de la teoría de ideales. En la parte final de su artículo definió el concepto de módulo sobre un anillo no conmutativo.

La descomposición primaria de un ideal en el anillo de polinomios sobre un cuerpo es una de las herramientas indispensables tanto en álgebra conmutativa como en geometría algebraica. Geométricamente, corresponde a la descomposición de una variedad afín en sus componentes irreducibles, y es por lo tanto un concepto geométrico importante.

Posteriormente, la descomposición primaria fue extendida a módulos, en concreto, todo submódulo de un módulo finitamente generado sobre un anillo conmutativo Noetheriano es intersección finita de submódulos primarios. En el caso especial de considerar un anillo como módulo sobre sí mismo, se obtiene la descomposición primaria para ideales en un anillo pues los submódulos son precisamente los ideales.

El primer algoritmo práctico y general de descomposición primaria en el anillo de polinomios fue dado por Gianni-Trager-Zacharias [6] en 1988, usando bases de Gröbner. Posteriormente, Shimoyama-Yokoyama [9], en 1996, proporcionaron un nuevo algoritmo, también usando bases de Gröbner, para obtener una descomposición primaria a partir de los ideales primos asociados minimales.

Procederemos ahora a exponer el contenido de este trabajo. Esta memoria se divide en tres capítulos estructurados de la siguiente forma.

Empezaremos el capítulo 1 tratando una secuencia de resultados básicos de la teoría de anillos conmutativos.

En la sección 1.1, introducimos los conceptos de ideal, producto de ideales, dominio de ideales principales (DIP), y anillo Noetheriano.

En la sección 1.2 continuamos con definiciones básicas como las de ideal primo, maximal, radical y cociente, o elemento primo y elemento irreducible. También comentamos algunos resultados que establecen la equivalencia entre estos elementos bajo ciertas condiciones, así como propiedades de estos tipos de ideales.

El capítulo 2 es la parte esencial de este trabajo y consta de seis secciones.

En la sección 2.1, introducimos la idea de descomposición primaria como una generalización de que todo DIP es un dominio de factorización única (DFU) y damos una primera justificación poco rigurosa para la existencia de la misma.

En la sección 2.2, comenzamos definiendo lo que es un ideal primario e ideal P-primario. A continuación, exponemos diferentes resultados sobre los mismos que acompañamos con varios ejemplos para aclarar estas ideas.

La sección 2.3 trata sobre dos resultados claves para expresar un ideal como la intersección finita de ideales primarios. Uno establece que la intersección de ideales P-primarios es un ideal P-primario, y otro el papel que juega el ideal cociente $(Q : a)$, donde Q es un ideal P-primario y $a \in R$, en ciertos casos particulares.

En la sección 2.4, definimos la descomposición primaria de un ideal, dando algunos ejemplos.

En la sección 2.5, hablamos primeramente de cómo obtener a partir de una descomposición primaria una descomposición primaria minimal. A continuación enunciamos y probamos el primer teorema de unicidad para la descomposición primaria de un ideal. Este habla de la independencia del número de términos, así como del conjunto de ideales primos que aparecen como ideales radicales de los ideales primarios, para cualquier descomposición primaria minimal que se tome. Además, damos ejemplos de descomposiciones primarias minimales de un ideal donde se ve que esta descomposición no es única, e incluso se pueden encontrar infinitas descomposiciones. Luego, presentamos el segundo teorema de unicidad para la descomposición primaria de un ideal I, probando que el término primario correspondiente a un ideal primo minimal de I está determinado de forma única por I, y por lo tanto independiente de la descomposición primaria minimal elegida.

En la última sección, sección 2.6, nos centramos en la descomposición primaria de un ideal en un anillo Noetheriano. Definimos el concepto de ideal irreducible y exponemos su

relación con los ideales primos y primarios, haciendo hincapié en un DIP. Probamos que todo ideal propio en un anillo Noetheriano se puede expresar como intersección finita de ideales irreducibles, y, como consecuencia, tendrá siempre una descomposición primaria, y por lo tanto una descomposición primaria minimal.

Para cerrar esta sección, particularizamos esta descomposición para ideales radicales y para los de la forma (f), donde $f = u\prod p_i^{e_i}$, y damos un par de ejemplos más, con mención especial en un anillo Noetheriano que no es un DFU.

En el capítulo 3 damos aplicaciones de la descomposición primaria en geometría.

En la sección 3.1, establecemos el diccionario álgebra–geometría, en un cuerpo algebraicamente cerrado y para ideales radicales, mediante la correspondencia biyectiva ideal–variedad que invierte las inclusiones. A continuación, usamos la descomposición primaria de un ideal en el anillo de polinomios para la obtención de la descomposición de una variedad en sus componentes irreducibles, explotando la descomposición primaria para contar la "multiplicidad" de los ceros de la variedad.

Finalizamos el capítulo 3, sección 3.2, usando el software SageMath [11] para hacer cálculos efectivos de la descomposición primaria de un ideal en el anillo de polinomios. SageMath utiliza los algoritmos de Shimoyama-Yokoyama ('sy'), por defecto, y de Gianni-Trager-Zacharias ('gtz').

Capítulo 1

PRELIMINARES

Se comenzará recordando una serie de resultados básicos de la teoría de anillos conmutativos, que se pueden encontrar en referencias básicas como [1, 8, 10], y que son adecuadas para el desarrollo de este trabajo.

1.1. Ideales

Teorema 1.1. ***Teorema de isomorfía para anillos conmutativos***
Sean R y S anillos conmutativos, y $f\colon R \to S$ un homomorfismo de anillos. Entonces f induce un isomorfismo de anillos $f : R/\ker f \to \operatorname{Im} f$, con $f(r + \ker f) = f(r)$ para todo $r \in R$.

Demostración. Sea $K = \ker f$. Veamos que f está bien definida. Tenemos que probar que si $r, s \in R$ son tales que $r + K = s + K$, entonces $f(r) = f(s)$. Esto es fácil de ver ya que $r + K = s + K$ implica $r - s \in K = \ker f$ y entonces $f(r) - f(s) = f(r - s) = 0_S$ y $f(r) = f(s)$. De aquí se sigue que hay una aplicación $f\colon R/K \to \operatorname{Im} f$ dada por la fórmula $f(r + K) = f(r)$.

También nótese que, para todo $r, s \in R$, tenemos $f((r+K)+(s+K)) = f((r+s)+K) = f(r+s) = f(r)+f(s) = f(r+K)+f(s+K)$ y $f((r+K)(s+K)) = f(rs+K) = f(rs) = f(r)f(s) = f(r+K)f(s+K)$. También, $f(1_R + K) = f(1_R) = 1_S$, el elemento identidad del subanillo $\operatorname{Im} f$ de S. Así, f es un homomorfismo de anillos. Finalmente, si $r, s \in R$ son tales que $f(r + K) = f(s + K)$ entonces $f(r - s) = f(r) - f(s) = 0_S$, y así $r - s \in K$ y $r + K = s + K$. Por lo tanto f es inyectiva, y de este modo f es un isomorfismo. □

Definición 1.2. Ideal
Sea R un anillo conmutativo. Un subconjunto I de R se dice que es un ideal de R si se satisfacen las siguientes condiciones:

- $I \neq \emptyset$;
- dados cualesquiera $a, b \in I$, entonces $a + b \in I$; y
- dados $a \in I$ y $r \in R$, entonces $r \cdot a \in I$.

Definición 1.3. Producto de ideales
Sean I, J dos ideales de un anillo conmutativo R. Entonces, el producto de I y J denotado por IJ será el ideal de R generado por el conjunto $\{ab : a \in I, b \in J\}$.

Observación 1.4. Sea R un anillo conmutativo y sean $I, J, K, I_1, \ldots, I_n$ ideales de R. Se tiene:

(i) Ciertamente $IJ = JI \subseteq I \cap J$.

(ii) Es fácil comprobar que $(IJ)K = I(JK)$ y que ambos son iguales al ideal (H) de R generado por el conjunto $H = \{abc : a \in I, b \in J, c \in K\}$. Un elemento de $(IJ)K = I(JK) =: IJK$ será de la forma $\sum_{i=1}^{t} a_i b_i c_i$ donde $t \in \mathbb{N}, a_1, \ldots, a_t \in I, b_1, \ldots, b_t \in J$ y $c_1, \ldots, c_t \in K$.

(iii) De (i) y (ii) se sigue que podemos definir el producto $\prod_{i=1}^{n} I_i$ de los ideales $I_1, \ldots, I_n$ de R: $\prod_{i=1}^{n} I_i = I_1 \cdots I_n = (L)$ donde $L = \{a_1 \cdots a_n : a_1 \in I_1, \ldots, a_n \in I_n\}$.

(iv) Es fácil ver que $I(J + K) = IJ + IK$.

(v) Las potencias I^m de I, para $m \in \mathbb{N}$, quedan definidas. Convencionalmente se determina que $I^0 = R$. Nótese que, por (iii), un elemento general de I^m (para $m > 0$) es de la forma $a_{11}a_{12} \cdots a_{1m} + a_{21}a_{22} \cdots a_{2m} + \cdots + a_{n1}a_{n2} \cdots a_{nm}$, donde $n \in \mathbb{N}$ y $a_{ij} \in I$ para todo $i = 1, \ldots, n$ y $j = 1, \ldots, m$.

En general, $IJ \subseteq I \cap J$, pero $I \cap J$ puede ser más grande que IJ.

- En $\mathbb{Z}$, $(2) \cdot (4) = (8) \subsetneq (2) \cap (4) = (4)$.
- En $K[x]$, $(x) \cdot (x) = (x^2) \subsetneq (x) \cap (x) = (x)$.
- En $K[x, y]$, $(x, y) \cdot (x, y) = (x^2, xy, y^2) \subsetneq (x, y) \cap (x, y) = (x, y)$.

Definición 1.5. Ideal principal
Un ideal se dice principal si está generado por un único elemento.

Definición 1.6. Dominio de ideales principales
Si en un dominio todo ideal es principal, se dice que es un dominio de ideales principales (DIP).

Ejemplo 1.7. Como ejemplos de DIP tenemos $\mathbb{Z}$ y $\mathbb{K}[x]$.

Pero $\mathbb{Z}[x]$ y $\mathbb{K}[x_1, \ldots, x_n]$ no lo son, ya que $(2, x)$ y $(x_1, \ldots, x_n)$ no son principales.

Definición 1.8. Anillo Noetheriano

Un anillo R se dice Noetheriano si todos sus ideales son finitamente generados. También se puede definir de otra forma. Sea $\mathcal{I}_R$ el conjunto de todos los ideales de R, entonces R es Noetheriano si el conjunto $(\mathcal{I}_R, \subseteq)$ es tal que existe $k \in \mathbb{N}$ tal que $I_k = I_{k+i}$ para todo $i \in \mathbb{N}$ (condición de cadena ascendente, CCA), o equivalentemente todo subconjunto no vacío de $\mathcal{I}_R$ contiene un elemento maximal con respecto a la inclusión (condición maximal). En otras palabras, R es Noetheriano si y solo si toda cadena ascendente $I_1 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$ de ideales de R es estacionaria y esto es así si todo conjunto no vacío de ideales de R tiene un elemento maximal con respecto a la inclusión.

Ejemplo 1.9.

- Los cuerpos, dominios euclidianos y DIPs son Noetherianos.
- $\mathbb{Z}[x]$, $\mathbb{Z}[x_1, \ldots, x_n]$, $K[x_1, \ldots, x_n]$ son Noetherianos (Teorema de la Base de Hilbert).
- El cociente de un anillo Noetheriano es Noetheriano. Así, $K[x_1, \ldots, x_n]/I$ es Noetheriano, donde I es un ideal de $K[x_1, \ldots, x_n]$.
- El anillo $R = \mathbb{Z}[\sqrt{5}i]$ es Noetheriano, ya que $\mathbb{Z}[\sqrt{5}i] \cong \mathbb{Z}[x]/(x^2 + 5)$.
- El anillo $\mathcal{C}([0, 1])$ de las funciones continuas en el intervalo $[0, 1]$ no es Noetheriano, ya que tiene una cadena estrictamente creciente infinita de ideales que no para

$$(x) \subset (x^{\frac{1}{2}}) \subset (x^{\frac{1}{4}}) \subset (x^{\frac{1}{8}}) \cdots$$

1.2. Ideales primos, maximales y radicales

Definición 1.10. Ideal maximal

Un ideal M de un anillo conmutativo R se dice maximal si M es un elemento maximal, respecto de la inclusión, del conjunto de ideales propios de R.

También se puede considerar la caracterización:

$$M \text{ es un ideal maximal } \Leftrightarrow \begin{array}{l} \textbf{i)}\ M \subset R; \\ \textbf{ii)}\ \text{no existe } I \text{ ideal de } R \text{ tal que } M \subsetneq I \subsetneq R. \end{array}$$

Lema 1.11. *Sea I un ideal de un anillo conmutativo R. Entonces I es maximal $\Leftrightarrow$ R/I es un cuerpo.*

Definición 1.12. Ideal primo
Sea P un ideal de un anillo conmutativo R. Se dice que P es un ideal primo cuando:

- P es un ideal propio de R;
- dados cualesquiera $a, b \in R$ con $a \cdot b \in P$, entonces $a \in P$ o $b \in P$.

Lema 1.13. *Sea I un ideal de un anillo conmutativo R. Entonces I es primo $\Leftrightarrow$ el anillo de la clase de restos R/I es un dominio.*

Proposición 1.14. *Todo ideal maximal es primo.*

Demostración. Es inmediato de los Lemas 1.11 y 1.13. □

El recíproco no siempre es cierto.

- En $\mathbb{Z}$, (0) es primo pero no es maximal, ya que $(0) \subsetneq (2)$.
- En $\mathbb{Z}[x]$, (x) es primo pero no es maximal, ya que $(x) \subsetneq (2, x)$.
- En $K[x, y]$, (x) es primo pero no es maximal, ya que $(x) \subsetneq (x, y)$.
- En $\mathbb{C}[x, y]$, $(x^2 + y^2 - 1)$ es primo pero no es maximal, ya que $(x^2 + y^2 - 1) \subsetneq (x, y)$.

Definición 1.15. Espectro primo
Sea R un anillo conmutativo. El espectro primo o espectro de R se define como el conjunto de ideales primos de R. Se denota por $\mathrm{Spec}(R)$, i.e.

$$\mathrm{Spec}(R) = \{P \subset R \mid P \text{ es un ideal primo de } R\}.$$

Lema 1.16. *Sea I un ideal de un anillo conmutativo R. Sea J un ideal de R, tal que $J \supseteq I$. Entonces el ideal J/I del anillo de la clase de restos R/I es primo $\Leftrightarrow$ J es un ideal primo de R.*

En otras palabras, $J/I \in \mathrm{Spec}(R/I) \Leftrightarrow J \in \mathrm{Spec}(R)$.

Lema 1.17. *Sea R un dominio y sean $a, b \in R \setminus \{0\}$. Entonces $(a) = (b)$ si y solo si a y b son asociados, es decir, $a = ub$ para alguna unidad u de R.*

Demostración.

($\Rightarrow$) Supongamos que $(a) = (b)$. Entonces $a = ub$ y $b = va$ para algunos $u, v \in R$. De aquí se sigue que $a = uva$, y entonces, por ser R un dominio y $a \neq 0$, se tiene $1 = uv$.

($\Leftarrow$) Supongamos que $a = ub$ para alguna unidad u de R. Entonces $a \in (b)$ y así $(a) \subseteq (b)$. Análogamente, por ser $b = u^{-1}a$, se tiene $(b) \subseteq (a)$. □

Definición 1.18. Ideal Radical
Sea R un anillo conmutativo e I un ideal de R.

Entonces,

$$\sqrt{I} = \{r \in R : \text{existe } n \in \mathbb{N} \text{ con } r^n \in I\},$$

es un ideal de R que contiene a I que se denomina radical de I. Un ideal I se dice radical si $I = \sqrt{I}$.

Demostración. Está claro que $I \subseteq \sqrt{I}$. Veamos que $\sqrt{I}$ es un ideal.

Si $r \in R$ y $a \in \sqrt{I}$ se tiene $ra \in \sqrt{I}$. Sean $a, b \in \sqrt{I}$ tales que existen $n, m \in \mathbb{N}$ tales que $a^n, b^m \in I$. Se tiene por el binomio de Newton,

$$(a+b)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} a^{n+m-1-i} b^i.$$

Ahora, para cada $i = 0, \ldots, n+m-1$, ya sea $n+m-1-i \geq n$ o $i \geq m$, se tendrá que $a^{n+m-1-i} \in I$ o $b^i \in I$. Por tanto $(a+b)^{n+m-1} \in I$ y $a+b \in \sqrt{I}$. Entonces $\sqrt{I}$ es un ideal de R. □

Un ideal es radical si, y solo si el anillo R/I es reducido (o libre de nilpotentes), i.e. R/I no tiene elementos nilpotentes distintos de cero: si $x \in R/I$, $x^n = 0$ para algún $n \in \mathbb{N}$, entonces $x = 0$.

En particular, todo ideal primo P es radical, ya que R/P es un dominio.

Ejemplo 1.19.

- Los ideales radicales en $\mathbb{Z}$ son el ideal (0) y los ideales generados por enteros libres de cuadrados. Así (6) y (30) son ideales radicales, pero (24) no, ya que $\sqrt{(24)} = (2 \cdot 3)$.
- Los ideales radicales en $K[x]$ son el ideal (0) y los ideales generados por polinomios libres de cuadrados. Así (x^2+1) y (x^2-1) son ideales radicales, pero $((x+1)^2)$ no, ya que $\sqrt{((x+1)^2)} = (x+1)$.
- En $\mathbb{Z}$, $\sqrt{(236600)} = (2 \cdot 5 \cdot 7 \cdot 13) = (910)$.
- En general, en un DFU, si $I = (a)$, con $a = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$, entonces $\sqrt{(a)} = (p_1 p_2 \cdots p_s)$.

Proposición 1.20. *Sea R un anillo conmutativo y sean I, J dos ideales de R. Entonces se tiene:*

(i) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$;

(ii) $\sqrt{\sqrt{I}} = \sqrt{I}$;

(iii) $\sqrt{I} = (1)$ *si y solo si* $I = (1)$;

(iv) si $\sqrt{I} + \sqrt{J} = (1)$, *entonces* $I + J = (1)$.

Observación 1.21. En general, la suma de ideales radicales no es un ideal radical, i.e. $\sqrt{I} + \sqrt{J} \neq \sqrt{I+J}$.

En un DIP, por ejemplo $\mathbb{Z}$ y $K[x]$, sí es cierto, i.e. se verifica $\sqrt{I} + \sqrt{J} = \sqrt{I+J}$.

- En $K[x,y]$ no es cierto. $(x^2+y)+(y) = (x^2, y)$, (x^2+y) e (y) son ideales radicales, pero (x^2, y) no lo es ya que $\sqrt{(x^2,y)} = (x,y)$.
- En $\mathbb{Z}[x]$ no es cierto. Los ideales $I = (2)$ y $J = (x^2+2)$ son ideales radicales, pues son ideales primos ya que están generados por elementos irreducibles. Pero $I + J$ no es un ideal radical, ya que $x^2 \in I + J$, pero $x \notin I + J$.

Proposición 1.22. *Sean* I, J *dos ideales de un anillo conmutativo* R. *Entonces se tiene* $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

El producto de ideales radicales no es necesariamente un ideal radical, i.e. $\sqrt{I}\sqrt{J} \neq \sqrt{IJ}$, pero $\sqrt{IJ} = \sqrt{I \cap J}$.

- En $\mathbb{Z}$, $\sqrt{(2)} \cdot \sqrt{(2)} = (4) \neq \sqrt{(2)\cdot(2)} = \sqrt{(4)} = (2)$.
- En $K[x]$, $\sqrt{(x)} \cdot \sqrt{(x)} = (x^2) \neq \sqrt{(x)\cdot(x)} = \sqrt{(x^2)} = (x)$.
- En $K[x,y]$, $\sqrt{(x,y)} \cdot \sqrt{(x,y)} = (x,y)^2 = (x^2, xy, y^2) \neq \sqrt{(x,y)\cdot(x,y)} = \sqrt{(x,y)^2} = (x,y)$.

Proposición 1.23. *Sea* P *un ideal primo de un anillo conmutativo* R. *Entonces,* $\sqrt{P^n} = P$ *para todo* $n \in \mathbb{N}$.

Definición 1.24. Elemento primo

Sea R un dominio. Un elemento $p \in R$ se dice que es un elemento primo cuando

(i) $p \neq 0$ y p no es una unidad de R, y

(ii) dados cualesquiera $a, b \in R$ tales que $p|ab$, entonces $p|a$ o $p|b$.

Definición 1.25. Elemento irreducible

Sea R un dominio. Un elemento $p \in R$ se dice que es un elemento irreducible de R cuando

(i) $p \neq 0$ y p no es una unidad de R, y

(ii) siempre que p se exprese como $p = ab$ con $a, b \in R$, entonces o bien a o bien b son una unidad.

En general los conceptos de elemento primo e irreducible no coinciden.

Proposición 1.26. *Sea R un dominio.*

Todo elemento primo es irreducible.

Demostración. Sea $p \in R$ un elemento primo. Supongamos que $p = bc$. Ya que $p \cdot 1 = bc$, $p|bc$, entonces $p|b$ o $p|c$.

Supongamos que $p|b$, i.e. $pr = b$ para algún $r \in R$. Así,

$$b \cdot 1 = b = pr = (bc)r = b(cr)$$

Ya que R es un dominio, $b(1 - cr) = 0$ implica $1 - cr = 0$, y así, c es una unidad. □

El recíproco de la Proposición 1.26 no es cierto, como veremos más abajo en el Ejemplo 1.31.

A continuación, caracterizaremos los elementos primos e irreducibles en función del ideal principal que generan.

Proposición 1.27. *Sea R un anillo. $p \in R$ es un elemento primo si, y solo si, el ideal principal (p) es un ideal primo.*

Demostración. Sea $p \in R$ un elemento primo. Ya que p no es una unidad entonces el ideal (p) es propio.

Supongamos que $ab \in (p)$. Entonces $ab = rp$. Así $p|ab$. Por ser p un elemento primo, entonces $p|a$ o $p|b$. Si $p|a$, entonces $a \in (p)$. En el otro caso, si $p|b$ entonces $b \in (p)$. Así (p) es un ideal primo.

Recíprocamente, supongamos que el ideal principal (p) es primo. Si $p|ab$ tenemos que $rp = ab$. Así $ab \in (p)$. Tenemos que $a \in (p)$, i.e. $p|a$ o $b \in (p)$, i.e. $p|b$.

Por lo tanto p es un elemento primo. □

Proposición 1.28. *Sea R un dominio. Sea $a \in R$, $a \neq 0$, $a \neq$ unidad.*

Entonces a es irreducible si, y solo si, el ideal principal (a) es maximal entre todos los ideales principales propios.

Demostración. Sea $a \in R$ un elemento irreducible. Supongamos que $(a) \subset (b) \subsetneq R$.

Tenemos que $a = rb$, para algún $r \in R$.

Ya que a es irreducible, tenemos que r o b son unidades. Pero b no puede ser unidad ya que el ideal (b) es propio. Por lo tanto r es unidad.

Así $b = r^{-1}a \in (a)$, por lo tanto $(a) = (b)$ y así el ideal (a) es maximal.

Recíprocamente, supongamos que el ideal principal (a) es maximal entre todos los ideales principales propios.

Supongamos que $a = bc$ con b, c no unidades. Así $(a) = (bc) \subsetneq (b)$. Y así, (a) no sería maximal. Por lo tanto a es irreducible. □

Si R es un DIP, entonces el elemento a es irreducible si, y solo si, el ideal (a) es maximal.

Lema 1.29. *Sea R un DIP y $p \in R \setminus \{0\}$. Entonces, son equivalentes:*

- *(p) es un ideal maximal de R;*
- *(p) es un ideal primo no nulo de R;*
- *p es un elemento primo de R;*
- *p es un elemento irreducible de R.*

Los polinomios irreducibles en $K[x]$, dependen del cuerpo K. Así, en $\mathbb{C}[x]$ los polinomios irreducibles son los polinomios de grado 1, en $\mathbb{R}[x]$ hay polinomios irreducibles de grado 1 y de grado 2, y en $\mathbb{Q}[x]$ hay polinomios irreducibles de cualquier grado, por ejemplo, $x^3 - 2$ es irreducible en $\mathbb{Q}[x]$.

Teorema 1.30. *Todo dominio de ideales principales es un dominio de factorización única.*

Demostración. Sea R un DIP. Veamos primero que todo elemento de R no nulo y que no es una unidad se puede factorizar en un número finito de elementos irreducibles de R. Suponemos que esto no se da. Entonces el conjunto Ω de todos los ideales de R de la forma (a), siendo a un elemento no nulo y distinto de la unidad, donde a no se factoriza de dicha forma, es no vacío. Así, el conjunto Ω tiene un elemento maximal respecto a la inclusión, (b), donde b es en particular un elemento no nulo y distinto de la unidad de R. Ahora bien, b en sí mismo no puede ser irreducible, ya que si fuese así $b = b$ sería una factorización de la forma deseada (con un único factor). Por lo tanto, $b = cd$ para algunos $c, d \in R$, ambos distintos de la unidad. De aquí se sigue fácilmente que $(b) \subset (c) \subset R$ y $(b) \subset (d) \subset R$. Por tanto, por la maximalidad de (b) en Ω, tenemos $(c) \notin \Omega$ y $(d) \notin \Omega$. Ni c y d son nulos o la unidad. Por eso c, d pueden expresarse como producto finito de muchos elementos irreducibles de R, y lo mismo para $b = cd$. Esto es una contradicción. Por tanto todo elemento de R no nulo y distinto de la unidad se puede factorizar como producto finito de elementos irreducibles de R.

Probemos ahora la unicidad de dichas factorizaciones. Supongamos $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ donde p_i y q_i son irreducibles para todo i. Sin pérdida de generalidad, podemos

suponer que $r < s$. Como p_i divide a $q_1 q_2 \cdots q_s$, deberá dividir a algún q_i. Reordenando los q_i podemos suponer que $p_1 | q_1$ y así $q_1 = u_1 p_1$ para alguna unidad u_1 en R. Por tanto $a = p_1 p_2 \cdots p_r = u_1 p_2 q_2 \cdots q_s$ o, lo que es lo mismo, $p_2 \cdots p_r = u_1 q_2 \cdots q_s$. Continuando de esta manera, podemos reordenar los q_i tal que $p_2 = u_2 q_2, p_3 = u_3 q_3, \ldots, p_r = u_r q_r$ y obtener $u_1 u_2 \cdots u_r q_{r+1} \cdots q_s = 1$. En este caso $q_{r+1} \cdots q_s$ es una unidad, lo que contradice el hecho de que $q_{r+1}, \ldots, q_s$ son irreducibles. Por lo tanto, $r = s$ y la factorización de a es única. □

El recíproco no siempre es cierto.

- $\mathbb{Z}[x]$ es un DFU que no es un DIP, ya que $(2, x)$ no es principal.
- $K[x, y]$ es un DFU que no es un DIP, ya que (x, y) no es principal.

El recíproco de la Proposición 1.26 no es cierta.

Ejemplo 1.31. Un elemento irreducible no es necesariamente un elemento primo

Sea el anillo $R = \mathbb{Z}[\sqrt{5}i] \subset \mathbb{C}$.

Veamos que no es un DFU. $2|6 = (1+\sqrt{5}i)(1-\sqrt{5}i)$, pero $2 \not| (1+\sqrt{5}i)$ ni $2 \not| (1-\sqrt{5}i)$, y así 2 no es primo. Se puede probar que 2 es irreducible. De hecho, $6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$ son dos factorizaciones de 6, y por lo tanto $\mathbb{Z}[\sqrt{5}i]$ no es un dominio de factorización única (DFU).

Acabamos de ver un ejemplo de un anillo $R = \mathbb{Z}[\sqrt{5}i]$ que no es un DFU y por tanto tampoco un DIP. Esto se ve también considerando el ideal $(2, 1 + \sqrt{5}i)$ de R que no es principal.

Proposición 1.32. *Sea R un dominio. Supongamos que todo elemento no unidad y distinto de cero se factoriza en irreducibles.*

Entonces R es un DFU si, y solo si, todo elemento irreducible es primo.

Demostración. Supongamos que R es un DFU y sea $x \in R$ un elemento irreducible. Supongamos que $x|ab$, i.e. $ab = cx$.

Elegimos factorizaciones $a = a_1 \cdots a_n$, $b = b_1 \cdots b_m$, y $c = c_1 \cdots c_r$. Por unicidad de la factorización,

$$a_1 \cdots a_n b_1 \cdots b_m = c_1 \cdots c_r x,$$

encontramos que x, salvo unidades, es uno de los elementos $a_1, \ldots, b_m$, i.e. $x|a$ o $x|b$ y concluimos que x es primo.

Supongamos que todo elemento irreducible es primo. Tenemos que probar que la factorización en irreducibles es única.

Supongamos que $a_1 \cdots a_m = b_1 \cdots b_n$ con a_i y b_j irreducibles. Ya que a_1 es primo, $a_1|b_j$ para algún j. Después de volver a numerar, podemos suponer que $a_1|b_1$. Entonces $b_1 = a_1 u$ y como b_1 es irreducible tenemos que u es una unidad. Por tanto a_1 y b_1 son asociados y $a_2 \cdots a_m = b_2 \cdots b_n$. Por inducción en $n + m$ vemos que $n = m$ y a_i es asociado con $b_{\sigma(i)}$ para $i = 2, \ldots, n$ como deseábamos. □

Observación 1.33. La característica más importante de la propiedad de la factorización única es que se conserva cuando se pasa de un dominio R al anillo de polinomios $R[x]$.

La prueba de esta afirmación se basa en el conocido lema de Gauss que afirma que un polinomio irreducible sobre $\mathbb{Z}$ (o más generalmente sobre un dominio de factorización única R) también será irreducible sobre $\mathbb{Q}$ (o el cuerpo de fracciones de R, K). Más precisamente, si $f \in R[x]$ es un polinomio reducible en $K[x]$ tal que $f = gh$ donde $g, h \in K[x]$ son no constantes, entonces existe un $c \in K[x]$ tal que $cg, \frac{h}{c} \in R[x]$ y así $f = (cg) \cdot (\frac{h}{c})$ es reducible en $R[x]$.

Ejemplo 1.34. DFU

- Todos los cuerpos, DIP, y por lo tanto los dominios euclidianos son DFU. En particular, el anillo de los enteros $\mathbb{Z}$.

- Si R es un DFU, entonces $R[x_1, \ldots, x_n]$ es un DFU. En particular, si K es un cuerpo, entonces $K[x_1, \ldots, x_n]$ es un DFU.

- En general, el cociente de un DFU no es necesariamente un DFU. Por ejemplo, $\mathbb{R}[x, y, z, w]/(xy - zw)$ no es un DFU ya que $\bar{x}\bar{y} = \bar{z}\bar{w}$ son dos factorizaciones diferentes del mismo elemento en irreducibles.

- También hemos visto en el Ejemplo 1.31 que $\mathbb{Z}[\sqrt{5}i] \cong \mathbb{Z}[x]/(x^2 + 5)$ no es un DFU.

- Los anillos de coordenadas $\mathbb{R}[x, y]/(y - x^2)$ de la parábola, y $\mathbb{R}[x, y]/(xy - 1)$ de la hipérbola en $\mathbb{R}^2$ son DFU.

  El anillo de coordenadas $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ de la circunferencia en $\mathbb{C}^2$ también es un DFU, ya que $\mathbb{C}[x, y]/(x^2 + y^2 - 1) \cong \mathbb{C}[t, t^{-1}] = \mathbb{C}[t]_t$, la localización de $\mathbb{C}[t]$ en t (la localización de un DFU es un DFU), donde el isomorfismo $\mathbb{C}[x, y]/(x^2 + y^2 - 1) \cong \mathbb{C}[t, t^{-1}]$ viene dado por $x \mapsto \frac{1}{2}(t - t^{-1})$, $y \mapsto \frac{1}{2}(t + t^{-1})$ y su inversa por $t \mapsto (x + iy)$, $t^{-1} \mapsto (x - iy)$.

  Veremos más adelante, Ejemplo 3.14, que el anillo de coordenadas $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$ de la circunferencia en $\mathbb{R}^2$ no es un DFU.

Definición 1.35. $\mathrm{Spec}(R)$ es un espacio topológico con la topología de Zariski, donde los conjuntos cerrados son $V_{\mathrm{Spec}}(I) \coloneqq \{P \in \mathrm{Spec}(R) \mid P \supseteq I\}$, para un ideal I de R.

Proposición 1.36. *Sea I un ideal de un anillo conmutativo R. Entonces,*

$$\sqrt{I} = \bigcap_{P \in V_{\mathrm{Spec}}(I)} P = \bigcap_{\substack{P \in \mathrm{Spec}(R) \\ P \supseteq I}} P.$$

Demostración. Sea $a \in \sqrt{I}$ y sea $P \in V_{\mathrm{Spec}}(I)$. Entonces existe $n \in \mathbb{N}$ tal que $a^n \in I \subseteq P$, tal que, por ser P primo, $a \in P$. Por tanto,

$$\sqrt{I} \subseteq \bigcap_{P \in V_{\mathrm{Spec}}(I)} P.$$

Para establecer la otra inclusión, veremos que si $x \notin \sqrt{I} \implies x \notin \bigcap_{P \in V_{\mathrm{Spec}}(I)} P$.

Dado $x \notin \sqrt{I}$, consideremos la colección Ω de todos los ideales $J \supset I$ tales que para todo $n \in \mathbb{N}$, $x^n \notin J$. Ordenamos parcialmente Ω por inclusión, y por el lema de Zorn Ω tiene un elemento maximal P.

Veamos que P es un ideal primo. Tomemos $a, b \notin P$, y usando la maximalidad de P, tenemos $P + (ab) \notin \Omega$; esto implica que $ab \notin P$ y así P es primo.

Ya que $P \supset I$, y P es un ideal primo, entonces $x \notin \bigcap_{P \in V_{\mathrm{Spec}}(I)} P$, ya que $x \notin P$. □

Ejemplo 1.37. En $\mathbb{Z}$, los ideales primos que contienen al ideal (24) son (2) y (3). Así,

$$\sqrt{(24)} = \bigcap_{\substack{P \in \mathrm{Spec}(\mathbb{Z}) \\ P \supseteq (24)}} P = (2) \cap (3) = (6).$$

Observación 1.38. En un anillo conmutativo la intersección finita de ideales primos es un ideal radical.

Sea $I = P_1 \cap \cdots \cap P_n$. Afirmamos que el ideal I es radical, i.e. $\sqrt{I} = I$.

Es consecuencia de la Proposición 1.22 que afirma que los radicales distribuyen con las intersecciones, y de que todo ideal primo es radical. Así

$$\sqrt{I} = \sqrt{P_1 \cap \cdots \cap P_n} = \sqrt{P_1} \cap \cdots \cap \sqrt{P_n} = P_1 \cap \cdots \cap P_n = I.$$

Teorema 1.39. *Sea I un ideal propio de un anillo conmutativo R. Entonces $V_{\mathrm{Spec}}(I) = \{P \in \mathrm{Spec}(R) : P \supseteq I\}$ tiene al menos un elemento minimal respecto de la inclusión. Ese elemento minimal se denomina ideal primo minimal de I o ideal primo minimal conteniendo a I. En el caso de que R sea no trivial, a los ideales primos minimales del ideal nulo (0) de R se les conoce a veces como los ideales primos minimales de R.*

Proposición 1.40. *Sean P, I ideales de un anillo conmutativo R con P primo y $P \supseteq I$. Entonces el conjunto no vacío $\Theta := \{P' \in \mathrm{Spec}(R) : P \supseteq P' \supseteq I\}$ tiene un elemento minimal respecto de la inclusión. Este será un ideal primo de I.*

Corolario 1.41. *Sea I un ideal propio de un anillo conmutativo R, y denotemos por $\mathrm{Min}(I)$ al conjunto de ideales primos minimales de I. Entonces $\sqrt{I} = \cap_{P \in \mathrm{Min}(I)} P$.*

Lema 1.42. *Sea P un ideal primo de un anillo conmutativo R, y sean $I_1, \ldots, I_n$ ideales de R. Los siguientes resultados son equivalentes:*

(i) $P \supseteq I_j$ *para algún* j *con* $1 \leq j \leq n$;

(ii) $P \supseteq \cap_{i=1}^{n} I_i$;

(iii) $P \supseteq \prod_{i=1}^{n} I_i$.

Demostración. Está claro que $i) \Rightarrow ii)$ y $ii) \Rightarrow iii)$.

Veamos que $iii) \Rightarrow i)$: supongamos que para todo j se tiene $P \not\supseteq I_j$. Entonces, para cada j existe $a_j \in I_j \setminus P$; pero entonces, $a_1 \cdots a_n \in \prod_{i=1}^{n} I_i \setminus P$ (por ser P primo), y eso contradice $iii)$. □

Corolario 1.43. *Sean $I_1, \ldots, I_n$ ideales de un anillo conmutativo R y P un ideal primo de R, tal que $P = \cap_{i=1}^{n} I_i$. Entonces $P = I_j$ para algún j con $1 \leq j \leq n$.*

Definición 1.44. Ideales comaximales

Sean $I, J, I_1, \ldots, I_n$, donde $n \in \mathbb{N}$ con $n \geq 2$, ideales de un anillo conmutativo R.

Se dice que I y J son comaximales (o coprimos) cuando $I + J = R$.

También, dada la familia de ideales $\{I_i\}_{i=1}^{n}$ se dice que son comaximales dos a dos si $I_i + I_j = R$ para $1 \leq i, j \leq n$ con $i \neq j$.

Ejemplo 1.45. (2) y (3) son comaximales en $\mathbb{Z}$, mientras que (6) y (10) no lo son, ya que $(6) + (10) = (2)$.

(x) e (y) son comaximales en $K[x, y]$ mientras que (x) y $(xy + x)$ no lo son, ya que $(x) + (xy + x) = (x)$.

Proposición 1.46. *Sea $\{I_i\}_{i=1}^{n}$ (donde $n \geq 2$) una familia de ideales comaximales dos a dos de un anillo conmutativo R. Entonces*

(i) $I_1 \cap \cdots \cap I_{n-1}$ *y* I_n *son comaximales, y*

(ii) $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.

Demostración.

(i) Sea $J := \cap_{i=1}^{n-1} I_i$. Supongamos que M es un ideal maximal de R tal que $J + I_n \subseteq M$. Entonces $I_n \subseteq M$ y $J = I_1 \cap \cdots \cap I_{n-1} \subseteq M$; entonces por el Lema 1.42 existe un $j \in \mathbb{N}$ con $1 \leq j \leq n-1$ tal que $I_j \subseteq M$, así que $I_j + I_n \subseteq M$. Pero esto es una contradicción ya que I_j e I_n son comaximales. Entonces no hay un ideal maximal de R que contenga a $J + I_n$, y entonces, $J + I_n = R$.

(ii) Probamos esto por inducción en n. Para $n = 2$, veamos que dados dos ideales comaximales I y J se tiene $I \cap J = IJ$.

De hecho, $IJ \subseteq I \cap J$. Por hipótesis, $I + J = R$. Por lo tanto, por la Observación 1.4, se tiene

$$I \cap J = (I \cap J)R = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J.$$

Pero $(I \cap J)I \subseteq JI$ y $(I \cap J)J \subseteq IJ$. Así, $(I \cap J) \subseteq IJ$.

Supongamos ahora que para $n = k \geq 3$ se cumple el resultado y así tendríamos $J := \cap_{i=1}^{k-1} I_i = \prod_{i=1}^{k-1} I_i$. Por (i), J e I_k son comaximales, y entonces $J \cap I_k = JI_k$. De esto se sigue que $\cap_{i=1}^{k} I_i = J \cap I_k = JI_k = \prod_{i=1}^{k} I_i$. □

Definición 1.47. Ideal cociente
Dados I, J dos ideales de un anillo conmutativo R se define el ideal cociente por $(I : J) = \{a \in R \mid aJ \subseteq I\}$; claramente es un ideal de R y $I \subseteq (I : J)$. En el caso particular $I = 0$ el ideal cociente $(0 : J) = \{a \in R : aJ = 0\} = \{a \in R : ab = 0 \text{ para todo } b \in J\}$ se llama anulador de J, y también se denota $\operatorname{Ann} J$ o $\operatorname{Ann}_R J$.

Proposición 1.48. *Sea H un subconjunto de un anillo conmutativo R, y sea I un ideal de R. Entonces $(I : H) \coloneqq (I : (H)) = \{a \in R : ah \in I \text{ para todo } h \in H\}$.*

Proposición 1.49. *Sean I, J, K ideales de un anillo conmutativo R, y sea $(I_\lambda)_{\lambda \in \Lambda}$ una familia de ideales de R. Entonces:*

(i) $((I : J) : K) = (I : JK) = ((I : K) : J)$;

(ii) $(\cap_{\lambda \in \Lambda} I_\lambda : K) = \cap_{\lambda \in \Lambda}(I_\lambda : K)$;

(iii) $(J : \sum_{\lambda \in \Lambda} I_\lambda) = \cap_{\lambda \in \Lambda}(J : I_\lambda)$.

Ejemplo 1.50. Sean $R = \mathbb{Z}$ o $R = K[x_1, \ldots, x_n]$, $I = (a)$, $J = (b)$ con $a, b \neq 0$.

- $I + J = (\gcd(a, b))$;
- $I \cap J = (\operatorname{lcm}(a, b))$;
- $I \cdot J = (ab)$;

- $I : J = \left(\dfrac{\operatorname{lcm}(a,b)}{b}\right) = \left(\dfrac{a}{\gcd(a,b)}\right)$;
- $\sqrt{I} = \sqrt{(a)} = (p_1 \cdots p_k)$, donde $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ es la factorización en irreducibles de a;
- I, J son comaximales $\iff R = I + J = (\gcd(a,b)) \iff \gcd(a,b) = 1$.

Capítulo 2

DESCOMPOSICIÓN PRIMARIA

2.1. Idea de la descomposición primaria

Ahora estudiaremos la teoría de la descomposición de ideales propios en un anillo conmutativo Noetheriano. Esta se podría interpretar como la generalización de que todo dominio de ideales principales es un dominio de factorización única.

Veamos la justificación de esta idea: consideremos un dominio de ideales principales R y un ideal propio y no nulo I de R. Entonces, I sería un ideal principal y así existiría un $a \in R$ no nulo y distinto de la unidad tal que $I = (a)$. Ahora bien, como todo DIP es un DFU, se tiene que existe $s \in \mathbb{N}$ tal que $p_1, \ldots, p_s \in R$ son elementos irreducibles con p_i y p_j no asociados para $i \neq j$ $(1 \leq i, j \leq s)$, u una unidad de R y $t_1, \ldots, t_s \in \mathbb{N}$, tal que $a = up_1^{t_1} \cdots p_s^{t_s}$.

Ya que $I = (a)$, podemos deducir, por la definición de producto de ideales y por la Observación 1.4, que $I = \prod_{i=1}^{s}(p_i^{t_i})$.

Ahora veremos otra expresión de I como intersección de ideales de un cierto tipo.

Sean $i, j \in \mathbb{N}$ con $1 \leq i, j \leq s$ y $i \neq j$, entonces (p_i) y (p_j) son ideales maximales de R y ya que p_i y p_j son no asociados, por el Lema 1.17 estos son dos ideales maximales de R distintos.

Por lo tanto, se tiene que $(p_i) \subset (p_i) + (p_j) \subseteq R$, ya que si $(p_i) = (p_i) + (p_j)$ tendríamos $(p_j) \subseteq (p_i) \subset R$, lo que implicaría $(p_i) = (p_j)$, y esto es una contradicción.

Por lo tanto $(p_i) + (p_j) = R$, y así (p_i) y (p_j) son comaximales.

Al ser (p_i) y (p_j) dos ideales comaximales, $(p_i^{t_i})$ y $(p_j^{t_j})$ también lo serán ya que $\sqrt{(p_i^{t_i})} = (p_i)$ y $\sqrt{(p_j^{t_j})} = (p_j)$, por la Proposición 1.23, y por la Proposición 1.20 (iv) tendremos que $(p_i^{t_i}) + (p_j^{t_j}) = R$.

Así, tenemos que $\{(p_j^{t_j})\}_{j=1}^s$ es una familia de ideales comaximales del anillo conmutativo R tal que $I = \prod_{i=1}^s (p_i^{t_i})$. Por la Proposición 1.46 (ii), I se puede expresar de la forma $I = (a) = (p_1^{t_1}) \cap \cdots \cap (p_s^{t_s})$.

Para cada $i = 1, \ldots, s$, el ideal $(p_i^{t_i}) = (p_i)^{t_i}$ es potencia de un ideal maximal de R, y este será un ejemplo de lo que llamaremos más adelante un ideal primario.

Y así ya hemos probado que efectivamente podemos hablar de descomposición primaria de un cierto ideal I en un DIP.

2.2. Ideales primarios

Ya hemos visto que efectivamente se puede hablar de descomposición primaria en un DIP. Ahora veremos que todo ideal propio de un anillo conmutativo Noetheriano tiene una descomposición primaria, es decir, que se puede expresar como intersección finita de ideales primarios.

Para esto necesitamos introducir una serie de definiciones y resultados.

Definición 2.1. Ideal primario
Sea Q un ideal de un anillo conmutativo R. Se dice que Q es un ideal primario de R si:

- **i)** $Q \subset R$, es decir, Q es un ideal propio de R, y
- **ii)** dados cualesquiera $a, b \in R$ con $ab \in Q$ pero $a \notin Q$, entonces existe $n \in \mathbb{N}$ tal que $b^n \in Q$.

Esto último, sería equivalente a decir que: dados $a, b \in R$ con $ab \in Q$ entonces $a \in Q$ o $b \in \sqrt{Q}$, siendo $\sqrt{Q}$ el radical de Q.

Observación 2.2. Es fácil ver que todo ideal primo en un anillo conmutativo R es un ideal primario de R. El recíproco no es cierto, por ejemplo, en $\mathbb{Z}$, (2^2) es primario pero no es un ideal primo.

Lema 2.3.

(i) Sea I un ideal de un anillo conmutativo R. Entonces I es primario $\Leftrightarrow$ el anillo R/I es no trivial y tiene la propiedad de que todo divisor de cero en R/I es nilpotente.

(ii) Sea $f\colon R \to S$ un homomorfismo de anillos conmutativos, y sea Q un ideal primario de S. Entonces $Q^c := f^{-1}(Q)$ es un ideal primario de R.

Demostración.

(i) ($\Rightarrow$) Supongamos que I es primario. De $I \neq R$ se deduce que R/I es no trivial. Sea $b \in R$ tal que el elemento $b+I$ en R/I es un divisor de cero, así que existe $a \in R$ tal que $a + I \neq 0_{R/I}$, con $(a+I)(b+I) = ab + I = 0_{R/I}$. Estas condiciones significan que $a \notin I$ pero $ab \in I$, y como I es primario, existe $n \in \mathbb{N}$ tal que $b^n \in I$. Y así, $(b+I)^n = b^n + I = 0_{R/I}$.

($\Leftarrow$) Supongamos que R/I es no trivial y que todo divisor de cero en R/I es nilpotente. Veamos ahora que si $xy \in I$ con $x \notin I$ entonces $\exists n \in \mathbb{N}$ tal que $y^n \in I$. De $xy \in I$ se tiene $xy + I = 0_{R/I}$. Pero $xy + I = (x+I)(y+I)$ y así $y + I$ es un divisor de cero. Por hipótesis se tiene que $\exists n \in \mathbb{N}$ tal que $(y+I)^n = 0_{R/I}$ lo que implica $y^n + I = 0_{R/I}$ y así $y^n \in I$. Por lo tanto, I es primario.

(ii) El homomorfismo compuesto de anillos $R \xrightarrow{f} S \to S/Q$ (en el cual el segundo homomorfismo es la sobreyección natural) tiene como núcleo Q^c, y por el Teorema de isomorfía de anillos (Teorema 1.1) se sigue que R/Q^c es isomorfo a un subanillo de S/Q. Ahora si un anillo conmutativo R' es no trivial y tiene la propiedad de que todo divisor de cero es nilpotente, entonces cada subanillo de R' tendrá las mismas dos propiedades. Ahora, se sigue de (i) que Q^c es un ideal primario de R.

□

Lema 2.4. *Sea Q un ideal primario de un anillo conmutativo R. Entonces $P := \sqrt{Q}$ es un ideal primo de R y se dice que Q es P-primario.*

Además, P es el menor ideal primo de R que contiene a Q, y así todo ideal primo de R que contenga a Q debe contener a P. Entonces P es el único ideal primo minimal de Q.

Demostración. Ya que $1 \notin Q$, se tendrá $1 \notin \sqrt{Q} = P$, y así P es propio.

Supongamos que tenemos $a, b \in R$ con $ab \in \sqrt{Q}$ pero $a \notin \sqrt{Q}$. Entonces existe $n \in \mathbb{N}$ tal que $(ab)^n = a^n b^n \in Q$; sin embargo, ninguna potencia positiva de a pertenece a Q, y así tampoco habrá ninguna potencia a^n perteneciente a Q. Por ser Q primario, se sigue de la definición que $b^n \in Q$ y así $b \in \sqrt{Q}$. Por lo tanto $P = \sqrt{Q}$ es primo.

Para probar el enunciado del último párrafo, nótese que si $P' \in \mathrm{Spec}(R)$ y $P' \supseteq Q$, entonces podemos tomar radicales (y usando la Proposición 1.23, $\sqrt{P^n} = P$) obtenemos que $P' = \sqrt{P'} \supseteq \sqrt{Q} = P$. Por lo tanto, P es el único ideal primo minimal de Q. □

Corolario 2.5. *Un ideal es primo si, y solo si, es radical y primario.*

Demostración. Por el lema anterior si Q es primario y radical, entonces $\sqrt{Q} = Q$ que es primo. □

Nótese que existen ideales radicales que no son primos (y por lo tanto no primarios), por ejemplo el ideal $(6) \subset \mathbb{Z}$; y existen ideales primarios que no son primos (y por lo tanto no radicales), por ejemplo el ideal $(4) \subset \mathbb{Z}$.

Observación 2.6. Sea $f\colon R \to S$ un homomorfismo de anillos conmutativos, y sea Q' un ideal P'-primario de S. Antes vimos (Lema 2.3 (ii)) que $Q'^c := f^{-1}(Q')$ es un ideal primario de R. También se tiene que $\sqrt{Q'^c} = P'^c$ (usando que, en general, se verifica que para cualquier ideal J, $(\sqrt{J})^c = \sqrt{J^c}$), y así Q'^c sería precisamente un ideal P'^c-primario de R.

Ya hemos visto que todo ideal primo es primario. También hemos establecido anteriormente que toda potencia positiva de un ideal maximal en un DIP es primario. Generalizamos este resultado para cualquier anillo conmutativo.

Proposición 2.7. *Sea Q un ideal de un anillo conmutativo R tal que $\sqrt{Q} = M$, un ideal maximal de R. Entonces Q es un ideal primario (de hecho, es M-primario).*

Como consecuencia, toda potencia positiva M^n $(n \in \mathbb{N})$ de un ideal maximal M será un ideal M-primario.

Demostración. Como $Q \subseteq \sqrt{Q} = M \subset R$, es claro que Q es propio. Sean $a, b \in R$ tales que $ab \in Q$ pero $b \notin \sqrt{Q}$. Como $\sqrt{Q} = M$ es maximal y $b \notin M$, se debe tener que $M + (b) = R$, y así $\sqrt{Q} + \sqrt{(b)} = R$.

Por lo tanto, por Proposición 1.20 (iv), $Q + (b) = R$. Entonces existe $d \in Q$, $c \in R$ tales que $d + cb = 1$, y $a = a \cdot 1 = a(d + cb) = ad + c(ab) \in Q$ porque $d, ab \in Q$. Por lo tanto Q es M-primario.

La última afirmación es una consecuencia inmediata ya que $\sqrt{M^n} = M$ para todo $n \in \mathbb{N}$. □

Corolario 2.8. *Sea M un ideal maximal y Q un ideal tal que $M^n \subseteq Q \subseteq M$ para algún $n \geq 1$. Entonces Q es un ideal M-primario.*

Esta proposición nos permite aumentar el número de ejemplos de ideales primarios.

Ejemplo 2.9. Sea R un DIP que no es un cuerpo. Entonces el conjunto de todos los ideales primarios de R es $\{0\} \cup \{(p^n)\}$, donde p es un elemento irreducible de R, $n \in \mathbb{N}$.

Demostración. Ya que $(0) \in \operatorname{Spec}(R)$ por ser R un dominio, entonces (0) es primario.

Para un elemento irreducible p de R y $n \in \mathbb{N}$, el ideal (p^n) es una potencia del ideal maximal (p) de R y entonces es un ideal primario de R. Así, (p^n) es un ideal primario de R.

Recíprocamente, un ideal primario no nulo de R debe de ser de la forma (a) para algún $a \in R$ no nulo, y a distinto de una unidad por ser todo ideal primario propio. Además, podemos expresar a como producto de elementos irreducibles de R. Si a fuese divisible por dos elementos irreducibles p, q de R los cuales son no asociados, entonces (p) y (q) serían dos ideales maximales distintos de R, y serían ambos ideales primos minimales de (a), lo cual es una contradicción. De esto se concluye que (a) es generado por una potencia positiva de algún elemento irreducible de R. □

Observación 2.10. Este resultado se da en un DFU para ideales principales pero no se verifica en general para ideales arbitrarios, como veremos a continuación.

Ejemplo 2.11.

- Los ideales primarios en un DIP son de la forma (0) y (p^n), con p un elemento irreducible. Así, en $\mathbb{Z}$, (3), (4), (5) y (8) son ideales primarios, mientras que (6) y (24) no son primarios. En $K[x]$ los ideales primarios son de la forma (0) y (p^n) con p un polinomio irreducible.

- El ideal (x) en $K[x, y]$ es primario ya que es un ideal primo. El ideal $(x, y)^n$ en $K[x, y]$ es primario ya que es potencia del ideal maximal (x, y).

- El ideal $Q = (x^2, y)$ en $K[x, y]$ es primario ya que $(x, y)^2 \subseteq (x^2, y) \subseteq (x, y)$, donde (x, y) es un ideal maximal.

- Sea $R = K[x, y]$ o $R = \mathbb{Z}[x, y]$. Los ideales (x^2, y), (x^2, y^2), (x^2, y^3), ..., son ideales primarios con radical el ideal primo (x, y).

- Sean R un DFU y p un elemento irreducible. Entonces Q es un ideal (p)-primario si, y solo si, $Q = (p^n)$.

  El ideal (p^n) es (p)-primario: si $ab \in (p^n)$ entonces $ab = cp^n$ para algún $c \in R$. Pero, ahora los n factores de p están todos contenidos en a (en cuyo caso $a \in (p^n)$), o al menos uno de ellos está contenido en b (en cuyo caso $b^n \in (p^n)$).

  Recíprocamente, sea Q un ideal (p)-primario, y sea n el mayor entero tal que $Q \subseteq (p^n)$ (tal entero existe ya que $Q \subseteq \sqrt{Q} = (p)$). Si q es un elemento de Q no contenido en (p^{n+1}), entonces $q = rp^n$ para algún $r \in R$ y $r \notin (p)$. Ya que $r \notin (p)$ y Q es (p)-primario, se sigue que $p^n \in Q$. Esto prueba que $Q = (p^n)$.

En particular, todas las potencias de un ideal maximal M son ideales M-primarios. Podríamos sospechar que las potencias de un ideal primo P deberían ser ideales P-primarios, pero en general esto no es verdad, como se verá en los siguientes ejemplos.

Tampoco se verifica que todo ideal M-primario sea una potencia de un maximal, ni es cierto que un ideal P-primario sea una potencia de un primo.

Ejemplo 2.12. Ideal primario que no es una potencia de un ideal primo (maximal)
Sea K un cuerpo y el anillo $R = K[x, y]$. Sea $M = (x, y)$ un ideal maximal de R. Entonces (x, y^2) es un ideal M-primario de R que no es potencia de ningún ideal primo (o de ningún maximal) de R.

Demostración. Tenemos $M^2 = (x^2, xy, y^2) \subseteq (x, y^2) \subseteq (x, y) = M$, y entonces tomando radicales obtenemos por la Proposición 1.23 que $M = \sqrt{M^2} \subseteq \sqrt{(x, y^2)} \subseteq \sqrt{M} = M$. Así, $\sqrt{(x, y^2)} = (x, y) = M$ es un ideal maximal de R, y de esto se sigue que (x, y^2) es M-primario. Además, (x, y^2) no es una potencia positiva de ningún ideal primo P (o de ningún maximal) de R porque, si lo fuese, deberíamos tener que $P = M$, ya que si $P^i = (x, y^2)$ para algún i entonces $M = \sqrt{(x, y^2)} = \sqrt{P^i} = P$. Como las potencias de M forman una cadena descendiente $M \supseteq M^2 \supseteq \cdots \supseteq M^i \supseteq M^{i+1} \supseteq \cdots$, deberíamos tener $(x, y^2) = M$ o M^2; pero ninguno de estos casos es correcto ya que $x \notin M^2$ (ya que todo término no nulo que aparece en un polinomio en M^2 es al menos de grado 2), mientras que $y \notin (x, y^2)$ (ya que si no $y = xf + y^2 g$ para ciertos $f, g \in R$, y la evaluación de x, y en $0, y$ lleva a una contradicción). □

Ejemplo 2.13. Ideal primario que no es una potencia de un ideal primo
Sea $R = \mathbb{Z}[x]$. El ideal $I = (4, x)$ es primario, con primo asociado $\sqrt{(4, x)} = (2, x)$. Pero $I = (4, x)$ no es una potencia del ideal primo $(2, x)$.

Otra cosa a tener en cuenta es que aunque todo potencia positiva de un ideal maximal de un anillo conmutativo R es un ideal primario de R, no necesariamente se da que toda potencia positiva de un ideal primo de R sea un ideal primario. A continuación veamos un ejemplo de esto:

Ejemplo 2.14. Potencia de un ideal primo que no es primario
Sea K un cuerpo y R el anillo dado por $R = K[x, y, z]/(xz - y^2)$. Sean $\bar{x}, \bar{y}, \bar{z}$ las imágenes naturales de x, y, z en R. Entonces $P := (\bar{x}, \bar{y})$ es un ideal primo de R pero P^2 no es primario.

Ya que $\sqrt{P^2} = P \in \mathrm{Spec}(R)$, este ejemplo también muestra que un ideal que tiene radical primo no es necesariamente primario.

Demostración. El ideal (x, y) de $K[x, y]$ generado por x y y es maximal. Su extensión a $K[x, y][z] = K[x, y, z]$ es un ideal primo y está también generada por x e y. Ahora, en

$K[x,y,z]$ tenemos $(x,y) \supseteq (xz-y^2)$, así que por el Lema 1.16, $P = (\bar{x},\bar{y}) = (x,y)/(xz-y^2) \in \mathrm{Spec}(R)$.

Veamos ahora que P^2 no es primario. Nótese que por la Proposición 1.23 $\sqrt{P^2} = P$. Ahora $\bar{x}\bar{z} = \bar{y}^2 \in P^2$. Sin embargo, tenemos $\bar{x} \notin P^2$ y $\bar{z} \notin P = \sqrt{P^2}$ (como se verá más abajo), y así P^2 no sería primario.

• $\bar{x} \notin P^2$, ya que si esto no fuera cierto, deberíamos tener $x = x^2f+xyg+y^2h+(xz-y^2)d$ para algunos $f,g,h,d \in K[x,y,z]$, y esto no es posible ya que todo término de la derecha de la igualdad tiene al menos grado 2.

• Análogamente, si tuviésemos $\bar{z} \in P$, deberíamos tener $z = xa + yb + (xz-y^2)c$ para algunos $a,b,c \in K[x,y,z]$, y obtendríamos una contradicción evaluando x,y,z en $0,0,z$. □

Proposición 2.15. *Sea R un anillo Noetheriano.*

(i) Para cualquier ideal I de R, existe un $n \in \mathbb{N}$ tal que $(\sqrt{I})^n \subset I$.

(ii) Si Q es un ideal P-primario, $\sqrt{Q} = P$, entonces Q siempre contiene una potencia del ideal primo P.

Demostración.

(i) Ya que R es un anillo Noetheriano, tenemos $\sqrt{I} = (x_1,\ldots,x_k)$ pues todo ideal de R es finitamente generado.

Como $x_i \in \sqrt{I}$, existe n_i tal que $x_i^{n_i} \in I$. Sea $n = n_1 + \cdots + n_k$.

Obsérvese que $(\sqrt{I})^n$ está generado, por el teorema multinomial, por elementos de la forma $x_1^{r_1}\cdots x_k^{r_k}$, donde $r_1 + \cdots + r_k = n$.

Nótese que, para cada elemento de este tipo, $r_i \geq n_i$ para algún i, pues de lo contrario contradice el hecho de que $r_1 + \cdots + r_k = n$.

Esto significa que cada $x_1^{r_1}\cdots x_k^{r_k} \in I$. Concluimos que $(\sqrt{I})^n \subset I$, ya que cada uno de sus generadores está en I.

(ii) Es consecuencia de (i) ya que $(\sqrt{Q})^n = P^n \subset Q$. □

Ejemplo 2.16. Ideal con radical primo y que no es primario
Sea $R = K[x,y]$. El ideal $I = (x^2,xy)$ no es primario y $\sqrt{(x^2,xy)} = (x)$. Esto muestra un ejemplo de un ideal con radical primo y que no es primario.

Ejemplo 2.17. Ideal no primario que contiene una potencia de un ideal primo
Sea $R = \mathbb{Z}[x]$. El ideal $I = (x^2,2x)$ no es primario. El ideal (x) es primo y $(x)^2 \subseteq (x^2,2x)$. Además, $\sqrt{(x^2,2x)} = (x)$. Esto muestra un ejemplo de un ideal que contiene una potencia de un ideal primo y que no es primario.

2.3. Ideales como intersección de ideales primarios

Ahora pasemos a estudiar la presentación de ideales de un anillo conmutativo R como intersección finita de ideales primarios de R. Para esto necesitamos antes mencionar algunos lemas.

Lema 2.18. *Sea P un ideal primo de un anillo conmutativo R, y sean $Q_1, \ldots, Q_n$ (con $n \geq 1$) ideales P-primarios de R. Entonces $\cap_{i=1}^n Q_i$ es también un ideal P-primario.*

Demostración. Por el uso repetido de la Proposición 1.22, tenemos que $\sqrt{Q_1 \cap \cdots \cap Q_n} = \sqrt{Q}_1 \cap \cdots \cap \sqrt{Q}_n = P \subset R$. Esto demuestra, entre otras cosas, que $\cap_{i=1}^n Q_i$ es propio. Supongamos que existen $a, b \in R$ tales que $ab \in \cap_{i=1}^n Q_i$ pero $b \notin \cap_{i=1}^n Q_i$. Entonces existe un entero j con $1 \leq j \leq n$ tal que $b \notin Q_j$. Como $ab \in Q_j$ y Q_j es P-primario, se sigue que $a \in P = \sqrt{Q_1 \cap \cdots \cap Q_n}$. Por lo tanto $\cap_{i=1}^n Q_i$ es P-primario. □

Lema 2.19. *Sean $a \in R$ y Q un ideal P-primario de un anillo conmutativo R.*

(i) Si $a \in Q$, entonces $(Q : a) = R$.

(ii) Si $a \notin Q$, entonces $(Q : a)$ es P-primario, y así, en particular, $\sqrt{(Q : a)} = P$.

(iii) Si $a \notin P$, entonces $(Q : a) = Q$.

Demostración.

(i) Es inmediato por la definición de ideal cociente y por la Proposición 1.48.

(ii) Sea $b \in (Q : a)$. Entonces tenemos $ab \in Q$ y $a \notin Q$ y, por ser Q un ideal P-primario, $b \in P = \sqrt{Q}$. Por lo tanto $Q \subseteq (Q : a) \subseteq P$. Ahora, tomando radicales obtenemos que $P = \sqrt{Q} \subseteq \sqrt{(Q : a)} \subseteq \sqrt{P} = P$, y así $\sqrt{(Q : a)} = P$.

Ahora supongamos que $c, d \in R$ son tales que $cd \in (Q : a)$ pero $d \notin P$. Entonces $cda \in Q$ pero $d \notin P$ y Q es P-primario. Por lo tanto $ca \in Q$ y $c \in (Q : a)$. De esto se sigue que $(Q : a)$ es P-primario.

(iii) $Q \subseteq (Q : a)$ se sigue inmediatamente de la definición de ideal P-primario. Por otro lado, si $b \in (Q : a)$ y $a \notin P$, entonces $ab \in Q$, y por ser Q un ideal P-primario tenemos $b \in Q$.

□

2.4. Definición de descomposición primaria y propiedades

Ahora que ya hemos expuesto los distintos resultados y definiciones, ya podemos introducir formalmente el concepto de descomposición primaria.

Definición 2.20. Descomposición primaria
Sea I un ideal propio de un anillo conmutativo R. Una descomposición primaria de I es una expresión de I como intersección finita de ideales primarios de R. Una descomposición primaria de I

$$I = Q_1 \cap \cdots \cap Q_n \quad \text{con} \quad \sqrt{Q_i} = P_i, \quad \text{para} \quad i = 1, \ldots, n,$$

(entendiendo que Q_i es P_i-primario para todo $i = 1, \ldots, n$, siempre que usemos esta terminología) se dice descomposición primaria minimal de I precisamente cuando

(i) $P_1, \ldots, P_n$ son n ideales primos distintos de R, y

(ii) para todo $j = 1, \ldots, n$, tenemos $Q_j \not\supseteq \cap_{\substack{i=1 \\ i \neq j}}^{n} Q_i$.

Esta última condición se puede reemplazar por: para todo $j = 1, \ldots, n$, tenemos que $I \neq \cap_{\substack{i=1 \\ i \neq j}} Q_i$, y así Q_j no es redundante y realmente es necesario en la descomposición primaria $I = \cap_{i=1}^{n} Q_i$.

Decimos que I es un ideal descomponible de R si tiene una descomposición primaria.

Ejemplo 2.21. Dos ejemplos de descomposiciones primarias.

- Sea $R = \mathbb{Z}$. Entonces $(12) = (4) \cap (3)$, donde $Q_1 = (4) = P_1^2$, $P_1 = (2)$ y $Q_2 = P_2 = (3)$.
- Sea $R = K[x, y]$. Entonces $(x^2, xy) = (x) \cap (x, y)^2$, donde $Q_1 = P_1 = (x)$ y $Q_2 = P_2^2$ con $P_2 = (x, y)$.

Este ejemplo no es típico ya que en este ejemplo los ideales primarios son potencias de ideales primos.

- Para un ideal primo P, P^n puede no ser primario.
- Que un ideal Q sea P-primario, no implica que $Q = P^n$.

2.5. Descomposición primaria minimal

Antes de continuar con propiedades y resultados de descomposición primaria hagamos una serie de aclaraciones.

Observación 2.22. Sea I un ideal propio de un anillo conmutativo R, y sea $I = Q_1 \cap \cdots \cap Q_n$ con $\sqrt{Q}_i = P_i$ para $i = 1, \ldots, n$, una descomposición primaria de I.

(i) Si dos de los P_i, por ejemplo P_j y P_k con $1 \leq j, k, \leq n$ y $j \neq k$, son iguales, entonces podemos reemplazar los términos Q_j y Q_k por $Q_j \cap Q_k$ en nuestra descomposición primaria (teniendo en cuenta que $\sqrt{Q_1 \cap \cdots \cap Q_n} = \sqrt{Q}_1 \cap \cdots \cap \sqrt{Q}_n$) y así obtener otra descomposición primaria de I con $n-1$ términos. De hecho, podemos hacer esto repetidamente para obtener una descomposición primaria de I donde todos los radicales de los términos primarios sean todos diferentes.

(ii) Podemos refinar nuestra descomposición primaria para producir una donde no haya ningún término redundante. Primero, descartemos Q_1 si y solo si $I = \cap_{i=2}^{n} Q_i$, esto es, si y solo si $Q_1 \supseteq \cap_{i=2}^{n} Q_i$; entonces consideremos $Q_2, \ldots, Q_n$. Sigamos haciendo este proceso. Así, en el j-ésimo paso descartamos Q_j si y solo si contiene la intersección de aquellos Q_i con $i \neq j$ que no hayan sido previamente excluidos. Si no hiciésemos esto con Q_j, en el paso j-ésimo, entonces al llegar al paso n-ésimo Q_j no contendría la intersección de aquellos Q_i con $i \neq j$ que no fueron eliminados. Siguiendo este camino obtendríamos una descomposición primaria de I donde ningún término sería redundante.

(iii) Por lo tanto, empezando con una descomposición primaria de I dada, podemos comenzar con el proceso descrito en **(i)** y luego perfeccionarlo usando **(ii)** para llegar a un descomposición primaria minimal.

(iv) Así es claro que todo ideal descomponible de R tiene una descomposición primaria minimal.

(v) Nótese que, si I tiene una descomposición primaria con t términos la cual no es minimal, entonces de $(i), (ii)$ y (iii) se sigue que I tiene una descomposición primaria minimal con menos de t términos.

(vi) Las expresiones '*descomposición primaria normal*' y '*descomposición primaria reducida*' son otras formas de llamarle a la '*descomposición primaria minimal*'.

Ejemplo 2.23.

- En $\mathbb{Z}$, la descomposición primaria $(24) = (2^2) \cap (2^3) \cap (3)$ no es minimal. Aplicando (i) de la observación anterior, ya que (2^2) y (2^3) son ideales (2)-primarios, los reemplazamos por $(2^2) \cap (2^3) = (2^3)$, y así una descomposición primaria minimal es $(24) = (2^3) \cap (3)$.

- En $K[x,y]$, la descomposición primaria $I = (x^2, xy) = (x) \cap (x,y)^2 \cap (x^2, y)$ no es minimal. Aplicando (i) de la observación anterior, ya que $(x,y)^2$ y (x^2,y) son ideales (x,y)-primarios (el ideal (x,y) es maximal), los reemplazamos por $(x,y)^2 \cap (x^2,y) = (x,y)^2$, y así una descomposición primaria minimal es $I = (x^2, xy) = (x) \cap (x,y)^2$.

  También es minimal la descomposición $I = (x^2, xy) = (x) \cap (x^2, y)$ como se verá en el Ejemplo 2.33.

Las descomposiciones primarias minimales tienen ciertas propiedades de unicidad.

Teorema 2.24. *Sea I un ideal descomponible de un anillo conmutativo R, y sea $I = Q_1 \cap \cdots \cap Q_n$ con $\sqrt{Q_i} = P_i$ para $i = 1, \ldots, n$, una descomposición primaria minimal de I. Sea $P \in \operatorname{Spec}(R)$. Entonces los siguientes enunciados son equivalentes:*

(i) $P = P_i$ para algún i con $1 \leq i \leq n$;

(ii) existe $a \in R$ tal que $(I : a)$ es P-primario;

(iii) existe $a \in R$ tal que $\sqrt{(I : a)} = P$.

Demostración.
$(i) \Rightarrow (ii)$ Supongamos que $P = P_i$ para algún i con $1 \leq i \leq n$. Como la descomposición primaria $I = \cap_{j=1}^n Q_j$ es minimal, existe $a_i \in \cap_{\substack{j=1 \\ j \neq i}}^n Q_j \setminus Q_i$. Por la Proposición 1.49 (ii), tenemos

$$(I : a_i) = (\cap_{j=1}^n Q_j : a_i) = \cap_{j=1}^n (Q_j : a_i).$$

Pero, por el Lema 2.19 (i) y (ii), tenemos que $(Q_j : a_i) = R$ para $j \neq i, 1 \leq j \leq n$, mientras que $(Q_i : a_i)$ es P_i-primario. Como $P = P_i$, se sigue que $(I : a_i)$ es P-primario.
$(ii) \Rightarrow (iii)$ Esto es inmediato ya que el radical de un ideal P-primario es igual a P.
$(iii) \Rightarrow (i)$ Supongamos que $a \in R$ es tal que $\sqrt{(I : a)} = P$. Por propiedades del ideal cociente (Proposición 1.49 (ii)), se tiene $(I : a) = (\cap_{i=1}^n Q_i : a) = \cap_{i=1}^n (Q_i : a)$. Por el Lema 2.19 (i) y (ii), tenemos que $(Q_i : a) = R$ si $a \in Q_i$, mientras que $(Q_i : a)$ es P_i-primario si $a \notin Q_i$. Por lo tanto,usando la Proposición 1.22, tenemos que

$$P = \sqrt{(I : a)} = \bigcap_{\substack{i=1 \\ a \notin Q_i}}^n \sqrt{(Q_i : a)} = \bigcap_{\substack{i=1 \\ a \notin Q_i}}^n P_i.$$

Ya que P es un ideal propio de R, se sigue que hay al menos un entero i con $1 \leq i \leq n$ para el cual $a \notin Q_i$, y además por el Corolario 1.43, $P = P_i$ para algún i. $\square$

Ejemplo 2.25. En el Ejemplo 2.21, tenemos

- Sea $R = \mathbb{Z}$. $I = (12) = (4) \cap (3)$, con $P_1 = (2) = \sqrt{(I : 6)}$ y $P_2 = (3) = \sqrt{(I : 4)}$.
- Sea $R = K[x, y]$. Entonces $I = (x^2, xy) = (x) \cap (x, y)^2$, con $P_1 = (x) = \sqrt{I : (y^2)}$ y $P_2 = (x, y) = \sqrt{I : (x)}$.

Corolario 2.26. ***PRIMER TEOREMA DE UNICIDAD PARA LA DESCOMPOSICIÓN PRIMARIA***
Sea I un ideal descomponible de un anillo conmutativo R y sean $I = Q_1 \cap \cdots \cap Q_n$ con $\sqrt{Q_i} = P_i$ para $i = 1, \ldots, n$ y $I = Q'_1 \cap \cdots \cap Q'_{n'}$ con $\sqrt{Q'_i} = P'_i$ para $i = 1, \ldots, n'$, dos descomposiciones primarias minimales de I. Entonces $n = n'$ y tenemos que $\{P_1, \ldots, P_n\} = \{P'_1, \ldots, P'_n\}$.

En otras palabras, el número de términos que aparecen en una descomposición primaria minimal de I es independiente de cual sea la descomposición primaria, como también lo es el conjunto de ideales primos que aparecen como radicales de los elementos primarios.

Demostración. Esto es inmediato por el Teorema 2.24, ya que establece que para $P \in \mathrm{Spec}(R)$ tenemos que P es igual a uno de los $P_1, \ldots, P_n$, si y solo si existe $a \in R$ para el cual $\sqrt{(I : a)} = P$. Como este segundo enunciado es completamente independiente de la descomposición primaria de I que se tome, el enunciado anterior será igual de independiente. □

El teorema anterior es uno de los pilares fundamentales del álgebra conmutativa. Este nos lleva al concepto de "ideal primo asociado" de un ideal descomponible.

Definición 2.27. Sea I un ideal descomponible de un anillo conmutativo R, y sea $I = Q_1 \cap \cdots \cap Q_n$ con $\sqrt{Q_i} = P_i$ para $i = 1, \ldots, n$, una descomposición primaria minimal de I. Entonces el conjunto de n elementos $\{P_1, \ldots, P_n\}$, el cual es independiente de la descomposición primaria de I que se tome, se denomina *el conjunto de ideales primos asociados de I* y se denota por $\mathrm{Ass}(I)$ o $\mathrm{Ass}_R(I)$. A los miembros de $\mathrm{Ass}(I)$ se les conoce como 'ideales primos asociados' o 'primos asociados' de I, y se dice que *pertenecen* a I.

Observación 2.28. Sea I un ideal descomponible de un anillo conmutativo R, y sea $P \in \mathrm{Spec}(R)$. Por el Teorema 2.24 se sigue que $P \in \mathrm{Ass}(I)$ si y solo si existe $a \in R$ tal que $(I : a)$ es P-primario, y este caso se da si y solo si existe $b \in R$ tal que $\sqrt{(I : b)} = P$.

Proposición 2.29. *Sea I un ideal descomponible de un anillo conmutativo R, y sea $P \in \mathrm{Spec}(R)$. Entonces P es un ideal primo minimal de I si y solo si P es un miembro minimal (respecto de la inclusión) de $\mathrm{Ass}(I)$.*

En particular, todos los ideales primos minimales de I pertenecen a $\mathrm{Ass}(I)$*, de modo que I tiene solo un número finito de ideales primos minimales, y si* $P_1 \in \mathrm{Spec}(R)$ *con* $P_1 \supseteq I$*, entonces existe* $P_2 \in \mathrm{Ass}(I)$ *con* $P_1 \supseteq P_2$*.*

Demostración. Sea $I = Q_1 \cap \cdots \cap Q_n$ con $\sqrt{Q_i} = P_i$ para $i = 1, \ldots, n$, una descomposición primaria minimal de I. Nótese que $P \supseteq I$ si y solo si $P = \sqrt{P} \supseteq \sqrt{I}$, y por la Proposición 1.22 se tiene que $\sqrt{I} = \cap_{i=1}^{n} \sqrt{Q_i} = \cap_{i=1}^{n} P_i$.

Por el Lema 1.42, se sigue que $P \supseteq I$ si y solo si $P \supseteq P_j$ para algún j con $1 \leq j \leq n$, esto es, si y solo si $P \supseteq P'$ para algún $P' \in \mathrm{Ass}(I)$.
($\Rightarrow$) Supongamos que P es un ideal primo minimal de I. Entonces, por el razonamiento expuesto justo antes, $P \supseteq P'$ para algún $P' \in \mathrm{Ass}(I)$. Pero $\mathrm{Ass}(I) \subseteq V_{\mathrm{Spec}}(I)$, y entonces $P = P'$ tiene que ser un elemento minimal de $\mathrm{Ass}(I)$ con respecto a la inclusión.
($\Leftarrow$) Supongamos que P es un elemento minimal de $\mathrm{Ass}(I)$. Por lo tanto $P \supseteq I$, y por la Proposición 1.40 existe un ideal primo minimal P' de I tal que $P \supseteq P'$. Por lo tanto, por el primer párrafo de esta demostración, existe $P'' \in \mathrm{Ass}(I)$ tal que $P' \supseteq P''$. Pero entonces, $P \supseteq P' \supseteq P''$, y como P es un elemento minimal de $\mathrm{Ass}(I)$, debe darse que $P = P' = P''$. Por lo tanto $P = P'$ es un ideal primo minimal de I.

El resto de afirmaciones se prueban teniendo en cuenta la Proposición 1.40 del capítulo anterior que dice que el conjunto no vacío $\Theta := \{P' \in \mathrm{Spec}(R) : P \supseteq P' \supseteq I\}$ tiene un elemento minimal respecto de la inclusión, y el hecho de que $\mathrm{Ass}(I)$ es un conjunto finito. □

Terminología. Sea I un ideal descomponible de un anillo conmutativo R. Acabamos de ver que los elementos minimales de $\mathrm{Ass}(I)$ son precisamente los ideales primos minimales de I. Estos ideales primos son llamados primos '*minimales*' o '*aislados*' de I. Los primos asociados restantes de I, es decir, los primos asociados de I que no son minimales, se denominan primos '*embebidos*' o '*inmersos*' de I.

Observación 2.30. Un ideal descomponible de un anillo conmutativo R no tiene por qué tener necesariamente ningún primo embebido: un ideal primario Q de R es ciertamente descomponible porque "$Q = Q$" es una descomposición primaria minimal de Q, y así $\sqrt{Q}$ es el único primo asociado de Q.

Ejemplo 2.31.

- Sea $R = \mathbb{Z}[x]$. El ideal $I = (x^2, 2x)$ tiene las siguientes descomposiciones primarias

$$(x^2, 2x) = (x) \cap (x^2, 2) = (x) \cap (x^2, 2 + x) = (x) \cap (x^2, 2x, 4),$$

con $\sqrt{(x)} = (x)$ primo minimal, y $\sqrt{(x^2, 2)} = \sqrt{(x^2, 2 + x)} = \sqrt{(x^2, 2x, 4)} = (2, x)$ primo embebido (ideal maximal).

- Sea $R = \mathbb{Z}[x, y]$. Una descomposición primaria minimal del ideal $I = (2, x^2, xy)$ es:

$$(2, x^2, xy) = (2, x) \cap (2, x^2, y),$$

con $\sqrt{(2, x)} = (2, x)$ primo minimal y $\sqrt{(2, x^2, y)} = (2, x, y)$ primo embebido (ideal maximal).

- Sea $R = \mathbb{Z}[x]$. Una descomposición primaria del ideal $I = (4, 2x, x^2)$ es:

$$(4, 2x, x^2) = (4, x) \cap (2, x^2),$$

con $\sqrt{(4, x)} = \sqrt{(2, x^2)} = (2, x)$ primo minimal. Esta descomposición no es minimal. De hecho la descomposición primaria minimal es

$$(4, 2x, x^2) = (4, 2x, x^2),$$

con $\sqrt{(4, 2x, x^2)} = (2, x)$, ya que el ideal $I = (4, 2x, x^2)$ es primario.

- Sea $R = \mathbb{Z}[x]$. Una descomposición primaria minimal del ideal $I = (9, 3x + 3)$ es:

$$(9, 3x + 3) = (3) \cap (9, x + 1),$$

con $\sqrt{(3)} = (3)$ primo minimal y $\sqrt{(9, x + 1)} = (3, x + 1)$ primo embebido (ideal maximal).

El Primer Teorema de unicidad para la Descomposición Primaria, junto con la motivación para la descomposición primaria que viene de la teoría de factorización única en un DIP, nos hace preguntarnos si una descomposición primaria minimal de un ideal I en un anillo conmutativo R está determinada de forma única por I. Pero esto no es cierto, como se ve a continuación en los siguientes ejemplos.

Ejemplo 2.32. Descomposición primaria minimal no es única
Sea K un cuerpo y el anillo $R = K[x, y]$. En R, sea $M = (x, y)$, $P = (y)$, $Q = (x, y^2)$, $I = (xy, y^2)$. Nótese que M es un ideal maximal de R, P un ideal primo de R y Q un ideal M-primario de R diferente de M^2. Tenemos que $I = Q \cap P$ y $I = M^2 \cap P$ son dos descomposiciones primarias minimales de I con distintos términos M-primarios.

Demostración. Es claro que $I \subseteq P$ y $I \subseteq M^2 \subseteq Q$; por lo tanto $I \subseteq M^2 \cap P \subseteq Q \cap P$.

Sea $f \in Q \cap P$. Como $f \in P$, todo término monomial que aparece en f involucra a y; sumemos todos estos términos monomiales que tienen grado al menos 2 para formar un polinomio $g \in I$ tal que $f - g = cy$ para algún $c \in K$.

Afirmamos que $c = 0$, ya que si no fuese así tendríamos $y = c^{-1}cy \in (Q \cap P) + I = Q \cap P \subseteq Q$, y así $y = hx + ey^2$ para algunos $h, e \in R$, lo cual es imposible.

Así $f = g \in I$ y hemos probado que $I = M^2 \cap P = Q \cap P$. Además, estas ecuaciones dan dos descomposiciones primarias de I porque $P \in \text{Spec}(R)$ y M^2 es M-primario. Finalmente, ambas descomposiciones primarias son minimales porque $x^2 \in M^2 \backslash P$, $x^2 \in Q \backslash P$, $y \in P \backslash Q$, $y \in P \setminus M^2$. Así hemos construido dos descomposiciones primarias minimales de I con diferentes términos M-primarios. □

Ejemplo 2.33. Infinitas descomposiciones primarias minimales distintas
Sea $R = K[x, y]$. El ideal $I = (x^2, xy)$ tiene infinitas descomposiciones primarias minimales distintas. Hemos visto en el Ejemplo 2.21 la descomposición primaria $I = (x^2, xy) = (x) \cap (x, y)^2$. Nótese que $(x, y)^2 = (x^2, xy, y^2)$.

$I = (x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^2) = (x) \cap (x^2, xy, y^n)$ para todo $n \in \mathbb{N}$.

Veamos que $(x^2, xy) = (x) \cap (x^2, xy, y^n)$.

Claramente el lado izquierdo está incluido en el lado derecho.

Para el otro contenido, sea r un elemento del lado derecho.

$$r = q_1 x = q_2 x^2 + q_3 xy + q_4 y^n,$$

con q_i polinomios en $K[x, y]$. Se sigue que x divide a q_4, y por lo tanto $r \in (x^2, xy)$, ya que

$$r = q_1 x = q_2 x^2 + q_3 xy + q_4' xy^n = q_2 x^2 + (q_3 + q_4' y^{n-1}) xy.$$

(x) es un primo minimal o aislado y (x, y) es un primo embebido o inmerso.

Se tiene:

- $\sqrt{I \colon (y)} = (x)$, primo minimal.
- $\sqrt{I \colon (x)} = (x, y)$, primo embebido.

Desde el punto de vista geométrico, en $\mathbb{R}[x, y]$, $V(x^2, xy)$ es el eje y junto con el punto $(0, 0)$. La variedad irreducible $\{(0, 0)\}$ que corresponde al ideal primo (x, y) está embebida o inmersa en la variedad irreducible $V(x)$, el eje y.

Otra manera de ver que tiene infinitas descomposiciones primarias minimales distintas. El ideal $I = (x^2, y - cx)$ es un ideal primario en $K[x, y]$, ya que $K[x, y]/I \cong K[x]/(x^2)$ y el único divisor de cero $\bar{x}$ es nilpotente. Además, si $c \neq d$ entonces $(x^2, y - cx) \neq (x^2, y - dx)$. Por otro lado,

$$(x^2, xy) = (x) \cap (x^2, y - cx).$$

" $\subset$" $xy = cx^2 + x(y - cx) \in (x) \cap (x^2, y - cx)$.

" $\supset$" sea r un elemento del lado derecho.

$$r = q_1 x = q_2 x^2 + q_3 (y - cx) = q_2 x^2 + q_3 y - c q_3 x,$$

con q_i polinomios en $K[x,y]$. Se sigue que x divide a q_3, $q_3 = q_3'x$ y por lo tanto $r \in (x^2, xy)$, ya que

$$r = q_1x = q_2x^2 + q_3'xy - cq_3'x^2 = (q_2 - cq_3')x^2 + q_3'xy.$$

Así, $(x^2, xy) = (x) \cap (x^2, y - cx)$ es una descomposición primaria minimal, con (x) ideal primo minimal y $\sqrt{(x^2, y-cx)} = (x,y)$ ideal primo inmerso. Por lo tanto, (x^2, xy) tiene infinitas descomposiciones primarias minimales distintas.

Los primos minimales asociados son simplemente los primos que son minimales entre los primos que contienen a I. Existe una correspondencia, como veremos en la Observación 3.11 (véase Capítulo 3, pág. 44):

Primos minimales asociados de $I \iff$ Componentes irreducibles (en la única descomposición minimal) de $V(I)$.

Así $V(x^2, xy) = V(x)$ es la única descomposición minimal de $V(x^2, xy)$ en variedades irreducibles.

Una pregunta que nos podemos hacer es que, para un ideal I descomponible en un anillo conmutativo R y para un ideal primo minimal P perteneciente a I, el término P-primario en una descomposición primaria minimal de I se determina por I de forma única y es independiente de la descomposición primaria minimal. Esta cuestión es la que se enuncia en el llamado 'Segundo Teorema de Unicidad para la Descomposición Primaria', que expondremos a continuación.

Teorema 2.34. ***SEGUNDO TEOREMA DE UNICIDAD PARA LA DESCOMPOSICIÓN PRIMARIA***

Sea I un ideal descomponible de un anillo conmutativo R, y sea $\mathrm{Ass}(I) = \{P_1, \ldots, P_n\}$. *Sean $I = Q_1 \cap \cdots \cap Q_n$ con $\sqrt{Q_i} = P_i$ para $i = 1, \ldots, n$ y $I = Q_1' \cap \cdots \cap Q_n'$ con $\sqrt{Q_i'} = P_i$, para $i = 1, \ldots, n$, dos descomposiciones primarias minimales de I.*

Entonces, para cada i con $1 \leq i \leq n$ para el cual P_i es un ideal primo minimal perteneciente a I, tenemos $Q_i = Q_i'$.

En otras palabras, en una descomposición primaria minimal de I, el término primario correspondiente a un ideal primo aislado de I está determinado de forma única por I y es independiente de la descomposición primaria minimal tomada.

Demostración. Si $n = 1$ es trivial. Ahora supongamos $n > 1$. Sea P_i un ideal primo minimal perteneciente a I. Ahora existe $a \in \cap_{\substack{j=1 \\ j \neq i}}^{n} P_j \setminus P_i$, ya que si no por el Lema 1.42 se tendría $P_j \subset P_i$ para algún $j \in \mathbb{N}$ con $1 \leq j \leq n$ y $j \neq i$, lo cual contradice el hecho de que P_i es un ideal primo minimal perteneciente a I.

Para cada $j = 1, \ldots, n$, con $j \neq i$ existe $h_j \in \mathbb{N}$ tal que $a^{h_j} \in Q_j$.

Sea $t \in \mathbb{N}$ tal que $t \geq \text{máx}\{h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n\}$. Entonces $a^t \notin P_i$, y por el Lema 2.19 (iii) tenemos que $(I : a^t) = (\cap_{j=1}^n Q_j : a^t) = \cap_{j=1}^n (Q_j : a^t) = Q_i$ por ser Q_i un ideal P_i-primario. Así hemos probado que $Q_i = (I : a^t)$ para t suficientemente grande. Del mismo modo, $Q_i' = (I : a^t)$ para t suficientemente grande. Por lo tanto, $Q_i = Q_i'$. □

Hemos visto que las descomposiciones primarias minimales de un ideal no son únicas.

Sin embargo, esta "no unicidad" es muy sutil, ya que solo puede darse en los ideales primarios de las componentes embebidas.

Más concretamente, hemos probado que en una descomposición primaria minimal:

- **los ideales primos subyacentes de todos los ideales primarios están determinados de forma única (Corolario 2.26);**
- **los ideales primarios correspondientes a todos los ideales primos minimales o aislados están determinados de forma única (Teorema 2.34).**

Otra cuestión es estudiar si todo ideal propio en un anillo conmutativo admite una descomposición primaria. Esto puede parecer cierto por el hecho de que todo ideal propio en un DIP posee una descomposición primaria. Pero esto no es así, como se ve en el siguiente ejemplo.

Ejemplo 2.35. El ideal nulo (0) en el anillo $\mathcal{C}([0,1])$ de las funciones continuas de variable real definidas en el intervalo $[0,1]$ no es descomponible, es decir, no tiene una descomposición primaria.

Recordemos, por el Ejemplo 1.9, que el anillo $\mathcal{C}([0,1])$ no es Noetheriano.

También hay que notar que todo ideal maximal de $\mathcal{C}([0,1])$ es de la forma:

$$M_x = \{f \in \mathcal{C}([0,1]) \mid f(x) = 0\}, \text{ para algún } x \in [0,1].$$

Si el ideal (0) de $\mathcal{C}([0,1])$ fuera descomponible, entonces existirían un número finito de ideales primos minimales de $\mathcal{C}([0,1])$.

Pero esto no puede ser ya que todo ideal maximal M_x de $\mathcal{C}([0,1])$ contiene un ideal primo minimal ya que todo ideal maximal ideal es también un ideal primo.

Por lo tanto para probar que el ideal (0) de $\mathcal{C}([0,1])$ no es descomponible es suficiente probar que si $x \neq y \in [0,1]$ entonces cualesquiera dos primos minimales $P_1 \subseteq M_x, P_2 \subseteq M_y$ son diferentes.

Ya que $[0,1]$ es Hausdorff y normal, existe un conjunto abierto U tal que $x \in U$ e $y \notin \overline{U}$. Por el Lema de Urysohn existen $f, g \in \mathcal{C}([0,1])$ tal que $f(U) = 0, f(y) = 1, g(x) = 1$, y $g(X \setminus U) = 0$. Así $fg = 0$. Por lo tanto, $fg \in P_1$ pero $g \notin P_1$, ya que $g(x) \neq 0$, y así $f \in P_1$. Pero $f \notin P_2$, ya que $f(y) \neq 0$. Por lo tanto $P_1 \neq P_2$.

2.6. Descomposición primaria en un anillo Noetheriano

Volvamos ahora a centrarnos en la existencia de descomposición primaria para todo ideal propio en un anillo conmutativo Noetheriano. Introduzcamos una serie de conceptos y resultados para probar dicha descomposición.

Definición 2.36. Ideal irreducible
Sea I un ideal de un anillo conmutativo R. Decimos que I es irreducible si I es propio y no puede expresarse como intersección de dos ideales de R estrictamente mayores.

Entonces tendremos que I es irreducible si y solo si $I \subset R$ y, siempre que $I = I_1 \cap I_2$ con I_1, I_2 ideales de R, entonces $I = I_1$ o $I = I_2$.

Las ideas claves para la prueba de la existencia de descomposición primaria para todo ideal propio en un anillo Noetheriano es precisamente que todo ideal propio se puede expresar como intersección finita de ideales irreducibles de R, y que todo ideal irreducible es primario.

Proposición 2.37. *En un anillo R todo ideal primo es un ideal irreducible.*

Demostración. Supongamos que $J \neq R$ es primo y $J = I_1 \cap I_2$. Entonces $I_1 I_2 \subseteq I_1 \cap I_2 = J$; ya que J es primo, entonces $I_1 \subseteq J$ o $I_2 \subseteq J$. Veamos que esto es cierto.

Supongamos que $I_1 \not\subset J$. Entonces existe algún $a \in I_1$ tal que $a \notin J$. Sea b un elemento cualquiera de I_2. Entonces $ab \in I_1 \cap I_2 \subset J$, y así $a \in J$ o $b \in J$, por ser J un ideal primo. Por lo tanto $b \in J$, y en consecuencia $I_2 \subset J$.

Pero si $I_1 \subseteq J = I_1 \cap I_2$, tenemos $I_1 \subseteq I_2$; en particular, $J = I_1 \cap I_2 = I_1$, así concluimos que $J = I_1$; análogamente, si $I_2 \subseteq J$, entonces deducimos que $J = I_2$, y así se satisface la condición de irreducibilidad. □

El recíproco de la Proposición 2.37 no es cierto. Existen ideales irreducibles que no son primos.

Ejemplo 2.38. Sea $R = \mathbb{Z}$.

- El ideal (4) es irreducible ya que el único ideal que contiene a (4) es (2), y $(2) \cap (2) = (2)$.
- $J = (p^n)$ es irreducible, donde p es un primo y $n > 0$. Si $(p^n) = (a) \cap (b) = (\text{lcm}(a, b))$ entonces tenemos $a = \pm p^i$, $b = \pm p^j$ para algunos i, j, $0 \leq i, j \leq n$; y además $\text{máx}\{i, j\} = n$.

  Por lo tanto $(p^n) = (a)$ o $(p^n) = (b)$, así (p^n) es irreducible. Sin embargo, el ideal $J = (p^n)$ es primo solo cuando $n = 1$.

Observación 2.39. Un elemento $p \in R$ es primo si, y solo si, el ideal principal (p) es un ideal primo (véase Proposición 1.27). Esto no es verdad para ideales irreducibles: un ideal irreducible puede estar generado por un elemento que no es irreducible. Por ejemplo, en $\mathbb{Z}$, el ideal (4) es irreducible.

Aquí tenemos una situación delicada (curva peligrosa  , según el grupo de matemáticos Nicolas Bourbaki), ya que a muchos matemáticos no les entusiasma el término ideal "irreducible" por esta razón.

Proposición 2.40. *Sea R un anillo conmutativo Noetheriano e I un ideal irreducible de R. Entonces I es primario.*

Demostración. Por definición de ideal irreducible, $I \subsetneq R$. Supongamos que $a, b \in R$ son tales que $ab \in I$ pero $b \notin I$. Ahora, $(I : a) \subseteq (I : a^2) \subseteq \cdots \subseteq (I : a^i) \subseteq \cdots$ es una cadena ascendente de ideales de R y entonces, por ser R Noetheriano, existe $n \in \mathbb{N}$ tal que $(I : a^n) = (I : a^{n+i})$ para todo $i \in \mathbb{N}$.

Veamos que $I = \{I + (a^n)\} \cap \{I + (b)\}$. Es claro que $I \subseteq \{I + (a^n)\} \cap \{I + (b)\}$. Sea $r \in \{I + (a^n)\} \cap \{I + (b)\}$; entonces podemos escribir $r = g + ca^n = h + db$ para ciertos $g, h \in I$ y $c, d \in R$. Por lo tanto, $ra = ga + ca^{n+1} = ha + dab$, y como $ab, g, h \in I$, tenemos $ca^{n+1} = ha + dab - ga \in I$.

Por lo tanto $c \in (I : a^{n+1}) = (I : a^n)$ y entonces $r = g + ca^n \in I$. De aquí se sigue que $I = \{I + (a^n)\} \cap \{I + (b)\}$, que es lo que queríamos probar.

Ahora I es irreducible y $I \subset I + (b)$ porque $b \notin I$. Por lo tanto $I = I + (a^n)$ y $a^n \in I$. Así hemos probado que I es un ideal primario de R. □

Pero no todo ideal primario es irreducible. Esto se ve en el siguiente ejemplo.

Ejemplo 2.41. Ideal primario no irreducible

- Sea $R = K[x, y]$ el anillo conmutativo de polinomios sobre el cuerpo K. El ideal $I = (x^2, xy, y^2) = (x, y)^2$ es (x, y)-primario pero reducible porque $I = (x, y^2) \cap (x^2, y)$.

- En el Ejemplo 2.31 hemos visto que el ideal $I = (4, 2x, x^2) \subset \mathbb{Z}[x]$ era primario, y que no era irreducible ya que $I = (4, 2x, x^2) = (4, x) \cap (2, x^2)$.

De hecho, se puede probar que:

Proposición 2.42. *En un dominio de ideales principales todo ideal primario es irreducible.*

Demostración. En el Ejemplo 2.9, hemos visto que todo ideal primario en un DIP es de la forma (0) o (p^n), con p un elemento irreducible. Por el Ejemplo 2.38, hemos visto que (p^n) es un ideal irreducible.

El ideal (0) es irreducible ya que si $(0) = (a) \cap (b) = (\text{lcm}(a, b))$, entonces $a = 0$ o $b = 0$. □

Corolario 2.43. *Sea R un dominio de ideales principales (DIP). Entonces un ideal es primario, si y solo, si, es irreducible.*

Demostración. Es consecuencia de que un DIP es Noetheriano y de las Proposiciones 2.40 y 2.42. □

Observación 2.44. Veamos una prueba directa de que todo ideal primario $\neq (0)$ de la forma (p^n) en un DIP es irreducible.

Sea (a) un ideal en un DIP y supongamos que $(a) \neq (p^n)$, para algún elemento p irreducible y n un entero positivo. $a = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$. Entonces $(a) = (p_1^{n_1}) \cap (p_2^{n_2} \cdots p_s^{n_s})$. Ya que $(a) \neq (p_1^{n_1})$ y $(a) \neq (p_2^{n_2} \cdots p_s^{n_s})$, entonces (a) no sería irreducible, con lo cual es una contradicción.

Proposición 2.45. *Sea R un anillo conmutativo Noetheriano. Entonces todo ideal propio de R se puede expresar como una intersección finita de ideales irreducibles de R.*

Demostración. Denotemos por $\sum$ al conjunto de todos los ideales propios de R que no pueden expresarse como intersección finita de ideales irreducibles de R. Queremos probar que $\sum = \emptyset$. Supongamos que esto no sea así. Entonces, por ser R Noetheriano, $\sum$ tiene un elemento maximal I respecto de la inclusión.

Entonces I en sí mismo no es irreducible, ya que de lo contrario podríamos escribir $I = I \cap I$ y I no estaría en $\sum$. Por ser I propio, se sigue que $I = I_1 \cap I_2$ para algunos I_1, I_2 ideales de R tales que $I \subset I_1$ y $I \subset I_2$. Nótese que esto implica que tanto I_1 como I_2 son ideales propios. Por la elección de I, debe darse $I_i \notin \sum$ para $i = 1, 2$. Por ser I_1 y I_2 propios, de aquí se sigue que ambos se pueden expresar como intersección finita de ideales irreducibles de R; por tanto $I = I_1 \cap I_2$ tienen la misma propiedad y esto es una contradicción. Entonces $\sum = \emptyset$ y la prueba es completa. □

Observación 2.46.

- Una de las razones de por que se hace la descomposición minimal de ideales en ideales primarios y no en ideales irreducibles, es que la intersección de ideales irreducibles no es irreducible, por ejemplo, en $\mathbb{Z}$, $(2) \cap (3) = (6)$, $(4) \cap (3) = (12)$ no son irreducibles, sin embargo la intersección de ideales P-primarios es P-primario.

- Otra razón de por que no se hace la descomposición minimal de ideales en ideales irreducibles es que dicha descomposición necesariamente no es única.

  Consideremos el Ejemplo 2.41, el ideal $I = (x^2, xy, y^2) = (x, y)^2$ del anillo $K[x, y]$.

  $$I = (x, y^2) \cap (x^2, y) = (x + y, x^2) \cap (x, (x + y)^2).$$

  Veamos que $I \subsetneq J_1, J_2, J_3, J_4$, donde $J_1 = (x, y^2)$, $J_2 = (x^2, y)$, $J_3 = (x + y, x^2)$ y $J_4 = (x, (x + y)^2)$.

  Se tiene que $\dim_K K[x, y]/I = 3$, pues una K-base es $\{1, x, y\}$.

  Por otro lado,

  $$\dim_K K[x, y]/J_1 = \dim_K K[x, y]/J_2 = \dim_K K[x, y]/J_3 = \dim_K K[x, y]/J_4 = 2,$$

  ya que sus K-bases son respectivamente, $\{1, y\}$, $\{1, x\}$, $\{1, y\}$, y $\{1, y\}$.

  Por lo tanto, el ideal I es distinto de todos los J_i, $i = 1, 2, 3, 4$.

Teorema 2.47 (**Teorema de Lasker–Noether**). *Sea I un ideal propio de un anillo conmutativo Noetheriano R. Entonces I tiene una descomposición primaria y por lo tanto también una descomposición primaria minimal.*

Demostración. Es inmediato teniendo en cuenta la Proposición 2.45, I puede expresarse como intersección finita de ideales irreducibles de R, y la Proposición 2.40, un ideal irreducible de R es primario. □

Proposición 2.48. *Si I es un ideal radical entonces no tiene primos embebidos.*

Demostración. Ya que $I = \bigcap_{i=1}^{n} Q_i$ es una descomposición primaria minimal, por el primer teorema de unicidad de la descomposición primaria, el número n está fijado por I en todas las descomposiciones primarias, i.e. I no tiene una descomposición primaria con menos, o igual, de $n - 1$ ideales primarios.

Sea $I = \sqrt{I}$. Entonces $I = \sqrt{I} = \sqrt{\bigcap_{i=1}^{n} Q_i} = \bigcap_{i=1}^{n} \sqrt{Q_i} = \bigcap_{i=1}^{n} P_i$ es también una descomposición primaria para I, donde cada Q_i es P_i-primario.

Ahora, si para algunos $i \neq j$ (por ejemplo para 1 y 2), $P_2 \subset P_1$, entonces $I = \bigcap_{i=2}^{n} P_i$ la cual sería una descomposición primaria con $n - 1$ elementos, una contradicción. □

Corolario 2.49. *Si I es un ideal radical entonces tiene una única descomposición primaria minimal.*

Es fácil expresar la relación entre descomposición primaria y factorización única en el sentido clásico (véase [4, Proposition 3.11]).

Proposición 2.50 ([4]). *Sea R un dominio Noetheriano. Si $f \in R$ y $f = u\prod p_i^{e_i}$ tal que u es una unidad de R, y los p_i son primos generando los distintos ideales (p_i), entonces $(f) = \cap(p_i^{e_i})$ es la descomposición minimal primaria de (f).*

En el anillo de polinomios es muy importante destacar el cuerpo base sobre el que se trabaja.

Ejemplo 2.51. Dos descomposiciones diferentes que dependen del cuerpo base

- Sea $R = \mathbb{Q}[x, y]$. Entonces $I = (y-x^2, y-x+1)$ es un ideal primo y su descomposición primaria coincide con I.
- Sea $R = \overline{\mathbb{Q}}[x, y]$. Entonces $I = (y - x^2, y - x + 1)$ no es un ideal primo, $\overline{\mathbb{Q}}[x, y]/I \cong \overline{\mathbb{Q}}[x]/(x^2 - x + 1)$, y el polinomio $x^2 - x + 1$ no es irreducible en $\overline{\mathbb{Q}}[x]$ ya que tiene dos raíces $\frac{1}{2} \pm \frac{1}{2}i\sqrt{3}$. Así, la variedad $V(I) = \{(\frac{1}{2} - \frac{1}{2}i\sqrt{3}, -\frac{1}{2} - \frac{1}{2}i\sqrt{3}), (\frac{1}{2} + \frac{1}{2}i\sqrt{3}, -\frac{1}{2} + \frac{1}{2}i\sqrt{3})\}$. Por otro lado, el ideal I es radical en $\overline{\mathbb{Q}}[x, y]$. La descomposición primaria del ideal I en $\overline{\mathbb{Q}}[x]$ es $I = (x - \frac{1}{2} + \frac{1}{2}i\sqrt{3}, y + \frac{1}{2} + \frac{1}{2}i\sqrt{3}) \cap (x - \frac{1}{2} - \frac{1}{2}i\sqrt{3}, y + \frac{1}{2} - \frac{1}{2}i\sqrt{3})$, donde estos dos últimos ideales son maximales (y por tanto, primos).

Ejemplo 2.52. Descomposición en un anillo Noetheriano que no es un DFU
Hemos visto (Ejemplo 1.31) que el anillo $R = \mathbb{Z}[\sqrt{5}i]$ no es un DFU ya que 6 tiene dos factorizaciones distintas $6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$, sin embargo, vimos que hay una forma generalizada de "factorización única" de ideales en una amplia clase de anillos (los anillos Noetherianos).

Ya que $R = \mathbb{Z}[\sqrt{5}i]$ es Noetheriano, el ideal (6) admite la siguiente descomposición primaria (véase [2])

$$(6) = (2, 1 + \sqrt{5}i)^2 \cap (3, 1 + \sqrt{5}i) \cap (3, 1 - \sqrt{5}i),$$

donde $(3, 1 + \sqrt{5}i)$, $(3, 1 - \sqrt{5}i)$ son ideales primos y $(2, 1 + \sqrt{5}i)$ es un ideal maximal.

Capítulo 3

INTERPRETACIÓN GEOMÉTRICA DE LA DESCOMPOSICIÓN PRIMARIA

3.1. Aplicaciones en geometría

Sea $\mathbb{K}^n = \{(x_1, \ldots, x_n) \mid x_i \in K, i = 1, \ldots, n\}$ el espacio afín de dimensión n.

Sean $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. La variedad afín o los ceros del conjunto $\{f_1, \ldots, f_s\}$ es

$$V\{f_1, \ldots, f_s\} = \{x \in \mathbb{K}^n \mid f_i(x) = 0, \text{ para todo } i = 1, \ldots, s\}.$$

Una variedad afín se llama también un conjunto algebraico.

Los polinomios $\{f_1, \ldots, f_s\}$ o el ideal generado por $\{f_1, \ldots, f_s\}$, $J = (f_1, \ldots, f_s)$, definen la misma variedad:

$$V\{f_1, \ldots, f_s\} = V(J) = V(f_1, \ldots, f_s).$$

Además, para un ideal J, $V(J) = V(\sqrt{J})$, i.e. los ceros de un ideal y su radical son los mismos. Esto es consecuencia de que el conjunto de ceros de f^m es el mismo que el conjunto de ceros de f (contados sin multiplicidad).

Recíprocamente, para $S \subset \mathbb{K}^n$, el ideal (o ideal de anulación) de S es:

$$I(S) = \{f \in K[x_1, \ldots, x_n] \mid f(x) = 0 \text{ para todo } x \in S\}.$$

Si W es una variedad de $\mathbb{K}^n$, entonces $I(W)$ es un ideal radical. Además, se verifica

$$V\big(I(W)\big) = W.$$

Una cuestión natural es preguntar si $I\big(V(J)\big) = J$. No es difícil probar que $J \subset I\big(V(J)\big)$. El siguiente contraejemplo muestra que la otra inclusión no es cierta en general.

Sea $J = (x^2) \subset \mathbb{C}[x]$. Entonces $V(J) = \{0\}$ y $I\big(V(J)\big) = (x) \neq J$.

Este ejemplo nos da una intuición del porqué no se da la otra inclusión. El ideal (x^2) consiste de los polinomios que tienen una raíz de multiplicidad al menos 2 en el origen. El operador $V(\cdot)$ no "ve" la multiplicidad: para que un polinomio esté en el ideal $I\big(V(J)\big)$, solo necesita anularse en $x = 0$.

Por otro lado, si K es un cuerpo algebraicamente cerrado, entonces se verifica

$$I\big(V(J)\big) = \sqrt{J}.$$

Así, excepto las multiplicidades, los ideales están determinados de forma única por las variedades, como veremos más adelante.

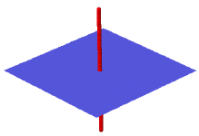
Definición 3.1. Variedad irreducible

Una variedad afín $V \subseteq \mathbb{K}^n$ se dice irreducible si, siempre que V se escriba como $V = V_1 \cup V_2$ donde V_1, V_2 son variedades afines, entonces $V = V_1$ o $V = V_2$.

Ejemplo 3.2. La variedad afín $V(xz, yz)$ no es irreducible ya que

$$V(xz, yz) = V\big((x, y) \cdot (z)\big) = V(x, y) \cup V(z),$$

i.e. es la unión del eje z con el plano $z = 0$.



Por otro lado, no está del todo claro cuando una variedad es irreducible. Si esta definición se corresponde con nuestra intuición geométrica, está claro que un punto, una recta o un plano deberían ser variedades irreducibles. La variedad $V(y - x^2, z - x^3)$ en $\mathbb{R}^3$ es irreducible.

Proposición 3.3. ***Condición de cadena descendente (CCD)***

Cualquier cadena descendiente de variedades

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$$

en $\mathbb{K}^n$ se estabiliza, es decir, existe un entero positivo N tal que $V_N = V_{N+1} = \cdots$.

Demostración. Pasando a los ideales correspondientes se obtiene una cadena ascendente de ideales en el anillo Noetheriano $K[x_1, \ldots, x_n]$

$$I(V_1) \subseteq I(V_2) \subseteq I(V_3) \subseteq \cdots .$$

Por la condición de cadena ascendiente (CCA) de ideales en $K[x_1, \ldots, x_n]$, existe N tal que $I(V_N) = I(V_{N+1}) = \cdots$. Como $V(I(W)) = W$ para cualquier variedad W, se tiene que $V_N = V_{N+1} = \cdots$. □

Teorema 3.4. *Sea $V \subseteq \mathbb{K}^n$ una variedad afín. Entonces V puede expresarse como unión finita $V = V_1 \cup \cdots \cup V_m$, donde cada V_i es una variedad irreducible.*

Demostración. Supongamos que V es una variedad afín la cual no puede expresarse como unión finita de irreducibles. Entonces V no es irreducible, y así $V = V_1 \cup V_1'$ donde $V \neq V_1$ y $V \neq V_1'$. Además, o bien V_1 o bien V_1' no puede ser unión finita de irreducibles, porque de lo contrario lo sería V. Supongamos que V_1 no es unión finita de irreducibles. Repitiendo el argumento anterior, podemos escribir $V_1 = V_2 \cup V_2'$ donde $V \neq V_2$ y $V \neq V_2'$, y V_2 no es unión finita de irreducibles. Continuando con esto proceso, obtenemos una sucesión infinita de variedades

$$V \supseteq V_1 \supseteq V_2 \supseteq \cdots$$

con

$$V \neq V_1 \neq V_2 \neq \cdots ,$$

y esto contradice la condición de cadena descendiente. □

Definición 3.5. Descomposición minimal de una variedad afín en variedades irreducibles
Sea $V \subseteq \mathbb{K}^n$ una variedad afín. Una descomposición

$$V = V_1 \cup \cdots \cup V_m$$

donde cada V_i es una variedad irreducible, se llama descomposición minimal (o, a veces llamada, descomposición irredundante) si $V_i \nsubseteq V_j$ para $i \neq j$. También, llamamos a las V_i componentes irreducibles de V.

Teorema 3.6. *Sea $V \subseteq \mathbb{K}^n$ una variedad afín. Entonces V tiene una descomposición minimal*

$$V = V_1 \cup \cdots \cup V_m,$$

(así cada V_i es una variedad irreducible y $V_i \nsubseteq V_j$ para $i \neq j$). Además, esta descomposición minimal es única salvo el orden en que se escriben las $V_1, \ldots, V_m$.

Demostración. Por el Teorema 3.4, V se puede escribir de la forma $V = V_1 \cup \cdots \cup V_m$, donde cada V_i es una variedad irreducible. Si una V_i está contenida en algún V_j, con $i \neq j$, podemos eliminar V_i, y V sería la unión de los restantes V_j para $j \neq i$. Repitiendo este proceso llegamos a una descomposición minimal de V.

Para probar la unicidad, supongamos que $V = V_1' \cup \cdots \cup V_l'$ es otra descomposición minimal de V. Entonces, para cada V_i en la primera descomposición, tenemos

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \cdots \cup V_l') = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_l').$$

Por ser V_i irreducible, se sigue que $V_i = V_i \cap V_j'$ para algún j, i.e. $V_i \subseteq V_j'$. Aplicando el mismo argumento para V_j' (usando los V_i para descomponer V), se llega a que $V_j' \subseteq V_k$ para algún k, y, entonces,

$$V_i \subseteq V_j' \subseteq V_k.$$

Por minimalidad, $i = k$, y se sigue que $V_i = V_j'$. Por lo tanto, toda V_i aparece en $V = V_1' \cup \cdots \cup V_l'$, lo que implica $m \leq l$. Un argumento similar prueba que $l \leq m$ y así $l = m$. Por lo tanto, los V_i' son tan solo una permutación de los V_i y la unicidad queda probada. □

La correspondencia Ideal–Variedad

Teorema 3.7 ([3]). *Sea K un cuerpo arbitrario.*

Las aplicaciones

$$\textit{Ideales de } K[x_1, \ldots, x_n] \xrightarrow{\quad V \quad} \textit{Variedades afines de } \mathbb{K}^n$$

y

$$\textit{Variedades afines de } \mathbb{K}^n \xrightarrow{\quad I \quad} \textit{Ideales de } K[x_1, \ldots, x_n]$$

invierten las inclusiones, i.e. si $J_1 \subset J_2$ son ideales entonces $V(J_1) \supset V(J_2)$, y de manera análoga, si $W_1 \subset W_2$ son variedades entonces $I(W_1) \supset I(W_2)$.

Además para cualquier variedad W, $V(I(W)) = W$, así que I es inyectiva.

Por lo tanto la aplicación I es inyectiva, i.e. no puede haber dos variedades distintas que den el mismo ideal.

Pero dos ideales distintos pueden dar la misma variedad, i.e. V no es inyectiva. Por ejemplo, para los ideales de $K[x]$, $J_1 = ((x-1)(x-3))$ y $J_2 = ((x-1)^2(x-3))$, $J_1 \neq J_2$, $J_2 \subsetneq J_1$, se tiene

$$V(J_1) = V(J_2) = \{1, 3\} \subset \mathbb{K}.$$

Teorema 3.8 ([3]). *Si K es un cuerpo algebraicamente cerrado (por ejemplo $\mathbb{C}$) y nos restringimos a ideales radicales, entonces las aplicaciones*

$$\textit{Ideales radicales de } K[x_1,\dots,x_n] \xrightarrow{\ V\ } \textit{Variedades afines de } \mathbb{K}^n$$

y

$$\textit{Variedades afines de } \mathbb{K}^n \xrightarrow{\ I\ } \textit{Ideales radicales de } K[x_1,\dots,x_n]$$

son biyecciones que invierten las inclusiones y además son inversas entre sí.

Sea K un cuerpo algebraicamente cerrado (por ejemplo $\mathbb{C}$).

Además esta correspondencia Ideal–Variedad (diccionario Álgebra–Geometría) se puede detallar en la siguiente tabla, donde se suponen que todos los ideales son radicales y el cuerpo K es algebraicamente cerrado.

$$\{\text{Ideales radicales de } K[x_1,\dots,x_n]\} \underset{I}{\overset{V}{\longleftrightarrow}} \{\text{Variedades afines de } \mathbb{K}^n\}$$
$$J \longrightarrow V(J)$$
$$I(W) \longleftarrow W$$

$$\{\text{Ideales primos de } K[x_1,\dots,x_n]\} \underset{I}{\overset{V}{\longleftrightarrow}} \{\text{Variedades irreducibles de } \mathbb{K}^n\}$$

$$\{\text{Ideales maximales de } K[x_1,\dots,x_n]\} \underset{I}{\overset{V}{\longleftrightarrow}} \{\text{Puntos de } \mathbb{K}^n\}$$

$$\{\text{Intersección de ideales en } K[x_1,\dots,x_n]\} \underset{I}{\overset{V}{\longleftrightarrow}} \{\text{Unión de variedades en } \mathbb{K}^n\}$$
$$J_1 \cap J_2 \longrightarrow V(J_1) \cup V(J_2)$$
$$I(W_1) \cap I(W_2) \longleftarrow W_1 \cup W_2$$

$$\{\text{Producto de ideales en } K[x_1,\dots,x_n]\} \underset{I}{\overset{V}{\longleftrightarrow}} \{\text{Unión de variedades en } \mathbb{K}^n\}$$
$$J_1 J_2 \longrightarrow V(J_1) \cup V(J_2)$$
$$\sqrt{I(W_1)I(W_2)} \longleftarrow W_1 \cup W_2$$

$$\{\text{Suma de ideales en } K[x_1,\dots,x_n]\} \underset{I}{\overset{V}{\longleftrightarrow}} \{\text{Intersección de variedades en } \mathbb{K}^n\}$$
$$J_1 + J_2 \longrightarrow V(J_1) \cap V(J_2)$$
$$\sqrt{I(W_1) + I(W_2)} \longleftarrow W_1 \cap W_2$$

$$\{\text{DPM de } J \text{ en } K[x_1,\dots,x_n]\ \} \underset{I}{\overset{V}{\longleftrightarrow}} \{\text{DCI de } V(J) \text{ en } \mathbb{K}^n\ \}$$
$$J = \sqrt{J} = P_1 \cap \cdots \cap P_m \longrightarrow V(J) = V(P_1) \cup \cdots \cup V(P_m)$$
$$I(W) = I(W_1) \cap \cdots \cap I(W_m) \longleftarrow W = W_1 \cup \cdots \cup W_m$$

donde DPM = Descomposición primaria minimal y DCI = Descomposición en componentes irreducibles.

$$\{\text{CCA en } K[x_1,\dots,x_n]\} \underset{I}{\overset{V}{\longleftrightarrow}} \{\text{CCD en } \mathbb{K}^n\}$$

donde CCA = Condición de cadena ascendente y CCD = Condición de cadena descendente.

Observación 3.9. Surge de manera natural la pregunta si los conceptos de ideal irreducible y variedad irreducible están estrechamente relacionados. Veamos que en principio no existe un fuerte vínculo.

- El ideal J puede ser irreducible y la variedad $V(J)$ no irreducible.

  Sea $J = (f) \subseteq \mathbb{R}[x,y]$ donde $f = y^2 + x^2(x-1)^2$. f es irreducible en $\mathbb{R}[x,y]$, ya que si consideramos el polinomio en $(\mathbb{R}[x])[y]$, al ser de grado 2, es reducible si y solo si tiene una raíz en $\mathbb{R}[x]$. Pero $y^2 = -x^2(x-1)^2$ no tiene soluciones en $\mathbb{R}[x]$.

  Ya que $\mathbb{R}[x,y]$ es un DFU, f es primo, y por lo tanto el ideal $J = (f)$ que genera es un ideal primo y por lo tanto es un ideal irreducible (véase Proposición 2.37).

  Sin embargo, $V(J) = \{x \in \mathbb{R}^2 \mid f(x) = 0\} = \{(0,0),(1,0)\}$ es reducible.

- La variedad $V(J)$ puede ser irreducible y el ideal J no irreducible.

  En el Ejemplo 2.41 vimos que el ideal $J = (x^2, xy, y^2) = (x,y)^2$ del anillo $R = K[x,y]$ era reducible porque $J = (x,y^2) \cap (x^2,y)$. Pero $V(J) = \{(0,0)\}$ es irreducible.

Sea $R = K[x_1,\dots,x_n]$. Las nociones de ideales primos minimales (o aislados) y embebidos (o inmersos) se inspiran en la geometría. En efecto, pasando al espectro $\mathrm{Spec}(R)$ de todos los ideales primos de R y observando los conjuntos algebraicos (variedades) del tipo $V(S)$ para subconjuntos $S \subset R$, una inclusión estricta de ideales primos $P_1 \subsetneq P_2$ se refleja a nivel de los conjuntos algebraicos como una inclusión estricta $V(P_1) \supsetneq V(P_2)$. En particular, el conjunto algebraico $V(P_2)$ está "embebido" o "inmerso" en el mayor $V(P_1)$ y, asimismo, se dice que P_2 es un ideal primo embebido asociado a un ideal J si tenemos $P_1, P_2 \in \mathrm{Ass}(J)$ con $P_1 \subsetneq P_2$.

Geométricamente, si $J = Q_1 \cap \cdots \cap Q_m$ es una descomposición primaria de un ideal J en el anillo $K[x_1,\dots,x_n]$, tenemos que $V(J) = V(Q_1) \cup \cdots \cup V(Q_m) = V(P_1) \cup \cdots \cup V(P_m)$, donde $P_i = \sqrt{Q_i}$ para $i = 1,\dots,m$. Entonces habremos descompuesto la variedad

$V(J)$ como unión de subvariedades irreducibles $V(P_i)$. Como los anillos de coordenadas de variedades son siempre Noetherianos, se tendrá que la descomposición de una variedad en un número finito de subvariedades irreducibles siempre es posible.

Pero esta descomposición primaria encierra más información que no está recogida en $V(J)$: además de obtener subvariedades cuya unión sea $V(J)$ se tienen también ideales primarios cuyos ceros son estas subvariedades. Estos ideales primarios contienen 'información extra de la multiplicidad'. Por ejemplo la variedad dada por el ideal en $\mathbb{R}[x]$

$$J = ((x-a_1)^{k_1} \cdots (x-a_m)^{k_m}) = (x-a_1)^{k_1} \cap \cdots \cap (x-a_m)^{k_m}$$

es el subconjunto $V(J) = \{a_1, \ldots, a_m\}$ de $\mathbb{R}$; pero el ideal también asocia a cada punto a_i una multiplicidad k_i y la descomposición primaria $J = (x-a_1)^{k_1} \cap \cdots \cap (x-a_m)^{k_m}$ recuerda estas multiplicidades.

En dimensiones superiores la información adicional en cada subvariedad es más complicada que una simple multiplicidad.

Ejemplo 3.10. Recordemos el Ejemplo 2.33 para ilustrar el origen de la terminología.

Sea $I = (x^2, xy) \subset \mathbb{R}[x, y]$ y dos descomposiciones primarias minimales de I:

$$I = (x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^2).$$

En general las componentes irreducibles de la variedad $V(I)$ definida por el ideal I son los ceros de los primos aislados de I, y los ceros de los primos embebidos son subespacios irreducibles de estas componentes (por lo que están "embebidas" o "inmersas" en las componentes irreducibles).

En este ejemplo, $V(I)$ es el conjunto de puntos con $x^2 = xy = 0$, que es justamente el eje y en $\mathbb{R}^2$.

Solo hay una componente irreducible de esta variedad (el eje y), que es el lugar geométrico del primo minimal o aislado $P_1 = (x)$, $X_1 = V(x)$. El lugar geométrico del primo embebido $P_2 = (x, y)$, $X_2 = V(x, y)$ es el origen $(0, 0)$, el cual es un subespacio irreducible embebido en el eje y.

Además, el origen (0,0) es un punto gordo ("*fat point*"): un punto con multiplicidad > 1, que está determinado por un ideal primario que no es primo, cuyo radical es un ideal maximal. En este caso por (x^2, y), o por (x^2, xy, y^2).

Significado geométrico de que la descomposición minimal no sea única

La descomposición primaria minimal de un ideal J puede contener lo que denominamos componente embebidas, es decir, una subvariedad X_2 contenida en otra X_1 de la descomposición, la cual no es visible en $V(J)$. Las otras componentes son las componentes minimales o aisladas. En el Ejemplo 3.10, $X_2 = V(x, y)$ y $X_1 = V(x)$. La correspondiente afirmación algebraica es que el ideal primo $P_2 = (x, y)$ contiene al otro ideal primo $P_1 = (x)$ que aparecen como ideales radicales en la descomposición de J. Así, P_2 es embebido o inmerso y P_1 es minimal o aislado.

La razón intuitiva por la que se produce esta componente embebida es que X_2 tiene una mayor "multiplicidad" en I que X_1 (en un sentido que no podemos precisar aquí). Podemos indicar esto en el dibujo por "punto gordo" ("*fat point*") X_2 sobre una "recta fina" X_1.

Observación 3.11. Los ideales primos minimales o aislados de un ideal J en $K[x_1, \ldots, x_n]$ de la variedad $V(J)$ se corresponden justamente con las subvariedades maximales, es decir, las componentes irreducibles de $V(J)$.

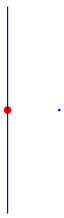
Desde el punto de vista geométrico, los ideales primarios (y lo que es más importante, la descomposición primaria) ofrecen una forma de visualizar, o al menos identificar, las componentes embebidas o inmersas en su variedad. De hecho, desde el punto de vista geométrico, podría ser mejor aceptar temporalmente la definición de un ideal primario como algo extraño, llegar al teorema de la descomposición primaria, y cosechar los beneficios de la intuición geométrica sólo después de analizar la información recabada.

Ejemplo 3.12. La descomposición primaria del ideal $I = (xy, x^3 - x^2, x^2y - xy) \subset K[x, y]$ corresponde a una intersección de tres variedades:

$$I = (xy, x^3 - x^2, x^2y - xy) = (x) \cap (x - 1, y) \cap (x^2, y), \quad \text{con}$$

- $\sqrt{I : (y)} = (x)$, primo minimal.
- $\sqrt{I : (x^2)} = (x - 1, y)$, primo minimal.
- $\sqrt{I : (x^2 - x)} = (x, y)$, primo embebido.

Esta intersección consiste en el eje y, el punto aislado $(1, 0)$, algo no inmediatamente discernible del sistema de ecuaciones, y el punto $(0, 0)$ (variedad "embebida" en el eje y).



Volviendo a los ideales primarios, brevemente: esta nilpotentización es precisamente la idea de dar un extra de desenfoque a este punto $(0,0)$ como una subvariedad embebida en el eje y. Así que, en cierto sentido, no es más que una versión un poco más matizada de la idea de que, digamos, $(x,y)^2$ debería corresponder geométricamente a un punto de multiplicidad 2, donde ahora se puede identificar un punto como un punto repetido aunque $(x,y)^2$ no aparezca en la descomposición primaria de este ideal.

Ejemplo 3.13. Sean los ideales primos $P_1 = (x,y)$ y $P_2 = (x,z)$, y el ideal maximal $M = (x,y,z)$ en el anillo $R = K[x,y,z]$.

Sea el ideal $J = P_1 \cdot P_2 = (x^2, xy, xz, yz)$. Entonces tenemos dos descomposiciones primarias minimales distintas de J:

$$J = P_1 \cap P_2 \cap M^2 = P_1 \cap P_2 \cap (x^2, y, z),$$

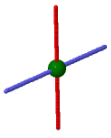
donde $M^2 = (x^2, xy, xz, y^2, yz, z^2)$, con $P_1 = (x,y)$ y $P_2 = (x,z)$ primos minimales y $\sqrt{(x^2,y,z)} = \sqrt{M^2} = (x,y,z)$ primo embebido, con

- $\sqrt{J\colon (z)} = (x,y)$, primo minimal.
- $\sqrt{J\colon (y)} = (x,z)$, primo minimal.
- $\sqrt{J\colon (x)} = (x,y,z)$, primo embebido.

Desde el punto de vista geométrico en $\mathbb{R}^3$, $V(J) = V(P_1) \cup V(P_2) \cup V(M^2)$ sería la unión de las siguientes variedades irreducibles:

- el eje z, $V(P_1)$,
- el eje y, $V(P_2)$,
- el origen $(0,0,0)$, $V(M^2)$,

donde el origen es un punto gordo ("*fat point*"): un punto con multiplicidad > 1, que está determinado por un ideal primario que no es primo, cuyo radical es un ideal maximal.



En el Ejemplo 1.34 vimos anillos de coordenadas de variedades que eran DFU. Ahora probaremos que el anillo de coordenadas de la circunferencia de radio 1 en $\mathbb{R}^2$ no es un DFU.

Ejemplo 3.14 ([5])**.** Sea $R = \mathbb{R}[x,y]/(x^2+y^2-1)$ el anillo de coordenadas de la circunferencia de radio 1, $X = V(x^2+y^2-1) \subset \mathbb{R}^2$. Entonces R no es un DFU.

x^2+y^2-1 es irreducible, ya que si fuera producto de dos polinomios lineales implicaría geométricamente que X sería la unión de dos rectas. Además es primo porque irreducible implica primo en un DFU y $\mathbb{R}[x,y]$ lo es por serlo $\mathbb{R}$. Entonces (x^2+y^2-1) es un ideal primo y en consecuencia $R = \mathbb{R}[x,y]/(x^2+y^2-1)$ es un dominio.

Pero veamos que R no es un DFU. Lo haremos probando que $\bar{x} \in R$ es irreducible pero no primo.

$V(\bar{x})$ será la unión de dos puntos, $a = (0,1)$ y $b = (0,-1)$. En particular, $\bar{x}$ no es 0 en R, si no $V(\bar{x})$ sería todo X, ni unidad en R, si no $V(\bar{x})$ sería el vacío.

• Veamos que $\bar{x}$ no es primo. Esto se puede ver geométricamente, considerando la equivalencia entre ideal primo y variedad irreducible. Como ya hemos visto que $V(\bar{x}) = a \cup b$, está claro que no es un ideal primo. Si lo queremos probar de forma algebraica, se tiene que $\bar{x}$ divide claramente a $\bar{x}^2 = (1+\bar{y})(1-\bar{y})$ en R, pero no a $(1+\bar{y})$ ni a $(1-\bar{y})$, por lo que no sería primo. Y esto lo podemos afirmar porque si $\bar{x}|(1+\bar{y})$ implicaría $1+y = gx+h(x^2+y^2-1)$ para algunos $g,h \in \mathbb{R}[x,y]$ y sustituyendo en el punto a llegaríamos a que $0 = 2$, lo cual es una contradicción.

• Ahora probemos que $\bar{x}$ es irreducible. Supongamos que no fuese así. Entonces tendríamos $\bar{x} = \bar{f}\bar{g}$ para dos no unidades $\bar{f}$ y $\bar{g}$ de R.

Podemos verlo de forma intuitiva. $\bar{x}$ se anula en X exactamente en los dos puntos a y b con multiplicidad 1, lo que significaría que uno de los factores, pongamos $\bar{f}$, se anularía en a con multiplicidad 1, y el otro $\bar{g}$ exactamente en b. Pero esto se correspondería con que la curva $V(f)$ en $\mathbb{R}^2$ cortaría a la circunferencia X en exactamente un punto a con multiplicidad 1 y esto es geométricamente imposible.

Veámoslo de forma formal. Nótese que todo elemento $\bar{h} \in R$ tiene un representante único de la forma $h_0 + xh_1 \in \mathbb{R}[x,y]$ con $h_0, h_1 \in \mathbb{R}[y]$. Definimos una "norma" $N\colon R \to \mathbb{R}[y]$ que lleva $\bar{h} \longmapsto {h_0}^2 + (y^2-1){h_1}^2$. En particular, N es multiplicativa y se tiene

$$N(\bar{x}) = y^2 - 1 = (y+1)(y-1) = N(\bar{f})N(\bar{g}),$$

ya que $\bar{x} \in R$ tiene por representante $0 + x \cdot 1 \in \mathbb{R}[x,y]$. Como $\mathbb{R}[y]$ es un DFU, entonces solo tenemos dos posibilidades (salvo simetría en $\bar{f}$ y $\bar{g}$):

- $N(\bar{f})$ es constante. Entonces $f_0^2 + (y^2-1)f_1^2$ sería constante. Pero los coeficientes principales de f_0^2 y $(y^2-1)f_1^2$ son no negativos y así la suma no se puede cancelar,

y por lo tanto f_0 es constante y $f_1 = 0$. Pero entonces $\bar{f}$ sería una unidad en R, en contra de nuestra suposición.

- $N(\bar{f}) = a(y-1)$ para algún $a \in \mathbb{R} \setminus \{0\}$. Entonces $f_0^2 + (y^2-1)f_1^2 = a(y-1)$ y así $(y-1)|f_0$. Entonces podríamos escribir $f_0 = (y-1)f_0'$ para algún polinomio $f_0' \in \mathbb{R}[y]$ y obtenemos $(y-1)f_0'^2 + (y+1)f_1^2 = a$. Esto es de nuevo una contradicción ya que el lado izquierdo tiene que tener el término principal positivo no constante.

  Así que ninguno de estos casos se puede dar, con lo que concluimos que $\bar{x}$ es irreducible.

3.2. Ejemplos con SageMath

En la última sección de este trabajo exponemos algunos ejemplos usando el software SageMath [11] para hacer cálculos efectivos de la descomposición primaria de un ideal en el anillo de polinomios, y para determinar la descomposición de la variedad correspondiente en sus componentes irreducibles. SageMath utiliza los algoritmos de Shimoyama-Yokoyama ('sy'), por defecto, y de Gianni-Trager-Zacharias ('gtz').

El código de SageMath puede consultarse en el Anexo A de este trabajo.

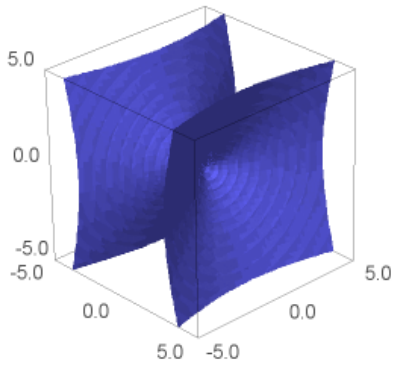
Ejemplo 3.15. Sea el ideal $J = (x^6 - (y^2+z^2)^2) \subset \mathbb{Q}[x,y,z]$. Nótese que este ideal es principal. $x^6 - (y^2+z^2)^2 = (x^3+y^2+z^2)\cdot(x^3-y^2-z^2)$. Su descomposición primaria es (véase A.1):

$$J = (x^6 - (y^2+z^2)^2) = (x^3+y^2+z^2) \cap (x^3-y^2-z^2), \quad \text{con}$$

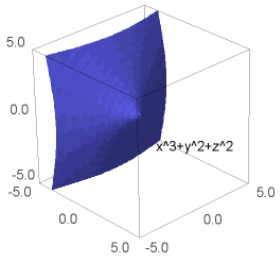
- $\sqrt{J : (x^3-y^2-z^2)} = (x^3+y^2+z^2)$, primo minimal.

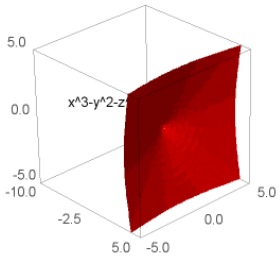
- $\sqrt{J : (x^3+y^2+z^2)} = (x^3-y^2-z^2)$, primo minimal.

La superficie $V(x^6 - (y^2+z^2)^2)$ en $\mathbb{R}^3$



tiene dos componentes irreducibles $V(x^3+y^2+z^2)$ y $V(x^3-y^2-z^2)$.





Ejemplo 3.16. Sea el ideal

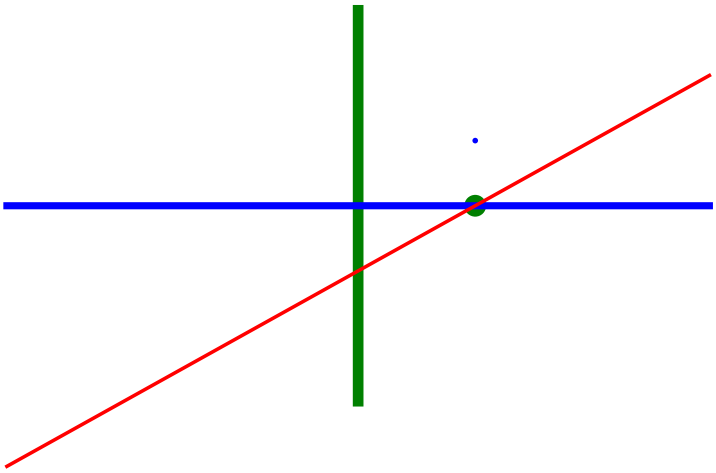
$$J = \left(x^5y^2 - x^4y^3 - 2x^4y^2 + x^3y^3 + x^3y^2, x^4y^4 - x^3y^5 - x^4y^3 + x^3y^3\right) \subset \mathbb{Q}[x,y].$$

Su descomposición primaria es (véase A.2):

$$J = (x-y-1) \cap (y^2) \cap (x^3) \cap (y-1, x-1) \cap (x^2 - 2xy + y^2 - 2x + 2y + 1, y^3), \quad \text{con}$$

- $\sqrt{J : (x^3y^4 - x^3y^3)} = (x - y - 1)$, primo minimal.
- $\sqrt{J : (x^5y - 2x^4y^2 + x^3y^3 - x^5 + x^3y^2 + 2x^4 - x^3y - x^3)} = (y)$, primo minimal.
- $\sqrt{J : (xy^4 - y^5 - xy^3 + y^3)} = (x)$, primo minimal.
- $\sqrt{J : (x^4y^3 - x^3y^4 - x^3y^3)} = (y - 1, x - 1)$, primo minimal (es un ideal maximal).
- $\sqrt{J : (x^4y^3 - x^3y^4 - x^4y^2 + x^3y^2)} = (y, x - 1)$, primo embebido (es un ideal maximal).

Desde el punto de vista geométrico, la variedad $V(J)$ en $\mathbb{R}^2$ es la unión de las rectas $y = x - 1$, $y = 0$ (el eje x) con multiplicidad 2, $x = 0$ (el eje y) con multiplicidad 3, el punto $(1, 1)$ y el punto gordo ("*fat point*") $(1, 0)$ embebido, con multiplicidad 6.



La descomposición minimal de $V(J)$ en variedades irreducibles es:

$$V(J) = V(x - y - 1) \cup V(y) \cup V(x) \cup V(y - 1, x - 1).$$

Ejemplo 3.17. Sea el ideal $J = (y^4 - y^2, xy^3 - xy, x^3y - xy, x^4 - x^2) \subset \mathbb{Q}[x, y]$.

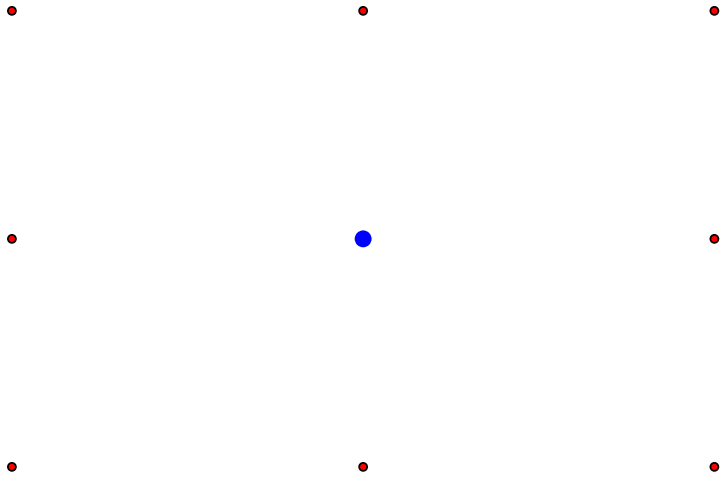
Su descomposición primaria es (véase A.3):

$$\begin{aligned} J = &(y + 1, x + 1) \cap (y + 1, x) \cap (y + 1, x - 1) \cap (y - 1, x + 1) \\ &\cap (y - 1, x) \cap (y - 1, x - 1) \cap (y, x + 1) \cap (y, x - 1) \cap (y^2, xy, x^2). \end{aligned}$$

- $\sqrt{J : (x^2y^2 - x^2y - xy^2 + xy)} = (y+1, x+1)$, primo minimal (es un ideal maximal).
- $\sqrt{J : (x^2y^2 - x^2y + y^3 - y^2)} = (y + 1, x)$, primo minimal (es un ideal maximal).
- $\sqrt{J : (x^2y^2 - x^2y + xy^2 - xy)} = (y+1, x-1)$, primo minimal (es un ideal maximal).
- $\sqrt{J : (x^2y^2 + x^2y - xy^2 - xy)} = (y-1, x+1)$, primo minimal (es un ideal maximal).

- $\sqrt{J : (x^2y^2 + x^2y - y^3 - y^2)} = (y - 1, x)$, primo minimal (es un ideal maximal).
- $\sqrt{J : (x^2y^2 + x^2y + xy^2 + xy)} = (y-1, x-1)$, primo minimal (es un ideal maximal).
- $\sqrt{J : (x^2y^2 + x^3 - xy^2 - x^2)} = (y, x + 1)$, primo minimal (es un ideal maximal).
- $\sqrt{J : (x^2y^2 - x^3 + xy^2 - x^2)} = (y, x - 1)$, primo minimal (es un ideal maximal).
- $\sqrt{J : (y^3 - y)} = (x, y)$, primo minimal (es un ideal maximal).

Desde el punto de vista geométrico, la variedad $V(J)$ en $\mathbb{R}^2$ es la unión de 9 puntos: $(-1,-1)$, $(0,-1)$, $(1,-1)$, $(-1,1)$, $(0,1)$, $(1,1)$, $(-1,0)$, $(1,0)$ y el punto gordo ("*fat point*") $(0,0)$ con multiplicidad 3.



La descomposición minimal de $V(J)$ en variedades irreducibles es:

$$V(J) = V(y+1, x+1) \cup V(y+1, x) \cup V(y+1, x-1) \cup V(y-1, x+1)$$
$$\cup V(y-1, x) \cup V(y-1, x-1) \cup V(y, x+1) \cup V(y, x-1) \cap V(x, y).$$

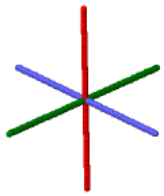
Ejemplo 3.18. Sea el ideal $J = (xy, xz, yz) \subset \mathbb{Q}[x, y, z]$.

Su descomposición primaria es (véase A.4):

$$J = (y, x) \cap (z, x) \cap (y, z), \quad \text{con}$$

- $\sqrt{J : (z)} = (y, x)$, primo minimal.
- $\sqrt{J : (y)} = (z, x)$, primo minimal.
- $\sqrt{J : (x)} = (y, z)$, primo minimal.

Desde el punto de vista geométrico, la variedad $V(J)$ en $\mathbb{R}^3$ es la unión de tres rectas: $y = x = 0$ (eje z), $z = x = 0$ (eje y) y $z = y = 0$ (eje x).



La descomposición minimal de $V(J)$ en variedades irreducibles es:

$$V(J) = V(y, x) \cup V(z, x) \cup V(y, z).$$

Ejemplo 3.19. Sea el ideal

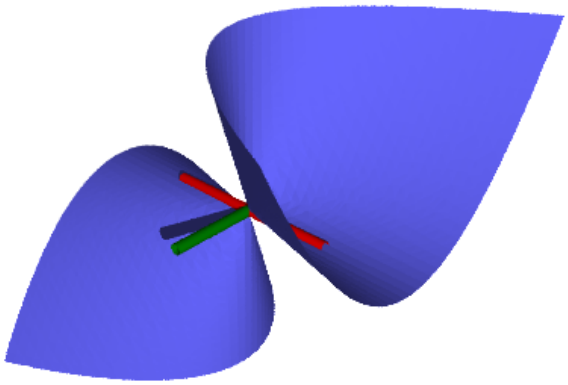
$$J = ((y^2 - xz) \cdot (z^2 - x^2y), (y^2 - xz) \cdot z) \subset \mathbb{Q}[x, y, z].$$

Su descomposición primaria es (véase A.5):

$$J = (y^2 - xz) \cap (x^2, z) \cap (y, z^2), \quad \text{con}$$

- $\sqrt{J : (z^2)} = (y^2 - xz)$, primo minimal.
- $\sqrt{J : (y^3 - xyz)} = (x, z)$, primo minimal.
- $\sqrt{J : (x^2y^2 - x^3z)} = (y, z)$, primo embebido.

Desde el punto de vista geométrico, la variedad $V(J)$ en $\mathbb{R}^3$ es la unión de una superficie $y^2 - xz = 0$, y dos rectas: $x = z = 0$ (eje y, "la recta verde") y $z = y = 0$ (eje x, "la recta roja") que está embebida en la superficie $y^2 - xz = 0$.



La descomposición minimal de $V(J)$ en variedades irreducibles es:

$$V(J) = V(y^2 - xz) \cup V(x, z).$$

Bibliografía

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Series in Mathematics, Westview Press, Boulder, CO, 2016.

[2] S. T. Chapman, F. Gotti, M. Gotti, *How do elements really factor in* $\mathbb{Z}[\sqrt{-5}]$, Advances in commutative algebra, 171–195, Trends Math., Birkhäuser/Springer, Singapore, 2019.

[3] D. A. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, Fourth edition, Undergraduate Texts in Mathematics, Springer, Cham, 2015.

[4] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, GTM 150, Springer-Verlag, New York, 1995.

[5] A. Gathmann, *Commutative Algebra*, `https://www.mathematik.uni-kl.de/~gathmann/class/commalg-2013/commalg-2013.pdf`.

[6] P. Gianni, B. Trager, G. Zacharias, *Gröbner Bases and Primary Decomposition of Polynomial ideals*, J. Symbolic Computation 6 (1988), 149–167.

[7] E. Noether, *Idealtheorie in Ringbereichen*, 1921 (traducido al inglés por D. Berlyne, *Ideal Theory in Rings*, arXiv:1401.2577v1 `https://arxiv.org/abs/1401.2577`, 2014).

[8] R. Y. Sharp, *Steps in Commutative Algebra*, 2nd ed. LMS, Student Texts 51, Cambridge University Press, 2000.

[9] T. Shimoyama, K. Yokoyama, *Localization and Primary Decomposition of Polynomial Ideals*, J. Symbolic Computation 22 (1996), 247–277.

[10] I. Swanson, *Primary decompositions*, `https://www.math.purdue.edu/~iswanso/primdec.pdf`.

[11] The Sage Developers, *SageMath, the Sage Mathematics Software System* (Version 9.2), 2020, `http://www.sagemath.org`.

A. Anexo: Código SageMath

A.1. Ejemplo 3.15

```
R.<x,y,z> = QQ[]
```

```
J=R.ideal(x^6-(y^2+z^2)^2)
```

```
J.primary_decomposition()
```

```
[Ideal (x^3 + y^2 + z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field,
Ideal (x^3 - y^2 - z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field]
```

```
J.primary_decomposition_complete()
```

```
[(Ideal (x^3 + y^2 + z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field,
Ideal (x^3 + y^2 + z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field),
(Ideal (x^3 - y^2 - z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field,
Ideal (x^3 - y^2 - z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field)]
```

```
J.associated_primes()
```

```
[Ideal (x^3 + y^2 + z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field,
Ideal (x^3 - y^2 - z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field]
```

```
J.minimal_associated_primes()
```

```
[Ideal (x^3 - y^2 - z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field,
Ideal (x^3 + y^2 + z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field]
```

```
J.embedded_primes()
```

```
[]
```

```
a1=R.ideal(x^3 - y^2 - z^2)
```

```
(J.quotient(a1)).radical()
```

```
Ideal (x^3 + y^2 + z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field
```

```
a2=R.ideal(x^3 + y^2 + z^2)
```

```
(J.quotient(a2)).radical()
```

```
Ideal (x^3 - y^2 - z^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field
```

A.2. Ejemplo 3.16

```
R.<x,y,z> = QQ[]
```

```
J=R.ideal(x^5*y^2-x^4*y^3-2*x^4*y^2+x^3*y^3+x^3*y^2,          \
   x^4*y^4-x^3*y^5-x^4*y^3+x^3*y^3)
```

```
J.primary_decomposition()
```

```
[Ideal (x - y - 1) of Multivariate Polynomial Ring in x, y, z over Rational
Field, Ideal (y - 1, x - 1) of Multivariate  Polynomial Ring in x, y, z
over Rational Field, Ideal (y^2) of Multivariate Polynomial Ring in x, y, z
over Rational Field, Ideal (x^3) of Multivariate Polynomial Ring in x, y, z
over Rational Field, Ideal (x^2 - 2*x*y + y^2 -2*x + 2*y + 1, y^3) of
Multivariate Polynomial Ring in x, y, z over Rational Field]
```

```
J.associated_primes()
```

```
[Ideal (x - y - 1) of Multivariate Polynomial Ring in x, y, z over Rational
Field, Ideal (y - 1, x - 1) of Multivariate Polynomial Ring in x, y, z over
```

```
Rational Field, Ideal (y) of Multivariate Polynomial Ring in x, y, z over
Rational Field, Ideal (x) of Multivariate Polynomial Ring in x, y, z over
Rational Field, Ideal (y, x - 1) of Multivariate Polynomial Ring in x, y, z
over Rational Field]
```

```
J.minimal_associated_primes()
```

```
[Ideal (x - y - 1) of Multivariate Polynomial Ring in x, y, z over Rational
Field, Ideal (y) of Multivariate Polynomial Ring in x, y, z over Rational
Field, Ideal (y - 1, x - 1) of Multivariate Polynomial Ring in x, y, z
over Rational Field, Ideal (x) of Multivariate Polynomial Ring in x, y, z
over Rational Field]
```

```
J.embedded_primes()
```

```
[Ideal (y, x - 1) of Multivariate Polynomial Ring in x, y, z over Rational
Field]
```

A.3. Ejemplo 3.17

```
R.<x,y,z> = QQ[]
```

```
J=R.ideal(y^4-y^2,x*y^3-x*y,x^3*y-x*y,x^4-x^2)
```

```
J.primary_decomposition()
```

```
[Ideal (y + 1, x + 1) of Multivariate Polynomial Ring in x, y, z over
Rational Field, Ideal (y + 1, x) of Multivariate Polynomial Ring in x,
y, z over Rational Field, Ideal (y+ 1, x - 1) of Multivariate Polynomial
Ring in x, y, z over Rational Field, Ideal (y - 1,x + 1) of Multivariate
Polynomial Ring in x, y, z over Rational Field, Ideal (y - 1, x) of
Multivariate Polynomial Ring in x, y, z over Rational Field, Ideal
(y - 1, x - 1) of Multivariate Polynomial Ring in x, y, z over Rational
Field, Ideal (y, x + 1) of Multivariate Polynomial Ring in x, y, z over
Rational Field, Ideal (y^2, x*y, x^2) of Multivariate Polynomial Ring
in x, y, z over Rational Field, Ideal (y, x - 1) of Multivariate
Polynomial Ring in x, y, z over Rational Field]
```

```
J.associated_primes()
```

```
[Ideal (y + 1, x + 1) of Multivariate Polynomial Ring in x, y, z over
Rational Field, Ideal (y + 1, x) of Multivariate Polynomial Ring in x,
y, z over Rational Field, Ideal (y+ 1, x - 1) of Multivariate Polynomial
Ring in x, y, z over Rational Field, Ideal (y - 1, x + 1) of Multivariate
Polynomial Ring in x, y, z over Rational Field, Ideal (y - 1, x) of
Multivariate Polynomial Ring in x, y, z over Rational Field, Ideal
(y - 1, x - 1) of Multivariate Polynomial Ring in x, y, z over Rational
Field, Ideal (y, x + 1) of Multivariate Polynomial Ring in x, y, z over
Rational Field, Ideal (y, x) of Multivariate Polynomial Ring in x, y, z
over Rational Field, Ideal (y, x - 1) of Multivariate
Polynomial Ring in x, y, z over Rational Field]
```

```
J.minimal_associated_primes()
```

```
[Ideal (y + 1, x + 1) of Multivariate Polynomial Ring in x, y, z over
Rational Field, Ideal (y + 1, x - 1) of Multivariate Polynomial Ring in x,
y, z over Rational Field, Ideal (y + 1, x) of Multivariate Polynomial
Ring in x, y, z over Rational Field, Ideal (y - 1, x+ 1) of Multivariate
Polynomial Ring in x, y, z over Rational Field, Ideal (y - 1, x - 1) of
Multivariate Polynomial Ring in x, y, z over Rational Field, Ideal
(y - 1, x) of Multivariate Polynomial Ring in x, y, z over Rational
Field, Ideal (y, x + 1) of Multivariate Polynomial Ring in x, y, z over
Rational Field, Ideal (y, x - 1) of Multivariate Polynomial Ring in x, y, z
over Rational Field, Ideal (y, x) of  Multivariate
Polynomial Ring in x, y, z over Rational Field]
```

```
J.embedded_primes()
```

```
[]
```

A.4. Ejemplo 3.18

```
R.<x,y,z> = QQ[]
```

```
J=R.ideal(x*y,x*z,y*z)
```

```
J.primary_decomposition()
```

```
[Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over Rational Field]
```

```
J.primary_decomposition_complete()
```

```
[(Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over Rational Field),
(Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over Rational Field),
(Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over Rational Field)]
```

```
J.associated_primes()
```

```
[Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over Rational Field]
```

```
J.minimal_associated_primes()
```

```
[Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over Rational Field]
```

```
J.embedded_primes()
```

```
[]
```

A.5. Ejemplo 3.19

```
R.<x,y,z> = QQ[]
```

```
J=((y^2-x*z)* (z^2-x^2*y),(y^2-x*z)*z)*R
```

```
J.primary_decomposition('gtz')
```

```
[Ideal (-y^2 + x*z) of Multivariate Polynomial Ring
in x, y, z over Rational Field, Ideal (z^2, y) of Multivariate Polynomial
Ring  in x, y, z over Rational Field, Ideal (z, x^2) of
Multivariate Polynomial Ring in x, y, z over Rational Field]
```

```
J.associated_primes()
```

```
[Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (y^2 - x*z) of Multivariate Polynomial Ring in x, y, z over Rational
Field, Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over
Rational Field]
```

```
J.minimal_associated_primes()
```

```
[Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over Rational Field,
Ideal (-y^2 + x*z) of Multivariate Polynomial Ring in x, y, z over Rational
Field]
```

```
J.embedded_primes()
```

```
[Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over Rational Field]
```

```
a1=(z^2)*R
```

```
(J.quotient(a1)).radical()
```

```
Ideal (y^2 - x*z) of Multivariate Polynomial Ring in x, y, z over Rational
Field
```

```
a2=(y^3 - x*y*z)*R
```

```
(J.quotient(a2)).radical()
```

```
Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over Rational Field
```

```
a3=(x^2*y^2 - x^3*z)*R
```

```
(J.quotient(a3)).radical()
```

```
Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over Rational Field
```