Anillos y módulos.
Polinomios de Sharma y factorización

MARGARITA GÓMEZ PUERTAS

Departamento de Álgebra

Grado en Matemáticas

Universidad de Granada. 2017

Trabajo Fin de Grado

Anillos y módulos.

Polinomios de Sharma y factorización

Margarita Gómez Puertas

Dirección: Pascual Jara Martínez

Grado en Matemáticas
Universidad de Granada
Granada, 2017

Introducción

Uno de los campos de trabajo en el que se adquiere destreza en el manejo y las aplicaciones del Álgebra Abstracta es la teoría de dominios de integridad. Aparentemente es una teoría simple, pero rápidamente aparecen pequeños matices de propiedades que se verifican en $\mathbb{Z}$, el anillo de los números enteros, y que no se tiene por qué verificar en dominio o anillo, aún cuando éstos verifiquen propiedades tan restrictivas como el ser un DIP ó un DFU; estas sutilezas ayudan a comprender el por qué de las definiciones y de la jerarquía y dependencia de los condiciones impuestas.

Todo comienza cuando se quiere extender el anillo de los números enteros a anillos de enteros en cuerpos que son extensiones finitas de $\mathbb{Q}$; por ejemplo $\mathbb{Z}[i]$, el anillo de los enteros de Gauss, ó $\mathbb{Z}[\omega]$, el anillo de los enteros de Eisentein. Tenemos que $\mathbb{Z}[i]$ es un DE, y por tanto podemos hacer una división con resto, y como consecuencia es un DIP y un DFU. Pero existen otros anillos, por ejemplo $\mathbb{Z}[\sqrt{-5}]$, en el que esto no ocurre, ya que no es un DFU. Aún hay otros, como por ejemplo $\mathbb{Z}[\theta]$, donde $\theta = \frac{1+\sqrt{-19}}{2}$, que es un DIP, pero no es un DE.

Se observe que el estudio de estos anillos nos adentra, de forma sencilla en la teoría abstracta de la interrelación de estos tres conceptos que hasta ahora hemos mencionado. Para un estudio en profundidad necesitamos primero determinar el marco de trabajo y la herramientas a utilizar. En nuestro caso hemos optado por la aritmética: la divisibilidad y sus propiedades. La divisibilidad en un dominio nos lleva a una relación de equivalencia en la que cada clase está formada por elementos asociados entre sí, y a un conjunto parcialmente ordenado en el conjunto cociente, lo que permite definir el mcd y el mcm de dos elementos como el ínfimo y el supremo en el conjunto cociente. La introducción de mcd y mcm permite definir un nuevo tipo de dominios: los dominos GCD, que son aquellos en los que cada par de elementos tiene un mcd, y por dualidad los dominios LCM; ambos conceptos coinciden. Tenemos entonces una primera clasificación de los dominios

$$\text{DE} \Rightarrow \text{DIP} \Rightarrow \text{DFU} \Rightarrow \text{GCD}.$$

Es importante señalar que los contenidos entre estas clases de dominios son estrictos. Ahora todo consiste en alojar a cada domino en una de estas clases. La primera parte del trabajo esta dedicada a estudiar esta situación, que podemos llamar clásica, y a ver si estas clases se mantienen estables ante determinadas construcciones: anillo de polinomios y anillo de series de potencias formales.

La segunda parte consiste en eliminar la condición de ser dominio, y por tanto ver que ocurre a un anillo conmutativo general. Para esa generalización nos hemos centrado en el caso de los DIPs, definiendo los AIPs (anillos de ideales principales). Lo primero es ver un teorema de estructura; en efecto, todo AIP es un producto directo de un número finito de DIPs y de AIPs, y lo segundo es determinar cada una de estas partes. En este punto sería de interés estudiar los módulos sobre cada

uno estos tipos de anillos, pero esto excedía el contenido de este trabajo. Las herramientas necesarias para obtener esta descomposición no son elementales y muestran el interés y el modo de proceder cuando uno se enfrenta al estudio de un teorema de estructura.

Termina la segunda parte con caracterizaciones de AIP, por ejemplo, cada ideal primo es principal, la caracterización de cuando un anillo de polinomios $A[X]$ es un AIP; de forma similar el caso de un dominios se tiene que $A[X]$ es un AIP si, y sólo si, A es un producto de cuerpos, o el hecho de que todo AIP es un cociente de un producto de DIPs.

Para cerrar la teoría, y de cara a posteriores desarrollos en ámbitos no conmutativos, se estudia cuando un ideal primo de un anillo de polinomios es principal, apareciendo los que hemos llamado polinomios de Sharma que dan título a este trabajo.

El contenido de los capítulos es el siguiente: En el primero se introducen los conceptos fundamentales de la teoría de anillos conmutativos, y en el segundo las nociones clásicas sobre dominios de integridad y su comportamiento ante la construcción del anillo de polinomios. En el capítulo tercero se trata la teoría de estructura de anillos de ideales principales para lo que necesitamos conceptos como noetheriano, artiniano y completación. Una vez obtenidos los resultados sobre la estructura, la aplicamos al caso del anillo de series de potencias formales. El capítulo cuarto está dedicado al resultado de Kaplansky sobre caracterización de AIPs mediante ideales primos, resultado que posteriormente fue extendido por Cohen al caso de anillos noetherianos, y a la caracterización de anillos A para los que $A[X]$ es un AIP. El capítulo quinto estudia ideales primos principales, y la caracterización de sus generadores. a lo que llamamos polinomios de Sharma.

Introduction

One of the fields of work in which the handling and applications of abstract algebra are deployed is the theory of integrity domains. Apparently it is a simple theory, but, quickly, we notice that there are small aspects which are fulfilled in $\mathbb{Z}$, and they does not have to be verified in any domain or ring, even when these rings fulfill so restrictive conditions like being an unique factorization domain or a principal ideal domain. These subtleties help to understand the reason of some definitions and the hierarchy and dependence on conditions imposed.

It all begins when we want to extend the ring of integers, $\mathbb{Z}$, to rings of integers in fields that are finite extensions of $\mathbb{Q}$, for example $\mathbb{Z}[i]$, Gauss integer ring, or $\mathbb{Z}[\omega]$, Eisenstein integer ring. It is known that $\mathbb{Z}[i]$ is an euclidean domain so we can do a division with remainder, and as a consequence, it is a principal ideal domain and an unique factorization domain. However, there are some rings, like $\mathbb{Z}[\sqrt{-5}]$, in which this is not true because they are not an unique factorization domain. In addition, there are some rings, like $\mathbb{Z}[\theta]$, where $\theta = \frac{1+\sqrt{-19}}{2}$, that are principal ideal domains but they are not an euclidean domain.

The study of these rings leads us easily into the abstract theory of the interrelationship of these three concepts which have been previously mentioned. For an in-depth study we first need to determine the framework and tools we have to use. In our case we have chosen arithmetic: divisibility and its properties. The divisibility in a domain leads us into a equivalence relation in which each equivalence class is a set of associated elements and into a partially ordered set in the quotient set; which allows us to define greatest common divisor and least common multiple of two elements as the lowest and the highest element in the set quotient. The introduction of greatest common ddivisor and least common multiple allows us to define a new kind of domains: the GCD domains, which are domains in which any two elements has greatest common divisor, and by duality the LCM domains. Both concepts are the same so we have a first classification of the domains:

$$\text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{GCD}.$$

It is important to note that the contents between these classes are strict. For example, an unique factorization domain must fulfill another condition to be a principal ideal domain, this condition is that each non-zero prime ideal is maximal.

Now, we only have to classify each domain in one of these classes. The first part of this paper is dedicated to study this situation, that we can name classic, and if these classes do not change with some constuctions, like the polynomial rings and formal power series rings. To study this, we need to see some basic notions of commutative rings and some results of their most important properties to transfer them to the case of the domains mentioned above. For example, results like Chinese

Remainder Theorem or Nakayama's Lemma will be proved. Furthermore we will see properties and characterizations of these domains, for example, the characterization of unique factorization domains using principal minimal prime ideals, and how they relate to each other, seeing, among other things, the demonstrations of the implications mentioned above. One of the most important properties of these domains will be when the prime and irreducible elements coincide. As we know, every prime element is irreducible but reciprocal is not always true. When the reciprocal is fulfilled we will say that the prime condition is fulfilled.

Unique factorization domains will be studied in more depth, seeing their relation with some conditions that can characterize them, like divisor chain condition or prime condition, for example we will see that if a domain fulfills these two conditions is an unique factorization domain or that it is only necessary that a domain fulfills the divisor chain condition so that it exists a factorization, although this one is not unique. This part ends with some Atiyah-Macdonald's exercises about polynomial rings and the ideal called nilradical, Nil(R).

The second part tries to eliminate the condition of being a domain and study what happens to a commutative ring. For this generalization, we have focused on principal ideal domains by defining the principal ideal rings (PIR). First, we have to see a structure theorem. Indeed, we will prove that any PIR is a direct product of a finite number of principal ideal domains and principal ideal rings. We also have to determine each of these parts. Proving this structure theorem requires studying properties of Noetherian and Artinian rings so that will be the first thing we will see, also proving a structure theorem for Artinian rings that will allow us to decompose an Artinian ring as a direct product of Artinian rings with only a maximal ideal. We will study special principal ideal rings which, as we shall see, coincide with local Artinian rings in which the maximal ideal is principal. These ones are the rings that appear in the structure theorem.

At this point, it would be interesting to study modules over these rings but this would exceed the content of this paper. Required tools to obtain this descomposition are not basic and they show the interest and the procedure when we deal with the study of a structure theorem.

This part ends with some chacarterizations of principal ideal rings, for example, the characterization of polynomial rings that are principal ideal rings or any principal ideal ring is a quotient of a product of principal ideal domains. This one is due to Hungerford and to prove it we need the concept of v-ring and a structure theorem of Noetherian local rings whose demonstration is not going to be proved because it is too complex at this level. Hungerford's Theorem's demonstration will be based, since we already have a product of principal ideal domains and special principal ideal rings, in proving that each special principal ideal ring is a quotient of a principal ideal domain. Along with these results, come some characterizations using nilpotent elements, such as that an Artinian ring is a principal ideal ring if, and only if, nilradical ideal is a principal ideal. Also, we will see that it is enough that each prime ideal of a ring is principal to have a principal ideal ring, a result known as Kaplansky's theorem and, similarly to principal ideal domains, we will show that $R[X]$ is a principal ideal ring if, and only if, A is a finite product of fields.

We will also study, as it has been mentioned before, polynomial rings and formal power series ring seeing, among other things, that the divisor chain condition or the unique factorization is maintained when we build these rings. The demonstrations in both of them are very similar since, as we know, a ring is the generalization of the previous one. Something of the polynomials that does not exist in

the formal power series rings is the content of a polynomial. We will see results about this concept as Gauss's lemma or Dedekind-Mertens's lemma.

To close the theory and with regard to studies in the non-commutative case, it will be studied when a prime ideal in a polynomial ring is principal. In this way, a new kind os polynomials is going to appear, we have named them Sharma polynomials that title this paper. Before study them, it is necessary to study invertible ideals, fractional ideals and localizations of a ring. We will see the relation between invertible ideals and finitely generated ideals localizated in a maximal ideal. More precisely, we have that an ideal is invertible if, and only if, it is finitely generated and is a principal ideal in each localization of a maximal ideal. Finally, we conclude the study with two theorems due to Sharma. The first one shows us that if we have a prime ideal in $R[X]$ whose intersection with R is the empty set, then, this ideal is principal, more precisely generated by a polynomial of least degree in the ideal $a_0X^d + \ldots + a_{d-1}X + a_d$, if, and only if, there does not exist $t \notin (a_0)$ such that $a_i t \in (a_0)$ for each $i \in \{1, \ldots, d\}$. The second one shows us that in a Noetherian integral domain, R, a prime ideal in $R[X]$ whose intersection with R is the empty set is invertible if there exist a polynomial of least degree in the ideal and his content is an invertible ideal.

The content of the chapters is the following one: In the first one we introduce basic concepts of commutative ring theory and in the second one basic ideas of integral domains and their behaviour in the face of the construction of polynomial rings. In the third chapter we address the structure theory of principal ideal rings, for this we will need ideas like noetherian rings, artinian rings or completation. Having reach this point, we apply this to formal power rings. Fourth chapter is dedicated to a Kaplansky theorem about characterizations of principal ideal rings using prime ideals, theorem that was extended by Cohen to noetherian rings, and the characterization of rings R that verify $R[X]$ is a principal ideal ring. The last one studies principal prime ideals in $R[X]$ and the characterization of their generators, who we name Sharma polynomials.

Índice general

Capítulo I

Anillos

1. Anillos conmutativos

Definición. 1.1.
Un conjunto A con dos operaciones binarias, $+$ y $\times$ se dice **anillo** si se cumplen las siguientes propiedades:

(1) $(A, +, 0)$ es un grupo abeliano, es decir, la operación es asociativa y conmutativa, 0 es el **elemento cero** y para todo $x \in A$ existe $-x \in A$, llamado **elemento opuesto** de x, tal que $x + (-x) = 0$.
(2) $(A, \times, 1)$ es un monoide, es decir, la operación es asociativa, 1 es el **elemento uno**.
(3) **Propiedad distributiva del producto respecto a la suma**:

$$(a + b) \times c = a \times c + b \times c \text{ para todos } a, b, c \in A,$$
$$a \times (b + c) = a \times b + a \times c \text{ para todos } a, b, c \in A.$$

Un anillo A es **conmutativo** si $a \times b = b \times a$ para todos $a, b \in A$. En este trabajo, salvo que si indique lo contrario, todos los anillos son conmutativos.

Observación. 1.2.
(1) A partir de ahora notaremos $xy = x \times y$.
(2) Un anillo A se llama **trivial** si $0 = 1$. En lo que sigue los anillos considerados serán no triviales.

Definición. 1.3.
Sea A un anillo. Un subconjunto B de A se llamará **subanillo** si:

(1) B es un subgrupo de A para la suma $+$.
(2) B es cerrado para el producto $\times$.
(3) $1 \in B$.

Definición. 1.4.
Un **ideal** de un anillo A es un subconjunto $\mathfrak{a} \subseteq A$ de manera que:

(1) $\mathfrak{a}$ es subgrupo de A.
(2) Para todo $r \in A$ y para todo $x \in \mathfrak{a}$ se cumple que $rx \in \mathfrak{a}$.

Definición. 1.5.
Dados dos ideales $\mathfrak{a}$,$\mathfrak{b} \subseteq A$ definimos:

(1) $\mathfrak{a}+\mathfrak{b} = \{a+b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$
(2) $\mathfrak{a}\mathfrak{b} = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$
(3) $(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid xb \in \mathfrak{a}, \text{ para todo } b \in \mathfrak{b}\}$

Observación. 1.6.
Para cada ideal $\mathfrak{a} \subseteq A$ se tiene $1 \in \mathfrak{a}$ si, y sólo si, $\mathfrak{a} = A$.

Definición. 1.7.
Dados dos anillos A y B y $f : A \longrightarrow B$ una aplicación, diremos que f es un **homomorfismo de anillos** cuando se cumplan:

(1) $f(x+y) = f(x)+f(y)$ para todos $x, y \in A$.
(2) $f(xy) = f(x)f(y)$ para todos $x, y \in A$.
(3) $f(1) = 1$.

Dado un homomorfismo de anillos $f : A \longrightarrow B$, podemos considerar los conjuntos **imagen de** f, definido $\mathrm{Im}(f) = \{f(x) \mid x \in A\}$, y **núcleo de** f, definido $\mathrm{Ker}(f) = \{x \in A \mid f(x) = 0\}$.
Veamos las características que tienen estos conjuntos:

(1) $\mathrm{Im}(f)$ es un subanillo de B.
(2) $\mathrm{Ker}(f)$ es un ideal de A.

Definición. 1.8.
Un anillo conmutativo en el que se cumple que para todo $0 \neq x \in A$ existe $x^{-1} \in A$ tal que $xx^{-1} = 1$ diremos que es un **cuerpo**. El elemento, x^{-1} es único, y lo llamaremos el **inverso** de x.

Definición. 1.9.
Diremos que un elemento $x \in A$ es **invertible** en el anillo A cuando exista su inverso $x^{-1} \in A$.
Notamos por $U(A)$ al conjunto de elementos invertibles de A, así pues, $U(A)$ es un subgrupo del monoide multiplicativo de A.

Definición. 1.10.
Un elemento x de un anillo A se dirá **divisor de cero** si existe $0 \neq y \in A$ de manera que $xy = 0$.

Definición. 1.11.
Un anillo diremos que es un **dominio de integridad** (DI) cuando no tiene divisores de cero no nulos.

Definición. 1.12.
Sea A un anillo y $X \subseteq A$ un conjunto no vacío. Definimos el ideal de A **generado** por X, que denotaremos por (X), como el menor ideal de A que contiene a X y que no es otro que la intersección de todos los ideales que contienen a X.
Diremos que X es un **sistema de generadores** de (X). En particular se tiene $(X) = \{\sum_{i=1}^{t} x_i r_i \mid x_i \in X, r_i \in A\}$.

Definición. 1.13.
Un ideal se dice **finitamente generado** cuando está generado por un conjunto finito de elementos del anillo. Cuando $X = \{x_1, \ldots, x_n\}$, el ideal generado por este conjunto lo notaremos $(x_1, \ldots, x_n)$.

Definición. 1.14.
Diremos que un ideal de un anillo A es **principal** cuando pueda ser generado por un conjunto con un solo elemento. Al ideal generado por un solo elemento a lo podemos notar también como Aa.

Definición. 1.15.
Llamaremos **dominio de ideales principales** (DIP) a un dominio de integridad donde todos los ideales sean principales. Análogamente, llamaremos **anillo de ideales principales** (AIP) a un anillo donde todos los ideales son principales.

Definición. 1.16.
Dado un anillo A y un ideal $\mathfrak{a} \subseteq A$, definimos el **anillo cociente** de A sobre el ideal $\mathfrak{a}$ como

$$A/\mathfrak{a} = \{x + \mathfrak{a} \mid \ x \in A\},$$

de manera que x e y pertenecen a la misma clase de equivalencia si, y solo si, $x - y \in \mathfrak{a}$.
Tenemos que $A/\mathfrak{a}$ es un anillo con operaciones:
(1) $(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$.
(2) $(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}$.
(3) $0 + \mathfrak{a}$, elemento cero.
(4) $1 + \mathfrak{a}$, elemento uno.

Para que la definición sea correcta, tendríamos que ver que estas operaciones no dependen del representante que elijamos en una clase de equivalencia. Veámoslo para el producto:

DEMOSTRACIÓN. Sean $x + \mathfrak{a} = x' + \mathfrak{a}$ e $y + \mathfrak{a} = y' + \mathfrak{a}$. Así $x - x' \in \mathfrak{a}$ y $y - y' \in \mathfrak{a}$, entonces $x(y - y') + (x - x')y = xy - x'y' \in \mathfrak{a}$, luego $xy + \mathfrak{a} = x'y' + \mathfrak{a}$, y la operación no depende de los representantes elegidos. □

Proposición. 1.17.
Sea A un anillo y $\mathfrak{a} \subseteq A$ un ideal, se verifica:

(1) Si $\mathfrak{b}$ es un ideal de A conteniendo a $\mathfrak{a}$, entonces $\mathfrak{b}/\mathfrak{a} = \{b + \mathfrak{a} \mid \ b \in \mathfrak{b}\}$ es un ideal de $A/\mathfrak{a}$.
(2) Dados $\mathfrak{b}_1, \mathfrak{b}_2 \subseteq A$, ideales de A y $\mathfrak{a} \subseteq A$ un ideal tal que $\mathfrak{a} \subseteq \mathfrak{b}_1$ y $\mathfrak{a} \subseteq \mathfrak{b}_2$, entonces $\mathfrak{b}_1/\mathfrak{a} = \mathfrak{b}_2/\mathfrak{a}$ si, y sólo si, $\mathfrak{b}_1 = \mathfrak{b}_2$.
(3) Si $\mathfrak{b}'$ es un ideal de $A/\mathfrak{a}$, existe único ideal $\mathfrak{b} \subseteq A$ tal que $\mathfrak{a} \subseteq \mathfrak{b}$ y $\mathfrak{b}' = \mathfrak{b}/\mathfrak{a}$.

Teorema. 1.18.
Dado un anillo A, son equivalentes:

(a) A es un cuerpo.
(b) Los únicos ideales de A son el total y el 0.
(c) Todo homomorfismo de anillos $f : A \longrightarrow B$ es inyectivo.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si $\mathfrak{a}$ es un ideal no trivial, existe $0 \neq x \in \mathfrak{a}$ y como A es un cuerpo, existe x^{-1} tal que $xx^{-1} = 1$, luego $1 \in \mathfrak{a}$, y se tiene $\mathfrak{a} = A$.

(b) $\Rightarrow$ (c). $\mathrm{Ker}(f)$ es un ideal del anillo A; como $f(1) = 1 \neq 0$, se tiene $1 \notin \mathrm{Ker}(f)$, luego $\mathrm{Ker}(f) = 0$, y f es una aplicación inyectiva.

(c) $\Rightarrow$ (a). Sea x un elemento de A y supongamos que no tiene inverso, entonces $Ax \subsetneq A$ y $A/Ax \neq 0$. Consideramos la proyección $p : A \longrightarrow A/Ax$ que, por hipótesis, es inyectiva, luego $\mathrm{Ker}(f) = Ax = 0$, así $x = 0$ y A es un cuerpo. □

Definición. 1.19.
Sea A un anillo:

(1) Un ideal $\mathfrak{p}$ diremos que es **primo** si no es el total y siempre que $xy \in \mathfrak{p}$ con $x, y \in A$, se tiene $x \in \mathfrak{p}$ ó $y \in \mathfrak{p}$.
(2) Un ideal $\mathfrak{m}$ diremos que es **maximal** si no es el total y si existe un ideal conteniéndolo propiamente, entonces ese ideal es necesariamente el total. Esto es, si $\mathfrak{m} \subsetneq \mathfrak{a} \subseteq A$, entonces $\mathfrak{a} = A$.

Teorema. 1.20.
Dado A un anillo y $\mathfrak{a}$ un ideal propio de A, se cumple:

(1) $\mathfrak{a}$ es primo si, y solo si, $A/\mathfrak{a}$ es dominio de integridad.
(2) $\mathfrak{a}$ es maximal si, y solo si, $A/\mathfrak{a}$ es un cuerpo.

DEMOSTRACIÓN. (1). ($\Rightarrow$). Consideramos $x + \mathfrak{a}, y + \mathfrak{a} \in A/\mathfrak{a}$ de manera que $(x + \mathfrak{a})(y + \mathfrak{a}) = 0 + \mathfrak{a}$. Entonces $xy \in \mathfrak{a}$, luego $x \in \mathfrak{a}$ ó $y \in \mathfrak{a}$ (por ser $\mathfrak{a}$ un ideal primo). De esta manera que $x + \mathfrak{a} = 0 + \mathfrak{a}$ ó $y + \mathfrak{a} = 0 + \mathfrak{a}$ y así $A/\mathfrak{a}$ es un dominio de integridad.

($\Leftarrow$). Sea $xy \in \mathfrak{a}$, entonces $xy + \mathfrak{a} = (x + \mathfrak{a})(y + \mathfrak{a}) = 0 + \mathfrak{a}$, luego $x + \mathfrak{a} = 0 + \mathfrak{a}$ ó $y + \mathfrak{a} = 0 + \mathfrak{a}$, o lo que es lo mismo, $x \in \mathfrak{a}$ o $y \in \mathfrak{a}$. Así $\mathfrak{a}$ es un ideal primo.

(2). ($\Rightarrow$). Sea $x + \mathfrak{a} \neq 0 + \mathfrak{a}$, entonces $x \notin \mathfrak{a}$ y $\mathfrak{a} + (x) = A$. Así podemos poner $1 = m + rx$ donde $m \in \mathfrak{a}$, $r \in A$, por tanto $1 - rx = m$, y se tiene $1 - rx \in \mathfrak{a}$. Entonces $1 + \mathfrak{a} = rx + \mathfrak{a} = (r + \mathfrak{a})(x + \mathfrak{a})$. Como consecuencia, luego $x + \mathfrak{a}$ tiene inverso y $A/\mathfrak{a}$ es un cuerpo.

($\Leftarrow$). Sea $\mathfrak{b}$ un ideal de A conteniendo a $\mathfrak{a}$, entonces $\mathfrak{b}/\mathfrak{a}$ es un ideal de $A/\mathfrak{a}$. Por uno de los teoremas anteriores, $\mathfrak{b}/\mathfrak{a} = 0$ ó $\mathfrak{b}/\mathfrak{a} = A\mathfrak{a}$. Ahora bien, si $\mathfrak{b}/\mathfrak{a} = 0$, entonces $\mathfrak{b} = 0$, lo cual no es posible; luego $\mathfrak{b}/\mathfrak{a} = A/\mathfrak{a}$, lo cual ocurre si, y solo si, $\mathfrak{b} = A$, luego $\mathfrak{a}$ es maximal. □

Definición. 1.21.
Diremos que un ideal $\mathfrak{a}$ de un anillo A es **primario** cuando si $ab \in \mathfrak{a}$ y $a \notin \mathfrak{a}$, existe $n \in \mathbb{N}$ de manera que $b^n \in \mathfrak{a}$.

Definición. 1.22.
Un subconjunto Σ de un anillo A se dice **multiplicativamente cerrado** si:

(1) Para cualesquiera $x, y \in \Sigma$ se tiene $xy \in \Sigma$.
(2) $1 \in \Sigma$.

Para evitar casos triviales, podemos imponerle la condición $0 \notin \Sigma$

Teorema. 1.23.
Sea A un anillo, $\mathfrak{a} \subseteq A$ un ideal, y Σ un subconjunto multiplicativamente cerrado tal que $\mathfrak{a} \cap \Sigma = \emptyset$, existe un ideal $\mathfrak{b} \subsetneq A$ de manera que $\mathfrak{a} \subseteq \mathfrak{b}$, $\mathfrak{b} \cap \Sigma = \emptyset$, y $\mathfrak{b}$ es maximal con estas dos condiciones. En este caso, $\mathfrak{b}$ es un ideal primo del anillo A.

DEMOSTRACIÓN. Consideramos el conjunto $\Gamma = \{\mathfrak{c} \subsetneq A \mid \mathfrak{a} \subseteq \mathfrak{c} \text{ y } \mathfrak{c} \cap \Sigma = \emptyset\}$. Como $\mathfrak{a} \in \Gamma$, este conjunto es no vacío y podemos aplicar el lema de Zorn con lo que tenemos que existe un elemento maximal en ese conjunto, es decir, existe $\mathfrak{b} \subsetneq A$ tal que $\mathfrak{a} \subseteq \mathfrak{b}$ y $\mathfrak{b} \cap \Sigma = \emptyset$, siendo maximal para estas propiedades.
Veamos que el ideal $\mathfrak{b}$ es un ideal primo. Sean $x, y \in A$ tales que $xy \in \mathfrak{b}$ y supongamos $x \notin \mathfrak{b}$ e $y \notin \mathfrak{b}$. Entonces $\mathfrak{b} \subsetneq \mathfrak{b} + (x)$ y $\mathfrak{b} \subsetneq \mathfrak{b} + (y)$. Como $\mathfrak{b}$ es maximal en el conjunto Γ, se tiene $(\mathfrak{b} + (x)) \cap \Sigma \neq \emptyset$ y $(\mathfrak{b} + (y)) \cap \Sigma \neq \emptyset$, luego existen $s, t \in \Sigma$ tales que $s \in (\mathfrak{b} + (x)) \cap \Sigma$ y $t \in (\mathfrak{b} + (y)) \cap \Sigma$. Así $s = m + ax$, con $m \in \mathfrak{b}$, $a \in A$ y $t = n + by$, con $n \in \mathfrak{b}$, $b \in A$. Como Σ es multiplicativamente cerrado $st \in \Sigma$, ahora bien $st = mn + mby + axn + axby$. Como $m, n \in \mathfrak{b}$ entonces $mn + mby + axn \in \mathfrak{b}$. Además, $xy \in \mathfrak{b}$, luego $st \in \mathfrak{b}$. Tendríamos un elemento en la intersección que es vacía, hemos llegado a una contradicción, luego $x \in \mathfrak{b}$ ó $y \in \mathfrak{b}$ y $\mathfrak{b}$ es un ideal primo. □

Teorema. 1.24. (Teorema de Krull)
Sea A un anillo y $\mathfrak{a} \subsetneq A$ un ideal. Existe un ideal maximal de A conteniendo a $\mathfrak{a}$. Consecuentemente, todo anillo no trivial tiene, al menos, un ideal maximal.

DEMOSTRACIÓN. Aplicando el teorema anterior a $\mathfrak{a}$ y $\Sigma = \{1\}$, tenemos que existe un ideal maximal en A conteniendo a $\mathfrak{a}$. Para la segunda afirmación, si tomando $\mathfrak{a} = 0$ y $\Sigma = \{1\}$ tenemos que todo anillo no trivial tiene al menos un maximal. □

Definición. 1.25.
Dado x un elemento de un anillo A, diremos que x es **nilpotente** si existe $n \in \mathbb{N}$ tal que $x^n = 0$. Llamamos **nilradical** de A, $\mathrm{Nil}(A)$, al conjunto de todos los elementos nilpotentes de A.

Proposición. 1.26. (Propiedades de $\mathrm{Nil}(A)$)
Sea A un anillo, se verifica:

(1) $\mathrm{Nil}(A)$ *es un ideal.*
(2) $\mathrm{Nil}(A) = \cap\{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(A)\}$, *donde* $\mathrm{Spec}(A)$ *es el conjunto de los ideales primos de A.*

DEMOSTRACIÓN. (1). Si $x, y \in \mathrm{Nil}(A)$ existen $n, m \in \mathbb{N}$ tales que $x^n = 0$, $y^m = 0$. Así, con $t \geq n+m$ se tiene $(x-y)^t = 0$ y $x - y \in \mathrm{Nil}(A)$.
Sea $x \in A$, existe $n \in \mathbb{N}$ tal que $x^n = 0$. Dado $r \in A$ se tiene $(rx)^n = r^n x^n = 0$, luego $rx \in \mathrm{Nil}(A)$.
(2). ($\subseteq$). Sea $x \in \mathrm{Nil}(A)$, entonces $x^n = 0 \in \mathfrak{p}$ para todo $\mathfrak{p} \in \mathrm{Spec}(A)$, y $x \in \mathfrak{p}$ para todo $\mathfrak{p} \in \mathrm{Spec}(A)$.
($\supseteq$). Sea $x \notin \mathrm{Nil}(A)$, entonces $x^n \neq 0$ para todo $n \in \mathbb{N}$. Sea $\Sigma = \{x^n \mid n \in \mathbb{N}\}$ un conjunto multiplicativamente cerrado y $\Sigma \cap \mathrm{Nil}(A) = \emptyset$, luego existe un ideal primo $\mathfrak{p}$ de manera que $\mathrm{Nil}(R) \subseteq \mathfrak{p}$ y $\mathfrak{p} \cap \Sigma = \emptyset$. Así $x \notin \mathfrak{p}$, luego $x \notin \cap\{\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(A)\}$. □

Definición. 1.27.
Sea A un anillo, definimos el **radical de Jacobson** de A como $\mathrm{Jac}(A) = \cap\{\mathfrak{m} \mid \mathfrak{m} \subseteq A \text{ es maximal}\}$.

Proposición. 1.28.
Para cada $x \in A$ son equivalentes:
(a) $x \in \mathrm{Jac}(R)$.
(b) $1 - ax$ *es una unidad para todo* $a \in A$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Supongamos que $1-ax$ no es una unidad para algún elemento a del anillo A. Considerando (a) sabemos que hay algún ideal maximal que lo contiene, luego $1-ax \in \mathfrak{m}$, con $\mathfrak{m}$ ideal maximal. Ahora bien como $x \in \mathrm{Jac}(A)$, entonces $x \in \mathfrak{m}$, y se tiene $ax \in \mathfrak{m}$. De esta manera $1 \in \mathfrak{m}$, lo cual es una contradicción.
(b) $\Rightarrow$ (a). Supongamos $x \notin \mathfrak{m}$, con $\mathfrak{m}$ un ideal maximal de A. Entonces $\mathfrak{m} + (x) = A$, y por tanto $1 = n + rx$, con $r \in A$ y $n \in \mathfrak{m}$. Así, $1 - nx \in \mathfrak{m}$, y es una unidad, lo cual es una contradicción. □

Definición. 1.29.
Dado un anillo A y dos ideales $\mathfrak{a}, \mathfrak{b}$ decimos que son **comaximales** si $\mathfrak{a} + \mathfrak{b} = A$.

Lema. 1.30.
Sea A un anillo y $\mathfrak{b}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *ideales de A, si* $\mathfrak{b} + \mathfrak{a}_i = A$, *para todo* $1 \leq i \leq n$, *entonces*

$$A = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{b} + \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n.$$

DEMOSTRACIÓN. Ya que se verifica $\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$, basta probar que $A = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Hacemos inducción sobre n. Si $n = 1$ el resultado es cierto. Vamos a probarlo para $n = 2$, tenemos $A = \mathfrak{b} + \mathfrak{a}_1 = \mathfrak{b} + \mathfrak{a}_2$, luego existen $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$, $b_1, b_2 \in \mathfrak{b}$ tales que $1 = a_1 + b_1 = a_2 + b_2$, y haciendo el siguiente desarrollo tenemos:

$$1 = a_2 + (a_1 + b_1)b_2 = a_2 + a_1 b_2 + b_1 b_2 \in b + \mathfrak{a}_1 \mathfrak{a}_2.$$

Supongamos ahora que el resultado es cierto para n, y vamos a probarlo para $n+1$. Por hipótesis se verifica $A = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n$ y $A = \mathfrak{b} + \mathfrak{a}_{n+1}$, aplicando el resultado para el caso $n = 2$ resulta que $A = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n \mathfrak{a}_{n+1}$. □

Proposición. 1.31.
Sea A un anillo y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de A tales que $\mathfrak{a}_i + \mathfrak{a}_j = A$, $1 \leq i \neq j \leq n$, entonces

$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n.$$

DEMOSTRACIÓN. Hacemos la demostración por inducción. Si $n = 1$ el resultado es claramente cierto. Para $n = 2$, tenemos $A = \mathfrak{a}_1 + \mathfrak{a}_2$, luego existen $a_1 \in \mathfrak{a}_1$ y $a_2 \in \mathfrak{a}_2$ de manera que $1 = a_1 + a_2$. Entonces cada $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ tenemos

$$x = 1x = (a_1 + a_2)x = a_1 x + a_2 x \in \mathfrak{a}_1 \mathfrak{a}_2,$$

luego $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1 \mathfrak{a}_2$. La otra inclusión es clara. Supongamos que el resultado es cierto para n y vamos a probarlo para $n+1$. Por el lema anterior tenemos que $\mathfrak{a}_{n+1}$ verifica $\mathfrak{a}_{n+1} + \mathfrak{a}_1 \cdots \mathfrak{a}_n = A$, entonces aplicando el resultado para $n = 2$ tenemos

$$(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) \cap \mathfrak{a}_{n+1} = (\mathfrak{a}_1 \cdots \mathfrak{a}_n) \cap \mathfrak{a}_{n+1} = (\mathfrak{a}_1 \cdots \mathfrak{a}_n)\mathfrak{a}_{n+1},$$

y tenemos el resultado. □

Teorema. 1.32. (Teorema Chino del Resto)
Sea A un anillo y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales propios de A tales que $\mathfrak{a}_i + \mathfrak{a}_j = A$ para $1 \leq i \neq j \leq n$, entonces el homomorfismo canónico $f : A \longrightarrow \prod\{A/\mathfrak{a}_i \mid 1 \leq i \leq n\}$ es sobreyectivo, y $\operatorname{Ker}(f) = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

DEMOSTRACIÓN. El homomorfismo f está definido como:

$$f(a) = (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n)$$

para todo $a \in A$. Tenemos $\operatorname{Ker}(f) = \{a \in A \mid f(a) = 0\} = \{a \in A \mid a + \mathfrak{a}_i = 0$, para todo $1 \leq i \leq n\} = \{a \in A \mid a \in \mathfrak{a}_i$ para todo $1 \leq i \leq n\} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$ (en la última igualdad hemos utilizado la proposición anterior). Para ver la sobreyectividad hacemos inducción sobre n; para $n = 1$ el resultado es cierto. Lo suponemos cierto para n y vamos a probarlo para $n+1$; esto es, dados $x_1, \ldots, x_{n+1} \in A$, existe $x \in A$ tal que

$$x \equiv x_i \pmod{\mathfrak{a}_i},$$

para cada $1 \leq i \leq n+1$. Por hipótesis de inducción existe $y \in A$ tal que $y \equiv x_i \pmod{\mathfrak{a}_i}$ para cada $1 \leq i \leq n$. Dado que $\mathfrak{a}_{n+1} + \mathfrak{a}_i = A$ para todo $1 \leq i \leq n$ aplicando el último lema tenemos la igualdad $A = \mathfrak{a}_{n+1} + \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_{n+1} + \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$ y podemos escribir $y - x_{n+1}$ de la siguiente forma: $y - x_{n+1} = a + b$ con $a \in \mathfrak{a}_{n+1}$ y $b \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. Definimos entonces $x = y - b$ y vamos a comprobar que éste es el elemento que buscábamos:

$$x - x_{n+1} = y - b - x_{n+1} = a \in \mathfrak{a}_{n+1},$$

$$x - x_i = y - b - x_i = (y - x_i) - b \in \mathfrak{a}_i,$$

para todo $1 \leq i \leq n$. □

Lema. 1.33. (Lema de Nakayama)
Sea $\mathfrak{m}$ *un ideal maximal de* A *y* $\mathfrak{a}$ *un ideal finitamente generado. Si* $\mathfrak{a}\mathfrak{m} = \mathfrak{a}$ *entonces* $\mathfrak{a} = 0$.

DEMOSTRACIÓN. Como $\mathfrak{a}\mathfrak{m} = \mathfrak{a}$, si $\{a_1, \ldots, a_t\}$ es un sistema de generadores de $\mathfrak{a}$, para cada índice i se tiene una expresión $a_i = \sum_{j=1}^{t} a_{ij} a_j$, con $a_{ij} \in \mathfrak{m}$. Se tiene entonces $\big((a_{ij})_{ij} - (\delta_{ij})_{ij}\big)(a_j)_j = 0$. Por tanto $\det\big((a_{ij})_{ij} - (\delta_{ij})_{ij}\big)\mathfrak{a} = 0$. Como $\big((a_{ij})_{ij} - (\delta_{ij})_{ij}\big) = 1 - m$, para un $m \in \mathfrak{m}$, resulta ser invertible, luego $\mathfrak{a} = 0$. □

Capítulo II

Dominios de integridad

2. Divisibilidad

Definición. 2.1.
Sea D un dominio de integridad y sean $a, b \in D$ decimos que a **divide** a b, y escribimos $a|b$, si existe $c \in D$ de manera que $b = ac$.

Definición. 2.2.
Sean a y b elementos de un dominio de integridad D, decimos que a es **asociado** a b si $a|b$ y $b|a$ y lo notamos por $a \sim b$.

Definición. 2.3.
Sean a y b elementos de un dominio de integridad D, llamamos **máximo común divisor** de a y b a un elemento $c \in D$ de manera que $c|a$, $c|b$ y si existe $e \in D$ tal que $e|a$ y $e|b$, entonces $e|c$. Lo notaremos por $\text{mcd}\{a, b\}$ o (a, b). Diremos que a y b son **primos relativos** si $(a, b) = 1$.

Definición. 2.4.
Sean a y b elementos de un dominio de integridad D, llamamos **mínimo común múltiplo** y notamos por $\text{mcm}\{a, b\}$ o $[a, b]$ a un elemento $c \in D$ de manera que $a|c$, $b|c$ y si existe otro elemento $d \in D$ cumpliendo esta propiedad, entonces $c|d$.

Observación. 2.5.
La existencia o unicidad de estos elementos no está garantizada, veamos algunos ejemplos:

1. En $\mathbb{Z}[\sqrt{-5}]$ los elementos $2(1+\sqrt{-5})$ y 6 no tienen máximo común divisor ya que 2 y $(1+\sqrt{-5})$ son divisores comunes pero no existe ningún otro divisor común que sea múltiplo de ambos.

2. En el mismo anillo que el ejemplo anterior, 2 y $1+\sqrt{-5}$ tienen máximo común divisor 1 pero no tienen mínimo común múltiplo.

3. El máximo común divisor y mínimo común múltiplo no son únicos, por ejemplo en $\mathbb{Z}$ dados dos números no nulos n y m, el opuesto de un máximo común divisor (respectivamente mínimo común múltiplo) también es un máximo común divisor (respectivamente mínimo común múltiplo). Sin embargo, dados a y b elementos de un dominio de integridad D, si c y c' son

ambos máximo común divisor de a y b entonces son asociados y lo mismo pasa con el mínimo común múltiplo.

Definición. 2.6.
Un elemento a de un dominio de integridad D se llama **divisor propio** o **factor propio** de un elemento b si a no es invertible y si $a|b$ y $b \nmid a$. Un elemento se llama **irreducible** cuando no es ni cero ni invertible ni tiene factores propios.

Definición. 2.7.
Un elemento p de un dominio de integridad se dice **primo** si siempre que $p|ab$ con $a, b \in D$ entonces $p|a$ ó $p|b$.

Lema. 2.8.
En un dominio de integridad D, todo elemento primo es irreducible.

DEMOSTRACIÓN. Sea $p \in D$ primo, y a un factor propio de p, existe $b \in D$ de manera que $p = ab$, entonces $p|ab$ y por ser p primo $p|a$ o $p|b$. Ahora bien al ser a un divisor propio, es imposible $p|a$, luego tenemos $p|b$, luego $p \sim b$ y en este caso a sería una unidad, lo cual es una contradicción. Así, p no tiene factores propios, y es irreducible. □

Observación. 2.9.
El recíproco de este último resultado no es siempre cierto, por ejemplo, en $\mathbb{Z}[\sqrt{-5}]$ se tiene $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, luego 2 es irreducible y divide a $(1+\sqrt{-5})(1-\sqrt{-5})$, sin embargo no divide a ninguno de los dos factores del producto.

Definición. 2.10.
Sea D un dominio de integridad, notamos por D^* al conjunto $D \setminus \{0\}$. Un elemento $a \in D^*$ tiene una **factorización en elementos irreducibles** si existen elementos irreducibles $p_1, \ldots, p_n \in D$ tales que $a = p_1 \cdots p_n$. Dos factorizaciones en irreducibles $a = p_1 \cdots p_n$ y $a = q_1 \cdots q_m$ se llaman **esencialmente iguales** si $n = m$ y existe una permutación $\sigma \in S_n$ de manera que $q_i \sim p_{\sigma(i)}$

Dos notas finles antes de estudiar tipos especiales de dominios de integridad.

Observación. 2.11.
Sea D un dominio de integridad y $0 \neq a, b \in D$, si existe el mínimo común múltiplo de a y b, $m = [a, b]$, entonces $m \neq 0$ y $dm = ab$ con d un máximo común divisor de a y b. En particular $(a, b)[a, b] = ab$.

Observa que el recíproco no es cierto, ya que en $\mathbb{Z}[\sqrt{-5}]$ tenemos $\text{mcd}\{2, 1+\sqrt{-5}\} = 1$, pero no existe el mcm.

Definición. 2.12.
Dado D un dominio de integridad, se denomina **cuerpo de fracciones** de D y se denota $Q(D)$ al mínimo cuerpo que contiene a D, es decir, si existe otro cuerpo K conteniendo a D, entonces $Q(D) \subseteq$

K. Este cuerpo siempre existe y se construye de la siguiente manera:
Consideramos el producto cartesiano $D \times D^*$ y una relación de equivalencia en $D \times D^*$ definida para $(a,b),(c,d) \in D \times D^*$ por $(a,b) \sim (c,d)$ si $ad = cb$.

Para cada par $(a,b) \in D \times D^*$ consideramos la clase de equivalencia en $\dfrac{D \times D^*}{\sim}$ que notaremos por $\frac{a}{b}$.

Proposición. 2.13.
En la situación anterior tenemos que $\dfrac{D \times D^*}{\sim}$ *es un cuerpo con las siguientes operaciones:*

1. *Suma:*
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$
2. *Producto:*
$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

3. Dominio de ideales principales

Empezamos viendo algunos ejemplos de dominios de ideales principales que, recordamos, son dominios de integridad donde todos los ideales son principales.

Ejemplo. 3.1.
(1) $\mathbb{Z}$ es un dominio de ideales principales.
(2) $\mathbb{Z}[X]$ no es dominio de ideales principales, por ejemplo, el ideal $(2, X)$ no es principal.

Teorema. 3.2.
Sea D un dominio de ideales principales y $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots$ una cadena ascendente de ideales, existe $m \in \mathbb{N}$ tal que $(a_m) = (a_{m+k})$ para todo $k \in \mathbb{N}$.

DEMOSTRACIÓN. Ya que $\cup_i(a_i)$ es un ideal de D, entonces existe $a \in D$ de manera que $\cup_i(a_i) = (a)$, y tiene que existir $m \in \mathbb{N}^*$ con $a \in (a_m)$. De esta manera:

$$(a) \subseteq (a_m) \subseteq \cup_i(a_i) = (a).$$

Luego $(a) = (a_m) = (a_{m+k})$ para todo $k \in \mathbb{N}$. □

Definición. 3.3.
Diremos que un dominio verifica la **condición de cadena de divisores** cuando toda cadena ascendente de divisores sea estacionaria. Esto significa que si tenemos $a_0, a_1, \ldots$ una sucesión de elementos de manera que $a_1|a_0, a_2|a_1, \ldots$, existe $n \in \mathbb{N}$ tal que $a_n \sim a_{n+1} \sim a_{n+2} \cdots$ Observa que verificar la condición de cadena de divisores es equivalente verificar la **condición de cadena ascendente para ideales principales**.

Lema. 3.4.
En un dominio de ideales principales se verifica:
(1) Todo elemento irreducible genera un ideal maximal.
(2) Todo irreducible es primo.

DEMOSTRACIÓN. (1). Sea D un dominio de ideales principales y $a \in D$ un elemento irreducible. Como a no es invertible, (a) es un ideal propio de D. Tomamos $x \in D$ tal que $(a) \subseteq (x) \subseteq D$, entonces $a \in (x)$ y existe c tal que $a = cx$. Como a es irreducible, c o x es invertible. Si lo es x, entonces $(x) = D$ y si lo es c, $a \sim x$ y $(x) = (a)$, luego (a) es maximal.
(2). Si p es irreducible, entonces (p) es un ideal maximal y por lo tanto primo. Es fácil ver que si (p) es un ideal primo, entonces p es un elemento primo. Veámoslo: supongamos $p|ab$, entonces existe

c tal que $ab = pc$, luego $ab \in (p)$, por ser (p) primo, $a \in (p)$ o $b \in (p)$, o lo que es lo mismo $p|a$ ó $p|b$. □

Observa que para cada elemento primo $p \in A$ siempre se tiene que $(p) \subseteq A$ es un ideal primo.

Teorema. 3.5.
Sea D un dominio de ideales principales, se verifican:

(1) Cada ideal primo no nulo está generado por un elemento irreducible.
(2) Todo ideal primo no nulo es maximal.

DEMOSTRACIÓN. (1). Dado $\mathfrak{p} \subseteq D$ un ideal primo, entonces $\mathfrak{p} = (p)$ con $p \in D$ necesariamente primo y por tanto irreducible.
(2). Si $\mathfrak{p}$ es primo, está generado por un elemento irreducible y por tanto, por el lema, es un ideal maximal. □

4. Dominio de Factorización Única

Definición. 4.1.
Un dominio D se llama **atómico** si cada elemento no nulo y no invertible es un producto de elementos irreducibles.

Definición. 4.2.
Un dominio D es un **dominio de factorización única**, DFU, si cada elemento no nulo y no invertible a es, de forma única, un producto de elementos irreducibles, esto es, si $a = p_1 \cdots p_r = q_1 \cdots q_s$ es un producto de elementos irreducibles, entonces $r = s$ y existe $\sigma \in S_r$ tal que $p_i = q_{\sigma(i)}$ para cada $i = 1, \ldots, r$.

Como r está completamente determinado por a, lo llamamos la longitud de a, y lo representamos por $l(a)$. Observa que $l(a)$ está definido para todo elemento no nulo si definimos $l(u) = 0$, para cada elemento invertible $u \in D$.

En particular, para $a \neq 0$, si b es un factor propio de a, entonces $l(b) < l(a)$.

Ejemplo. 4.3.
El anillo $\mathbb{Z}[\sqrt{10}]$ es un dominio atómico y no un dominio de factorización única. Por ejemplo, $6 = 2 \times 3 = (4 + \sqrt{10})(4 - \sqrt{10})$ tiene dos factorizaciones en irreducibles distintas.

Teorema. 4.4.
Todo dominio de ideales principales es un dominio de factorización única.

DEMOSTRACIÓN. Sea D un dominio de ideales principales y $a \in D$ un elemento no nulo que no es invertible, vamos a probar que a tiene un factor irreducible.
Si a es irreducible tenemos el resultado y si no lo es, tenemos una factorización $a = a_1 a_1'$, con a_1 y a_1' no invertibles. Si a_1 es irreducible lo tenemos y si no volvemos a reiterar el proceso. Así tenemos una sucesión de factores $a_1, a_2, \ldots$, si alguno es irreducible hemos acabado y si no como $a_i | a_{i-1}$ para cada $i \in \mathbb{N}$, tenemos una cadena de ideales $(a) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$ Sabemos que esta cadena es estacionaria, esto es, existe $m \in \mathbb{N}$ de manera que $(a_m) = (a_{m+k})$ para todo $k \in \mathbb{N}$. Tenemos entonces $a_m \sim a_{m+1}$, luego a'_{m+1} es invertible, lo cual es una contradicción, luego sí que encontramos un factor irreducible.

Sea a un elemento no nulo y no invertible, si a es irreducible sabemos que tiene una factorización única en irreducibles luego suponemos que tampoco es irreducible. Si a no es irreducible, aplicando el resultado anterior existe un factor irreducible de a, lo llamamos p_1. Así, $a = p_1 b_1$, si hacemos lo mismo con b_1 tendremos que es irreducible o tiene un factor irreducible, siguiendo el proceso tendríamos $b_1, b_2, \ldots$ alguno de ellos irreducible ya que si ninguno lo fuera esta sucesión se prolongaría indefinidamente. Tendríamos $b_i | b_{i-1}$ para cada $i \in \mathbb{N}$, luego una cadena ascendente

$$(a) \subsetneq (b_1) \subsetneq (b_2) \subsetneq \cdots$$

Como estamos en un dominio de ideales principales, esta cadena es finita, y existe m tal que b_m es irreducible, y a tiene una factorización en irreducibles.

Probamos ahora que la factorización es única, sea $a = p_1 \cdots p_r = q_1 \cdots q_s$ con $p_1, \ldots, p_r, q_1, \ldots, q_s$ irreducibles. Si $r = 1$, entonces q_1 es irreducible, luego $s = 1$ y tenemos $p_1 = q_1$. Ahora lo suponemos cierto para $r-1$ y lo comprobamos para $r > 1$. Consideramos p_r, que por ser irreducible, es también primo y por tanto existe $j \in \{1, \ldots, s\}$ tal que $p_r | q_j$. Sin pérdida de generalidad podemos suponer $j = s$ y tenemos $p_r \sim q_s$, es decir, existe $u \in U(D)$ de manera que $p_r = uq_s$ y tenemos

$$p_1 \cdots p_{r-1} u q_s = q_1 \cdots q_s,$$

y simplificando

$$p_1 \cdots p_{r-1} u = q_1 \cdots a_{s-1}.$$

Aplicando la hipótesis de inducción se obtiene el resultado. □

Lema. 4.5.
Si D es un dominio de factorización única, entonces:

(1) Cada elemento irreducible es primo.
(2) Cada par de elementos tiene un máximo común divisor.
(3) Toda cadena de divisores es estacionaria.

DEMOSTRACIÓN. (1). Sea p en D un elemento irreducible y supongamos que $p|ab$ para $a, b \in D$. Si a es una unidad, p esta asociado con b y por tanto lo divide y lo mismo pasa si es una unidad b. Suponemos entonces que ni a ni b son unidades, entonces existen factorizaciones únicas en irreducibles, $a = p_1 \ldots p_r$ y $b = q_1 \ldots q_s$.

Ya que $p|ab$, existe $c \in D$ de manera que $ab = pc$, luego $(p_1 \cdots p_r)(q_1 \cdots q_s) = ab = pc$. Así, por la unicidad de descomposición, existe $i \in \{1, \ldots, r\}$ ó $j \in \{1, \ldots, s\}$ tal que $p \sim p_i$ ó $p \sim q_j$, esto es que $p|a$ ó $p|b$, luego p es un elemento primo.

(2). En un dominio de factorización única, el máximo común divisor se expresa fácilmente utilizando la descomposición en irreducibles de los elementos. El máximo común divisor sería el producto de los irreducibles comunes a los dos elementos elevados al mínimo exponente.

(3). Sea $(a_1) \subseteq (a_2) \subseteq \cdots$ una cadena ascendente de divisores. Tenemos $a_i = b_i a_{i+1}$. Si la cadena no fuese estacionaria, podemos suponer que es estrictamente ascendente, y para cada índice i existe un producto de factores irreducibles h_i tal que $a_i = h_i a_{i+1}$. Si $a_1 \neq 0$, sea $s = l(a_1) < \infty$; como se tiene la relación $a_1 = h_1 a_2 = h_1 h_2 a_3 = \cdots$, resulta que llegaremos a un índice j tal que $l(h_1 h_2 \cdots h_j) > s = l(a_1)$, lo que es ua contradicción. □

Definición. 4.6.
Diremos que un dominio de integridad verifica la **condición de primo** cuando cada elemento irreducible sea primo.

Definición. 4.7.
Diremos que un dominio de integridad es **GCD** cuando cada par de elementos del dominio tenga máximo común divisor. Equivalentemente, decimos que es **LCM** cuando cada par de elementos tenga mínimo común múltiplo.
Todo GCD es un LCM, y viceversa. Ver [1].

Teorema. 4.8.
Sea D un dominio de integridad. Son equivalentes:
(a) D es un dominio de factorización única.
(b) Cada elemento no nulo y no invertible de D es un producto de elementos primos.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si D es un dominio de factorización única, todo elemento no nulo y no invertible es producto de irreducibles, como todo irreducible es primo, tenemos lo que buscamos.
(b) $\Rightarrow$ (a). Como en un dominio de integridad todo elemento primo es irreducible, ya tenemos que todo elemento no nulo y no invertible es producto de irreducibles, nos queda ver que este es único. Para ello, consideramos un elemento $a \in D$ con dos factorizaciones:

$$a = p_1 \cdots p_t = q_1 \cdots q_s.$$

Si $t = 1$, entonces por ser elementos primos, necesariamente $s = 1$ y $p_1 = q_1$. Lo suponemos cierto para $t-1$ con $t > 1$, como $p_1 | q_1 \cdots q_s$, existe $i \in \{1, \ldots, s\}$ de manera que $p_1 | q_i$, podemos suponer,sin pérdida de generalidad, $i = 1$, y de esta manera $p_1 \sim q_1$, luego $p_1 = uq_1$ con u un elemento invertible de D. Entonces $p_2 \cdots p_t = uq_2 \cdots q_s$, de aquí deducimos $t = s$ y la existencia de σ:{2,...,t}$\longrightarrow${2,...,t} de manera que $p_i \sim q_{\sigma(i)}$. Extendiendo esta aplicación a $\{1, \ldots, t\}$ de forma obvia, $\sigma(1) = 1$, tenemos el resultado. □

Señalamos que las factorizaciones en elementos primos son necesariamente únicas.

Lema. 4.9.
Si D verifica la condición de cadena de divisores, D es un dominio atómico.

DEMOSTRACIÓN. Vamos a ver que cada elemento de D no nulo y no invertible es producto de elementos irreducibles. Sea $a \in D$ no nulo y no invertible, como a no es irreducible existe una factorización propia $a = a_0 a_0'$, si a_0 no es irreducible (en caso de serlo ya tendríamos un factor irreducible), tenemos una factorización propia $a_0 = a_1 a_1'$. Así nos queda una sucesión $a_0, a_1, a_2, \ldots$ que en caso de no encontrar ningún irreducible sería infinita lo cual es imposible, luego tenemos que todo elemento no nulo y no invertible tiene un factor irreducible.

Ahora, dado un elemento no nulo y no invertible $a \in D$ sabemos que tiene una factorización de la forma $a = p_1 a_1$ con p_1 irreducible. Si a_1 es irreducible ya hemos acabado, en caso de no serlo sabemos que tiene una factorización de la forma $a_1 = p_2 a_2$ con p_2 irreducible. Repitiendo el proceso, si no encontramos a_k irreducible tendríamos una cadena de divisores infinita $a_1, a_2, \ldots$, lo cual es una contradicción. Luego a tiene una factorización en irreducibles. □

Vamos a ver una serie de caracterizaciones de los dominios de factorización única que nos serán muy útiles para saber si un dominio es dominio de factorización única de una manera más fácil de la que sería comprobar la definición.

Teorema. 4.10.
Sea D un dominio de integridad. Son equivalentes:

(a) D es un dominio de factorización única.
(b) D verifica la condición de primo y de cadena de divisores.
(c) D es GCD y dominio atómico.
(d) D verifica la condición de primo y es atómico.
(e) D es LCM y cumple la condición de cadena de divisores.

DEMOSTRACIÓN. (a) ⇒ (b), (c). Ya lo hemos probado.

(b) ⇒ (c). También lo hemos visto.

(c) ⇒ (a). Como ya tenemos dominio atómico, solo tenemos que ver la unicidad de la factorización. Sea $a \in D$ no nulo y no invertible con dos descomposiciones

$$a = p_1 \cdots p_n = q_1 \cdots q_s.$$

Hacemos inducción sobre n. Si $n = 1$, como p_1 es primo, existe i tal que $p_1 | q_i$. Podemos suponer sin pérdida de generalidad que $i = 1$ y $q_1 = p_1 u$ con u unidad de D. Así, tendríamos $1 = u q_2 \ldots q_s$, luego $s = 1$ y las dos factorizaciones son esencialmente la misma.

Sea $n > 1$ y la afirmación cierta para los naturales menores que n, igual que antes existe i tal que $p_1 | q_i$ y sin pérdida de generalidad podemos poner $i = 1$ y $q_1 = p_1 u$ con u un elemento invertible. Entonces se tiene $p_2 \cdots p_n = u q_2 \cdots q_t$ y por hipótesis de inducción las dos factorizaciones son esencialmente la misma.

(d) ⇒ (c). Por ser atómico, tenemos factorizaciones en irreducibles, y por tanto primos. A partir de ahí, sabemos como calcular el máximo común divisor.

(a) ⇒ (e). Ya que en un DFU existen en mcm y se cumple la condición de cadena de divisores.

(e) ⇒ (c). Igual que antes, todo LCM es GCD y en el lema anterior hemos probado que si un dominio cumple la condición de cadena de divisores, es atómico.

(a) ⇒ (d) Por ser dominio de factorización única tenemos que es atómico y que cumple la condición de primo. □

Lema. 4.11.
Sea D un dominio de integridad. Son equivalentes:

(a) D es un dominio de factorización única
(b) Cada ideal primo no nulo contiene un elemento primo no nulo, esto es, un ideal primo principal no nulo.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Sea $\mathfrak{a}$ un ideal primo no nulo y $p \in \mathfrak{a}$ un elemento no invertible. Tenemos $p = p_1 \cdots p_t$ con p_i irreducible. Como hemos visto, cada p_i es primo y como $\mathfrak{a}$ es un ideal primo, existe i tal que $p_i \in \mathfrak{a}$.

(b) $\Rightarrow$ (a). Sea $C = \{a \in D \mid a \text{ es invertible ó } a = p_1 \cdots p_t \text{ producto de primos}\}$. Vamos a ver que este conjunto es D^*. Es obvio que C es multiplicativamente cerrado, entonces sabemos que existe un ideal primo $\mathfrak{a}$ que es maximal entre los que verifican $\mathfrak{a} \cap C = \emptyset$. Por hipótesis, $\mathfrak{a}$ tiene un elemento primo, lo cual es una contradicción con que la intersección sea vacía, luego $C = D^*$. Tenemos entonces que D es un dominio de factorización única, ya que cada elemento no nulo y no invertible es producto de primos. □

Definición. 4.12.
Diremos que un ideal no trivial es **minimal** cuando no contenga ningún otro ideal no nulo, y es un ideal **primo minimal** si es primo y no contiene propiamente ningún ideal primo.

Así, con este último lema hemos llegado a la conclusión de que un dominio es dominio de factorización única si, y solo si, todo ideal primo minimal es un ideal primo principal. Veamos que cada ideal principal es minimal:

Proposición. 4.13.
En un dominio de factorización única, todo ideal primo principal es un ideal primo minimal.

DEMOSTRACIÓN. Si (p) es un ideal primo principal, ya sabemos que necesariamente p tiene que ser primo, consideramos un ideal primo $\mathfrak{a} \subsetneq (p)$ que es propio. Tenemos que para cada $x \in \mathfrak{a}$, $x = ph_1 \in \mathfrak{a}$ con $h_1 \in D$, entonces $h_1 \in \mathfrak{a} \subset (p)$ implica $h_1 = ph_2$ con $h_2 \in D$. Tenemos por tanto $x = p^2h_2$, y así $h_2 \in \mathfrak{a} \subset (p)$. Siguiendo el proceso llegamos a una expresión $x = p^n h_n$ para cada $n \in \mathbb{N}^*$ y $h_n = ph_{n+1}$. Como consecuencia, la longitud de los divisores de x no está acotada, lo que es una contradicción. □

Teorema. 4.14.
Sea D un dominio de integridad, son equivalentes:

(a) D es un dominio de factorización única en el que cada ideal primo no nulo es maximal.
(b) D es un dominio de ideales principales.

DEMOSTRACIÓN. (b) $\Rightarrow$ (a). Trivial
(a) $\Rightarrow$ (b). Dado un ideal $\mathfrak{a} \subsetneq D$, consideramos $\Sigma = \{Da \mid \mathfrak{a} \subseteq Da\}$. Este conjunto es no vacío, ya que por hipótesis cada ideal primo no nulo es maximal, está generado por un elemento irreducible y $\mathfrak{a}$ está contenido en un ideal maximal no nulo.
Tomamos una cadena descendente de divisores de Σ, $(a_1) \supseteq (a_2) \supseteq \cdots$, se tiene $a_2 = a_1x_1, a_3 = a_2x_2, \ldots$ Si ninguno de estos factores x_i es invertible, tenemos que a_t tiene al menos t factores no invertibles. Ahora bien, para cada $t \in \mathbb{N}$ tenemos $0 \neq a \in (a_t)$, luego $a = b_t a_t$ y tiene al menos t factores no invertibles, lo cual es una contradicción dado que D es un dominio de factorización única, luego la cadena es estacionaria. Tenemos entonces que en Σ hay elementos minimales.
Sea $\mathfrak{a} \subseteq Da$ con Da minimal en Σ, entonces $\mathfrak{a} = \mathfrak{a}_1 a$. Si $\mathfrak{a}_1 \subsetneq D$, existe un ideal principal propio tal que $\mathfrak{a}_1 \subseteq Db$, y tendríamos $\mathfrak{a} \subseteq Dba \subseteq Da$, y por la minimalidad de Da tenemos $Dba = Da$, por lo que b es invertible, lo cual es una contradicción ya que Db es propio. Luego $\mathfrak{a}_1 = D$ y $\mathfrak{a} = Da$, es decir, es un ideal principal. Como era un ideal arbitrario tenemos que todos los ideales son principales y por tanto D es un dominio de ideales principales. □

Podemos entonces plantearnos la pregunta siguiente a partir de la proposición 4.13: ¿Cuándo la condición de que un ideal primo principal sea minimal caracterizara a un dominio de factorización única ?
Para responder a esta pregunta vamos a hacer la definición de dominio noetheriano y análogamente artiniano:

Definición. 4.15.
Diremos que un anillo es **noetheriano** cuando para cualquier cadena de ideales

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots,$$

existe $n \in \mathbb{N}$ de manera que $\mathfrak{a}_n = \mathfrak{a}_{n+k}$ para todo $k \in \mathbb{N}$.

Definición. 4.16.
Diremos que un anillo es **artiniano** cuando para cualquier cadena de ideales

$$\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \cdots,$$

existe $n \in \mathbb{N}$ de manera que $\mathfrak{a}_n = \mathfrak{a}_{n+k}$ para todo $k \in \mathbb{N}$.

Definición. 4.17.
Llamaremos **dimensión de Krull** de un anillo (noetheriano o artiniano) al supremo de la longitud de cadenas de ideales primos. Cuando posteriormente hablemos de dimensión de un anillo, nos estaremos refiriendo a la dimensión de Krull.

Lema. 4.18.
Un anillo A es noetheriano si, y solo si, todo ideal es finitamente generado.

DEMOSTRACIÓN. ($\Rightarrow$). Sea $\mathfrak{a}$ un ideal de A. Tomamos un elemento $x_1 \in \mathfrak{a}$, si $(x_1) = \mathfrak{a}$ hemos acabado y si no lo es, tomamos $x_2 \in \mathfrak{a}$ de manera que $x_2 \notin (x_1)$. Así, formamos (x_1, x_2). Si este es todo $\mathfrak{a}$ habremos acabado y si no tomamos otro elemento. Así tenemos un algoritmo por el cual conseguimos una cadena ascendente:

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$$

Si el algoritmo acabara en algún momento, tendríamos $\mathfrak{a} = (x_1, \ldots, x_n)$ y por tanto el ideal sería finitamente generado. Si el algoritmo fuese infinito, tendríamos una cadena ascendente infinita de ideales de A, que es noetheriano, lo cual es imposible. Así el algoritmo debe terminar y el ideal ser finitamente generado.
($\Leftarrow$). Sea ahora una cadena ascendente de ideales de A:

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$$

Consideramos el ideal $\mathfrak{a} = \cup_{i\in\mathbb{N}}\mathfrak{a}_i$ que sabemos es finitamente generado por hipótesis. Tomamos entonces un conjunto de generadores de $\mathfrak{a}$, $\{x_1, \ldots, x_n\}$. Cada uno de los elementos de ese conjunto pertenecen a un ideal de la cadena, como la cadena es ascendente, si ponemos $x_i \in \mathfrak{a}_{n_i}$, tenemos $\{x_1, \ldots, x_n\} \subseteq \mathfrak{a}_{\text{máx}\{n_i |\, i\in\{1,\ldots,n\}\}}$. Tenemos entonces:

$$\mathfrak{a} = (x_1, \ldots, x_n) \subseteq \mathfrak{a}_{\text{máx}\{n_i |\, i\in\{1,\ldots,n\}\}} \subseteq \cup_{i\in\mathbb{N}}\mathfrak{a}_i = \mathfrak{a}.$$

Es claro entonces que la cadena es estacionaria a partir de $\mathfrak{a}_{\text{máx}\{n_i |\, i\in\{1,\ldots,n\}\}}$. Como era una cadena cualquiera, tenemos que el anillo es noetheriano. □

Lema. 4.19.
Sea D un dominio noetheriano, son equivalentes:
(a) D es un dominio de factorización única
(b) Todo ideal primo principal es un ideal primo minimal.

DEMOSTRACIÓN. La implicación de (a) hacia (b) acabamos de probarla, luego solo tenemos que ver la otra:
En general, no tenemos que un ideal primo minimal sea principal, la condición de noetheriano es suficiente para que se cumpla. Dados $\mathfrak{p} \subset (p)$. Para cada $x \in \mathfrak{p}$ tenemos $x = p^n h_n$ para cada $n \in \mathbb{N}^*$. Tenemos una cadena ascendente $(h_1) \subset (h_2) \subset \cdots \subset (h_n) \subset \cdots$, que por hipótesis es estacionaria, esto es, existe $t \in \mathbb{N}$ tal que $(h_t) = (h_{t+k})$ para todo natural k y para cada $s \in \mathbb{N}$ existe $u_s \in D$ invertible, tal que $h_t = u_s h_{t+s}$, lo que es una contradicción dado que $h_t = p h_{t+1}$. □

5. Dominios euclídeos

El problema con los DIP y los DFU es que no podemos hacer cálculos, por ejemplo, no tenemos algoritmos para calcular el mcd ó el mcm de dos elementos, aunque sabemos que existen. Para corregir esta dificultad introducimos un nuevo tipo de dominos de integridad.

Definición. 5.1.
Un dominio de integridad D se llama **euclídeo** si existe una aplicación $\delta : D^* \longrightarrow \mathbb{N}$, la **aplicación grado**, tal que:
(1) Si $a, b \in D^*$ verifican $a|b$, entonces $\delta(a) \leq \delta(b)$
(2) **Algoritmo de la división**. Para cada $n, m \in D$ con $n \neq 0$ existen $c, r \in D$ tales que $m = nc + r$ con r=0 ó $\delta(r) < \delta(n)$

Ejemplo. 5.2.
(1) El anillo $\mathbb{Z}$ de los números enteros es un dominio euclídeo siendo la aplicación grado el valor absoluto.
(2) Si K es un cuerpo, el anillo de polinomios con coeficientes en K es un dominio euclídeo con aplicación dada por $\delta(f) = 2^{\text{grad}(f)}$.
(3) El anillo $\mathbb{Z}[i]$ de los enteros de Gauss es un dominio euclídeo con aplicación grado definida como $\delta(a + bi) = a^2 + b^2$ para cada $a + bi \in \mathbb{Z}[i]$.

Vemos ahora la relación entre estos dominios y los que hemos estudiado anteriormente:

Proposición. 5.3.
Si D es un dominio euclídeo, entonces todo ideal es principal, es decir, D es dominio de ideales principales.

DEMOSTRACIÓN. Dado un ideal, $\mathfrak{a} \subset D$, consideramos el conjunto $A = \{\delta(a) \mid \ a \in \mathfrak{a}\}$. Como es un subconjunto de $\mathbb{N}$ tendrá mínimo, lo llamamos d, y tomamos un elemento $a \in \mathfrak{a}$ de manera que $\delta(a) = d$. Vamos a ver que este elemento genera a todo el ideal $\mathfrak{a}$. Es claro que $(a) \subset \mathfrak{a}$. Veamos la otra inclusión: Sea $x \in \mathfrak{a}$, existen $c, r \in D$ de manera que $x = ac + r$ con $r = 0$ ó $\delta(r) < \delta(a)$. Si $r \neq 0$, de la relación $r = x - ac \in \mathfrak{a}$, llegamos a una contradicción ya que a era el elemento de menor grado en $\mathfrak{a}$. Tenemos entonces que $r = 0$ y por tanto $x \in (a)$, luego el ideal es principal. □

Teorema. 5.4.
Todo dominio euclídeo es un dominio de factorización única.

DEMOSTRACIÓN. Esto es claro ya que todo dominio de ideales principales es de factorización única, luego por la proposición anterior tenemos el resultado. □

6. Anillo de polinomios

Existen construcciones para las que DE se mantiene, por ejemplo si K es un cuerpo, $K[X]$ es un DE, pero esta situación no es general; veamos que existen propiedades que se mantienen por la construcción de polinomios.

Definición. 6.1.
Dado un anillo A y una indeterminada X, definimos el **anillo de polinomios** $A[X]$ como el conjunto $\left\{\sum_{i=0}^{t} a_i X^i \mid a_i \in A\right\}$.

Definición. 6.2.
Sea A un GCD, un polinomio $f = a_0 + a_1X + \cdots + a_nX^n$ en A[X] se dice **primitivo** cuando el máximo común divisor de $a_0, \ldots, a_n$ es 1. A este máximo común divisor se le llama el **contenido** de f, y lo representamos por $\mathbf{c}(f)$. Tenemos que un polinomio f es primitivo cuando $\mathbf{c}(f) = 1$. En particular, en un GCD cada polinomio $f \in D[X]$ se escribe como $f = \mathbf{c}(f)f'$, siendo f' un polinomio primitivo.

Uno de nuestros objetivos principales es saber cuando podemos factorizar un polinomio. Veamos entonces algunos resultados en anillos de polinomios que son dominio de factorización única.

Teorema. 6.3. (Lema de Gauss)
En un dominio de factorización única, el producto de polinomios primitivos es primitivo.

DEMOSTRACIÓN. Sea $f = a_nx^n + \cdots + a_1x + a_0$ y $g = b_mx^m + \cdots + b_1x + b_0$ dos polinomios primitivos. Si el producto no fuese primitivo tendríamos un primo p que divide a todos los coeficientes del producto. Como tanto f como g son primitivos, sabemos que este elemento p no puede dividir a todos los coeficientes de f ni de g, tomamos i como el menor índice de manera que no divida a a_i y hacemos lo análogo con g obteniendo j. Tendríamos que p divide al coeficiente de grado $i + j$ del producto de f y g, luego a todos sus sumandos. Luego p es primo y divide a a_ib_j, tenemos por tanto que $p|a_i$ o $p|b_j$, lo cual es una contradicción y por lo tanto fg es primitivo. □

Corolario. 6.4.
Si D es un dominio de factorización única, para cada par de polinomios $f, g \in D[X]$ se tiene que $\mathbf{c}(fg) = \mathbf{c}(f)\,\mathbf{c}(g)$.

Lema. 6.5.
Sea D un GCD, con cuerpo de fracciones K:

(1) Para cada polinomio no nulo f de $K[X]$ existen $k \in K$ y $g \in D[X]$ polinomio primitivo de manera que $f = kg$.
(2) Si tenemos otra factorización del tipo anterior $f = k_2 g_2$, entonces existe una unidad u en D de manera que $g_2 = ug$ y $k_2 = u^{-1}k$.

DEMOSTRACIÓN. (1). Si f es un polinomio no nulo de $K[X]$, sabemos que existe $b \in D$ tal que $bf \in D[X]$. Además, también sabemos que existe $a \in D$ y un polinomio primitivo $g \in D[X]$ de manera que $bf = ag$, luego tomando $k = \frac{a}{b}$, tenemos $f = kg$.
(2). Si $f = kg = k_2 g_2$, siendo estas factorizaciones del tipo anterior, existe $b \in D$ de manera que $bkg = bk_2 g_2 \in D[X]$, y tenemos el resultado. □

Corolario. 6.6.
Sea D un GCD, con cuerpo de fracciones K, cada dos polinomios $f, g \in D[X]$ primitivos y asociados en $K[X]$ son también asociados en $D[X]$.

DEMOSTRACIÓN. Si existe $0 \neq k \in K$ de manera que $f = kg$, si $k = \frac{a}{b}$ se tiene $bf = ag$. Si $\mathbf{c}(bf) = \mathbf{c}(ag)$, entonces $a \sim b$ y tenemos el resultado. □

Lema. 6.7.
Sea D un GCD, con cuerpo de fracciones K. Un polinomio irreducible en $D[X]$ es también irreducible en $K[X]$.

DEMOSTRACIÓN. Sea f irreducible en $D[X]$, si f no fuese irreducible en $K[X]$, existen f_1, f_2 polinomios de $K[X]$ de manera que $f = f_1 f_2$, luego existen $0 \neq a_1, a_2 \in D$ de manera que $a_1 f_1, a_2 f_2 \in D[X]$, pero entonces tendríamos que en $D[X]$ $a_1 a_2 f = (a_1 f_1)(a_2 f_2)$, lo cual es una contradicción y por tanto f es irreducible también en $K[X]$. □

Teorema. 6.8.
Sea D un anillo, son equivalentes:

(a) D es un dominio de integridad.
(b) $D[X]$ es un dominio de integridad.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Sean $fg = 0$ y $f \neq 0, g \neq 0$. Ponemos $n = \text{grad}(f)$ y $m = \text{grad}(g)$ y a_n, b_m coeficientes líderes de f y g respectivamente. Como $a_n, b_m \neq 0$, entonces $a_n b_m \neq 0$ y por tanto $fg \neq 0$.
(b) $\Rightarrow$ (a). Sea $a, b \neq 0$ $a, b \in D$ entonces dado que $ab \neq 0$ en $D[X]$, $ab \neq 0$ en D. □

Teorema. 6.9.
Si D es un dominio de factorización única entonces $D[X]$ es dominio de factorización única.

DEMOSTRACIÓN. Primero veremos que todo polinomio primitivo en $D[X]$, de grado positivo, tiene un factor irreducible. Sea f un polinomio primitivo, si es irreducible ya hemos acabado, y si no lo es sabemos que tiene una factorización de la forma $f = f_1 f_2$ con f_1, f_2 de grado menor o igual que el de f, luego reiterando el proceso que evidentemente es finito encontramos un factor irreducible.
Una vez que sabemos eso, dado cualquier polinomio primitivo f sabemos que tiene un factor irreducible, ponemos $f = f_1 g$ con f_1 irreducible y g obviamente primitivo, si g es irreducible ya habremos acabado y si no, este tendrá otro factor irreducible. Como cada factor es de grado menor, este proceso es finito y tendremos una factorización en irreducibles de cualquier polinomio primitivo.
Ahora dado cualquier polinomio f, podemos escribirlo como $f = \mathbf{c}(f) f_1$ con f_1 primitivo. Como D es dominio de factorización única, podemos factorizar $\mathbf{c}(f)$ y, como hemos visto antes, hacemos la factorización en irreducibles de f_1. Asi, juntando las dos tendremos una factorización en irreducibles de f.
Ahora nos queda ver que las factorizaciones son únicas. Sea f un polinomio de $D[X]$ y dos factorizaciones de este en irreducibles,

$$f = f_1 \cdots f_n = g_1 \cdots g_m.$$

Consideramos estas factorizaciones en $K[X]$ siendo K el cuerpo de fracciones de D. Sabemos que $K[X]$ es un dominio euclídeo definiendo la división habitual luego los irreducibles son primos. Además, en $K[X]$, la factorización es única y por tanto $n = m$ y cada f_i es asociado a $g_{\sigma(i)}$ siendo σ una permutación de n elementos. Así, como hemos visto en un lema anterior, también son asociados en $D[X]$ y por tanto las dos factorizaciones son esencialmente iguales. □

Nuestro objetivo en lo que sigue es extender la teoría más allá de los DFU. Veamos, por ahora, algunos resultados técnicos.

Proposición. 6.10.
Sea D un dominio de integridad, son equivalentes:

(a) D verifica la condición de cadena ascendente para ideales principales.
(b) $D[X]$ verifica la condición de cadena ascendente para ideales principales.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Sea $(f_1) \subseteq (f_2) \subseteq \cdots$ cadena ascendente de $D[X]$. Si K es el cuerpo de fracciones de D, en $K[X]$ existe $t \in \mathbb{N}$ tal que $(f_t) = (f_{t+k})$ para cada $k \in \mathbb{N}$, por tanto existe g_k tal que $f_{t+k} = g_k f_t$ para cada $k \in \mathbb{N}$. Como $f_{t+k} | f_t$ resulta que g_k es invertible en $K[X]$ para cada $k \in \mathbb{N}$, luego $g_k \in K$. En particular, el grado de f_t y de f_{t+k} son iguales para todo $k \in \mathbb{N}$. Por otra parte $f_{t+k} | f_t$ en $D[X]$ luego existe h_k de manera que $f_t = h_k f_{t+k}$ para cada $k \in \mathbb{N}$. Como sabemos que f_t y f_{t+k} tienen el mismo grado, obtenemos $h_k \in D$ para cada $k \in \mathbb{N}$. Como $f_{t+k} = g_k f_t$ y $f_t = h_k f_{t+k}$, tenemos $g_k = \frac{1}{h_k}$ para cada $k \in \mathbb{N}$. Tenemos entonces una sucesión $\{h_k\}$ y resulta $f_t = h_1 f_{t+1} = h_2 f_{t+2} = \cdots$, como $f_{t+2} | f_{t+1}$, tenemos $h_2 | h_1$ e igual para el resto $h_{t+k} | h_{t+k+1}$, obteniendo una cadena de ideales principales en D: $(h_1) \subseteq (h_2) \subseteq \cdots$, que sabemos es estacionaria, es decir, existe $m \in \mathbb{N}$ de manera que $(h_m) = (h_{m+s})$ para cada $s \in \mathbb{N}$. Por tanto, existe un elemento invertible u_k de manera que $u h_{m+s} = h_m$. Tenemos entonces que $f_t = h_m f_{t+m} = u_1 h_{m+1} f_{t+m} = h_{m+1} f_{t+m+1}$ de donde se deduce $f_{t+m+1} = u_1 f_{t+m}$. Para el resto se hace igual y nos queda $f_{t+m+k} = u_k f_{t+m}$, luego la cadena ascendente es estacionaria.
(b) $\Rightarrow$ (a). Dada una cadena ascendente de ideales principales en D, $(a_1) \subseteq (a_2) \subseteq \cdots$, si la consideramos en $D[X]$, entonces $t \in \mathbb{N}$ de manera que $(a_t) = (a_{t+k})$ para todo $k \in \mathbb{N}$ y existen $g_k \in D[X]$ tales que $a_t = g_k a_{t+k}$ para todo $k \in \mathbb{N}$. Así, $g_k \in D$ y la cadena es también estacionaria en D. □

Si no imponemos la condición de ser GCD, no podemos hablar de contenido; vamos pues a extender esta definición.

Definición. 6.11.
Dado un polinomio f de un anillo de polinomios $A[X]$, llamamos el ideal **contenido** como el ideal generado por los coeficientes del polinomio f. Lo notaremos por $\mathbf{C}(f)$.

Una extensión del Lema de Gauss es el siguiente resultado.

Teorema. 6.12. (Lema de Dedekind-Mertens)
Sea A un anillo y $f, g \in A[X]$ con $\operatorname{grad}(g) = m$, entonces $\mathbf{C}(f)^m \mathbf{C}(fg) = \mathbf{C}(f)^{m+1} \mathbf{C}(g)$.

DEMOSTRACIÓN. Siempre se da $\mathbf{C}(fg) \subseteq \mathbf{C}(f)\mathbf{C}(g)$, y por tanto $\mathbf{C}(f)^m \mathbf{C}(fg) \subseteq \mathbf{C}(f)^{m+1} \mathbf{C}(g)$. Veamos la otra inclusión: Lo probaremos por inducción sobre $n = \operatorname{grad}(f)$ y $m = \operatorname{grad}(g)$. Si $n = 0$ o $m = 0$, el resultado es cierto para arbitrario n ó m respectivamente. Si uno de los dos polinomios es un monomio, entonces el resultado también se da sea cual sea el otro. Suponemos entonces

f, g arbitrarios y el resultado cierto para $n < \text{grad}(f) = r$ y para $m < \text{grad}(g) = s$. Si notamos $f = a_0 + \ldots + a_r X^r$ y $g = b_0 + \ldots + b_s X^s$. Definimos:

- $f_1 = f - a_r X^r$
- $g_1 = g - b_s X^s$
- $h = fg = \sum_{k=0}^{r+s} c_k X^k$
- $h_1 = f_1 g = \sum_{k=0}^{r+s-1} c_{1,k} X^k$
- $h_2 = f g_1 = \sum_{k=0}^{r+s-1} c_{2,k} X^k$

Tenemos $\mathbf{C}(h_1) = \mathbf{C}(f_1 g) = (c_{1,0}, \ldots, c_{1,r+s-1}) = (c_0, \ldots, c_{r-1}, c_r - b_0 a_r, \ldots, c_{r+s-1} - b_{s-1} a_r) \subseteq (c_0, \ldots, c_{r+s}) + (b_0, \ldots, b_{s-1}) a_r = \mathbf{C}(fg) + \mathbf{C}(g) a_r$.
De igual forma se tiene $\mathbf{C}(h_2) \subseteq \mathbf{C}(fg) + \mathbf{C}(f) b_s$.
Tenemos que $\mathbf{C}(f)^{s+1}\mathbf{C}(g)$ está generado por elementos de la forma $a_0^{n_0} \cdots a_r^{n_r} b_i$, con $\sum_{j=0}^{r} n_j = s+1$. Vamos a ver que cada elemento de esta forma está contenido en $\mathbf{C}(f)^s \mathbf{C}(fg)$. Dividimos en casos:

- $n_r \neq 0, i = s$, entonces $a_0^{n_0} \cdots a_r^{n_r} b_s$ es múltiplo de $a_r b_s \in \mathbf{C}(fg)$ y tenemos entonces el resultado.
- $n_r \neq 0, i < s$, entonces $a_0^{n_0} \cdots a_r^{n_r} b_i \in \mathbf{C}(f)^s a_r \mathbf{C}(g_1) \subseteq \mathbf{C}(f)^s \mathbf{C}(fg)$
- $n_r = 0$, entonces $a_0^{n_0} \cdots a_{r-1}^{n_{r-1}} b_i \in \mathbf{C}(f_1)^{s+1} \mathbf{C}(g) \subseteq \mathbf{C}(f_1)^s \mathbf{C}(fg)$

Tenemos entonces la otra inclusión y por tanto el resultado. □

Definición. 6.13.
Dado un anillo A y $X_1, \ldots, X_n$ un conjunto de indeterminadas, definimos el **anillo de polinomios** en esas indeterminadas como el conjunto de expresiones formales finitas

$$\left\{ \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X^{i_1} \cdots X^{i_n} \mid a_{i_1,\ldots,i_n} \in A \right\}.$$

7. Ejercicios de Atiyah-Macdonald

Los siguientes resultados aparecen como ejercicios en el libro de Atiyha–Macdonald, ver [3].

Ejercicio 1

Sea x un elemento nilpotente de un anillo A. Entonces $1+x$ es una unidad de A. Así podemos deducir que la suma de un elemento nilpotente y una unidad es una unidad.

DEMOSTRACIÓN. Existe $n \in \mathbb{N}$ tal que $x^n = 0$ entonces:

(1) Si n es impar: 1=$1 + x^n = (1 + x)(1 + x + \cdots + x^{n-1})$ luego 1+x es unidad.
(2) Si n es par $1 = 1 - x^n = (1 + x)p(x)$, luego $1 + x$ tiene inverso y es unidad.

Si u es una unidad del anillo A y x es nilpotente, entonces xu^{-1} es nilpotente y $1 + xu^{-1}$ es una unidad y $u(1 + xu^{-1}) = u + x$ también lo es. □

Ejercicio 2

Sea A un anillo y sea $A[X]$ el anillo de polinomios en una indeterminada X con coeficientes en A y sea $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, se tiene:

(1) f es una unidad en $A[X]$ si, y solo si, a_0 es una unidad en A y $a_1, \ldots, a_n$ son nilpotentes.
(2) f es nilpotente si, y solo si, $a_0, a_1, \ldots, a_n$ son nilpotentes.
(3) f es un divisor de 0 si, y solo si, existe $a \neq 0$ en A de manera que $af = 0$.
(4) Dados f y g en $A[X]$, fg es primitivo si, y solo si, f y g son primitivos.

DEMOSTRACIÓN. (1). Si f es una unidad, existe g=$\sum_{j=0}^{m} b_j x^j$ tal que $fg = 1$, entonces $a_0b_0 = 1$ y a_0 es una unidad. Por tanto tenemos $a_nb_m = 0$,$a_nb_{m-1} + a_{n-1}b_m = 0$, luego $a_n^2b_{m-1} + a_na_{n-1}b_m = 0$, entonces $a_n^2b_{m-1} = 0$. Por inducción probamos $a_n^{r+1}b_{m-r} = 0$. Tomando $r = m$ resulta que a_n es nilpotente. Como f es una unidad y a_n es nilpotente tenemos $f - a_nX^n$ unidad. Aplicando esto sucesivamente obtenemos el resultado.
(2). (⇒). Si $f = a_nx^n + \ldots + a_1x + a_0$ es nilpotente existe p número natural de manera que $f^p = 0$. Si grad$(f) = 0$, entonces $f = a_0$ y a_0 es nilpotente. Ahora supongamos $n \in \mathbb{N}$ y el resultado cierto para los naturales menores que n, $f^p = (\sum_{i=1}^{n} a_i x^i)^p = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!}(a_0 + a_1x + \cdots + a_{n-1}x^{n-1})^j(a_nx^n)^{p-j} = a_n^p x^{np} + \sum_{j=1}^{p} \frac{p!}{j!(p-j)!}(a_0 + a_1x + \ldots + a_{n-1}x^{n-1})^j(a_nx^n)^{p-j} = 0$. Nos queda entonces que a_n es nilpotente y por hipótesis de inducción $a_0, \ldots, a_{n-1}$ también lo son.
(⇐). Si $a_0, \ldots, a_n$ son nilpotentes, es decir, existe n_i tal que $a_i^{n_i} = 0$, entonces $f = a_0 + a_1x + \cdots + a_nx^n$ es nilpotente ya que $f^{n_1 \cdots n_n} = 0$.
(3). La implicación hacia la izquierda es trivial, luego veamos la implicación hacia la derecha:
Sea $f = a_0 + \cdots + a_nx^n$ divisor de cero y sea $g = b_0 + \cdots + b_mx^m$ el polinomio de grado mínimo de manera que $fg = 0$. Tenemos en particular $a_nb_m = 0$, luego el polinomio a_ng tiene grado menor que m y $(a_ng)f = 0$, así como g era el de grado mínimo tenemos que necesariamente $a_ng = 0$. El coeficiente de grado $n + m - 1$ es $a_{n-1}b_m + a_nb_{m-1} = 0$. Como $a_nb_{m-1} = 0$, tenemos que $a_{n-1}b_m = 0$.

Procediendo de la misma forma para los demás tenemos $a_{n-1}g = 0$. Por inducción probamos $a_{n-r}g = 0$ para cada $r \in \{0, \ldots, n\}$. Basta tomar entonces cualquier coeficiente no nulo de g y tenemos lo que buscábamos.

(4). Es el lema de Gauss probado anteriormente. □

Ejercicio 3

En el anillo $A[X]$, el radical de Jacobson es igual al nilradical.

DEMOSTRACIÓN. Está claro que $\mathrm{Nil}(A[X]) \subseteq \mathrm{Jac}(A[X])$. Ahora bien, sea $f \in \mathrm{Jac}(A[X])$,entonces $1-fg$ es una unidad para todo $g \in A[X]$. Tomando $g = X$ tenemos que $1-fX$ es una unidad, luego si $\sum_{i=1}^{n} a_i X^i$, entonces $a_0, \ldots, a_n$ son nilpotentes y tenemos que f es nilpotente. □

Ejercicio 4

Sea un anillo A tal que cada ideal no contenido en el nilradical contiene un idempotente no nulo, es decir, un elemento $e \in A$ de manera que $e^2 = e \neq 0$. Demostrar que el nilradical y el radical de Jacobson de A son iguales.

DEMOSTRACIÓN. Sabemos que $\mathrm{Nil}(A) \subseteq \mathrm{Jac}(A)$. Sea $a \in \mathrm{Jac}(A) \setminus \mathrm{Nil}(A)$,existe $0 \neq e = e^2 \in (a)$, como $e \in (a)$ entonces e es de la forma ax con $x \in A$. Ahora bien dado que a está en la intersección de todos los maximales, $1-ay$ es una unidad para cada $y \in A$, entonces $1-e = 1-ax$ es una unidad; llamamos c a su inverso, entonces $ax = ax((1-ax)c) = (ax(1-ax))c = ((ax-(ax)^2))c = 0c = 0$ y de esta manera $ax = e = 0$, lo cual es una contradicción. Luego $\mathrm{Nil}(A) = \mathrm{Jac}(A)$. □

Capítulo III

Teorema de estructura

Vamos a extender la teoría a anillos de ideales principales, eliminando la condición de dominio. Para ello nos serán muy útiles algunos resultados sobre anillos noetherianos y artinianos que veremos antes de empezar con el estudio de tales anillos.

8. Anillos noetherianos

Lema. 8.1.
En un anillo noetheriano A todo conjunto de generadores de un ideal contiene un conjunto finito de generadores.

DEMOSTRACIÓN. Si el ideal $\mathfrak{a}$ es el total, entonces $1 \in \mathfrak{a}$. Podemos escribir $1 = r_1 a_1 + \cdots r_n a_n$ con $r_i \in A, a_i$ en un conjunto de generadores de $\mathfrak{a}$ para cada $i = 1, \ldots, n$. Tenemos pues que el subconjunto $\{a_1, \ldots, a_n\}$ es un conjunto finito de generadores y se da el resultado. Ahora suponemos $\mathfrak{a} \subseteq A$ un ideal propio, evidentemente si el ideal es trivial está generado por un solo elemento, el $0 \in A$. Sea B un conjunto cualquiera de generadores y C el conjunto de ideales generados por subconjuntos finitos de B. Por ser A un anillo noetheriano, C tiene elemento maximal $\mathfrak{b}$. Si este ideal no fuera el total A, entonces elegimos $x \in B \setminus \mathfrak{b}$ y tendríamos $\mathfrak{b} + (x) \in C$, lo cual es una contradicción por la maximalidad de $\mathfrak{b}$, luego, como queríamos, tenemos $\mathfrak{b} = A$. □

Teorema. 8.2. (Teorema de intersección de Krull)
Sea A un anillo noetheriano y $\mathfrak{m}$ un ideal maximal de A, entonces $\cap_{n \geq 1} \mathfrak{m}^n = 0$.

DEMOSTRACIÓN. Mostraremos primero que, para cualquier ideal maximal $\mathfrak{a}$ del anillo noetheriano, se tiene

$$\cap_{n\geq 1}\mathfrak{a}^n = \mathfrak{a}\cap_{n\geq 1}\mathfrak{a}^n.$$

Si probamos esto, localizando en $\mathfrak{a}$, como $\mathfrak{a}A_{\mathfrak{a}}$ es el radical de Jacobson, tendremos, por el lema de Nakayama, que $\cap_{n\geq 1}\mathfrak{a}^n = 0$. Luego pasemos a probar la igualdad anterior en el caso local. Nótese que la inclusión $\cap_{n\geq 1}\mathfrak{a}^n \supseteq \mathfrak{a}\cap_{n\geq 1}\mathfrak{a}^n$ es obvia, luego probamos la otra:
Sean entonces $a_1,\dots,a_n$ un conjunto de generadores de $\mathfrak{a}$. Entonces $\mathfrak{a}$ constará de sumas finitas de la forma

$$\sum_{i_1+\dots+i_r=n}\mathfrak{a}_{i_1\dots i_r}a_1^{i_1}\cdots a_r^{i_r}$$

con $\mathfrak{a}_{i_1\dots i_r}\in A$. En otras palabras, $\mathfrak{a}^n$ consiste de los elementos de la forma $g(a_1,\dots,a_r)$ para algún polinomio homogéneo $g(X_1,\dots,X_r)\in A[X_1,\dots,X_r]$ de grado n. Denotamos por H_m al conjunto de polinomios homogéneos f de grado m de manera que $f(a_1,\dots,a_r)\in\cap_{n\geq 1}\mathfrak{a}^n$ y sea $\mathfrak{b}$ el ideal de $A[X_1,\dots,X_r]$ generado por $\cup_m H_m$. Por el lema anterior existe un conjunto finito $\{f_1,\dots,f_k\}$ de elementos de $\cup_m H_m$ que genera a $\mathfrak{b}$. Sean $d_i=\text{grad}(f_i)$ y $d=\text{máx}\{d_i \mid i=1,\dots,k\}$. Si $b\in\cap_{n\geq 1}\mathfrak{a}^n$, en particular $b\in\mathfrak{a}^{d+1}$ y por lo tanto $b=f(a_1,\dots,a_r)$ para un polinomio f de grado $d+1$. Por definición, $f\in H_{d+1}\subseteq\mathfrak{b}=(f_1,\dots,f_k)$, luego existen $g_i\in A[X_1,\dots,X_r]$ de manera que

$$f=f_1g_1+\cdots+f_kg_k.$$

Como f, f_i son homogéneos, podemos omitir de cada g_i los términos que no sean de grado $\text{grad}(f)-\text{grad}(f_i)=d+1-d_i>0$ y suponer que g_i es homogéneo de grado $d+1-d_i>0$, y por lo tanto no son constantes. Por lo tanto

$$b=f(a_1,\dots,a_r)=\sum_i g_i(a_1,\dots,a_r)f_i(a_1,\dots,a_r)\in\mathfrak{a}\cap_{n\geq 1}\mathfrak{a}^n.$$

Así tenemos la otra inclusión y el resultado. □

Proposición. 8.3.
Sea A un anillo local noetheriano con ideal maximal principal $\mathfrak{a}=Aa$, se verifica:

(1) Cada elemento no nulo $x\in A$ se escribe de la forma $x=ua^n$ con $u\in A$ invertible y $n\in\mathbb{N}$.
(2) Los ideales no nulos de A son de la forma $\mathfrak{b}=Aa^k$ con $k\in\mathbb{N}$ y por tanto principales.

DEMOSTRACIÓN. (1). Si $0\neq x\in A$ existe $n\in\mathbb{N}$ tal que $x\in Aa^n\setminus Aa^{n+1}$, ya que $\cap_{j=1}^{\infty}Aa^j=0$, por el teorema de intersección de Krull. Escribimos entonces $x=ua^n$, como $u\notin Aa=\mathfrak{m}$, entonces u es invertible.
(2). Dado $0\neq\mathfrak{a}\subseteq A$, cada elemento $x\in\mathfrak{a}$ se escribe de la forma $x=ua^n$ con u invertible y n natural. Tomando k el mínimo tal que $a^k\in\mathfrak{a}$, tenemos $\mathfrak{a}=Aa^k$. □

Si A es un anillo local noetheriano con ideal maximal $\mathfrak{m}$, podemos definir una métrica d sobre A mediante $d(x,y)=\text{máx}\{n\in\mathbb{N} \mid x-y\in\mathfrak{m}^n\}$.

Ejemplo. 8.4.
Veamos algunos ejemplos de anillos locales noetherianos:

(1) $\mathbb{Z}_{p^n}$, para $n, p \in \mathbb{N}$ y p primo.
(2) $K[[X]]$, para K cuerpo.

Definición. 8.5.
Un anillo local noetheriano A con métrica d, que es completo para la misma, se llama **anillo local noetheriano completo**.

9. Anillos artinianos

Proposición. 9.1.
En un anillo artiniano todo ideal primo es maximal.

DEMOSTRACIÓN. Sea $\mathfrak{p}$ un ideal primo de A artiniano, entonces $A/\mathfrak{p}$ es un dominio de integridad artiniano. Dado $0 \neq x \in A/\mathfrak{p}$, consideramos la cadena descendente de ideales:

$$x(A/\mathfrak{p}) \supset x^2(A/\mathfrak{p}) \supset \cdots$$

Existe entonces $n \in \mathbb{N}$ tal que $x^n(A/\mathfrak{p}) = x^{n+1}(A/\mathfrak{p})$. Resulta que existe $y \in A/p$ tal que $x^n = yx^{n+1}$, entonces $1 = xy$. Así, x es una unidad y $(A/\mathfrak{p})$ es cuerpo, luego el ideal $\mathfrak{p}$ es maximal. □

Observación. 9.2.
En un anillo artiniano $\mathrm{Nil}(A) = \mathrm{Jac}(A)$.

Proposición. 9.3.
En un anillo artiniano hay un número finito de ideales primos.

DEMOSTRACIÓN. Consideramos el conjunto B de intersecciones finitas de ideales primos y por tanto maximales de A. Como A es un anillo artiniano, B tiene un elemento minimal, lo denotamos $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$. Para cada ideal maximal $\mathfrak{m}$, se tiene $\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t \subset \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$. Por la minimalidad resulta que $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t \subset \mathfrak{m}$, y por tanto $\mathfrak{m} = \mathfrak{m}_i$ para algún $i \in \{1, \ldots, t\}$. □

Corolario. 9.4.
En un anillo artiniano el nilradical es el producto de los ideales primos.

DEMOSTRACIÓN. Es consecuencia de que los ideales primos son los maximales y son comaximales dos a dos. □

Proposición. 9.5.
En un anillo artiniano el nilradical es nilpotente.

DEMOSTRACIÓN. Llamamos $\mathfrak{n} = \mathrm{Nil}(A)$ con A anillo artiniano. Por ser artiniano, existe $n \in \mathbb{N}$ de manera que $\mathfrak{n}^n = \mathfrak{n}^{n+1}$. Supongamos $\mathfrak{n}^n \neq 0$, llamamos Σ al conjunto

$$\Sigma = \{\mathfrak{a} \subset A \mid \ \mathfrak{a}\mathfrak{n}^n \neq 0\},$$

por la suposición anterior $\Sigma \neq \emptyset$. De nuevo, por ser A artiniano, existe $\mathfrak{a} \in \Sigma$ minimal. Sea $a \in \mathfrak{a}$ tal que $a\mathfrak{n}^n \neq 0$, entonces por la minimalidad de $\mathfrak{a}$ tenemos que $\mathfrak{a} = aA$. También se verifica la relación $\mathfrak{a}\mathfrak{n}\mathfrak{n}^n = \mathfrak{a}\mathfrak{n}^{n+1} = \mathfrak{a}\mathfrak{n}^n \neq 0$, y por la minimalidad tenemos $\mathfrak{a}\mathfrak{n} = aA$. Entonces existe $y \in \mathfrak{n}$ tal que $ay = a$, y es fácil ver que se tiene $ay^s = a$ para cada $s \in \mathbb{N}$. Ahora bien, y es nilpotente, ya que $y \in \mathfrak{n}$, luego existe s tal que $y^s = 0$, y por tanto $a = 0$, lo que es una contradicción. □

Teorema. 9.6. (Teorema de estructura de anillos artinianos)
Sea A un anillo artiniano con ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$. Entonces A es isomorfo a un producto:

$$A/\mathfrak{m}_1^{n_1} \times \cdots \times A/\mathfrak{m}_t^{n_t}$$

para $(n_1, \ldots, n_t) \in \mathbb{N}^t$. Además cada $A/\mathfrak{m}^{n_i}$ es un anillo local artiniano con un único ideal maximal.

DEMOSTRACIÓN. Tenemos $\mathrm{Nil}(A) = \mathfrak{m}_1 \cdots \mathfrak{m}_t$. Sabemos también que existe $n \in \mathbb{N}$ tal que $0 = \mathrm{Nil}(A)^n = \mathfrak{m}_1^n \cdots \mathfrak{m}_t^n$, como los ideales $\mathfrak{m}_i^n$ son comaximales resulta que $\mathfrak{m}_1^n \cdots \mathfrak{m}_t^n = \mathfrak{m}_1^n \cap \cdots \cap \mathfrak{m}_t^n$. Por el teorema chino del resto tenemos un isomorfismo

$$A \cong A/\mathrm{Nil}(A) \cong A/\mathfrak{m}_1^n \times \cdots \times A/\mathfrak{m}_t^n.$$

Los anillos $A/\mathfrak{m}_i^n$ son artinianos por serlo A, además $\mathfrak{m}_i/\mathfrak{m}_i^n$ es un ideal maximal y el único ideal primo en $A/\mathfrak{m}_i^n$. □

Tenemos que todo anillo artiniano es también un anillo noetheriano.

10. Anillos de ideales principales

Definición. 10.1.
Recordar que un **anillo de ideales principales** (AIP) es un anillo en el que todo ideal es principal.
Llamaremos **anillo de ideales principales especial** (AIPS) a un anillo de ideales principales que tiene un único ideal primo no nulo, el radical, éste es nilpotente y cada ideal es una potencia del radical. Por lo tanto tiene un número finito de ideales.

Lema. 10.2.
Sea A un anillo de ideales principales especial con ideal primo $\mathfrak{a} = Ap$ *con índice de nilpotencia* $k \in \mathbb{N}$. *Se verifica:*

(1) Todo elemento $a \in A$ *se escribe como* $a = up^e$, *siendo* u *un elemento invertible de A y* $0 \leq e$, *unívocamente determinado.*
(2) Los ideales de A son de la forma (p^e), *con* $e = 0, \ldots, k-1$.
(3) p *es un elemento irreducible.*

DEMOSTRACIÓN. (1). Si $a \in A \setminus \mathfrak{a}$, entonces a es invertible y si $a \in \mathfrak{a}$ existe una factorización $a = up^e$. Si existieran dos factorizaciones $up^e = a = vp^f$ con $0 \neq e < f < k$, entonces $p^e(u - vp^{f-e}) = 0$, como $u - vp^{f-e} \notin \mathfrak{a}$, entonces es invertible. Entonces tendríamos $p^e = 0$ lo cual contradice la elección de k.
(2). Trivial.
(3). Supongamos que p tuviese una factorización, $p = xy$. Tenemos $y = vp^f$ y $x = up^e$, entonces $p = uvp^{e+f}$. Por la unicidad se tiene $e + f = 1$, y entonces $e = 0$ y $f = 1$ ó $e = 1$ y $f = 0$. Por tanto x ó y es asociado con p y p es irreducible. □

Proposición. 10.3.
Sea A un anillo local artiniano con ideal maximal $\mathfrak{m}$ *y cuerpo residual* $K = A/\mathfrak{m}$. *Son equivalentes los siguientes enunciados:*

(a) Cada ideal de A es principal.
(b) El ideal maximal de A es principal.
(c) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$, *es la dimensión como K–espacio vectorial.*

DEMOSTRACIÓN. De forma evidente se da (a) ⇒ (b) ⇒ (c), luego nos queda ver la implicación $(c) \Rightarrow (a)$.
Si $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$, entonces $\mathfrak{m}\mathfrak{m}^2 = 0$, y por el lema de Nakayama tenemos $\mathfrak{m} = 0$, de manera que A sería un cuerpo y se tiene el resultado.

Si $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, entonces $\mathfrak{m}$ es un ideal principal. Tenemos entonces que existe $x \in A$ de manera que $xA = \mathfrak{m}$. Dado un ideal $\mathfrak{a}$ de A propio, tenemos $\mathfrak{a} \subseteq \mathfrak{m} = xA$. Ya que $\mathrm{Nil}(A)$ es nilpotente y $\mathrm{Nil}(A) = \mathfrak{m}$, existe $n \in \mathbb{N}$ de manera que $\mathfrak{m}^n = 0$. Tenemos entonces que existe $m \in \mathbb{N}$ de manera que $\mathfrak{a} \subseteq \mathfrak{m}^m = x^m A$ y $\mathfrak{a} \subsetneq \mathfrak{m}^{m+1} = x^{m+1}A$. Podemos encontrar entonces $y \in \mathfrak{a}$ tal que $y = rx^m$ con $r \in A$ y $y \notin \mathfrak{m}^{m+1} = x^{m+1}A$, luego $r \notin xA = \mathfrak{m}$, o lo que es equivalente, r es una unidad. Entonces $x^m \in yA \subseteq \mathfrak{a}$ y nos queda que $\mathfrak{a} = x^m A = \mathfrak{m}^m$, y por tanto, $\mathfrak{a}$ es un ideal principal. □

Con este último resultado tenemos entonces que los anillos locales artinianos los podemos clasificar en dos tipos, aquellos en los que el ideal maximal es principal y aquellos en los que no. Vemos algún ejemplo en cada caso:

Ejemplo. 10.4.
Anillos locales noetherianos con ideal maximal principal:
(1) El anillo $\mathbb{Z}_{p^n}$.
(2) $K[X]/(f^n)$ siendo K un cuerpo y f un polinomio irreducible.

Ejemplo. 10.5.
Anillo local noetheriano con ideal maximal no principal:
(1) En el anillo $F[X^2, X^3]/(X^4)$ con F cuerpo, notamos a la clase de la indeterminada X como x. Tenemos entonces (x^2, x^3) es el ideal maximal y no es principal. Además, si $\mathfrak{m} = (x^2, x^3)$, se tiene $\mathfrak{m}^2 = 0$ y $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 2$.

Corolario. 10.6.
Para un anillo de ideales principales local A son equivalentes:
(1) A es un anillo de ideales principales especial.
(2) A es un anillo artiniano local con ideal maximal principal.

DEMOSTRACIÓN. (a) ⇒ (b). Es trivial utilizando el lema anterior y la descripción de los ideales de un anillo de ideales principales especial.
(b) ⇒ (a). Es consecuencia de la proposición anterior. □

Corolario. 10.7.
Todo anillo de ideales principales especial es un anillo local noetheriano completo.

DEMOSTRACIÓN. Esto es consecuencia de que el ideal maximal es nilpotente, por lo que toda sucesión de Cauchy es finalmente estacionaria. □

Recordemos la construcción del **producto directo de anillos**, dados $A_1, \ldots, A_n$, definimos en el producto cartesiano $A = A_1 \times \cdots \times A_n$ las siguientes operaciones:

(1) Suma: $(a_1,\dots,a_n)+(b_1,\dots,b_n)=(a_1+b_1,\dots,a_n+b_n)$ para todo $(a_1,\dots,a_n),(b_1,\dots,b_n)\in A$.
(2) Producto: $(a_1,\dots,a_n)(b_1,\dots,b_n)=(a_1b_1,\dots,a_nb_n)$ para todo $(a_1,\dots,a_n),(b_1,\dots,b_n)\in A$.
(3) Uno: $(1,\dots,1)$.

Así diremos que $(A,+,\times)$ es el producto directo de $A_1,\dots,A_n$ y lo podemos denotar también por $A_1\oplus\cdots\oplus A_n$.

Proposición. 10.8.
El producto finito directo de anillos de ideales principales es un anillo de ideales principales.

DEMOSTRACIÓN. Veamos el caso de dos para después hacer inducción. Si $A=A_1\oplus A_2$. Es fácil ver que cada ideal $\mathfrak{a}$ de A se escribe de la forma $\mathfrak{a}=\mathfrak{a}_1\oplus\mathfrak{a}_2$. Si $\mathfrak{a}_i=A_ia_i$, entonces $\mathfrak{a}=Aa_1\oplus Aa_2=A(a_1,a_2)$, es decir, el ideal generado por $(a_1,a_2)\in A$. Si tenemos ahora el resultado cierto para $n-1$ y $A=A_1\oplus\cdots\oplus A_n=(A_1\oplus\cdots\oplus A_{n-1})\oplus A_n$, por hipótesis de inducción $A_1\oplus\cdots\oplus A_{n-1}$ es anillo de ideales principales, y al hacer el producto directo con A_n, como hemos visto en el caso de dos, tenemos un anillo de ideales principales, luego A es anillo de ideales principales. □

Vamos a ver ahora algunas propiedades de la estructura de anillos de ideales principales:

Lema. 10.9.
Sea A un anillo de ideales principales y $\mathfrak{p}_1\subsetneq\mathfrak{p}\subset A$ dos ideales primos. Se verifica:

1. *No existen otros ideales primos contenidos en $\mathfrak{p}$, como consecuencia la dimensión de A es a lo sumo* 1.
2. *Todo ideal primario contenido en $\mathfrak{p}$ contiene a $\mathfrak{p}_1$*
3. *Un ideal primo no maximal no tiene más ideales primarios que él mismo.*
4. *Cada dos ideales primos o son comaximales o son comparables.*

DEMOSTRACIÓN. (1). Tenemos $\mathfrak{p}_1=Ap_1$ y $\mathfrak{p}=Ap$, entonces $p_1=rp$ con $r\in\mathfrak{p}_1$,entonces $p_1=sp_1p$. Tenemos pues $p_1(1-sp)=0$. Si tenemos $\mathfrak{p}\subset\mathfrak{p}$ otro ideal primo, se tiene $p_1\in\mathfrak{p}$ y $\mathfrak{p}_1\subseteq\mathfrak{p}$. Por la misma razón $\mathfrak{p}\subseteq\mathfrak{p}_1$ y tenemos el resultado. Por tanto las cadenas de ideales primos son de longitud menor o igual que 1.
(2). Sea $\mathfrak{b}\subset\mathfrak{p}$ un ideal , como $p_1(1-sp)\in\mathfrak{b}$ y $(1-sp)\notin\mathfrak{b}$ tenemos $p_1\in\mathfrak{q}$, luego $\mathfrak{p}_1$ está contenido en cualquier ideal primario contenido en $\mathfrak{p}$. En particular $\mathfrak{p}_1$ es un ideal primario ya que es primo.
(3). Si $\mathfrak{p}_1$, está contenido en un ideal maximal $\mathfrak{p}_1\subsetneq\mathfrak{m}$ y por tanto $\mathfrak{p}_1$ no tiene más ideales primarios que él mismo.
(4). Si $\mathfrak{p}_1,\mathfrak{p}_2$ son ideales y no son comaximales, entonces existe un ideal maximal $\mathfrak{m}$ tal que $\mathfrak{p}_i\subseteq\mathfrak{p}_1+\mathfrak{p}_2\subseteq\mathfrak{m}$, se tiene entonces $\mathfrak{p}_1=\mathfrak{p}_2$ o $\mathfrak{p}_1\subseteq\mathfrak{m}=\mathfrak{p}_2$. □

Antes de demostrar el siguiente teorema que nos dirá la estructura que tienen los anillos de ideales principales necesitamos hacer algunas definiciones previas:

Definición. 10.10.
Sea A un anillo y $\mathfrak{a}$ un ideal propio de A, diremos que es un **ideal primario** si todo elemento $x \in \mathfrak{a}$ verifica que si $x = ab$ entonces, o bien $a \in \mathfrak{a}$ o bien $b \in \mathrm{Rad}(\mathfrak{a})$ donde $\mathrm{Rad}(\mathfrak{a}) = \cap_{\mathfrak{a}\subset\mathfrak{p}}\mathfrak{p}$, con $\mathfrak{p}$ ideal primo de A, esto es, existe $n \in \mathbb{N}$ tal que $b^n \in \mathfrak{a}$.

Lema. 10.11.
Si $\mathfrak{a}$ *es un ideal primario,* $\mathrm{Rad}(\mathfrak{a})$ *es el menor ideal primo que lo contiene.*

DEMOSTRACIÓN. En primer lugar vemos que $\mathrm{Rad}(\mathfrak{a})$ es efectivamente un ideal primo. Sea $x = ab \in \mathrm{Rad}(\mathfrak{a})$, existe $n \in \mathbb{N}$ de manera que $x^n \in \mathfrak{a}$, entonces tenemos $a^n b^n \in \mathfrak{a}$. Por ser $\mathfrak{a}$ primario, $a^n \in \mathfrak{a} \subseteq \mathrm{Rad}(\mathfrak{a})$ o bien $b^n \in \mathrm{Rad}(\mathfrak{a})$. Así o bien $a \in \mathrm{Rad}(\mathfrak{a})$ o bien $b \in \mathrm{Rad}(\mathfrak{a})$, luego es primo.
Por la definición que hemos dado de $\mathrm{Rad}(\mathfrak{a})$ es el menor primo que contiene $\mathfrak{a}$. □

Este hecho nos permite introducir la siguiente terminología: si $\mathfrak{a}$ es un ideal primario y $\mathfrak{p} = \mathrm{Rad}(\mathfrak{a})$, diremos que $\mathfrak{a}$ es un ideal $\mathfrak{p}$-primario.

Definición. 10.12.
Sea A un anillo y $\mathfrak{a}$ un ideal de A. Una **descomposición primaria** del ideal es una expresión de $\mathfrak{a}$ como intersección finita de ideales primarios,

$$\mathfrak{a} = \cap_{i=1}^{t} \mathfrak{q}_i.$$

con $\mathfrak{q}_i$ un ideal $\mathfrak{p}_i$-primario.
No todos los ideales de un anillo admiten una descomposición primaria, a los que si la admitan los llamaremos **ideales descomponibles**.
Si en la descomposición se cumple:

(1) $\mathfrak{p}_i \neq \mathfrak{p}_j$ para $i \neq j$.
(2) $\mathfrak{q}_j \not\supset \cap_{i\neq j}\mathfrak{q}_i$.

Se dice que la descomposición es **reducida e irredundante**.

Teorema. 10.13. (Teorema de Zariski-Samuel)
Sea A un anillo de ideales principales, entonces A es un producto directo finito de dominios de ideales principales y anillos de ideales principales especiales.

DEMOSTRACIÓN. Consideramos la descomposición primaria reducida e irredundante $0 = \cap_{i=1}^{t} \mathfrak{q}_i$ siendo $\mathfrak{q}_i$ un ideal $\mathfrak{p}_i$-primario. Dados $\mathfrak{p}_1$ y $\mathfrak{p}_2$, tenemos que son comaximales, ya que si $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$, entonces $\mathfrak{q}_1 = \mathfrak{p}_1$ y todo ideal $\mathfrak{p}_2$-primario contiene a $\mathfrak{p}_1$, contradiciendo que la descomposición es reducida e irredundante. Por el teorema chino del resto tenemos $A \cong \prod_{i=1}^{t} A/\mathfrak{q}_i$ y cada $A/\mathfrak{q}_i$ es un dominio de ideales principales si $\mathfrak{p}_i = \mathfrak{q}_i$ o un anillo de ideales principales especial si $\mathfrak{q}_i \neq \mathfrak{p}_i$, en cuyo caso $\mathfrak{p}_i$ es un ideal maximal y $\mathfrak{p}_i/\mathfrak{q}_i$ es un ideal nilpotente. □

podemos ahora caracterizar los anillos artinianos que son AIP.

Proposición. 10.14.
Sea A un anillo artiniano. Son equivalentes:

(a) A es un anillo de ideales principales.
(b) Nil(A) *es un ideal principal.*
(c) A es un producto directo finito de anillos de ideales principales especiales.

DEMOSTRACIÓN. (a) ⇒ (b). Trivial.
(b) ⇒ (c). Como A es artiniano,por el teorema de estructura de anillos artinianos, tenemos que $A \cong A_1 \times \cdots \times A_t$, con $A_i = A/\mathfrak{m}_i^{n_i}$ y $\mathfrak{m}_i$ ideal maximal para cada $i \in \{1, \ldots, t\}$. Si Nil$(A) = Ab$, con $b = (b_1, \ldots, b_t)$, entonces si notamos por p_i a las proyecciones tenemos $p_i(b) = b_i \in \text{Nil}(A_i)$.Si $x_i \in \text{Nil}(A_i)$ existe $n \in \mathbb{N}$ de manera que $x_i^n = 0$ y entonces $(0, \ldots, x_i, \ldots, 0) \in \text{Nil}(A) = Ab$. Existe entonces $a \in A$ tal que $x = ab$, luego $x_i = p_i(x) = p_i(ab) = ap_i(b) = ab_i$. Tenemos entonces $\text{Nil}A_i = A_i b_i$, es decir, un ideal principal. Como cada anillo local artiniano con ideal maximal principal es un anillo de ideales principales especial, tenemos que cada A_i es un anillo de ideales principales especial.
(c) ⇒ (a). Es consecuencia de que todo producto finito directo de anillos de ideales principales es un anillo de ideales principales. □

Corolario. 10.15.
Todo anillo de ideales principales es un producto directo de un producto directo finito de dominios de ideales principales y un anillo de ideales principales artiniano, que es un producto directo finito de anillos de ideales principales especiales.

Corolario. 10.16.
En un anillo de ideales principales todo ideal propio es producto de ideales primos.

11. Anillos de series de potencias formales.

Amén de los anillos de polinomios, los anillos de series de potencias formales permiten construir nuevos anillos con propiedades bien determinadas a la vista de los resultados del libro de Atiyah–Macdonald.

Proposición. 11.1.
Sea A un anillo. Entonces:

(1) Si A es un DI, entonces $A[[X]]$ también lo es.
(2) Un elemento $f \in A[[X]]$ es una unidad si, y solo si, el término independiente de f es una unidad en A.

DEMOSTRACIÓN. (1). Sean $P = \sum_i a_i X^i$ y $Q = \sum_i b_i X^i$. Si ambos son distintos de cero, tomamos $\mathfrak{a}, \mathfrak{b}$ como el menor índice de manera que $a_\mathfrak{a} \neq 0$ y $b_\mathfrak{b} \neq 0$. Así, el término de la posición $\mathfrak{a}+\mathfrak{b}$ es $a_\mathfrak{a} b_\mathfrak{b} \neq 0$ ya que A es un dominio de integridad y por tanto $PQ \neq 0$ y $A[[X]]$ es dominio de integridad.
(2). La demostración es análoga a la de los polinomios. □

Teorema. 11.2.
Si A es un dominio de ideales principales, entonces $A[[X]]$ es un dominio de factorización única.

DEMOSTRACIÓN. Basta ver que cada ideal primo no nulo $0 \neq \mathfrak{p} \subseteq A[[X]]$ contiene un elemento primo no nulo. Si $X \in \mathfrak{p}$ ya tenemos un elemento primo no nulo. Si $X \notin \mathfrak{p}$ definimos $\mathfrak{p}_0 = \{a \in A \mid a + XF \in \mathfrak{p} \text{ con } F \in A[[X]]\}$. Tenemos que $\mathfrak{p}$ y $\mathfrak{p}_0$ están generados por el mismo número de elementos, luego como $\mathfrak{p}_0$ ha de ser principal, $\mathfrak{p}$ también lo es, y por tanto tiene un elemento primo no nulo. □

Lema. 11.3.
Si un dominio de integridad A verifica la cadena de divisores, $A[[X]]$ también la verifica.

DEMOSTRACIÓN. Dada una cadena de ideales principales $(F_1) \subseteq (F_2) \subseteq \cdots$ en $A[[X]]$, si ponemos $F_i = \sum_j a_{i,j} X^j$ tenemos una cadena de ideales principales $(a_{1,0}) \subseteq (a_{2,0}) \subseteq \cdots$ en A, luego existe $n \in \mathbb{N}$ de manera que $(a_{n,0}) = (a_{n+k,0})$ para todo $k \in \mathbb{N}$. Entonces para cada $h \in \mathbb{N}$ existe $u_h \in A$ invertible

tal que $a_{n,0} = u_h a_{n+h,0}$. Si $F_t = G_h F_{t+h}$ en $A[[X]]$, entonces u_h es el término constante de G_h, y por tanto G_h es invertible, esto es $(F_t) = (F_{t+h})$ para todo $h \in \mathbb{N}$, luego es una cadena estacionaria.
Si la cadena $(a_{1,0}) \subseteq (a_{2,0}) \subseteq \cdots$ se estabiliza. Consideramos $(a_{1,1}) \subseteq (a_{2,1}) \subseteq \cdots$ y a esta le aplicamos el razonamiento anterior. Si esta se estabilizase, pasamos al siguiente y así sucesivamente. □

Corolario. 11.4.
Si A es un cuerpo, $A[[X]]$ es un dominio de ideales principales.

DEMOSTRACIÓN. Todo elemento de A es una unidad, luego todos los elementos de $A[[X]]$ que tengan término independiente son unidades. Los elementos no unidades de $A[[X]]$ están por tanto en el ideal principal generado por X, (X). Utilizando que todas las unidades están contenidas en un ideal propio y la proposición anterior tenemos que $A[[X]]$ es un dominio de integridad local cuyo ideal maximal es principal, luego es un dominio de ideales principales. □

12. v-anillos

Queremos ahora ver la relación existente entre AIP y DIP. Comenzamos con una definición.

Definición. 12.1.
Un anillo D diremos que es **v-anillo** si verifica:
(1) D es un dominio de integridad local noetheriano de característica 0.
(2) El ideal maximal $\mathfrak{m}$ de D es principal generado por $p1$, con $p \in \mathbb{Z}$ entero primo positivo.
(3) $D/\mathfrak{m}$ tiene característica p.

Lema. 12.2.
Se cumple:
(1) Todo v-anillo es un dominio de ideales principales.
(2) El único elemento irreducible de un v-anillo D es p.

DEMOSTRACIÓN. (1). Sea $\mathfrak{a}$ un ideal de un v-anillo D. Por ser noetheriano, este ideal es finitamente generado, pongamos $\mathfrak{a} = (a_1, \ldots, a_n)$. Además, este ideal ha de estar contenido en el maximal $(a_1, \ldots, a_n) \subseteq (p)$. Tenemos entonces $a_1 = pb_1$. Si $b_1 \notin (p)$ será invertible y en otro caso $b_1 = pc_1$ con $c_1 \in (p)$ o invertible. Si seguimos este algoritmo llegará un momento en el que llegaremos a una expresión del tipo $a_1 = p^{e_1}u_1$ con u_1 invertible ya que en el caso contrario tendríamos una cadena no estacionaria. Haciendo esto para cada a_i nos queda

$$(a_1, \ldots, a_n) = (p^{e_1}u_1, \ldots, p^{e_n}u_n) = (p^e)$$

siendo $e = \min\{e_i \mid i = 1, \ldots, n\}$. Por tanto es un ideal principal.
(2). El elemento p sabemos que es irreducible ya que genera un ideal maximal. Sea $q \in D$ otro elemento irreducible. Como no es invertible tenemos $q \in (p)$, luego $q = ph$. Como q es irreducible, o bien $q \sim p$ o bien $q \sim h$, pero en este caso p sería invertible, luego $q \sim p$. □

Teorema. 12.3.
Sea A un anillo local noetheriano completo con ideal maximal principal $\mathfrak{m} = Aa$, entonces A es un cociente de un anillo, como anillos locales, de series formales de potencias $D[[X]]$, donde:
(1) $D = A/\mathfrak{m}$ si $\operatorname{car}(A) = \operatorname{car}(A/\mathfrak{m}) = p$
(2) D es un v-anillo con cuerpo residual $A/(p1)$ isomorfo a $A/\mathfrak{m}$, si $\operatorname{car}(A) \neq \operatorname{car}(A/\mathfrak{m}) = p$.

No incluimos la demostración de este resultado.

Proposición. 12.4.
Si A es un v-anillo, entonces $A[[X]]$ es un dominio de factorización única.

DEMOSTRACIÓN. Sabemos que si A es un dominio de ideales principales entonces $A[[X]]$ es un dominio de factorización única, como todo v-anillo es un dominio de ideales principales, tenemos el resultado. □

Teorema. 12.5. (Teorema de Hungerford)
Todo anillo de ideales principales es un producto directo finito de anillos que son cocientes de dominios de ideales principales.

DEMOSTRACIÓN. Sabemos que todo anillo de ideales principales es producto de dominios de ideales principales y anillos de ideales principales especiales, luego probando que cada uno de estos es un cociente de un dominio de ideales principales tendremos el resultado.
Por el teorema anterior tenemos que todo anillo de ideales principales especial es un cociente de un anillo de series formales de potencias $D[[X]]$ donde D es un cuerpo, en cuyo caso tenemos el resultado, o bien D es un v-anillo.
Supongamos entonces que el anillo de ideales principales $(A, \mathfrak{m})$ es un cociente de un v-anillo. Sea $f : D[[X]] \longrightarrow A$ un homomorfismo sobreyectivo con $f(X) = a$ donde $\mathfrak{m} = Aa$. Si el ideal maximal de D es $(p1)$, entonces $\text{car}(D(p1)) = p \neq 0$ y $\text{car}(A/\mathfrak{m}) = p$ ya que $D[[X]]/(p1, X) \cong A/\mathfrak{m}$.
Si $p = \text{car}(A)$, entonces $p \in \text{Ker}(f)$ y $p \in D$ es irreducible, luego también lo es en $D[[X]]$, existe entonces un homomorfismo sobreyectivo $D[[X]]/(p1) = D/(p1)[[X]]$ y $D/(p1)$ es un cuerpo.
Si $p \neq car(A)$, entonces $0 \neq p = ua^n \in \mathfrak{m}$ $n \geq 1$. Si tomamos $F \in D[[X]]$ tal que $f(F) = p$, entonces $f(FX^n - p) = 0$, es decir, $FX^n - p \in \text{Ker}(f)$. Como $p \in D$ es irreducible, también lo es en $D[[X]]$. Como $D[[X]]$ es un dominio de factorización única, los elementos irreducibles generan ideales primos. Tenemos entonces que f descompone de la siguiente manera: $D[[X]] \longrightarrow D[[X]]/(FX^n - p) \longrightarrow A$ donde $f' : D[[X]]/(FX^n - p) \longrightarrow A$, la del diagrama anterior, es sobreyectiva.
Necesitamos ver que $D[[X]]/(FX^n - p)$ es un dominio de ideales principales, para ello vemos que es un anillo local noetheriano con ideal maximal principal. Notamos $[X]$ a la clase de X, entonces $[X] \notin (FX^n - p)$ ya que $f(X) = a \neq 0$. Por otra parte, $[FX^n - p] = 0$, luego $[p] = [FX^n] \in ([X])$. Sea $[G] \in D[[X]]/(FX^n - p)$ no invertible, entonces $G = \sum_{j=1}^{\infty} b_j \in D[[X]]$ tampoco es invertible y por tanto $b_0 \in (p1)$, entonces $[G] \in ([X])$. Nos queda $([X]) \subseteq D[[X]]/(FX^n - p) - (X)$, y por tanto $D[[X]]/(FX^n - p)$ es un anillo local noetheriano con ideal maximal principal como queríamos. □

Observación. 12.6.
Podemos enunciar el teorema anterior de la siguiente forma: Todo anillo de ideales principales es producto directo de anillos, siendo cada uno de estos anillos la imagen por un homomorfismo de un dominio de ideales principales.

Corolario. 12.7.
Todo anillo de ideales principales especial es la imagen por un homomorfismo de un dominio de ideales principales.

Corolario. 12.8.
Para un anillo de ideales principales A son equivalentes:

(a) A es producto directo finito de dominios de ideales principales.
(b) A no tiene elementos nilpotentes no nulos

DEMOSTRACIÓN. Es inmediato, ya que en la descomposición de un anillo de ideales principales como producto de dominios de ideales principales y anillos de ideales principales especiales, los elementos nilpotentes no nulos están en los anillos de ideales principales especiales. □

Capítulo IV

Teorema de Kaplansky

Los anillos noetherianos se pueden caracterizar por el hecho de que los ideals primos son finitamente generados. Este resultado tiene su origen en un teorema de Kaplansky sobre ideales principales que vamos a estudiar, ya que con los ideales principales tratamos de controlar la divisibilidad y la factorización.

13. AIP e ideales primos

Definición. 13.1.
Un conjunto de anillos y homomorfismos $\{A_i, \phi_i\}$ con $\phi_i : A_i \longrightarrow A_{i+1}$ se dice una **sucesión exacta** cuando $\mathrm{Im}(\phi_{i+1}) = \mathrm{Ker}(\phi_i)$. Se llamará **corta** si es del tipo $0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$.

Lema. 13.2.
Sea $\mathfrak{a}$ *un ideal maximal entre los ideales que no son finitamente generados de A, entonces* $\mathfrak{a}$ *es un ideal primo.*

DEMOSTRACIÓN. Si $\mathfrak{a}$ no fuese primo, existen $a, b \in A$ de manera que $ab \in \mathfrak{a}$ y $a, b \notin \mathfrak{a}$. Consideramos la siguiente sucesión exacta corta

$$0 \longrightarrow (\mathfrak{a} : a)a \xrightarrow{\alpha} \mathfrak{a} \times aA \xrightarrow{\beta} \mathfrak{a} + aA \longrightarrow 0.$$

Donde $\alpha(x) = (x, x)$ y $\beta(x, y) = x - y$. Dado que $\mathfrak{a} \subsetneq \mathfrak{a} + bA \subseteq (\mathfrak{a} : a)$, se tiene que $(\mathfrak{a} : a)$ es finitamente generado, luego $(\mathfrak{a} : a)a$ también lo es. Además, dado que $\mathfrak{a} \subsetneq \mathfrak{a} + aA$, tenemos que $\mathfrak{a} + aA$ es también finitamente generado. Por tanto $\mathfrak{a} \times aA$ es finitamente generado y $\mathfrak{a}$ también, lo cual es una contradicción y por tanto $\mathfrak{a}$ debe ser primo. □

Teorema. 13.3. (Teorema de Cohen)
Si A es un anillo, son equivalentes:

(a) A es noetheriano.
(b) Cada ideal primo es finitamente generado.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Lo probamos anteriormente.
(b) $\Rightarrow$ (a). Vamos a probar que todo ideal es finitamente generado, lo cual equivale a la definición de noetheriano. Supongamos que A tiene un ideal que no es finitamente generado, entonces el conjunto $\Sigma = \{\mathfrak{a} \mid \mathfrak{a} \text{ no es finitamente generado}\}$ es no vacío. Como, si $\{\mathfrak{a}_i\}$ es una cadena de elementos de Σ, entonces $\cup_i \mathfrak{a}_i$ es una cota superior en Σ, por el lema de Zorn, Σ tiene elementos maximales. Si $\mathfrak{a} \in \Sigma$ es maximal, por la hipótesis es finitamente generado, lo que es una contradicción. Tenemos por tanto que todo ideal de A es finitamente generado y por tanto A es noetheriano. □

En el caso de anillos principales tenemos.

Lema. 13.4.
Si $\mathfrak{a} \subseteq A$ es un ideal maximal entre los ideales no principales del anillo A, entonces $\mathfrak{a}$ es un ideal primo.

DEMOSTRACIÓN. Si $\mathfrak{a}$ no es un ideal primo, existen ideales $\mathfrak{b}, \mathfrak{c}$ de manera que $\mathfrak{bc} \subseteq \mathfrak{a}$ y $\mathfrak{b} \nsubseteq \mathfrak{a}$ $\mathfrak{c} \nsubseteq \mathfrak{a}$. Tenemos entonces que $\mathfrak{b}$ es principal, sea $b \in A$ de manera que $bA = \mathfrak{b}$. Como $b\mathfrak{c} \subseteq \mathfrak{bc} \subseteq \mathfrak{a}$, resulta $\mathfrak{a} \subsetneq \mathfrak{c} \subseteq (\mathfrak{a} : b)$ y así $(\mathfrak{a} : b)$ es un ideal principal. Sea $d \in A$ tal que $(\mathfrak{a} : b) = Ad$.
Para cada $a \in \mathfrak{a} \subseteq Ab$, existe $r \in A$ tal que $a = rb$, entonces $r \in (\mathfrak{a} : b) = Ad$ y existe $s \in A$ con $r = sd$. Así, $a = rb = sdb$ y tenemos $\mathfrak{a} \subseteq Adb \subseteq \mathfrak{a}$, por tanto, $\mathfrak{a}$ principal, lo que es una contradicción y por tanto tiene que ser un ideal primo. □

Teorema. 13.5. (Teorema de Kaplansky)
Si A es un anillo, son equivalentes:

(a) A es unillo de ideales principales.
(b) Cada ideal primo es principal

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Trivial

(b) ⇒ (a). Consideramos el conjunto de los ideales no principales de A, si este no fuera vacío, tendría un maximal. Este maximal sería primo y por tanto principal por hipótesis, lo cual es una contradicción, luego nuestro conjunto es vacío y todo ideal es principal. □

El siguiente resultado es bien conocido.

Teorema. 13.6.
Sea A un anillo, son equivalentes:

(a) A es un cuerpo
(b) $A[X]$ es un dominio de ideales principales.

DEMOSTRACIÓN. (a) ⇒ (b) Es inmediato ya que $A[X]$ es un dominio euclídeo.
(b) ⇒ (a). Si $A[X]$ es un dominiode integridad, entonces A es un dominio de integridad. Dado que cada ideal primo de $A[X]$ es maximal por ser dominio de ideales principales, entonces (X) es maximal y $\frac{A[X]}{(X)} \cong A$ es un cuerpo. □

Visto esto, veamos como se puede generalizar este teorema para anillos de ideales principales en el que vamos a usar este resultado visto anteriormente:

Proposición. 13.7.
En un anillo de ideales principales todo ideal propio es un producto de ideales primos.

DEMOSTRACIÓN. Es consecuencia de que todo anillo de ideales principales es producto directo finito de dominios de ideales principales y anillos de ideales principales especiales. □

Teorema. 13.8.
Sea A un anillo, son equivalentes:

(a) $A[X]$ es un anillo de ideales principales.
(b) A es producto finito de cuerpos.

DEMOSTRACIÓN. (b) ⇒ (a). Es trivial dado que el producto de anillos de ideales principales es un anillo de ideales principales.
(a) ⇒ (b). Supongamos que $A[X]$ es un anillo de ideales principales, entonces $\dim(A[X]) \leq 1$. Como $A \cong A[X]/(X)$ tenemos que $A[X]/A$ es también un anillo de ideales principales y es noetheriano,

se tiene $1 \geq \dim(A[X]) = \dim(A) + 1$ luego $\dim(A) = 0$ y A es un anillo artiniano, y por tanto un producto finito de anillos artinianos locales. Ponemos $A = A_1 \times \cdots \times A_t$ con A_i anillo artiniano local y principal, $A_i[X]$ es un anillo de ideales principales.

Sea entonces A un anillo artiniano local principal con $A[X]$ anillo de ideales principales y sea $\mathfrak{m} = (a) \subseteq A$ su ideal maximal. Si $a = 0$ tenemos que A es un cuerpo. En caso contrario, consideramos el ideal $(a, X) \subseteq A[X]$, que ha de ser principal, es decir, $(a, X) = (F)$. Tenemos entonces

$$\frac{A[X]}{(F)} \cong \frac{A[X]}{(a,X)} \cong \frac{A}{(a)} \cong \frac{A}{\mathfrak{m}}.$$

Sabemos $A/\mathfrak{m}$ es un cuerpo, luego (F) es un ideal maximal de $A[X]$. Por otra parte, $\frac{A[X]}{(a)} \cong \frac{A[X]}{\mathfrak{m}[X]} = (\frac{A}{\mathfrak{m}})[X]$ que es un dominio de integridad y por tanto (a) es primo en $A[X]$.

Tenemos $(a) \subseteq (F)$, luego existe $G \in A[X]$ tal que $GF = a \in (a)$. Si $F \in (a)$, existe $H \in A[X]$ de manera que $F = aH$, por otro lado $X \in (F)$ luego existe $L \in A[X]$ tal que $X = FL$, entonces $X = FL = aHL$ y existiría $b \in A$ tal que $1 = ab$ lo cual no puede ocurrir ya que $(a) \neq A$. Si $G \in (a)$, existe $H \in A[X]$ de manera que $G = aH$, por tanto $a = FG = aFH$ y $a(1 - FH) = 0$. Como $\mathrm{Jac}(A[X]) = \mathrm{Jac}(A)[X] = \mathfrak{m}[X] = (a)$ y $\mathrm{Div}(A[X]) = (a)$, (divisores de cero), tenemos $(1 - FH) \in \mathrm{Jac}(A[X])$ y $FH = 1 - (1 - FH) \in A[X]$ es invertible, esto es, $F \in A[X]$ es invertible, lo cual es una contradicción.

Por tanto cada A_i de $A = A_1 \times \cdots \times A_t$ es un cuerpo y A es producto de cuerpos. □

Capítulo V

Resultados de Sharma

Nuestro objetivo sigue siendo estudiar los ideales primos principales. En el caso de anillo de polinomios tiene resultados de interés que queremos estudiar. Podemos reducir el caso general al caso de dominos de integridad, por esto desarrollamos la teoría para esto súltimos.

14. Ideales invertibles

Definición. 14.1.
Sea A un anillo y $\Sigma \subseteq A$ un subconjunto multiplicativamente cerrado. Consideramos $A \times \Sigma$ y definimos una relación de equivalencia de manera que

$$(a_1, s_1) \sim (a_2, s_2) \text{ si existe } t \in \Sigma \text{ tal que } t(a_1 s_2 - a_2 s_1) = 0.$$

Llamamos $\Sigma^{-1}A = \dfrac{A \times \Sigma}{\sim}$ y representamos la clase $[(a,s)]$ por $\frac{a}{s}$.
En $\Sigma^{-1}A$ definimos operaciones
(1) Suma: $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$
(2) Producto: $\frac{a_1}{s_1} \times \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$
(3) Elemento 0: $\frac{0}{1}$
(4) Elemento 1: $\frac{1}{1}$

Así $\Sigma^{-1}A$ es un anillo.

Definición. 14.2.
El anillo $\Sigma^{-1}A$, con Σ multiplicativamente cerrado, se le llama la **localización** del anillo A en Σ.

Lema. 14.3.
La aplicación $\theta : A \longrightarrow \Sigma^{-1}A$, dada por $\theta(a) = \frac{a}{1}$, es un homomorfismo de anillos, que es inyectivo si, y sólo si, Σ no contiene divisores de cero.

DEMOSTRACIÓN. Tenemos:

$$\begin{aligned}\theta(a_1+a_2)&=\tfrac{a_1+a_2}{1}=\tfrac{a_1}{1}+\tfrac{a_2}{1}=\theta(a_1)+\theta(a_2).\\ \theta(a_1a_2)&=\tfrac{a_1a_2}{1}=\tfrac{a_1}{1}\tfrac{a_2}{1}=\theta(a_1)\theta(a_2).\\ \theta(1)&=\tfrac{1}{1}.\end{aligned}$$

Para la segunda parte basta tener en cuenta que se tiene $\mathrm{Ker}(\theta)=\{a\in A\mid \text{ existe } t\in\Sigma \text{ tal que } ta=0\}$. □

Dado $\mathfrak{a}$ un ideal de A se tiene un ideal de $\Sigma^{-1}A$, definimos:

$$\begin{aligned}\langle\theta(\mathfrak{a})\rangle&=\langle\{\tfrac{a}{1}\mid a\in\mathfrak{a}\}\rangle\\ &=\{\textstyle\sum_i \frac{a_i}{1}\frac{m_i}{s_i}\mid a_i\in\mathfrak{a}, m_i\in A,\ s_i\in\Sigma\}\\ &=\{\tfrac{a}{s}\mid a\in\mathfrak{a},\ s\in\Sigma\}=\mathfrak{a}^e.\end{aligned}$$

Dado $\mathfrak{b}$ un ideal de $\Sigma^{-1}A$, tenemos que $\theta^{-1}(\mathfrak{b})=\{a\in A\mid \frac{a}{1}\in\mathfrak{b}\}=\mathfrak{b}^c$, es un ideal de A.

Así, $\mathfrak{a}^{ec}=\{a\in A\mid \frac{a}{1}\in\mathfrak{a}^e\}=\{a\in A|\text{existe } t\in\Sigma \text{ tal que } ta\in\mathfrak{a}\}$, luego existen casos en los que $\mathfrak{a}\subsetneq\mathfrak{a}^{ec}$.

Ahora bien, ¿qué ocurre si $\mathfrak{a}=\mathfrak{p}$ es primo?

Si existiera $a\in\mathfrak{p}^{ec}\setminus\mathfrak{p}$, existe $t\in\Sigma$ tal que $ta\in\mathfrak{p}$, luego $t\in\mathfrak{p}$, y se tiene $1=\frac{t}{1}\frac{1}{t}\in\mathfrak{p}^e$, por tanto $\mathfrak{p}^{ec}=A$.

En resumen, si $\mathfrak{a}\cap\Sigma\neq\emptyset$, entonces $\mathfrak{a}^e=\Sigma^{-1}A$, y $\mathfrak{a}^{ec}=A$. Por otro lado, si $\mathfrak{a}\cap\Sigma=\emptyset$, entonces $\mathfrak{a}^e\neq\Sigma^{-1}A$.

De esta manera si tomamos $\mathfrak{a}=\mathfrak{p}$ primo y $\mathfrak{a}\cap\Sigma=\emptyset$, tendremos $\mathfrak{p}=\mathfrak{p}^{ec}$.

Lema. 14.4.
Sea $\mathfrak{p}$ un ideal primo del anillo A, entonces $A\setminus\mathfrak{p}$ es multiplicativamente cerrado.

DEMOSTRACIÓN. Se tiene $1\in A\setminus\mathfrak{p}$, ya que $1\notin\mathfrak{p}$. Si $s_1,s_2\in A\setminus\mathfrak{p}$, entonces $s_1,s_2\notin\mathfrak{p}$, $s_1s_2\notin\mathfrak{p}$, y $s_1s_2\in A\setminus\mathfrak{p}$. □

Notaremos al anillo $(A\setminus\mathfrak{p})^{-1}A$ simplemente como $A_{\mathfrak{p}}$.

Observación. 14.5.
El anillo $A_{\mathfrak{p}}$ tiene un único ideal maximal, es decir, es un anillo local. El ideal maximal es $\mathfrak{p}^e=\mathfrak{p}A_{\mathfrak{p}}$.

Sea D un dominio y K su cuerpo de fracciones, se tiene $K=\{\frac{a}{b}\mid a,b\in D,\ b\neq 0\}$. En particular $D\subseteq K$ es un subanillo, ya que $D\setminus\{0\}$ no contiene divisores de cero.

15. Ideales fraccionarios

Suponemos que tenemos un dominio de integridad D con cuerpo de fracciones K.

Definición. 15.1.
Un subconjunto $\mathfrak{a} \subseteq K$ es un **ideal fraccionario** de para D si:

(1) $a_1d_1 + a_2d_2 \in \mathfrak{a}$ para todo $d_1, d_2 \in D$ y $a_1, a_2 \in \mathfrak{a}$.
(2) $\mathfrak{a} \neq 0$.
(3) Existe $0 \neq b \in D$ tal que $\mathfrak{a}b \subseteq D$.

Definición. 15.2.
Un subconjunto $\mathfrak{a} \subseteq K$ es un **ideal entero** de D si:

(1) $\mathfrak{a}$ es un ideal fraccionario.
(2) $\mathfrak{a} \subseteq D$.

Observación. 15.3.
Todo ideal no nulo de D es un ideal entero.

Observación. 15.4.
Dado un ideal $\mathfrak{a}$ de K finitamente generado, $\mathfrak{a} = (\frac{a_1}{b_1}, \ldots, \frac{a_t}{b_t})$, podemos poner los generadores con denominador común y tenemos $\mathfrak{a} = (\frac{a_1}{s}, \ldots, \frac{a_t}{s})$, por tanto $s\mathfrak{a} = (a_1, \ldots, a_t) \subseteq D$, y es un ideal fraccionario de D.

Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales fraccionarios, tenemos:

(1) $\mathfrak{a}\mathfrak{b} = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ es un ideal fraccionario.
(2) $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ es un ideal fraccionario. En efecto, si $\mathfrak{a}d_1 \subseteq D$ y $\mathfrak{b}d_2 \subseteq D$, entonces $(\mathfrak{a} + \mathfrak{b})d_1d_2 \subseteq D$.
(3) $(\mathfrak{a} : \mathfrak{b}) = \{x \in K \mid bk \in \mathfrak{a} \text{ para todo } b \in \mathfrak{b}\}$. ¿Qué ocurre con $(\mathfrak{a} : \mathfrak{b})$? ¿Es un ideal fraccionario?

Lema. 15.5.
Si $\mathfrak{a}$ y $\mathfrak{b}$ son dos ideales fraccionarios y $(\mathfrak{a} : \mathfrak{b}) \neq 0$, entonces $(\mathfrak{a} : \mathfrak{b})$ es un ideal fraccionario.

DEMOSTRACIÓN. Sea $0 \neq d \in D$ tal que $d\mathfrak{a} \subseteq D$, y sea $0 \neq b \in \mathfrak{b}$, entonces $b(\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a}$, y se tiene $db(\mathfrak{a} : \mathfrak{b}) \subseteq d\mathfrak{a} \subseteq D$. □

Observación. 15.6.
Para dos ideales fraccionarios cualesquiera se tiene $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$

Definimos $\mathscr{L}(D) = \{\mathfrak{a} \subseteq D \mid \mathfrak{a} \text{ es un ideal fraccionario}\}$. Así el producto de ideales es una operación en $\mathscr{L}(D)$ que es asociativa y que tiene a D con elemento neutro. Por tanto $\mathscr{L}(D)$, con el producto, tiene estructura de monoide.
Dado $\mathfrak{a} \in \mathscr{L}(D)$ nos preguntamos si existe $\mathfrak{b} \in \mathscr{L}(D)$ tal que $\mathfrak{a}\mathfrak{b} = D$.

Para responder a esta pregunta, vamos a ver, dado $\mathfrak{a}$, como sería, en caso de existir, este ideal $\mathfrak{b}$. Podemos llamarlo $\mathfrak{a}^{-1}$.
Tendríamos $\mathfrak{a}\mathfrak{a}^{-1} = D$, por tanto $\mathfrak{a}^{-1} \subseteq (D : \mathfrak{a})$, y se tiene

$$D : \mathfrak{a} = (D : \mathfrak{a})D = (D : \mathfrak{a})\mathfrak{a}\mathfrak{a}^{-1} \subseteq D\mathfrak{a}^{-1} = \mathfrak{a}^{-1}.$$

Como consecuencia, $\mathfrak{a}^{-1} = (D : \mathfrak{a})$.
Para caracterizar los ideales $\mathfrak{a}$ que tienen inverso tendríamos que buscar una relación entre $\mathfrak{a}$ y $(D : \mathfrak{a})$, pero no existe ninguna lo que nos lleva a calcular $(D : (D : \mathfrak{a}))$, que sería $(\mathfrak{a}^{-1})^{-1}$, cuando tanto $\mathfrak{a}$ como su inverso son invertibles.
Tenemos: $\mathfrak{a} \subseteq (D : (D : \mathfrak{a})) = \{x \in D \mid x(D : \mathfrak{a}) \subseteq D\}$.
Tenemos pues la inclusión $\mathfrak{a} \subseteq (\mathfrak{a}^{-1})^{-1}$, que aplicada a $\mathfrak{a}^{-1}$ nos da la igualdad $\mathfrak{a}^{-1} = ((\mathfrak{a}^{-1})^{-1})^{-1}$; pero no siempre ocurre que $\mathfrak{a} = (\mathfrak{a}^{-1})^{-1}$.

Definición. 15.7.
Si D es un dominio de integridad, diremos que un ideal fraccionario $\mathfrak{a}$ es **invertible** si existe un ideal fraccionario $\mathfrak{b}$ de manera que $\mathfrak{a}\mathfrak{b} = D$.

Definición. 15.8.
Si D es un dominio, diremos que un ideal fraccionario $\mathfrak{a}$ es **divisorial** si $\mathfrak{a} = (D : (D : \mathfrak{a})) = (\mathfrak{a}^{-1})^{-1}$.

Lema. 15.9.
Sea $\mathfrak{a}$ un ideal fraccionario. Son equivalentes:
(a) $\mathfrak{a}$ es divisorial.
(b) $\mathfrak{a} = (D : \mathfrak{b})$ para algún ideal fraccionario $\mathfrak{b}$

DEMOSTRACIÓN. (a) $\Rightarrow$ (b) Trivial
(b) $\Rightarrow$ (a) Tenemos $(D : (D : \mathfrak{a})) = (D : (D : (D : \mathfrak{b}))) = (D : \mathfrak{b}) = \mathfrak{a}$. □

Proposición. 15.10.
Para cada ideal fraccionario $\mathfrak{a}$ se tiene $(D : (D : \mathfrak{a})) = \cap\{kD \mid \mathfrak{a} \subseteq kD\}$.

DEMOSTRACIÓN. Si $\mathfrak{a} \subseteq kD$, entonces $kD = (D : (D : kD)) \supseteq (D : (D : \mathfrak{a}))$ y $(D : (D : \mathfrak{a})) \subseteq \{kD \mid \mathfrak{a} \subseteq kD\}$. Luego tenemos una inclusión.
Veamos la otra: Para $0 \neq k \in K$ se tiene $\mathfrak{a} \subseteq kD$ si, y sólo si, $k^{-1}\mathfrak{a} \subseteq D$. Dado $x \in \cap\{kD \mid \mathfrak{a} \subseteq kD\} = \cap\{kD \mid k^{-1} \in (D : \mathfrak{a})\}$, tenemos entonces $x(D : \mathfrak{a}) \subseteq D$ y por tanto la otra inclusión. □

Como consecuencia de esto, si un ideal fraccionario es divisorial, entonces es intersección de los ideales fraccionarios principales que lo contienen y, además, para cada ideal fraccionario divisorial $\mathfrak{a}$ se tiene que $\mathfrak{a} \cap D$ es un ideal entero divisorial.

Proposición. 15.11.
Si un ideal no nulo es principal, $0 \neq \mathfrak{a} = D\frac{a}{b}$, *entonces* $\mathfrak{a}$ *es invertible y* $\mathfrak{a}^{-1} = D\frac{b}{a}$.

DEMOSTRACIÓN. La demostración es inmediata: $\frac{a}{b}D\frac{b}{a}D = \frac{a}{b}\frac{b}{a}D = D$. □

Proposición. 15.12.
Todo ideal fraccionario invertible, es finitamente generado.

DEMOSTRACIÓN. Sea $\mathfrak{a}\mathfrak{a}^{-1} = D$, entonces $1 = \sum_{i=1}^{t}\{a_i x_i \mid \ a_i \in \mathfrak{a},\ x_i \in \mathfrak{a}^{-1} = (D : \mathfrak{a})\}$. Así, dado cualquier $a \in \mathfrak{a}$, se tiene

$$a = \sum_i a a_i x_i = \sum_i \{a_i(a x_i) \mid \ a_i \in \mathfrak{a} x_i \subseteq D\}.$$

Por tanto, $a_1, \ldots, a_t$ es un sistema de generadores de $\mathfrak{a}$ como D–módulo. □

Consideremos ahora el caso en que D sea un **dominio local**, es decir, D tiene un único ideal maximal.

Proposición. 15.13.
Si D *es un dominio local, entonces todo ideal fraccionario invertible es principal.*

DEMOSTRACIÓN. Sea $\mathfrak{m}$ el único ideal maximal de D. Como existe $\mathfrak{a}^{-1}$ tal que $\mathfrak{a}\mathfrak{a}^{-1} = D$, tenemos una expresión $1 = \sum_i a_i b_i$, con $a_i \in \mathfrak{a}$ y $b_i \in \mathfrak{a}^{-1}$.
Si $a_i b_i \in \mathfrak{m}$ para todo índice i, entonces $1 \in \mathfrak{m}$, lo cual es una contradicción. Por tanto podemos suponer que existe un índice i tal que $a_i b_i \notin \mathfrak{m}$, entonces $a_i b_i$ es un elemento invertible en D, y existe $u \in D$ tal que $a_i b_i u = 1$. Dado $a \in \mathfrak{a}$, se tiene $a = a a_i b_i u = a_i(a b_i u)$ con $a_i \in \mathfrak{a}$ y $a b_i u \in D$. Luego a_i es un generador de $\mathfrak{a}$ y $\mathfrak{a}$ es un ideal principal. □

Teorema. 15.14.
Sea $\mathfrak{a} \in \mathscr{L}(D)$*. Son equivalentes:*

(a) $\mathfrak{a}$ *es invertible.*
(b) $\mathfrak{a}$ *es finitamente generado y* $\mathfrak{a}_\mathfrak{p} \in \mathscr{L}(D)$ *es principal para todo* $\mathfrak{p}$ *ideal primo de* $\mathfrak{a}$*.*

DEMOSTRACIÓN. (a) $\Rightarrow$ (b) Tenemos $\mathfrak{a}$ invertible, luego existe $\mathfrak{b}$ de manera que $\mathfrak{ab} = D$ y podemos escribir $1 = \sum_{i=1}^{t} a_i b_i$ con $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$. Sea $a \in \mathfrak{a}$, entonces $a = a1 = a\sum_{i=1}^{t} a_i b_i$, luego $\mathfrak{a} = (a_1, ldots, a_t)$ finitamente generado.
Dado que $D_\mathfrak{p} = (\mathfrak{ab})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathfrak{b}_\mathfrak{p}$, tenemos que $\mathfrak{a}_\mathfrak{p}$ es invertible. Por otro lado, tenemos que existe $0 \neq d \in D$ de manera que $\mathfrak{a}d \subseteq D$, luego $\mathfrak{a}_\mathfrak{p} d \subseteq D_\mathfrak{p}$. Luego $\mathfrak{a}_\mathfrak{p} \in \mathscr{L}(D_\mathfrak{p})$ y es principal.
(b) $\Rightarrow$ (a) Tenemos $\mathfrak{a}\mathfrak{a}^{-1} \subseteq D$ con $\mathfrak{a}^{-1} = (D : \mathfrak{a})$. Entonces $(\mathfrak{a}^{-1})_\mathfrak{p} = (D_\mathfrak{p} : \mathfrak{a}_\mathfrak{p}) = (\mathfrak{a}_\mathfrak{p})^{-1}$. Como $\mathfrak{a}_\mathfrak{p}$ es principal, es invertible y tenemos:

$$(\mathfrak{a}\mathfrak{a}^{-1})_\mathfrak{p} \subseteq D_\mathfrak{p}$$

$$(\mathfrak{a}\mathfrak{a}^{-1})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}(\mathfrak{a}^{-1})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})^{-1} = D_\mathfrak{p}.$$

Como esto es valido para cualquier ideal primo, tenemos $\mathfrak{a}\mathfrak{a}^{-1} = D$ y por tanto nuestro ideal es invertible. □

16. Ideales primos principales

Vamos a ver algunos resultados de Sharma para anillos de polinomios para los cuales necesitaremos este resultado previo sobre ideales primos en un anillo de polinomios:

Teorema. 16.1.
Dado un ideal primo $\mathfrak{p} \subseteq A[X]$, se tiene que $\mathfrak{p} \cap A$ es un ideal primo de A.

DEMOSTRACIÓN. Supongamos que no es primo, es decir, $\frac{A}{\mathfrak{p}\cap A}$ no es un dominio de integridad: existen $a, b \neq 0$ de manera que $ab = 0$. Es decir $a, b \notin \mathfrak{p} \cap A$ y $ab \in \mathfrak{p} \cap A$. Tenemos entonces $ab \in \mathfrak{p}$, como $\mathfrak{p} \subseteq A[X]$ es primo, o bien $a \in \mathfrak{p}$ o bien $b \in \mathfrak{p}$ y por tanto $a \in \mathfrak{p} \cap A$ o $b \in \mathfrak{p} \cap A$, lo cual es una contradicción, luego es primo. □

Teorema. 16.2.
Sea D un dominio de integridad y $\mathfrak{p}$ un ideal primo de $D[X]$ de manera que $\mathfrak{p} \cap D = 0$. Sea $p(X) = a_0X^d + \cdots + a_{d-1}X + a_d$ un polinomio de mínimo grado en $\mathfrak{p}$. Son equivalentes:
(a) $\mathfrak{p} = (p(x))$.
(b) No existe $t \notin (a_0)$ tal que $ta_i \in (a_0)$ para $1 \leq i \leq d$.

Llamamos a $p(X)$ un **polinomio de Sharma**.

DEMOSTRACIÓN. (a) ⇒ (b). Supongamos que existe $t \notin (a_0)$ de manera que $ta_i \in (a_0)$ para $1 \leq i \leq d$. Tenemos $ta_i = \alpha_i a_0$ para $1 \leq i \leq d$ y $\alpha_i \in D$. Tenemos entonces $a_0(tX^d + \alpha_1X^{d-1} + \cdots + \alpha_d) = tp(x) \in \mathfrak{p}$. Ahora bien, dado que $\mathfrak{p}$ es primo y $a_0 \notin \mathfrak{p}$ ya que $\mathfrak{p} \cap D = 0$ y $a_0 \neq 0$, tenemos $tX^d + \alpha_1X^{d-1} + \cdots + \alpha_d \in \mathfrak{p}$.
Como $\mathfrak{p} = (p(x))$ y el grado de $p(x)$ es d, existe $\lambda \in D$ de manera que $\lambda p(x) = tX^d + \alpha_1X^{d-1} + \ldots + \alpha_d$. De esta expresión obtenemos $t = \lambda a_0$, contradicción dado que habíamos supuesto $t \notin (a_0)$.
(b) ⇒ (a). Sea $g(x) \in \mathfrak{p}$, si consideramos $A = D[1/a_0][X]$, entonces $p(x)$ tiene un coeficiente líder invertible en A. Podemos encontrar $h(x), r(x) \in D[X]$ tales que

$$a_0^m g(x) = p(x)h(x) + r(x)$$

con $\text{grad}(r(x)) < d$. Tenemos entonces

$$r(x) = a_0^m g(x) - p(x)h(x) \in \mathfrak{p}.$$

Luego $r(x) = 0$ y por tanto $a_0^m g(x) = p(x)h(x)$. Elegimos N mínimo de manera que

$$a_0^N g(x) = p(x)h(x).$$

Si $N = 0$ obtenemos $g(x) \in (p(x))$. Supongamos entonces $N > 0$ y consideramos la proyección $D[X] \longrightarrow D/(a_0)[X]$. Entonces $0 = a_0^m g(x) + D/(a_0)[X] = p(x)h(x) + D/(a_0)[X]$. Si $h(x) + D/(a_0)[X] = 0$, cada coeficiente de $h(x)$ es múltiplo de a_0, llamamos $h'(x) = \frac{h(x)}{a_0}$ y tenemos $a_0^{N-1} g(x) = p(x)h'(x)$ lo cual contradice la minimalidad de N. Por tanto, $h(x) + R/(a_0)[X] \neq 0$. Luego $p(x)$ es un divisor de cero en $R/(a_0)[X]$, es decir, existe $t \notin (a_0)$ tal que $ta_i \in (a_0)$ para todo $1 \leq i \leq d$, contradicción con la hipótesis. Tenemos pues $g(x) = p(x)h(x)$, luego $\mathfrak{p} = (p(x))$. □

Corolario. 16.3.
Sea D un dominio de factorización única y $\mathfrak{p}$ un ideal primo de $D[X]$ de manera que $\mathfrak{p} \cap D = \{0\}$. Existe un polinomio irreducible $p(x)$ de grado mínimo entre los elementos no nulos de $\mathfrak{p}$ de manera que $\mathfrak{p} = (p(x))$.

DEMOSTRACIÓN. Tomamos $p(x) \in \mathfrak{p}$ del teorema anterior tal que el máximo común divisor de sus coeficientes,$a_0, \ldots, a_d$ sea 1 y supongamos que existe $t \notin (a_0)$ de manera que $ta_i \in (a_0)$ para todo $1 \leq i \leq d$, es decir, existen λ_i de manera que $ta_i = \lambda_i a_0$ para cada $1 \leq i \leq d$. Tenemos entonces

$$t \operatorname{mcd}(a_1, \ldots, a_d) = a_0 \operatorname{mcd}(\lambda_1, \ldots, \lambda_d).$$

Tenemos por tanto que $a_0 | t$ ya que $\operatorname{mcd}(a_0, \operatorname{mcd}(a_1, \ldots, a_d)) = 1$, lo cual es una contradicción. Luego no existe tal t y $\mathfrak{p} = (p(x))$. □

Como consecuencia, tenemos este resultado debido a Kaplansky.

Corolario. 16.4.
Sea D un dominio de integridad y $0 \neq a, b \in D$, entonces $(aX + b)$ es un ideal primo de $D[X]$ si, y solo si a no es divisor de cero y b no es divisor de cero en $D/(a)$.

DEMOSTRACIÓN. ($\Rightarrow$) Si $(aX + b)$ es un ideal primo, es inmediato por el teorema.
($\Leftarrow$) Si $mcd(a, b) = 1$, $(aX + b) = \mathfrak{q}$ es un ideal primo en $K[X]$ siendo K el cuerpo de fracciones de D. Consideramos $\mathfrak{p} = \mathfrak{q} \cap D$. Entonces claramente $(aX + b)$ es un ideal primo de $D[X]$ conteniendo a $(aX + b)$ tal que $\mathfrak{p} \cap D[X] = 0$. El resto es inmediato. □

Corolario. 16.5.
Sea D un dominio de integridad y $\mathfrak{a} \neq 0$ un ideal de $D[X]$ tal que $\mathfrak{a} \cap D = \{0\}$. Si existe un polinomio $p(x) \in \mathfrak{a}$ de grado mínimo en $\mathfrak{a}$ y $\mathbf{c}(p(x)) = D$, entonces $\mathfrak{a} = (p(x))$.

DEMOSTRACIÓN. Sea $p(x) = a_0X^d + \cdots + a_d$ y sea $t \in D$ tal que $ta_i \in (a_0)$, entonces dado que $\mathbf{c}(p(x)) = D$ tenemos $t \in (a_0)$. Luego, por el teorema, se da el resultado. □

Observación. 16.6.
El teorema es válido suponiendo únicamente que a_0 no sea divisor de cero.

Vamos a ver ahora algunas condiciones que dio Sharma para ver cuando un ideal es invertible.

Definición. 16.7.
Diremos que un anillo A es **regular** si es un anillo noetheriano de manera que cualquier localización con $\Sigma = A \setminus \mathfrak{p}$, para cada ideal primo $\mathfrak{p}$, cumple la siguiente propiedad: El mínimo número de generadores de su ideal maximal coincide con la dimensión de Krull.

Lema. 16.8.
Sea D un dominio regular. Todo ideal primo $\mathfrak{p}$ de $D[X]$ tal que $\mathfrak{p} \cap D = \{0\}$ es invertible en $D[X]$.

DEMOSTRACIÓN. El resultado estará probado viendo $\mathfrak{p}_{\mathfrak{m}}$ es principal para cada ideal maximal de $D[X]$. Cogemos entonces $\mathfrak{m}$ maximal en $D[X]$, entonces $\mathfrak{m} \cap D = \mathfrak{q}$ es un ideal primo de D. Vamos a ver $\mathfrak{p}_{\mathfrak{q}}[X]$ es principal. Si $\mathfrak{q} = (0)$ entones $D_{\mathfrak{q}} = K$, el cuerpo de fracciones de D y el resultado es trivial. Si $\mathfrak{q} \neq 0$, $D_{\mathfrak{q}}$ es un dominio de factorización única y el resultado es consecuencia del primer corolario. □

Teorema. 16.9.
Sea D un dominio de integridad noetheriano y $\mathfrak{p}$ un ideal primo de $D[X]$ tal que $\mathfrak{p} \cap D = (0)$. Si existe un polinomio $p(x) \in \mathfrak{p}$ de grado mínimo en $\mathfrak{p}$ de manera que su contenido es un ideal invertible de D entonces $\mathfrak{p}$ es invertible en $D[X]$.

DEMOSTRACIÓN. Sea $p(x) = a_0X^d + a_1X^{d-1} + \cdots + a_d$ y $\mathfrak{a} = \mathbf{C}(p(x))$ invertible. Para cada ideal $\mathfrak{q} \in \operatorname{Spec}(D)$, $\mathfrak{a}_{\mathfrak{q}}$ es un ideal principal. Es fácil ver que para cada $\mathfrak{q} \in \operatorname{Spec}(D)$ existe $h(x) \in D[X]$, $c \in D$ y $s \in R \setminus \mathfrak{q}$ tal que

$$\frac{p(x)}{1} = \frac{c}{s}\frac{h(x)}{1}$$

en $D_{\mathfrak{q}}[X]$ y $\mathbf{C}(h(x)) \not\subseteq \mathfrak{q}$. Sea $\mathfrak{b}$ el ideal generado por tales $h(x)$. De la expresión anterior obtenemos

$$\frac{s}{c}p(x) = h(x)$$

$$\frac{s}{c}\mathfrak{a} = \mathbf{C}(h(x)) \subseteq D,$$

de lo cual se deduce

$$h(x) \in \mathfrak{a}^{-1}p(x),$$

luego

$$\mathfrak{b} \subseteq \mathfrak{a}^{-1}p(x).$$

Además de $\frac{s}{c}p(x) = h(x)$ deducimos que dado $\mathfrak{q} \in \mathrm{Spec}(D)$, existe $s \in D \setminus \mathfrak{q}$ tal que $sp(x) \in \mathfrak{b}$, luego $p(x) \in \mathfrak{b}$.

Tenemos también $\frac{s}{c}\mathfrak{a} = \mathbf{C}(h(x)) \not\subseteq \mathfrak{q}$. Luego los elementos de la forma s/c generan $\mathfrak{a}^{-1}$ y como $s/cp(x) = h(x) \in \mathfrak{b}$, tenemos $\mathfrak{b} = \mathfrak{a}^{-1}p(x)$.

Por otro lado $sp(x) = ch(x) \in \mathfrak{p}$ dado que $p(x) \in \mathfrak{p}$. Como $\mathfrak{p} \cap D = (0)$, tenemos $h(x) \in \mathfrak{p}$ por ser un ideal primo.

Tenemos como conclusión que para cada $\mathfrak{q} \in \mathrm{Spec}(D)$, existe un polinomio $h(x) \in \mathfrak{p}$ de grado d y cuyo contenido no está contenido en $\mathfrak{q}$. Ahora, fijamos $\mathfrak{q}_1 \in \mathrm{Spec}(D)$, existe un polinomio $g(x) \in \mathfrak{p}$ de grado d, mínimo grado entre los elementos de $\mathfrak{p}$, con $\mathbf{C}(g(x)) \not\subseteq \mathfrak{q}_1$. Entonces el representante $g'(x)$ de $g(x)$ en $\mathfrak{p}_{\mathfrak{q}}[X]$ tiene grado mínimo entre los elementos de tal conjunto y $\mathbf{C}(g'(x)) = D_{\mathfrak{q}_1}$, luego por el tercer corolario $\mathfrak{p}_{\mathfrak{q}_1}[X]$ es principal y por tanto invertible en $D[X]$. □

Índice alfabético

Bibliografía

[1] D. D. Anderson, *GCD domains, Gauss' lemma and content of polynomials*, Non-noetherian commutative ring theory. Math. Appl. 520. Kluwer Acad. Publ, 2000, pp. 1–13. 4.7.

[2] G. Angermuller, *Triangular systems and a generalization of primitive polynomials*, J. Symb. Comp. **68** (2015), 316–325.

[3] M. F. Atiyah and I. G. Macdonald, *Introducción al álgebra conmutativa*, Reverté, Barcelona, 1973. 7

[4] J.-H. Chun and J.-W. Park, *Principal ideals in skew polynomial rings*, Comm. Korean Math. Soc. **14** (1999), 699–706.

[5] W. Cortes and M. Ferrero, *Principal ideals in ore extensions*, Math. J. Okayama Univ. **46** (2004), 77–84.

[6] T. W. Hungerford, *On the structure of principal ideal rings*, Pacific J. Math. **25** (1968), 543–547.

[7] I. Kaplansky, *Commutative rings*, Chicago Univ. Press, 1974.

[8] W. M. McGovern and M. Sharma, *Gaussian property of the rings r(x) and r(x)*, Comm. Algebra **44** (2016), 1636–1646.

[9] P. K. Sharma, *A note on ideals in polynomial rings*, Arch. Math. (Basel) **37** (1981), 325–329.

[10] _____, *Polynomials contained in a finite number of maximal ideals*, Comm. Algebra **31 (7)** (2003), 3159–3170.