Descomposición primaria

Jorge Gil Yuba
Trabajo de fin de grado de Matemáticas
Universidad de Zaragoza

Director del trabajo: Javier Otal Cinca
7 de julio de 2022

Introducción

El origen de la **Descomposición primaria** se encuentra principalmente en *el Teorema fundamental de la Aritmética.*

Este resultado establece que todo número (natural) $n > 1$ se descompone de modo único como el producto de un número finito de números más pequeños que ya no se pueden descomponer, los cuales se llaman *irreducibles* (o *primos*). Dicho de otro modo, se puede escribir de modo único de la forma $n = p_1^{e_1} \cdots p_r^{e_r}$ donde $p_1, \cdots, p_r$ son irreducibles y $e_1, \cdots, e_r \geq 1$. Estas expresiones se pueden trasladar de forma inmediata al anillo $\mathbb{Z}$ de los números enteros, y nos indican que todo número entero $n \neq 0$ se escribe de modo único de la forma $n = \pm p_1^{e_1} \cdots p_r^{e_r}$, los $p_1, \cdots, p_r$ son irreducibles (que excepcionalmente se conviene que puedan no aparecer para abarcar ± 1, las unidades de $\mathbb{Z}$) y $e_1, \cdots, e_r \geq 1$. Lo anterior en términos de ideales de $\mathbb{Z}$ implica

$$\langle n \rangle = \langle p_1^{e_1} \cdots p_r^{e_r} \rangle = \cdots = \langle p_1 \rangle^{e_1} \cap \cdots \cap \langle p_r \rangle^{e_r}. \tag{1}$$

Como todo ideal de $\mathbb{Z}$ es monógeno, deducimos que *todo ideal de $\mathbb{Z}$ es la intersección de un número finito de potencias de ideales primos.*

Más generalmente, un dominio A se dice que es un *dominio de factorización única* si todo elemento $0 \neq a \in A$ se escribe de modo único en una forma análoga $a = up_1^{e_1} \cdots p_r^{e_r}$ donde u es una unidad y se tienen las condiciones del párrafo anterior. Aquí, llamamos irreducible a un elemento que sólo es divisible por sí mismo y por cualquier unidad. Como antes, se tiene que $\langle a \rangle = \langle p_1 \rangle^{e_1} \cap \cdots \cap \langle p_r \rangle^{e_r}$, por lo que *todo ideal monógeno de un dominio de factorización única es la intersección de un número finito de potencias de ideales primos.*

Consideremos ahora el *espacio afín complejo n-dimensional*, $A^n := A^n(\mathbb{C}) = \overbrace{\mathbb{C} \times \cdots \times \mathbb{C}}^{n}$, con $n > 1$. Un subconjunto $V \subseteq A^n$ se dice que es *un conjunto algebraico* si sus puntos son los ceros de un conjunto de polinomios $F \in \mathbb{C}[X_1, \cdots, X_n]$, los cuales coinciden con los del ideal J de $\mathbb{C}[X_1, \cdots, X_n]$ generado por ellos. Se escribe $V = V(J)$. Por *el Teorema de la base de Hilbert* el ideal J está finitamente generado, por lo que los puntos de V son la solución de un sistema con un número finito de ecuaciones polinómicas. Un conjunto algebraico no vacío se dice *reducible* si es unión $V = V_1 \cup V_2$ de dos subconjuntos algebraicos propios y se dice *irreducible* en caso contrario. La irreducibilidad de V se caracteriza en términos de su *ideal de ceros* $I(V)$, que es el conjunto de los polinomios que pasan por los puntos de V. En efecto, V es irreducible si y solo si $I(V)$ es un ideal primo.

Es un resultado de esta teoría que *todo conjunto algebraico se descompone de modo único como una unión finita de conjuntos algebraicos irreducibles*, que son llamadas sus *componentes irreducibles.* Dado un ideal J de $\mathbb{C}[X_1, \cdots, X_n]$ si $V(J) = V_1 \cup \cdots \cup V_R$ es la descomposición de $V(J)$ en componentes irreducibles se tiene que $IV(J) = I(V_1) \cap \cdots \cap I(V_R)$ y cada $I(V_k)$ es un ideal primo. El Teorema de los ceros de Hilbert demuestra que $IV(J)$ es *el radical de J*, luego $IV(J) = J$ para ideales radicales. Así *todo ideal radical es intersección de un número finito de ideales primos.*

En los casos anteriores se observa como ciertos ideales son intersección de potencias de ideales primos. La extensión natural de esto a anillos es lo que se conoce como **Descomposición primaria** y es el tema objeto de este Trabajo Fin de Grado.

Llamamos **Descomposición primaria** de un ideal a una expresión del mismo como intersección de otros, de la forma $I = Q_1 \cap ... \cap Q_n$, donde los Q_i son un tipo concreto de ideales, llamados *primarios*. Este tipo de ideales es una extensión de las potencias de ideales primos, aunque, como veremos más adelante, no toda potencia de un ideal primo es primario, ni todo ideal primario es potencia de algún primo. Volviendo al caso de $\mathbb{Z}$, la descomposición dada en (1) es una descomposición primaria del ideal $\langle n \rangle$.

El primer Capítulo del trabajo supondrá una base de definiciones y resultados sobre la cual trabajaremos en después. Para empezar, definiremos los conceptos de anillo e ideal, que ya hemos utilizado a lo largo de la carrera en varias asignaturas. A partir de ellos, profundizaremos en el estudio del radical de un ideal, que es otro ideal que contiene a los elementos del anillo tales que alguna de sus potencias esté en el ideal original. Además, conoceremos los ideales maximales, primos y primarios, siendo fundamentales estos últimos para el desarrollo del trabajo, y daremos varios ejemplos que facilitarán la comprensión de todo lo anterior.

En el segundo Capítulo, entraremos de lleno en la **Descomposición primaria** de ideales. La primera duda que nos surge al respecto es si dicha descomposición, en caso de existir, es única. Lo cierto es que, a diferencia de $\mathbb{Z}$, donde sí existe unicidad en la descomposición, debida a la unicidad que nos asegura el *Teorema fundamental de la Aritmética*, en el caso general esta descomposición no es única. Sin embargo, existen dos criterios de unicidad que sí podemos probar. Estos criterios reciben el nombre de *Primer* y *Segundo teorema de unicidad*. En el *Primer teorema de unicidad* veremos que, suponiendo que nuestro ideal tenga una descomposición primaria $I = Q_1 \cap ... \cap Q_n$ minimal, concepto que veremos más adelante, entonces los ideales radicales de los Q_i son independientes de la descomposición que tengamos, y los llamaremos *primos asociados*, y en el *Segundo teorema de unicidad* veremos que algunos de los Q_i también son independientes de la descomposición.

Nuestra siguiente duda es si podemos asegurar que todo ideal tiene una descomposición primaria. Resolver esta duda es de lo que se ocupará el Capítulo 3 del trabajo. En primer lugar, estudiaremos un tipo de anillo, llamados *anillos Noetherianos*, en los que *Teorema de Lasker-Noether* nos permitirá asegurarlo. En los anillos que no pertenezcan a este tipo, no podremos hacerlo. Sin embargo, en este caso se pueden encontrar dos condiciones necesarias y suficientes para que todo ideal del anillo sea descomponible.

Una vez estudiado todo esto, nuestro objetivo será dar otra interpretación, en términos de *módulos* al estilo Bourbaki, de la descomposición primaria. Reescribiremos alguno de los teoremas importantes del trabajo, como el *Primer teorema de unicidad*, y lo ilustraremos todo con ejemplos en el anillo de los números enteros $\mathbb{Z}$, para facilitar su comprensión.

Summary

Considering the concepts of ring and ideal studied throughout the degree, a **Primary decomposition** of an ideal I in a ring A is an expression of I as a finite intersection of a specific type of ideals, called *primary ideals*, say $I = Q_1 \cap ... \cap Q_n$. An ideal Q in a ring A is *primary* if $Q \neq A$, in other words, it is a proper ideal, and if $xy \in Q$ implies either $x \in Q$ or $y^n \in Q$ for some $n > 0$.

Primary decomposition has its origin in the factorization of an integer n as a product of prime-powers, as $n = p_1^{e_1}...p_n^{e_n}$, given by the *Fundamental theorem of Arithmetic*, which can be rewritten in term of ideals as follows:

$$\langle n \rangle = \langle p_1^{e_1} \cdots p_r^{e_r} \rangle = \cdots = \langle p_1 \rangle^{e_1} \cap \cdots \cap \langle p_r \rangle^{e_r}.$$

This theorem ensures the uniqueness of that factorization in integers. Therefore, our main goal at this project will be to study the uniqueness in the case of primary descomposition of ideals.

We will start the first Chapter remembering such an important concept as the *radical* of an ideal, which is an ideal containing I and defined as

$$\sqrt{I} := \{a \in A \mid a^n \in I \text{ para algún } n > 0\}.$$

Some properties of the radical of an ideal are studied at this project so as to be used in later demonstrations.

We must remember other definitions from the degree, such as maximal or prime ideals, and the one of primary ideals, in order to prove the following theorem.

Theorem. *i) The ideal M is maximal $\Leftrightarrow$ A/M is a field.*

ii) The ideal P is prime $\Leftrightarrow$ A/P is a domain.

iii) The ideal Q es primary $\Leftrightarrow$ every zedrodivisor of A/M is nilpotent.

For instance, the prime ideals in $\mathbb{Z}$ are $p\mathbb{Z}$ with p prime, and the primary ones are $p^n\mathbb{Z}$ with p prime. Not every primary ideal is prime-power, like in the ring $K[x, y]$, where $\langle x, y^2 \rangle$ is primary, but it is not prime or a prime-power. Moreover, not every prime-power is a primary ideal. This occurs in the ring $K[x, y, z]/I$, with $I = \langle xy - z^2 \rangle$, where $\langle x + I, z + I \rangle$ is prime but not primary.

If Q is a primary ideal, $P = \sqrt{Q}$ is the smallest prime ideal which contains Q, and we say that Q is P-primary.

In the second Chapter, we will dive into the concept of **Primary decomposition**, giving its definition in first place. That decomposition is *minimal* if the $\sqrt{Q_i}$ are distinct and we have $\bigcap_{j \neq i} Q_i \nsubseteq Q_i$, for all i, and an ideal is called *decomposable* if it admits a primary decomposition. Every decomposable ideal admits a minimal primary decomposition.

Furthermore, before giving the next results, we need another notion. If I and J are ideals in a ringk A, their *ideal quotient* is $(I : J) = \{x \in A \mid xJ \subseteq I\}$. Some properties about it will help us in the demonstrations of the rest of the project.

Once we have set all these concepts and properties, we are able to give a *First uniqueness theorem.*

Theorem (First uniqueness theorem). *Let I be a descomposable ideal and $I = \bigcap_{i=1}^{n} Q_i$ a minimal primary decomposition of I. Let $P_i = \sqrt{Q_i}$, $i = 1, ..., n$. Then the P_i are precisely the prime ideals which occur in the set of ideals $\sqrt{(I : x)}$, and hence are independent of the particular decomposition of I.*

As an example, let $A = K[x, y]$ and $I = \langle x^2, xy\rangle$. Then, $I = P_1 \cap P_2^2$, with $P_1 = \langle x\rangle$. P_2^2 is primary and P_2 is prime. Thus P_1 and P_2 are the prime ideals referred to in the theorem.

The ideals of the theorem are said to *belong* to I, or to be *associated* with I, and the minimal elements of the set $\{P_1, ..., P_n\}$ are called *minimal* or *isolated* primes. The others are called *embedded* prime ideals.

The next step is to talk about *rings of fractions.* If S is a multiplicatively closed set, we consider the set of the pairs

$$A \times S = \{(a, s) \mid a \in A, s \in S\}.$$

and the equivalence relation given by $(a, b) \equiv (c, d)$ if and only if $(at - bs)u = 0$ for any $u \in S$. We denote by $\frac{a}{s}$ the equivalence class of (a, s), and define sum and product as

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

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

They are well defined and satisfy the ring properties, and the equivalence classes with them form the *ring of fractions*, denoted by $A[S^{-1}]$. Its ideals are $IA[S^{-1}] := \{\frac{a}{s} \mid a \in A, s \in S\}$, where I is an ideal of A. Thanks to them and the following definition, we can prove several results in order to reach the *Second uniqueness theorem.*

A set $\mathcal{P}$ of prime ideals primos belonging to I is called *isolated* if verifies:

$$\text{If } P \in \mathcal{P} \text{ and } P' \subseteq P, \text{ then } P' \in \mathcal{P}.$$

Theorem (Second uniqueness theorem). *Let I be a descomposable ideal, with $I = \bigcap_{i=1}^{n} Q_i$ a minimal primary decomposition, and let $\{P_{i_1}, ..., P_{i_m}\}$ be an isolated set of prime ideals belonging to I. Then $Q_{i_1} \cap ... \cap Q_{i_m}$ is independent of the decomposition.*

Now that we have acomplished our main goal thanks to the two uniqueness theorems, we wonder something else. We want to know whether we can ensure that every ideal has a primary decomposition. We study a type of ring called *Noetherian rings*, where every ideal is finitely generated. We give the following definition: let $B \subseteq A$, the *annihilator* of B is $Ann(B) = \{a \in A \mid ab = 0 \text{ for all } b \in B\}$.

We also give some properties about them, such as that every ideal in them is an intersection of irreducible ideals, or that the irreducible ideals in these rings are primary. They leads us to the following theorem.

Theorem (Lasker-Noether theorem). *In a Noetherian ring A, every ideal has a primary decomposition.*

That fact has aplications in other branches of mathematics, such as arithmetic and geometry.

In arithmetic, in a field K, an *algebraic integer* is an element $x \in K$ which is root of a unique monic and irreducible polynomian. They compose a Noetherian ring which contains $\mathbb{Z}$, so their ideals are decomposable.

Moreover, the rings in Algebraic Geometry are Noetherian, so all of their ideals are decomposable, and that gives an explicit proof that an affine algebraic set is decomposable, in the sense that it is a finite union of irreducible algebraic sets.

But, what happens if the ring we have is not Noetherian? In this case we have found the two following conditions, that together are equivalent to that every ideal is decomposable.

Condition 1: For any proper ideal I in A and every prime ideal P, there exists $x \notin P$ such that $S_P(I) = (I : x)$, where $S_P = A \setminus P$.

Condition 2: Let I be an ideal in A. Given a descending chain $S_1 \supseteq ... \supseteq S_n \supseteq ...$ of multiplicatively closed subsets of A, there exists an integer n such that $S_n(I) = S_{n+1}(I) = ...$

Once we have studied all of the previus issues, it would be interesting to give another point of view of the concept of **Primary decomposition**. We will do it in terms of Bourbaki style modules. Let A be a ring, an A-module is an abelian group M where A acts linearly, i.e., that satisfie the following axioms:

$$a(x + y) = ax + ay$$

$$(a + b)x = ax + bx$$

$$(ab)x = a(bx)$$

$$1x = x$$

for all $a, b \in A$, $x, y \in M$.

For instance, we must see the factors of $n = \pm p_1^{e_1} \cdots p_r^{e_r}$ in $\mathbb{Z}$ as zero divisors of $M = \mathbb{Z}/\langle n \rangle$, which we will see as a $\mathbb{Z}$-module.

We will study the notion of *associated prime* of a module M, which are the ideal primes P of M such that M contains a submodule isomorphic to A/P. The set of the associated primes of M is denoted by $Ass(M)$, and satisfies the following proposition:

Proposition. *Consider the set of ideals of A of the form $\{Ann(x) \mid 0 \neq x \in M\}$. Every maximal element of this set is an associated prime.*

This proposition, together with other several results about modules, give us another interpretation of the *First uniqueness theorem.*

Theorem (First uniqueness theorem)**.** *Let A be a Noetherian ring, I an ideal of A and $I = \bigcap_{i=1}^{k} Q_i$ a minimal primary decomposition of I, where Q_i is P_i-primary. Then*

$$Ass(A/I) = \{P_1, ..., P_k\}$$

and in particular, the set of primes $\{P_1, ..., P_k\}$ is uniquely determinated by I.

Índice general

Capítulo 1

Ideales primarios

Recordemos que un *anillo, $(A,+,\cdot)$* es una estructura formada por un conjunto A con dos operaciones internas, *suma* $(+)$ y *producto* $(\cdot)$, donde *$(A,+)$* es un grupo abeliano y el producto es asociativo y verifica la propiedad distributiva respecto de la suma. De aquí en adelante con la palabra anillo nos referiremos a un anillo conmutativo con identidad. Un *cuerpo* es un anillo en el que todos sus elementos son *unidades*, es decir, $\forall a \in A \ \exists \ b \in A$ tal que $ab = 1$, identidad distinta del 0 de la suma. A b se le llama *inverso* de a y se denota a^{-1}. Un subconjunto S de A se dice *subanillo* de A si es cerrado para la suma y el producto, y contiene al elemento neutro de A.

Dados dos anillos A y B, un *homomorfismo de anillos* $f : A \to B$ es una aplicación que conserva las dos operaciones y tal que $f(1_A) = 1_B$. Si $f : A \to B$ y $g : B \to C$ son homomorfismos de anillos, entonces $g \circ f : A \to C$ también lo es. Si f es biyectiva, se le llama *isomorfismo.*

En lo que sigue, daremos por supuestos los resultados que se han estudiado en las materias del grado.

1.1. El radical de un ideal

El concepto central de este trabajo es el de ideal. Un *ideal* $I \trianglelefteq A$ es un subconjunto de A cerrado para la suma y para el producto con elementos de A, es decir, que si $b, c \in I$, $a \in A$, entonces $b + c, ab \in I$. I se dice *propio* si $I \neq 0, A$. La *intersección* de una familia de ideales de A es un ideal de A. Definimos el ideal *suma* de dos ideales como:

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

y el ideal producto como:

$$IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}.$$

Si $I \trianglelefteq A$, se define el *anillo cociente* A/I de A por I como el anillo dado por el conjunto de las clases de equivalencia respecto de la relación dada por $a \sim b \Leftrightarrow b - a \in I$. Sus elementos se denotan por $a + I$, con

$$a + I = \{a + b \mid a \in A, b \in I\}.$$

Los ideales de dicho anillo son de la forma $J/I = \{a + I \mid a \in J\}$, para un cierto $J \trianglelefteq A$ con $I \subseteq J$.

En este trabajo el siguiente concepto es fundamental, por lo que lo recordamos en detalle. Sea $I \trianglelefteq A$ ideal de A. El *radical* de I es

$$\sqrt{I} := \{a \in A \mid a^n \in I \text{ para algún } n > 0\}.$$

A continuación veremos una serie de propiedades del radical de un ideal.

Proposición 1.1. El radical $\sqrt{I}$ de I es un ideal que contiene a I.

Demostración. [5][Comentario tras la definición 1.2.3]. $\square$

Proposición 1.2. Sea A un anillo e I, J ideales de A.

i) $\sqrt{I} = A$ si y solo si $I = A$.

ii) Si $I \subseteq J$, entonces $\sqrt{I} \subseteq \sqrt{J}$.

iii) $\sqrt{I} = \sqrt{\sqrt{I}}$.

iv) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

v) $\sqrt{I^m} = \sqrt{I}$.

vi) Si $I \subseteq J$, entonces $\sqrt{J/I} = \sqrt{J}/I$.

Demostración. [5][Lema 1.2.1]. $\square$

Llamamos *nilradical* al radical de $\langle 0 \rangle$ y lo denotaremos $\mathcal{N}(A)$. A sus elementos se les dice *nilpotentes*. Un elemento $a \in A$ es un *divisor de cero* si $\exists\, b \neq 0 \in A$ tal que $ab = 0$. Un anillo sin divisores de cero se llama *dominio*. En particular, todo elemento de $\mathcal{N}(A)$ es un divisor de cero.

1.2. Ideales maximales, primos, primarios y ejemplos

Un ideal propio M de A se dice *maximal* (entre los ideales propios) si no existe ningún otro ideal I tal que $M \subset I \subset A$. Un ideal propio P de A se dice *primo* si $a, b \in P \Rightarrow a \in P$ o $b \in P$. Todo ideal maximal es primo. Un ideal propio Q de A se dice *primario* si $a, b \in P \Rightarrow a \in P$ o $b^n \in P$ para algún $n > 0$.

Teorema 1.3. *Todo anillo A posee elementos maximales. Además,*

i) El ideal M es maximal $\Leftrightarrow$ A/M es un cuerpo.

ii) El ideal P es primo $\Leftrightarrow$ A/P es un dominio.

iii) El ideal Q es primario $\Leftrightarrow$ todo divisor de cero de A/Q es nilpotente.

Demostración. *i)* y *ii)* [7][Teorema 1.2.4].
iii) Sea Q un ideal primario de A y $a = x + Q \neq Q$ un divisor de cero de A/Q, entonces $\exists$ $b = y + Q \neq Q \in A/Q$ tal que $ab = xy + Q = Q$, por tanto $xy \in Q$. Como Q es primario y $b = y + Q \neq Q$, es decir, $y \notin Q$, $\exists\, n > 0$ tal que $x^n \in Q$, luego $a^n = x^n + Q = Q$, y por tanto a es un nilpotente. Recíprocamente, si $xy \in Q$, $x \notin Q$, y $xy + Q = Q$ implica que $y + Q$ es nilpotente, entonces $y^n + Q = Q$, por lo que $y^n \in Q$. $\square$

Ejemplo 1.4.

1) Los ideales primos de $\mathbb{Z}$ son $p\mathbb{Z}$, con p primo, que son justamente los maximales. Además, los ideales primarios de $\mathbb{Z}$ son los $p^n\mathbb{Z}$, con p primo.

2) Sea nuestro anillo $K[x, y]$, con K cuerpo y tomamos $M = \langle x, y \rangle$, entonces $K[x, y]/M \cong K$, que es un cuerpo, luego M es maximal. Ahora, tomar $P = \langle x \rangle$, no es maximal porque $P \subset M$, pero $K[x, y]/M \cong K[y]$, que es un dominio, luego P es primo. Sin embargo, $Q = \langle x, y^2 \rangle$ no es primo ni potencia de primo, ya que y es divisor de cero de $K[x, y]/Q$, pero los divisores de cero de $K[x, y]/Q$ son los múltiplos de y, que son nilpotentes, por tanto sí que es primario.

3) No toda potencia de primo es un ideal primario. Tomamos $A = K[x, y, z]$, con K cuerpo, e $I = \langle xy - z^2 \rangle$. Sea $B = A/I$, y $P = \langle x + I, z + I \rangle$. Entonces P es primo, ya que se puede comprobar que B/P es un dominio. Notar que

$$(x + I)(y + I) = xy + I = xy - (xy - z^2) + I = z^2 + I \in P^2.$$

Además,

$$P^2 = \langle x^2 + I, xz + I, z^2 + I \rangle.$$

Si fuese primario, entonces x ó $y^k \in P^2$ para algún $k > 0$, algo que no se cumple, por tanto P no es primario.

Teorema 1.5. *Sea A un anillo e $I \trianglelefteq A$ un ideal. Entonces existe un ideal maximal $M \trianglelefteq A$ tal que $I \subseteq A$*

Demostración. [5][Teorema 1.1.2]. □

Corolario 1.6. Todo elemento no unidad de A está contenido en un ideal maximal.

Proposición 1.7. El radical de un ideal I es la intersección de todos los ideales primos que contienen a I.

Demostración. [5][Teorema 1.2.4]. □

Como consecuencia de esta proposición se deduce que $\mathcal{N}(A)$ es la intersección de todos los ideales primos de A.

Proposición 1.8. Sea Q ideal primario de un ideal A. Entonces $\sqrt{Q}$ es el ideal primo más pequeño que contiene a Q.

Demostración. Por 1.7 basta probar que $\sqrt{Q}$ es primo. Supongamos que $xy \in \sqrt{Q}$, entonces $(xy)^m \in Q$ para algún $m > 0$, por lo que x^m ó $y^{mn} \in Q$ para algún $n > 0$, luego, o bien $x \in \sqrt{Q}$, o bien $y \in \sqrt{Q}$. □

Si $P = \sqrt{Q}$, entonces Q se llama $P-$*primario.*

Proposición 1.9. Si $\sqrt{Q}$ es maximal, entonces Q es primario. En particular, las potencias de un ideal maximal M son $M-$primarios.

Demostración. Sea $M = \sqrt{Q}$, con M maximal, entonces la imagen de M en A/Q es el nilradical de A/Q, que es la intersección de todos los ideales primos, y por tanto uno de ellos, luego todos los demás primos lo contienen. Como M es maximal, el nilradical es el único ideal primo de A/Q. Por tanto, todo elemento de A/Q es unidad o nilpotente, luego todo divisor de cero de A/Q es nilpotente. □

Observación. El ejemplo 3 de 1.4 prueba que el resultado anterior es el mejor que podemos dar.

La siguiente proposición será útil en lo que sigue.

Proposición 1.10. Sean $I_1, ..., I_n$ ideales y P ideal primo conteniendo $\bigcap_{i=1}^n I_i$. Entonces $P \supseteq I_i$ para algún i. Si $P = \bigcap_{i=1}^n I_i$, entonces $P = I_i$ para algún i.

Demostración. Supongamos que $P \nsubseteq I_i$ para todo i. Entonces $\exists\, x_i \in I_i$, $x_i \in P$, $i = 1, ..., n$, por lo que $\prod x_i \in \prod I_i \subseteq \bigcap I_i$, pero $\prod x_i \notin P$ por ser P primo. Por tanto $P \nsupseteq \bigcap I_i$. Si $P = \bigcap I_i$, entonces $P \subseteq I_i$, y por tanto $P = I_i$ para algún i. □

Capítulo 2

Descomposición primaria

2.1. Definiciones

La descomposición primaria es el centro y el motivo de este trabajo. Para poder hablar de ella, primero hemos de definir el concepto y conocer algunas de sus propiedades. Una *descomposición primaria* de un ideal I en un anillo A es una expresión de I como intersección finita de ideales primarios, de la forma

$$I = \bigcap_{i=1}^{n} Q_i.$$

Si además se cumple que los $\sqrt{Q_i}$ son distintos entre sí y que $\bigcap\limits_{j \neq i} Q_i \nsubseteq Q_i$, $\forall i$, a la descomposición se le dice *minimal*. En el caso de que I admita una descomposición primaria, se le llama ideal *descomponible*. Es importante tener en cuenta que en general no todo ideal admitirá una descomposición primaria, por ello estudiar cúando ésto sí sucede será otro de los objetivos del trabajo.

A continuación, veremos que todo ideal I descomponible tendrá una descomposición primaria mínimal.

Lema 2.1. *Sea I un ideal descomponible, con una descomposición primaria $I = \bigcap\limits_{i=1}^{n} Q_i$. Si los ideales Q_i son P-primarios, $i = 1, ..., n$, entonces $Q = \bigcap_{i=1}^{n} Q_i$ es P-primario.*

Demostración. Por 1.2.*iv*), $\sqrt{Q} = \bigcap_{i=1}^{n} \sqrt{Q_i} = P$. Basta ver que Q es primario. Sea $xy \in Q$, $x \notin Q$, entonces $xy \in Q_i$, $x \notin Q_i$, para algún i, luego $y^n \in Q_i$ para un $n > 0 \Rightarrow y \in P$, y como $\sqrt{Q} = P$, $\exists m > 0$ tal que $y^m \in Q$. □

Teorema 2.2. *Sea $I \trianglelefteq A$, si I es descomponible, entonces tiene una descomposición primaria minimal.*

Demostración. Supongamos que $I = \bigcap_{i=1}^{n} Q_i$. Sean $P_1, ..., P_s$ los radicales distintos en el conjunto $\{\sqrt{Q_1}, ..., \sqrt{Q_n}\}$. Tomando Q'_i la intersección de los ideales P_i-primarios en la descomposición, por 2.1, Q'_i es P_i-primario y se tiene $I = \bigcap_{i=1}^{s} Q'_i$, cumpliéndose la primera parte de la definición. Si algún Q'_i contiene a $\bigcap_{j \neq i} Q'_i$, $I = \bigcap_{j \neq i} Q'_j$ también es una descomposición primaria de I. Así podemos eliminar algunos Q'_j hasta obtener $I = \bigcap_{j=1}^{k} Q'_j$ y cumplir la segunda parte de la definición. □

Para introducir el *Primer teorema de unicidad*, hemos de definir un concepto que utilizaremos en varias ocasiones a lo largo de la siguiente sección, y que nos será útil para probar una serie de resultados necesarios para poder probar el teorema. Sean I, J ideales del mismo anillo A, entonces definimos

$$(I : J) := \{x \in A \mid xJ \subseteq I\}.$$

El concepto anterior será de gran ayuda en las demostraciones que siguen, especialmente si tomamos como el J de la definición el ideal generado por un elemento $x \in A$. Ahora, veremos que estos conjuntos que hemos definido son ideales y analizaremos alguna de las propiedades que cumplen.

Proposición 2.3. Sea I un ideal de A. Entonces $J = (I : x)$ es un ideal de A.

Demostración. $0x = 0 \in I$ luego $0 \in J$. Sean $a, b \in J$, $t \in A$, entonces $bx, ax, tax \in I$, luego

$$bx - ax = (b - a)x \in I,$$

por tanto $b - a, ta \in J$. □

Lema 2.4. *Sea Q ideal P-primario de un anillo A y $x \in A$. Entonces:*

i) Si $x \in Q$, entonces $(Q : x) = A$.

ii) Si $x \notin Q$, entonces $(Q : x)$ es P-primario.

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

Demostración. *i*) Inmediato de la definición.

ii) Claramente $Q \subseteq (Q : x)$. Si $y \in (Q : x)$, $xy \in Q$. Como $x \notin Q$ y Q primario, $y^n \in Q$, para algún $n > 0$, luego $Q \subseteq (Q : x) \subseteq P$, y por tanto

$$P = \sqrt{Q} \subseteq \sqrt{(Q : x)} \subseteq \sqrt{P} = P.$$

Basta ver que Q es primario. Sea $yz \in (Q : x)$, $y \notin (Q : x)$, entonces $yzx \in Q$, y como $x, y \notin Q$, $xy \notin Q$, luego $z^n \in Q \subseteq (Q : x)$.

iii) $Q \subseteq (Q : x)$. Si $y \in (Q : x)$, $xy \in Q$, como $x \notin P$, entonces $x^n \notin Q$ para ningún $n > 0$, luego $y \in Q$. □

Lema 2.5. *Sean I_k y J ideales de un anillo A, entonces $(\bigcap_{k=1}^n I_k : J) = \bigcap_{k=1}^n (I_k : J)$.*

Demostración. $x \in (\bigcap_{k=1}^n I_k : J)$ si y solo si

$$xJ \subseteq \bigcap_{k=1}^{n} I_k \Leftrightarrow xJ \subseteq I_k, \forall k \Leftrightarrow x \in (I_k : J), \forall k \Leftrightarrow x \in \bigcap_{k=1}^{n} (I_k : J).$$

□

2.2. Primer teorema de unicidad

Una vez asentadas todas las propiedades de la sección anterior, ya nos encontramos en condiciones de dar una prueba para el *Primer teorema de unicidad.* Además, en esta sección daremos un ejemplo relacionado con este teorema y una serie de definiciones que nos ayudarán en el resto del trabajo.

Teorema 2.6 (Primer teorema de unicidad)**.** *Sea I ideal descomponible e $I = \bigcap_{i=1}^{n} Q_i$ descomposición primaria minimal de I. Sean $P_i = \sqrt{Q_i}$, $i = 1, ..., n$. Entonces los P_i son precisamente los ideales primos que aparecen en el conjunto de ideales $\sqrt{(I : x)}$, y por lo tanto son independientes de la descomposición particular de I.*

Demostración. Para cada $x \in A$,

$$(I : x) = (\bigcap_{i=1}^{n} Q_i : x) = \bigcap_{i=1}^{n} (Q_i : x),$$

por 2.5, y por tanto,

$$\bigcap_{i=1}^{n} \sqrt{(Q_i : x)} = \bigcap_{j : x \notin Q_j} P_j,$$

por 2.4.*ii*). Suponer que $\sqrt{(I : x)}$ es primo, entonces por 1.10 $\sqrt{(I : x)} = P_j$ para algún j. Por tanto, todo ideal primo de la forma $\sqrt{(I : x)}$ es uno de los P_j. Recíprocamente, para cada i, existe un $x_i \notin Q_i$ tal que $x_i \in \bigcap_{j \neq i} Q_i$, ya que la descomposición es minimal, y por lo tanto $\sqrt{(I : x_i)} = P_i$. □

Observación. De la última parte de la demostración anterior y 2.4.*ii*) se sigue que para cada i, existe $x_i \in A$ tal que $(I : x_i)$ es P_i-primario.

Ejemplo 2.7. Sea $I = \langle x^2, xy \rangle$ en $A = K[x, y]$. Entonces $I = P_1 \cap P_2^2$, con $P_1 = \langle x \rangle$, $P_2 = \langle x, y \rangle$. P_2^2 es primario por 1.9 por ser P_2 maximal. Por tanto, los ideales primos del teorema son P_1 y P_2. Además, $P_1 \subset P_2$, luego $\sqrt{I} = P_1 \cap P_2 = P_1$, pero I no es un ideal primario.

Los ideales primos P_i del teorema se dice que *pertenecen* a I, o que son *asociados* de I. Además, I es primario si y solo si tiene un solo primo asociado. Los elementos minimales de $\{P_1, ..., P_n\}$ se llaman primos *minimales* o *aislados* pertenecientes a I. El resto se llaman primos *inmersos*, como $P_2 = \langle x, y \rangle$ en el ejemplo anterior.

2.3. Anillos de fracciones

En esta sección construiremos unos anillos que generalizarán la noción de cuerpo de fracciones. Para ello hemos de definir el siguiente concepto. Sea A un anillo y $S \subseteq A$ un subconjunto, S es un *sistema multiplicativo* si S no contiene al cero, $1 \in S$ y dados $a, b \in S$, entonces $ab \in S$. Por ejemplo, si A es un dominio, $A \setminus \{0\}$ es un sistema multiplicativo.

La idea original es construir un anillo que contenga a A, en el que los elementos de S tengan inverso. Consideramos el conjunto de los pares

$$A \times S = \{(a, s) \mid a \in A, s \in S\}.$$

Y en él definimos la relación de equivalencia entre los pares dada por

$$(a, s) \equiv (b, t) \text{ si y solo si } (at - bs)u = 0, \text{ para algún } u \in S.$$

Se denota por $\frac{a}{s}$ a la clase de equivalencia de un par (a, s), y por $A\left[S^{-1}\right]$ al conjunto de las clases, definiendo la suma y el producto como sigue:

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

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Se puede comprobar fácilmente que las operaciones anteriores están bien definidas y satisfacen la definición de anillo con identidad. Además, existe un homomorfismo

$$f : A \to A\left[S^{-1}\right], \text{ dada por } f(x) = \frac{x}{1}, \tag{2.1}$$

que en general no es inyectivo.

Al anillo $A\left[S^{-1}\right]$ se le conoce como *anillo de fracciones* de A respecto S. Además, él y el homomorfismo cumplen las siguientes propiedades:

i) Si $s \in S$, $f(s) = \frac{s}{1}$ es una unidad de $A \to A\left[S^{-1}\right]$, cuyo inverso, $\frac{1}{s}$ denotamos por s^{-1}.

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

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

Además, todo anillo de fracciones cumple una propiedad universal:

Proposición 2.8. Sea $g : A \to B$ un homomorfismo de anillos tal que $g(s)$ es una unidad de B para todo $s \in S$. Entonces existe un único homomorfismo de anillos $h : A\left[S^{-1}\right] \to B$ tal que $g = h \circ f$.

Demostración. i) *Unicidad.* Si h satisface las condiciones, $h(\frac{a}{1}) = ff(a) = g(a)$ para todo $a \in A$, y por tanto, si $s \in S$,

$$h(\frac{1}{s}) = h((\frac{s}{1})^{-1}) = h(\frac{s}{1})^{-1} = g(s),$$

luego

$$h(\frac{a}{s}) = h(\frac{a}{1})h(\frac{1}{s}) = g(a)g(s)^{-1},$$

por lo que h está únicamente determinadad por g.

ii) *Existencia.* Sea $h(\frac{a}{s}) = g(a)g(s)^{-1}$. Entonces h es un homomorfiso de anillos bien definido. Supongamos que $\frac{a}{s} = \frac{a'}{s'}$, entonces $\exists u \in S$ tal que $(as' - a's)u = 0$, por lo que

$$(g(a)g(s') - g(a')g(s))g(u) = 0,$$

y como $g(u)$ es una unidad en B,

$$g(a)g(s)^{-1} = g(a')g(s')^{-1}.$$

□

A continuación, analizaremos cómo son los ideales de un anillo de fracciones a partir de los ideales del anillo original. Para ello, hemos de conocer la siguiente notación: dado un anillo A con un sistema multiplicativo $S \subseteq A$ y un ideal $I \trianglelefteq A$, escribiremos

$$IA\left[S^{-1}\right] := \{\frac{a}{s} \mid a \in I, s \in S\}.$$

Proposición 2.9. Sea A un anillo y $S \subseteq A$ un sistema multiplicativo. Dado $I \trianglelefteq A$, $IA\left[S^{-1}\right]$ es precisamente el ideal de $A\left[S^{-1}\right]$ generado por I.

Demostración. Sean $a, b \in I$, $c \in A$, y $s, t \in S$, entonces

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{ca}{s} \in IA\left[S^{-1}\right],$$

por lo que $IA\left[S^{-1}\right]$ es un ideal de $A\left[S^{-1}\right]$. Además, como

$$\frac{a}{s} = \frac{1}{s} \cdot \frac{a}{1},$$

se deduce que $I \trianglelefteq A$ es el ideal generado por I. □

2.4. Segundo teorema de unicidad

Para poder demostrar el segundo teorema de unicidad, hemos de probar varios resultados previos que harán que su demostración sea casi inmediata.

Proposición 2.10. Sea I un ideal descomponible. Entonces para cada ideal primo $P \supseteq I$ existe un ideal primo minimal tal que $P \supseteq Q \supseteq I$. Además los ideales primos minimales sobre I son exactamente los elementos minimales del conjunto de ideales primos asociados a I.

Demostración. Si $P \supseteq I = \bigcap_{i=1}^{n} Q_i$, entonces

$$P = \sqrt{P} \supseteq \bigcap_{i=1}^{n} \sqrt{Q_i} = \bigcap_{i=1}^{n} P_i$$

Por 1.10, se tiene que $P \supseteq P_i$ para algún i, por lo que P contiene un ideal primo minimal sobre I. □

Proposición 2.11. Sea I un ideal descomponible con una descomposición primaria minimal $I = \bigcap_{i=1}^{n} Q_i$, y sean $P_i = \sqrt{Q_i}$. Entonces

$$\bigcup_{i=1}^{n} P_i = \{x \in A \mid (I : x) \neq I\}.$$

En particular, si 0 es un ideal descomponible, el conjunto D de divisores de cero de A es la unión de los ideales primos asociados a 0.

Demostración. Podemos considerar $I = 0$, pasando al anillo cociente A/I. Basta probar que D es la unión de los ideales primos asociados a 0. Se tiene que

$$D \subseteq \bigcup_{i=1}^{n} P_i,$$

ya que $D = \bigcap_{x \neq 0} \sqrt{(0 : x)}$, y por la prueba de 2.6,

$$\sqrt{(0 : x)} = \bigcap_{x \notin Q_j} P_j \subseteq P_j,$$

para algún j. También por 2.6, cada P_i es de la forma $\sqrt{(0 : x)}$ para algún $x \in A$, por tanto $\bigcap P_i \subseteq D$. □

De esta proposición se deduce que si el ideal cero es descomponible, entonces el conjunto de divisores de cero del anillo es la unión de los ideales primos pertenecientes a 0, y el conjunto de elementos nilpotentes del anillo es la intersección de los ideales primos minimales pertenecientes a 0.

Proposición 2.12. Sea S un sistema multipicativo de A, y Q un ideal P-primario de A. Entonces:

i) Si $S \cap P \neq \emptyset$, $Q\left[S^{-1}\right] = A\left[S^{-1}\right]$

ii) Si $S \cap P = \emptyset$, $Q\left[S^{-1}\right]$ es $P\left[S^{-1}\right]$-primario y su contracción en A es Q.

Por tanto, hay una correspondencia biyectiva entre ideales primarios de $A\left[S^{-1}\right]$ y los ideales primarios que no cortan a S.

Demostración. i) Si $s \in S \cap P$, $s^n \in S \cap Q$ para algún $n > 0$, por lo que $\frac{s^n}{1} \in Q\left[S^{-1}\right]$, que es una unidad de $A\left[S^{-1}\right]$.

ii) Si $S \cap P = \emptyset$ y $(\frac{a}{1})(\frac{b}{1}) \in Q\left[S^{-1}\right]$, con $\frac{a}{1} \notin Q$, existe $s \in S$ tal que $abs \in Q$ y $as \notin Q$. Luego existe $n > 0$ tal que $b^n \in Q$, por lo que $\frac{b^n}{1} \in Q\left[S^{-1}\right]$. Por otro lado,

$$\sqrt{Q\left[S^{-1}\right]} = \sqrt{Q}\left[S^{-1}\right] = P\left[S^{-1}\right].$$

□

Para cada ideal I de un anillo A y cada sistema multiplicativo S, definimos la *contracción* en A del ideal $IA\left[S^{-1}\right]$, denotada por $S(I)$, como:

$$S(I) = \{a \in A \mid \frac{a}{1} \in IA\left[S^{-1}\right]\}.$$

Además, claramente se tiene que $S(I) = f^{-1}(IA\left[S^{-1}\right])$, siendo f el homomorfismo descrito en la definición de anillos de fracciones, en 2.1. Ahora, veremos una propiedad de la contracciones de los ideales.

Proposición 2.13. Sean S un sistema multiplicativo de A e I un ideal descomponible con $I = \bigcap_{i=1}^n Q_i$ una descomposición primaria minimal de I y $P_i = \sqrt{Q_i}$. Supongamos que $S \cap P_j = \emptyset$ para $j = 1, ..., m$ y que $S \cap P_j \neq \emptyset$ para $j = m+1, ..., n$. Entonces:

$$IA\left[S^{-1}\right] = \bigcap_{i=1}^{m} Q_i A\left[S^{-1}\right],$$

$$S(I) = \bigcap_{i=1}^{m} Q_i$$

son descomposiciones minimales.

Demostración. Por 2.12,

$$IA\left[S^{-1}\right] = \bigcap_{i=1}^{n} Q_i A\left[S^{-1}\right] = \bigcap_{i=1}^{m} Q_i A\left[S^{-1}\right],$$

y $Q_i A\left[S^{-1}\right]$ es $P_i A\left[S^{-1}\right]$-primario para $i = 1, ..., m$. Como los P_i son distintos, lo son los $P_i A\left[S^{-1}\right]$ $(i = 1, ..., m)$, por tanto la desposición primaria es minimal. Además,

$$S(I) = f^{-1}(IA\left[S^{-1}\right]) = \bigcap_{i=1}^{m} f^{-1}(Q_i A\left[S^{-1}\right]) = \bigcap_{i=1}^{m} Q_i,$$

por 2.12. □

Un conjunto $\mathcal{P}$ de ideales primos que pertenecen a I se llama *genéricamente estable* si verifica que:

$$\text{Si } P \in \mathcal{P} \text{ y } P' \subseteq P, \text{ entonces } P' \in \mathcal{P}.$$

En virtud de este concepto y a todas las proposiciones anteriores, ya estamos en condiciones de demostrar un segundo teorema de unicidad de la descomposición primaria.

Teorema 2.14 (Segundo teorema de unicidad)**.** *Sea I un ideal descomponible, con $I = \bigcap_{i=1}^{n} Q_i$ una descomposición primaria minimal, y supongamos que $\{P_{i_1}, ..., P_{i_m}\}$ es un conjunto genéricamente estable de ideales primos que pertenecen a I. Entonces $Q_{i_1} \cap ... \cap Q_{i_m}$ es independiente de la descomposición primaria.*

Descomposición. Si llamamos $S = A \setminus (P_{i_1} \cup ... \cup P_{i_m})$, entonces S es un sistema multiplicativo, y para cada ideal primo P asociado a I, tenemos que $P \cap S = \emptyset$, si $P \in \{P_{i_1} \cup ... \cup P_{i_m}\}$, o $P \cap S \neq \emptyset$, si $P \notin \{P_{i_1} \cup ... \cup P_{i_m}\}$. Entonces, por 2.13, $S(I) = Q_{i_1} \cap ... \cap Q_{i_m}$. $\square$

Corolario 2.15. Las componentes primarias minimales (es decir, las componentes primarias Q_i correspondientes a ideales primos minimales P_i) están únicamente determinadas por I.

Capítulo 3

El teorema de Lasker-Noether

En este Capítulo, demostraremos la existencia de una Descomposición primaria de cualquier ideal de una clase distinguida de anillos. El resultado es ahora conocido como el *Teorema de Lasker-Noether*, y prueba que todo ideal es descomponible si lo es de un tipo de anillo que mencionaremos a continuación. En 1905, E. Lasker [4] publicó una demostración de la descomponibilidad de todo ideal de un anillo de polinomios o un anillo de series de potencias convergentes. Unos pocos años más tarde, hacia 1921, y tras su fructífera y sistemática introducción de métodos algebraicos y condiciones de cadena en anillos, E. Noether [6] fue capaz de dar una demostración muy general para un tipo de anillos, llamados *Noetherianos* en su honor, que describiremos a continuación.

El teorema es una extensión entre otros de los tópicos mencionados en la Introducción y juega un importante papel en diversas ramas de las matemáticas, entre las que se incluyen la aritmética y la geometría, y que comentaremos en lo que sigue. La sencillez y elegancia de su demostración ponen de manifiesto, una vez más, la eficacia de los métodos algebraicos introducidos por Noether para la resolución de muchos problemas.

3.1. Anillos Noetherianos

En el capítulo anterior, para demostrar los teoremas de unicidad, hemos supuesto que el ideal I es descomponible, y nos gustaría poder asegurar que todo ideal lo es. En esta sección, veremos que hay una clase de anillos en los que todo ideal es descomponible, llamados anillos *Noetherianos*. Además, veremos aplicaciones de los teoremas de unicidad aplicados a anillos Noetherianos en otras ramas de las matemáticas, como la aritmética o la geometría. Recordemos que un anillo se dice *Noetheriano* si todo ideal $I \trianglelefteq A$ es finitamente generado.

Por ejemplo, $\mathbb{Z}$ es Noetheriano, ya que todo ideal es principal, es decir, está generado por un solo elemento . La condición de la definición es equivalente a otras dos condiciones, que veremos en el siguiente teorema.

Antes de empezar, hemos de mencionar un nuevo concepto. Un ideal propio I de un anillo A se dice *irreducible* si no se puede escribir como intersección de dos ideales que lo continen estrictamente.

Teorema 3.1. *Sea A un anillo. Las siguientes condiciones son equivalentes.*

i) A es Noetheriano.

ii) Toda cadena ascendente de ideales

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_s \subseteq \ldots$$

estabiliza, es decir, existe un s_0 con $I_s = I_{s_0}$ para todo $s \geq s_0$.

iii) Toda familia no vacía de ideales de A posee elemento maximal.

Demostración. Supongamos que A es Noetheriano y

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_s \subseteq \ldots$$

es una cadena ascendente de ideales. Ponemos $J = \bigcup_{i \geq 0} I_i$. J es un ideal de A. Como A es Noetheriano, J tiene una familia finita X que lo genera, por tanto podemos encontrar un s_0 tal que $X \subseteq I_{s_0}$. Por tanto $J = I_{s_0}$, lo que implica *ii*).

Veamos ahora que *ii*) implica *iii*). Si $\mathcal{F} \neq \emptyset$ es una familia de ideales sin elemento maximal, podemos encontrar una cadena infinita

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_s \subseteq \ldots$$

de ideales en $\mathcal{F}$ que no estabiliza.

Por último, supongamos que se cumple *iii*) y sea $I \trianglelefteq A$ un ideal, veamos que I es finitamente generado. Sea

$$\mathcal{F} = \{J \trianglelefteq A \mid J \subseteq I, J \text{ finitamente generado}\}.$$

El ideal cero está en $\mathcal{F}$, luego es no vacía, por lo que existe un $L \in \mathcal{F}$ maximal, y $L \subseteq I$. Si el contenido fuese estricto, podríamos elegir un $a \in I \setminus L$ tal que $L \subsetneq L_1 = L + Aa \subseteq I$. Como L_1 es finitamente generado, $L_1 \in \mathcal{F}$, luego se contradice que L sea maximal. Por tanto, $I = L$ es finitamente generado. □

Las siguientes construcciones conservan la propiedad de ser Noetheriano

Proposición 3.2. Sea A un anillo Noetheriano. Entonces

i) Si B es otro anillo Noetheriano, $A \times B$ es Noetheriano.

ii) Si $I \trianglelefteq A$ es un ideal, el cociente A/I es Noetheriano.

iii) Si $S \subseteq A$ es un sistema multiplicativo, el anillo de fracciones $A\left[S^{-1}\right]$ es Noetheriano.

Demostración. *i*) Tomamos un ideal J de $A \times B$, y sean

$$J_A = \{a \in A \mid (a, 0) \in J\}.$$
$$J_B = \{b \in B \mid (0, b) \in J\}.$$

Claramente, $J_A \trianglelefteq A$ y $J_B \trianglelefteq B$, y además $a \in J_A$ y $b \in J_B$ si y solo si $(a, b) \in J$, por tanto $J = J_A \times J_B$. Como A y B son Noetherianos, J_A y J_B tienen familias generadoras finitas X_A y X_B, entonces

$$X = \{(a, 0) \mid a \in X_A\} \cup \{(0, b) \mid b \in X_B\}$$

genera J.

ii) y *iii*) se prueban de forma análoga. En *ii* basta observar que si J/I es un ideal de A/I y X una familia generadora de J, entonces

$$\{a + I \mid a \in X\}$$

genera J/I. Para *iii*), recordemos que los ideales de $A\left[S^{-1}\right]$ son de la forma $IA\left[S^{-1}\right]$, con I ideal de A, luego está generado con

$$\{\frac{a}{1} \mid a \in Y\},$$

con Y una familia generadora finita de I. □

Teorema 3.3 (Teorema de la base de Hilbert)**.** *Si A es Noetheriano, $A[x]$ también lo es.*

Demostración. Lo razonaremos por reducción al absurdo. Suponer que existe un $I \trianglelefteq A[x]$ no es finitamente generado. Entonces $0 \neq I \neq A[x]$ y tomamos $f_1 \in I$ del menor grado posible. Así, podemos elegir una serie de polinomios $f_1, ..., f_r, f_{r+1}, ... \in I$ tal que cada uno cumple que $f_{r+1} \in I \setminus \langle f_1, ..., f_r \rangle$ y es de menor grado posible. Sea m_r el grado de f_r y a_r su coeficiente diector. Se tiene que $m_1 \leq m_2 \leq ... \leq m_r \leq ....$ Consideramos la cadena de ideales de A

$$\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq ... \langle a_1, ..., a_r \rangle \subseteq ...$$

Como A es Noetheriano, esta cadena estaciona, es decir, para un cierto r, $a_{r+1} \in \langle a_1, ..., a_r \rangle$, luego para ciertos $b_1, ..., b_r \in A$, $a_{r+1} = b_1 a_1 + ... + b_r a_r$. Sea

$$g = f_{r+1} - (b_1 f_1 x^{n_{r+1} - n_1} + ... + b_r f_r x^{n_{r+1} - n_r}),$$

es un polinomio de grado menor que f_{r+1}, que está en I pero no en $\langle f_1, ..., f_r \rangle$, lo que entra en contradicción con la elección de f_{r+1}. □

Corolario 3.4. Si A es Noetheriano, $A[x_1, ..., x_n]$ también lo es.

3.2. Descomposición primaria en anillos Noetherianos

Para demostrar que todo ideal I de un anillo Noetheriano A es descomponible, probaremos dos lemas, uno que probará que todo ideal es intersección de irreducibles, y otro que probará que estos últimos son siempre primarios en esta clase de anillos. En virtud de estos dos lemas lo que queremos probar será inmediato.

Lema 3.5. *Sea A anillo Noetheriano e $I \trianglelefteq A$, entonces I es intersección de ideales irreducibles.*

Demostración. Lo razonaremos por reducción al absurdo. Como el conjunto de ideales de A en los que el enunciado no se cumple es no vacío, por 3.1 entonces tiene un elemento maximal M. Como M es reducible, $M = J_1 \cap J_2$, con $J_1, J_2 \supset M$. Por tanto, J_1 y J_2 son intersección finita de ideales irreducibles, con lo que llegamos a una contradicción. □

Para poder demostrar el siguiente lema, hemos de introducir un nuevo concepto. Se llama *anulador* de un subconjunto B de A al conjunto

$$Ann(B) = \{b \in A \mid ab = 0 \text{ para todo } a \in B\}.$$

Se comprueba fácilmente que el anulador de un subconjunto es un ideal.

Lema 3.6. *En un anillo Noetheriano A, todos los ideales irreducibles son primarios.*

Demostración. Pasando al anillo cociente, basta probar que si el ideal cero es irreducible, entonces es primario. Sea $xy = 0$, con $y \neq 0$, y considerar la cadena de ideales $Ann(x) \subseteq Ann(x^2) \subseteq ...$, siendo $Ann(a) = \{b \in A \mid ab = 0\}$. Por 3.1, esta cadena estaciona, por lo que $Ann(x^r) = Ann(x^{r+1})$ para algún r, luego $\langle x^r \rangle \cap \langle y \rangle = 0$. Por tanto, si $a \in \langle y \rangle$, entonces $ax = 0$, y si $a \in \langle x^r \rangle$, entonces $a = bx^n$, luego $bx^{n+1} = 0$, por lo que $b \in Ann(x^{r+1}) = Ann(x^r)$, por lo que $a = bx^r = 0$. Como $\langle 0 \rangle$ es irreducible y $\langle y \rangle$, $x^r = 0$, por tanto $\langle 0 \rangle$ es primario. □

Teorema 3.7 (Teorema de Lasker-Noether)**.** *En un anillo Noetheriano A, todo ideal tiene una descomposición primaria.*

3.3. Aplicaciones

El objetivo de esta breve Sección es volver a los problemas mencionados en la Introducción y señalar la mejora de los mismos tras el estudio que hemos realizado.

3.3.1. Aplicaciones a la aritmética

La extensión natural de la Aritmética es la *Teoría de Números*, que aquí examinamos en su variante algebraica. El concepto fundamental es el de *número algebraico*, que se describe como sigue. Un *cuerpo de números* es un cuerpo K, que es una extensión finita del cuerpo $\mathbb{Q}$ de los números racionales. Un elemento $x \in K$ se denomina *entero algebraico* a secas, es algebraico sobre $\mathbb{Q}$ y por ello es raíz de un único polinomio mónico e irreducible $p_x(X) \in \mathbb{Q}[X]$. Si sucede que $p_x \in \mathbb{Z}[X]$, se dice que *x es un entero algebraico*. Por ejemplo, la unidad imaginaria $x = i$ es un entero algebraico porque $p_x = X^2 + 1$ pero $y = \frac{i}{2}$ no lo es ya que $p_y = X^2 + \frac{1}{4}$.

Es un resultado conocido (pero no es elemental) que los enteros algebraicos de K componen un anillo noetheriano que contiene a $\mathbb{Z}$. En la Sección 1.5 de [7] hemos estudiado al completo estos casos en el caso de extensiones cuadráticas. Muchos de ellos son dominios de factorización única, como el anillo de enteros de Gauss $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$, y muchos otros no, como el anillo $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Como todos son noetherianos, todos sus ideales son descomponibles, una afirmación que mejora sustancialmente lo expuesto en la Introducción.

3.3.2. Aplicaciones a la geometría

Los anillos de la Geometría Algebraica son noetherianos, pues a lo más son anillos de fracciones de un cociente de anillo de polinomios; por ejemplo, el anillo local de un conjunto algebraico irreducible en un punto ([5]). Sus ideales son todos descomponibles y esto proporciona, por ejemplo, una demostración explícita de que un conjunto algebraico afín es descomponible, en el sentido de que es unión finita de conjuntos algebraicos irreducibles. En efecto, sea $V \subseteq A^n$ un conjunto algebraico (no vacío). Existe un ideal $J \trianglelefteq \mathbb{C}[X_1, \cdots, X_n]$ tal que $V = V(J)$. Como el anillo es noetheriano, J es descomponible, es decir, podemos escribir $J = Q_1 \cap \cdots \cap Q_r$ donde los Q_k son ideales primarios. Se deduce que $V = V_1 \cup \cdots \cup V_r$, donde para todo k, $V_k = V(Q_k)$. Si $P_k = \sqrt{Q_k}$, se tiene que P_k es primo, $V_k = V(P_k)$ e $I(V_k) = IV(P_k) = P_k$. En consecuencia V_k es irreducible y la anterior es la descomposición de V en componentes irreducibles.

En realidad, se puede probar la existencia de las descomposiciones usando un *argumento noetheriano*. En efecto, si existen conjuntos algebraicos no descomponibles, la familia de ideales $\mathcal{F} = \{I(V) \mid V \text{ es un conjunto algebraico no descomponible}\}$ es no vacía y podemos elegir V tal que $I(V)$ sea maximal en $\mathcal{F}$. Entonces V es minimal entre los no descomponibles y debe ser reducible, unión de dos subconjuntos algebraicos propios, que por minimalidad deben ser descomponibles. Por lo tanto también lo es V, llegando a una contradicción. El argumento prueba que existe descomponibilidad pero la descomposición primaria permite calcular explícitamente las componentes irreducibles, lo que es una mejora evidente.

3.4. Descomposición primaria en anillos no-Noetherianos

En la Sección anterior, hemos visto que los anillos que aparecen en la Aritmética y la Geometría son Noetherianos. Por tanto, les podemos aplicar el Teorema de Lasker-Noether, que asegura que todos sus ideales son descomponibles. Desde un punto de vista meramente teórico, cabría preguntarse si existe una descomposición primaria en anillos no Noetherianos, es decir, si existen condiciones necesarias y suficientes que aseguren la descomponibilidad de todo ideal. La respuesta es afirmativa y existen tales criterios. Como los anillos no Noetherianos son en cierto modo excepcionales, era de esperar estos criterios fueran abstractos y no tuvieran excesiva aplicación práctica.

En lo que sigue vamos a desarrollar uno de ellos. Como su demostración además de laboriosa es extensa la esquematizaremos siempre que no se pierda la perspectiva.

A continuación, nos encontraremos dos condiciones necesarias para que todo ideal sea descomponible, y que juntas constituyen una condición suficiente. Para la demostración, nos apoyaremos en un lema y una proposición.

Lema 3.8. *Sea P un ideal primo minimal de A, y $S_p = A \setminus P$, entonces $S_P(\langle 0\rangle)$ (la contracción) es el ideal P-primario más pequeño. En particular, si P es un ideal primo minimal, $S_P(I)$ es P-primario, para todo ideal I contenido en P.*

Demostración. Es el ejercicio 11 de la página 56 de [1]. Omitiremos la demostración, ya que es sencilla pero demasiado farragosa. □

Condición 1. Para cada ideal I propio de A y todo ideal primo P, existe $x \notin P$ tal que $S_P(I) = (I : x)$, donde $S_P = A \setminus P$.

Proposición 3.9. Sea A un ideal que cumple la condición 1. Entonces todo ideal de A es intersección de ideales primarios.

Demostración. Sea I un ideal de A y P_1 un primo minimal que lo contenga. Entonces, por 3.8 $Q_1 = S_{P_1}(I)$ es P_1-primario y $Q_1 = (I : x)$ para algún $x \in A \setminus P_1$. Además, $I \subseteq Q_1 \cap I + \langle x\rangle$. Recíprocamente, si $y = a + tx \in I + \langle x\rangle$, con $a \in I$ e $y \in Q_1$, entonces $tx = 0$ en A/P_1, por tanto, como $x \notin P_1$, $t \in P_1 = \sqrt{Q_1} = (I : x)$, de lo que se deduce que $tx \in I$, luego $y \in I$ y por lo tanto $Q_1 \cap I + \langle x\rangle \subseteq I$.
Ahora, sea I_1 un ideal maximal del conjunto de ideales $J \supseteq I$ tales que $Q_1 \cap J = I$. Escogemos I_1 tal que $x \notin I_1$ y por tanto $I_1 \nsubseteq P_1$. Repitiendo la construcción, ahora para I_1, y así sucesivamente, en el paso n-ésimo se cumplirá que $I = Q_1 \cap ... \cap Q_n \cap I_n$, donde los Q_i son primarios e I_n maximal entre los ideales J que contienen a $I_{n-1} = I_n \cap Q_n$ e $I_n \nsubseteq P_n$. Como $I_{n-1} \subset I_n$, entonces, o bien alcanzamos el resultado en un número finito de pasos, o bien se llegará a él tras un número infinito de ellos. □

Además de la condición anterior, necesitaremos la siguiente condición para alcanzar nuestro objetivo:

Condición 2. Sea I un ideal de A. Consideramos una cadena descendente $S_1 \supseteq ... \supseteq S_n \supseteq ...$ de sistemas multiplicativos de A, entonces existe un entero n tal que $S_n(I) = S_{n+1}(I) = ...$

Teorema 3.10. *Sea A un anillo. Son equivalentes:*

i) Todo ideal de A es descomponible.

ii) A satisface la condición 1 y la condición 2.

Demostración. *i)* $\to$ *ii)* Si todo ideal tiene una descomposición primaria $I = \bigcap_{i=1}^n Q_i$, entonces el conjunto de ideales $S(I)$, con S sistema multiplicativo, es finito por 2.13, ya que los ideales de dicho conjunto son intersección de algunos de los Q_i, por lo que se cumple la condición 2. Veamos que satisface la condición 1. En primer lugar, notar que si S, S' son dos sistemas multiplicativos tales que $S \subseteq S'$, de 2.13 se deduce que $S(I) \subseteq S'(I)$, por tanto, si tenemos $S_1 \supseteq ... \supseteq S_n \supseteq ...$, entonces $S_1(I) \supseteq ... \supseteq S_n(I) \supseteq ...$, y toda cadena descendente tiene un límite inferior, llamémosle $S_f(I)$, y por el Lema de Zorn se da el resultado.
ii) $\to$ *i)* Si A satisface las dos condiciones, entonces es intersección de un número finito o infinito de ideales primarios, por 3.9. Con la notación dada en la condición 1, $S_n = S_{P_1} \cap ... \cap S_{P_n}$ cumple que $S_n \cap I_n \neq \emptyset$, ya que $I_n \nsubseteq P_n = A \setminus S_{P_n}$. Por tanto, por definición de contracción, es claro que

$1 \in S_n(I_n)$, y por ser ideal, $S_n(I_n) = A$. Entonces $S_n(I) = Q_1 \cap ... \cap Q_n \cap A = Q_1 \cap ... \cap Q_n$. Esto implica que $\{S_n\}_{n\in\mathbb{N}}$ es una secuencia decreciente de sistemas multiplicativos de A, que debe estabilizar por la condición 2, y por tanto existe un $n \in \mathbb{N}$ tal que $I_n = A$, por lo que I tiene una descomposición primaria. $\square$

Anexo: Descomposición primaria y primos asociados

El objetivo de este anexo es dar otra interpretación a la descomposición primaria. Esta interpretación está relacionada con los *módulos*, cuya definición recordaremos a continuación.

Sea A un anillo, un A-*módulo* es un grupo abeliano M en el que A actúa linealmente, es decir, es un par (M, μ), donde μ es una aplicación $\mu : A \times M \to M$, donde denotamos $\mu(a, x) = ax$ para $a \in A$, $x \in M$, que cumple los siguientes axiomas:

$$a(x + y) = ax + ay$$

$$(a + b)x = ax + bx$$

$$(ab)x = a(bx)$$

$$1x = x$$

para todo $a, b \in A$, $x, y \in M$.

Equivalentemente, M es un grupo abeliano con un homomorfismo de anillos $A \to End(M)$, donde $End(M)$ es el anillo de endomorfismos del grupo abeliano M.

Un subgrupo N de un módulo M se llama *submódulo* si para cada $a \in A$ y cada $n \in N$, $an \in N$. Además, el grupo abeliano M/N resulta ser un módulo y se llama *módulo cociente* de M por N.

Nuestra idea es ver los anillos que hemos tratado durante todo el trabajo como A-módulos. Pongamos el ejemplo de $\mathbb{Z}$, donde ya hemos visto que todo elemento n se puede descomponer como producto de irreducibles de la siguiente forma: $n = \pm p_1^{e_1} \cdots p_r^{e_r}$. Como se observa en el capítulo 7 de [8], la idea es pensar en los factores de la descomposición anterior como los divisores de cero del anillo $M = \mathbb{Z}/\langle n \rangle$, que veremos como un $\mathbb{Z}$-módulo.

A lo largo del anexo trabajaremos con módulos al estilo de Bourbaki [2]. Empezaremos definiendo conceptos básicos acerca de ellos. Es importante notar que no daremos la demostración de alguno de los resultados que aparecerán.

En este trabajo ya dimos una definición de primos asociados relacionada con la descomposición primaria de un ideal, noción que ampliaremos a conjuntos invariantes por la acción de A, como por ejemplo un módulo cociente. Sin embargo, este concepto admite otra definición diferente cuando hablamos de módulos. Sea A un anillo y M un A-módulo. Se llama *primo asociado* de M a un ideal primo P de A tal que M contiene un submódulo isomorfo a A/P. Se denota al conjunto de los primos asociados de M por $Ass(M)$. Veamos cómo funciona con un ejemplo:

Ejemplo 1. Sea $n \in \mathbb{Z}$, $\alpha, \beta \in \mathbb{N}$ y $n = p^\alpha q^\beta$ para dos primos $p \neq q$, entonces el Z-módulo $M = \mathbb{Z}/\langle n \rangle$ tiene $Ass(\mathbb{Z}/\langle n \rangle) = \{\langle p \rangle, \langle q \rangle\}$. Además, $m = p^{\alpha-1} q^\beta \bmod n \in \mathbb{Z}/\langle n \rangle$ tiene $Ann(m) = \langle p \rangle$, y análogamente para q. Así, solo es posible que se cumpla $\mathbb{Z}/\langle l \rangle \subseteq \mathbb{Z}/\langle n \rangle$ si l es divisor de n.

Esto ilustra la idea de que los primos asociados p y q son los factores irreducibles de n. El nuevo punto de vista acerca de la descomposición primaria basado en módulos y primos irreducibles de A/I generaliza lo ocurrido en este ejemplo.

Proposición 2. i) Sea $x \in M$ tal que $Ann(x) = P$ es primo, entonces

$$0 \neq y \in Ax \Rightarrow Ann(y) = P.$$

ii) Considerar el conjunto de ideales

$$\{Ann(x) \mid 0 \neq x \in M\}.$$

Todo elemento maximal de este conjunto es un primo asociado.

iii) Si $L \subseteq M$ y $N = M/L$ entonces $Ass(M) \subseteq Ass(L) \cup Ass(N)$.

Demostración. *i)* y *iii)* [8][Lema 7.4.]. *ii)* Suponer que $x \in M$ está elegido tal que $Ann(x)$ es maximal entre los anuladores, y veamos que P es primo. Sea $fg \in Ann(x)$, entonces $fgx = 0$. Hay dos posibilidades: si $gx = 0$, entonces $g \in Ann(x)$. Si no, entonces $Ann(x) \subseteq Ann(gx)$, y por la maximalidad de éste último, $Ann(x) = Ann(gx)$, luego $f \in Ann(x)$. □

Corolario 3. Si A es Noetheriano y M un A-módulo, entonces

$$\{\text{Divisores de cero de } M \text{ en } A\} = \bigcup_{P \in Ass(M)} P.$$

Demostración. Para cada $0 \neq m \in M$, cada $a \in Ann(m)$ está contenido en un ideal $Ann(x)$ que es maximal, luego está en $Ass(M)$. □

Ejemplo 4. $N = M/L$ puede tener primos asociados que no estén en $Ass(M)$. Tomamos como ejemplo $Ass(\mathbb{Z}/\langle 2 \rangle) = \{\langle 2 \rangle\}$, pero $\langle 2 \rangle \notin Ass(\mathbb{Z})$. Por tanto, en la sucesión exacta

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/\langle n \rangle \to 0$$

los primos asociados de $N = \mathbb{Z}/\langle n \rangle$ no tienen nada que ver con los de $L = \mathbb{Z}$ ni $M = \mathbb{Z}$, pero sí con la naturaleza de la inclusión $L \hookrightarrow M$.

A continuación, veremos un resultado importante, que asegura que todo módulo finito sobre un anillo Noetheriano puede expresarse como extensión de módulos A/P_i donde los P_i son ideales primos.

Teorema 5. Sea A un anillo Noetheriano y M un A-módulo finito, entonces existe una cadena de submódulos

$$0 = M_0 \subset M_1 \subset ... \subset M_n = M$$

tal que $M_i/M_{i-1} \cong A/P_i$, donde P_i es ideal primo de A, $i = 1, ..., n$. Además

$$Ass(M) = \{P_1, ..., P_n\},$$

y en particular $Ass(M)$ es un conjunto finito.

Demostración. [8][Teorema 7.6.]. □

Si queremos hablar de descomposición primaria, es conveniente que miremos los ideales primarios desde nuestro nuevo punto de vista, y los comparemos con los conceptos que hemos definido a lo largo del anexo.

Teorema 6. Sea A un anillo Noetheriano y Q un ideal de A. Entonces

$$Q \text{ es } P\text{-primario} \iff Ass(A/Q) = \{P\}.$$

Demostración. [8][Teorema 7.8.]. □

A partir de aquí, tendremos en cuenta la definición de *descomposición primaria* que hemos venido utilizando durante todo el trabajo. Los problemas de existencia y unicidad que tuvimos siguen apareciendo. Ya vimos en el *teorema de Lasker-Noether* (3.7) que en un anillo Noetheriano todo ideal es descomponible. En particular, gracias al anulador, se puede probar fácilmente la siguiente proposición:

Proposición 7. Si B es un anillo Noetheriano, entonces

$$\text{Si } 0 \subset B \text{ es descomponible } \Longrightarrow 0 \subset B \text{ es primario.}$$

Demostración. [8][Lema 7.11.]. □

El problema de la existencia tiene la misma solución, por tanto, que dimos anteriormente, pero sigue existiendo el problema de la unicidad. Una vez asentado este nuevo punto de vista acerca de la descomposición primaria, estamos en condiciones de dar otra interpretación a los teoremas de unicidad utilizando las nuevas definiciones para reescribir su enunciado.

Teorema 8 (Primer teorema de unicidad)**.** Sea A un anillo Noetheriano, $I \subset A$ un ideal, e $I = Q_1 \cap ... \cap Q_k$ una descomposición primaria minimal, donde Q_i es P_i-primario, $i = 1, ..., k$. Entonces

$$Ass(A/I) = \{P_1, ..., P_k\},$$

y en particular, el conjunto de primos $\{P_1, ..., P_k\}$ está únicamente determinado por I, y por tanto no depende de la descomposición.

Demostración. [8][Teorema 7.12.]. □

En el caso del *Segundo teorema de unicidad*, tanto el enunciado como los pasos a seguir para poder demostrarlo se mantienen, y por tanto no será necesario tratarlos de nuevo.

Bibliografía

[1] **M.F. Atiyah, I.G Macdonald.** *Introduction to Commutative Algebra*, Addison-Wesley, Reading MA 1969. Traducción: *Introducción al Álgebra conmutativa*, Reverté, Barcelona, 1980.

[2] **N. BOURBAKI.** *Algèbre commutative.* Hermann, Paris 1964.

[3] **W. Fulton.** *Algebraic curves: An Introduction to Algebraic Geometry*, 3rd Edition. Addison Wesley, Reading MA 2008.
`http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`
Traducción de la primera edición: *Curvas Algebraicas*, Reverté, Barcelona 1971. `https://www.ugr.es/~pjara/D/Docen12/AC/Files/Texto.pdf`

[4] **E. Lasker.** *Zur Theorie der Moduln und Ideale.* Math. Ann. 60 (1905), 19-116.

[5] **C.M. Martínez.** *Notas para el curso de Curvas algebraicas.* Anillo Digital Docente. Universidad de Zaragoza 2021.

[6] **E. Noether.** *Idealtheorie in Ringbereichen.* Math. Ann. 83 (1921), 24-66.

[7] **J. Otal.** *Notas para el curso de Estructuras algebraicas.* Anillo Digital Docente. Universidad de Zaragoza 2020.

[8] **M. Reid.** *Undergraduate Commutative Algebra*, Cambridge UP, Cambridge 1995.