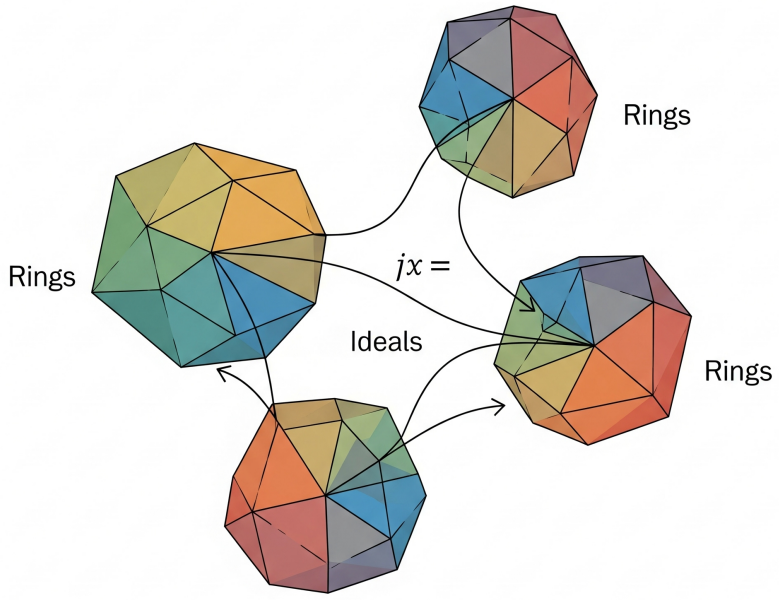
Universidad de Cantabria

Facultad de Ciencias

Álgebra conmutativa



Autores: Alberto Campuzano y Silvia Rifá

4º Doble Grado Física y Matemáticas

Última edición: 1 de junio de 2025

Estos apuntes, elaborados por Alberto Campuzano y Silvia Rifá, recogen lo visto en la asignatura de Álgebra Conmutativa (G92) de la Universidad de Cantabria. En la guía docente de la asignatura viene la bibliografía recomendada y seguida por el profesor, si bien otro tipo de referencias han sido debidamente citadas a lo largo del documento. Estas notas se corresponden con los conocimientos impartidos en las clases así como los ejercicios dispuestos en el aula virtual. No se pretende tomar propiedad de la autoría de las demostraciones o ejercicios aquí expuestos, simplemente se recopilan dichos resultados con fin de ordenarlos de cara al estudio. Sea dicho también que ciertas demostraciones sí que son propias, así como es obvio, los comentarios realizados a lo largo de las notas. Esperamos que sean de utilidad.

Índice general

Capítulo 1: Introducción

Comenzaremos estas notas introduciendo las nociones básicas y propiedades que atañen a la asignatura.

1.1. Anillos

Introducimos la estructura algebraica básica sobre la que se desarrollará toda la asignatura: los *anillos*. Se dará su definición formal, ejemplos y ciertas propiedades y relaciones.

Definición 1.1.1. Llamamos anillo a una tupla $(A, +, \cdot)$ que verifica las siguientes propiedades:

(I) $(A, +)$ es un grupo conmutativo con elemento neutro 0_A.

(II) la aplicación $\cdot : A \times A \longrightarrow A$ verifica que:

  (1) Es interna, $\forall a, b \in A, a \cdot b \in A$..

  (2) Cumple la propiedad asociativa, es decir, $\forall a, b, c \in A, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Unitario Tiene elemento neutro, que denotamos como 1_A.

(III) Se cumple la propiedad distributiva: $\forall a, b, c \in A, (a+b) \cdot c = a \cdot c + b \cdot c$ y $a \cdot (b+c) = a \cdot b + a \cdot c$.

Si adicionalmente se tiene que el producto $(\cdot)$ es conmutativo, entonces diremos que A es un *anillo conmutativo y unitario*. Ponemos a continuación una serie de ejemplos de anillos, conmutativos y no conmutativos, si bien todos son unitarios.

Ejemplo 1.1.1. Anillos más comunes:

Anillos no conmutativos:

- Las matrices $M_n(A)$ donde A es un anillo con $n > 1$.
- Los cuaterniones, $\mathbb{H}$.
- El conjunto de todos los enfomorfismos de R-módulos en sí mismo, $\mathrm{End}_R(M)$.

Anillos conmutativos

- Si A es un anillo conmutativo, $A[x]$ su anillo de polinomios también lo es.
- Los cuerpos $\mathbb{K}$.

- Los enteros, $\mathbb{Z}$.

Del mismo modo introducimos los subanillos:

Definición 1.1.2. Sea A un anillo y $B \subseteq A$ un subconjunto de A no vacío, entonces, B es un subanillo de A si:

(I) B es un subgrupo de A.

(II) Es un anillo con las operaciones de A restringidas a B.

(III) Si $1_A = 1_B$.

Y damos de nuevo una serie de ejemplos

Ejemplo 1.1.2. Subanillos.

- $\mathbb{Z} \subseteq \mathbb{Q}$.
- $\mathbb{C} \subseteq \mathbb{H}$.
- $\mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{Q} \times \mathbb{Q}$ con las operaciones coordenada a coordenada.

Observación 1.1.1. Nótese que es muy importante la última condición de la definición 1.1.2, pues si consideramos $\mathbb{Z} \times \{0\}$, se verifican los dos primeros requisitos, pero $1_{\mathbb{Z}\times\{0\}} = (1,0) \neq (1,1) = 1_{\mathbb{Z}\times\mathbb{Z}}$.

Comenzamos ahora con las primeras propiedades de los anillos.

Proposición 1.1.1. *En un anillo A, se tiene que* $\forall x \in A, 0_A \cdot x = 0$.

Demostración. Sea $x \in A$, tenemos que

$$x = 1_A \cdot x = (0_A + 1_A) \cdot x = 0_A \cdot x + 1_A \cdot x \Rightarrow 0_A = 0_A \cdot x$$

, donde se ha hecho uso de la existencia de neutro para la suma y producto de A y la propiedad distributiva de la definición 1.1.1. ■

Ahora bien, podemos plantearnos a partir de la demostración anterior, ¿qué ocurre en un anillo en el que $0_A = 1_A$?¿Cómo son los elementos? Respondemos a esta pregunta de manera muy rápida.

Teorema 1.1.1. $A \cong \{0\}$ *el anillo trivial* $\iff 1_A = 0_A$.

Demostración. La implicación de izquierda a derecha es trivial mientras que la de derecha a izquierda se sigue de la siguiente cadena de igualdades:

$$\forall x \in A, x = 1_A \cdot x = 0_A \cdot x = 0_A \Rightarrow x = 0_A, \forall x \in A$$

donde hemos hecho uso de la proposición 1.1.1 en la última igualdad. ■

1.2. Homomorfismos

Ahora, una vez hemos visto cómo son los anillos, nos interesa saber cómo relacionarlos. Para ello, introducimos el morfismo asociado a la categoría de anillo, los *homomorfismos* al igual que tenemos las aplicaciones lineales para la categoría vectorial o las aplicaciones continuas para la topología [[1], pág 4.].

Definición 1.2.1. Sean A y B dos anillos y $f : A \longrightarrow B$ una aplicación, decimos que es un *homomorfismo* de anillos si se verifica:

(I) $\forall x, y \in A, f(x +_A y) = f(x) +_B f(y)$.

(II) $\forall x, y \in A, f(x \cdot_A y) = f(x) \cdot_B f(y)$.

(III) $f(1_A) = 1_B$.

Podríamos pensar qué es lo que pasa con 0_A, pues las tres condiciones que damos van a la suma, producto y neutro del producto, pero esta duda nos la resuelve la siguiente propiedad:

Propiedad 1.2.1. Si $f : A \longrightarrow B$ es un homomorfismo de anillos, entonces $f(0_A) = 0_B$.

Demostración. $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) \Rightarrow 0_B = f(0_A)$. ■

Observación 1.2.1. Si intentamos hacer lo mismo para 1_A tenemos que

$$f(1_A) \stackrel{?}{=} f(1_A) \cdot f(1_A).$$

donde no podemos despejar como antes porque la existencia del inverso no está garantizada.

De modo que, básicamente lo que le exigimos a una aplicación para que me *relacione* bien dos anillos es que la suma y el producto se respeten y los neutros de ambas operaciones vayan a sus correspondientes entre anillos.

Ejemplo 1.2.1. Consideramos la aplicación:

$$\begin{aligned} \varphi : &\mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z} \\ &m \longmapsto (m, 0) \end{aligned}$$

Vemos que no es un homomorfismo, puesto que verifica:

(I) $\varphi(m + n) = (m + n, 0) = (m, 0) + (n, 0) = \varphi(m) + \varphi(n)$

(II) $\varphi(m \cdot n) = (m \cdot n, 0) = (m, 0) \cdot (n, 0) = \varphi(m) \cdot \varphi(n)$.

sin embargo, no cumple que

(III) $\varphi(1) = (1, 0) \neq (1, 1) = 1_{\mathbb{Z}\times\mathbb{Z}}$.

Otra propiedad fundamental a la hora de introducir el tipo de aplicaciones que relacionan nuestra categoría es cómo se comportan estos con la composición, probamos por tanto un *clásico*:

Proposición 1.2.1. *Sea $f : A \longrightarrow B$ y $g : B \longrightarrow C$ dos homomorfismos de anillos, entonces $g \circ f : A \longrightarrow C$ es un homomorfismo de anillos*

Demostración. Veamos que se cumplen las condiciones exigidas por la definición 1.2.1:

(I) $\forall a, b \in A$ se tiene que

$$(g \circ f)(a +_A b) = g(f(a) +_B f(b)) = g(f(a)) +_C g(f(b)) = (g \circ f)(a) +_C (g \circ f)(b)$$

Donde se ha utilizado que f y g verifican las condiciones I y II de la definición de homomorfismo (1.2.1).

(II) Se procede de manera análoga al caso anterior para el producto.

(III) $(g \circ f)(1_A) = g(f(1_A)) = g(1_B) = 1_C$ por ser f y g homomorfismos.

■

Queda por definir la idea de isomorfismo de anillos. No vamos a innovar en este sentido y nos quedamos con la que *cualquiera* podría pensar.

Definición 1.2.2. Un *isomorfismo de anillos* es un homomorfismo biyectivo, $f : A \longrightarrow B$.

Teorema 1.2.1. *Sea $f : A \longrightarrow B$ un isomorfismo de anillos, entonces la aplicación inversa $f^{-1} : A \longrightarrow B$ es un homomorfismo de anillos.*

Demostración. Veamos que se cumplen las condiciones exigidas por la definición 1.2.1:

(I) $\forall x, y \in B$ queremos ver que $f^{-1}(x +_B y) = f^{-1}(x) +_A f^{-1}(y)$. Llamando $a = f^{-1}(x)$ y $b = f^{-1}(y)$ en virtud de la biyectividad de f tenemos que

$$f(a + b) = f(a) + f(b) = x + y \Rightarrow f^{-1}(f(a + b)) = f^{-1}(x) + f^{-1}(y) = f^{-1}(x + y)$$

(II) Se procede de manera análoga al caso anterior para el producto.

(III) Como $f(1_A) = 1_B$, por la biyectividad tenemos que $f^{-1}(1_B) = 1_A$.

■

La consistencia entre los elementos neutros por homomorfismos nos permite responder a preguntas como ¿cuántos homomorfismos de anillos hay entre $\mathbb{Z}/3\mathbb{Z}$ y $\mathbb{Z}/4\mathbb{Z}$?. La respuesta es ninguno, puesto que si existiese uno tendríamos que

$$0_4 = f(0_3) = f(1_3 + 1_3 + 1_3) = 3_4\#.$$

Teorema 1.2.2. *Consideremos ahora Ring la clase de todos los anillos. Si A es un anillo tal que $\forall B$ anillo $\exists! f : B \longrightarrow A$ homomorfismo, entonces $A \cong \{0\}$*

Demostración. En primer lugar veamos que el anillo 0 verifica esta propiedad. Sea B un anillo cualquiera, solo puede existir una aplicación $f : B \longrightarrow 0$ que será la constante 0 por lo que se verifica la hipótesis.
Ahora comprobemos que es el único, salvo isomorfismo, que la verifica. Sea A un anillo que verifica las condiciones del enunciado, en particular tenemos que, tomando $B = 0$ debe existir $f : 0 \longrightarrow A$ homomorfismo, pero entonces se tiene que $f(0) = 1_A = 0_A$ y por el teorema 1.1.1 tenemos que $A \cong \{0\}$. ■

Teorema 1.2.3. *Sea Ring la clase de todos los anillos. Si A es un anillo tal que $\forall B$ anillo $\exists! f : A \longrightarrow B$ homomorfismo, entonces $A \cong \mathbb{Z}$-*

Demostración. Sea B un anillo, consideramos $A = \mathbb{Z}$ y entonces existe un homomorfismo:

$$\varphi : \mathbb{Z} \longrightarrow B \tag{1.1}$$

$$z \longmapsto \begin{cases} 0 & \text{si } z = 0 \\ (1_B + \cdots^z + 1_B) & \text{si } z > 0 \\ -(1_B + \cdots^z + 1_B) & \text{si } z < 0 \end{cases} \tag{1.2}$$

Este homomorfismo es único puesto que $\mathbb{Z}$ está generado por el 1, todo elemento de $\mathbb{Z}$ tiene su imagen en función de $f(1)$ y este por un homomorfismo es necesariamente 1_B. Supongamos ahora que existe otro anillo A que cumple la hipótesis. Entonces por las condiciones del enunciado deben existir:

$$\varphi : \mathbb{Z} \longrightarrow A$$
$$\vartheta : A \longrightarrow \mathbb{Z}$$

homomorfismos.
Considerando ahora la composición, tenemos:

$$\varphi \circ \vartheta : A \longrightarrow A$$
$$\vartheta \circ \varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$$

donde por la unicidad tenemos que necesariamente son la identidad y por tanto $A \cong \mathbb{Z}$. ■

Capítulo 2: Repaso

Daremos a continuación un repaso a conceptos de la asignatura de Estructuras algebraicas. De los apuntes de la misma han sido extraídas las definiciones que damos a continuación [2].

Definición 2.0.3. Sea R un anillo, diremos que $I \subseteq R$ es un ideal si:

(I) $I \neq \emptyset$.

(II) Si $a, b \in I$ entonces $a + b \in I$.

(III) Si $a \in I$ y $b \in R$ entonces $ab \in I$.

2.1. Teoremas de isomorfía en anillos

Estos teoremas, extendidos de los grupos a anillos, nos ayudan a comparar distintos anillos relacionados por homomorfismos y nos ayudan a comprender la estructura de los mismos. Además, nos servirán para aprovechar las propiedades de ciertos tipos de ideales y su relación con el anillo cociente.

Teorema 2.1.1 (Primer teorema de isomorfía)**.** *Sean R y S anillos, $f : R \longrightarrow S$ un homomorfismo de anillos, entonces se cumple que:*

$$R \Big/ Kerf \cong Imf$$

Teorema 2.1.2 (Segundo teorema de isomorfía)**.** [1] *Sean R un anillo, I un ideal de R y A un subanillo de R entonces se cumple que:*

$$A \Big/ (A \cap I)) \cong (A + I) \Big/ I$$

Teorema 2.1.3 (Tercer teorema de isomorfía)**.** *Sea R un anillo e I, J ideales de R con $I \subseteq J$. Entonces J/I es un ideal de R/I y se tiene que:*

$$(R/I) \Big/ (J/I) \cong R \Big/ J$$

[1] Destacar aquí que este teorema se puede extender en función de lo que se entienda por anillo. En el contexto de esta asignatura como los anillos son unitarios necesariamente los ideales *propios* no contienen 1_R de manera que un ideal no es un anillo. Este teorema requiere cierto *tecnicismo* a la hora de saber si se está pasando de ideales a anillos y de qué manera definimos estos. En cualquier caso esto es un *detalle* que no nos ocupará mucho en esta asignatura porque no haremos uso de él. En palabras de Luis Felipe: *no conocía la existencia de un segundo teorema de isomorfía de anillos.*

2.2. Dominios, cuerpos, DIP, DFU...

Clasificamos los anillos en función de ciertas propiedades que nos permitirán definir conceptos que tenemos bien trabajados, como la factorización, la divisibilidad, etc.

Definición 2.2.1. Sea R un anillo unitario y $a \in R$, decimos que a es una *unidad de* R si a tiene inverso para el producto, es decir, si existe $b \in R$ tal que $a \cdot b = 1_R$. Denotamos al conjunto de todas las unidades como R^*.

Definición 2.2.2. Sea R un anillo conmutativo y $a \in R$ un elemento, decimos que este es *divisor del cero* si existe $c \in R, c \neq 0_R$ tal que $a \cdot c = 0_R$

Definición 2.2.3. Sea R un anillo unitario y $a \in R$, se dice que a es nilpotente si $\exists n \in \mathbb{N}_{\geq 1}$ tal que $a^n = 0_R$.

Definición 2.2.4. Sea D un anillo, decimos que es *dominio de integridad* o simplemente *dominio* si se tiene que:

(I) D es un anillo conmutativo.

(II) D es un anillo unitario.

(III) El único divisor del cero en D es 0_D.

Definición 2.2.5. Sea D un dominio de integridad y $a \in D \backslash D^*$, decimos que:

(A) a es *irreducible* en D si se tiene que, si $a = bc, b, c \in D$ entonces $b \in D^* \vee c \in D^*$.

(B) a es *primo* en D si se tiene que, si $a \mid bc, b, c \in D$ entonces $a \mid b \vee a \mid c$.

Observación 2.2.1. En un dominio D, si a es primo entonces se puede demostrar que a es irreducible.

Definición 2.2.6. Sea F un anillo, decimos que es *cuerpo* si se tiene que:

(I) F es un anillo conmutativo.

(II) F es un anillo unitario.

(III) $F^* = F \backslash 0_F$

Propiedad 2.2.1. Sea R un anillo, son equivalentes:

(I) R es cuerpo.

(II) R tiene exactamente dos ideales

Demostración. Probemos ambas implicaciones:

- ($\Rightarrow$) Supongamos que R es cuerpo y veamos que sus ideales son (0) y $(1) = R$, que son distintos entre sí por ser cuerpo. Sea I un ideal de R, si $I = (0)$ hemos terminado. Supongamos ahora que $I \neq (0)$, entonces, $\exists t \in R \backslash \{0\}$ con $t \in I$. Como R es cuerpo tenemos que $\exists t^{-1}$ y por tanto $t \cdot t^{-1} \in I$, es decir, $1 \in I$ de manera que $I = (1)$.

- ($\Leftarrow$) Ahora supongamos que únicamente tenemos dos ideales. Entonces necesariamente $R \neq \{0\}$ porque tenemos dos ideales distintos y por tanto al menos un elemento que no es el cero. Sea $t \in R\backslash\{0\}$, veamos que tiene inverso. Consideramos $I = (t)$, como $t \neq 0$ entonces $(t) \neq (0)$ y por tanto $1 \in (t)$. Por definición de ideal generado $\exists s \in R$ tal que $1 = t \cdot s$ de modo que $s = t^{-1}$, como queríamos ver.

■

Proposición 2.2.1 (Ley de cancelación)**.** *Sean D un dominio y $a, b, c \in D$ con $a \neq 0_D$ se cumple que, si $ab = ac$ entonces $b = c$.*

Definición 2.2.7. Sea R un anillo e I un ideal de R. Decimos que I es un ideal *primo* si:

(I) $I \neq R$.

(II) $\forall a, b \in R$ tales que $ab \in I$ se tiene que $a \in I$ o $b \in I$.

Definición 2.2.8. Sea R un anillo e I un ideal de R. Decimos que I es un ideal *maximal* si:

(I) $I \neq R$.

(II) $\forall J$ ideal de R con $I \subseteq J \subseteq R$ se tiene que $I = J$ o $J = R$.

Observación 2.2.2. a primo en $D \iff (a)$ es un ideal primo de D

Observación 2.2.3. Todo ideal maximal es primo.

Teorema 2.2.1. *Sea R un anillo e I un ideal de R, entonces:*

$$R/I \text{ es dominio} \iff I \text{ es un ideal primo}$$

$$R/I \text{ es cuerpo} \iff I \text{ es un ideal maximal}$$

Demostración. Probemos cada una de las afirmaciones de este teorema:

(I) Veamos que dominio sii primo.

($\Rightarrow$) En primer lugar, como R/I es dominio entonces $0_{R/I} = 0_R + I$ es divisor del cero, de manera que existe un elemento $a + I$, disinto del cero, de modo que $(a + I)(0_R + I) = 0 + I$. De aquí tenemos que $a \notin I$ y por tanto $I \neq R$. Una vez visto esto, dados $a, b \in R$ tales que $ab \in R$, tenemos que $(a + I) \cdot (b + I) = (ab + I) = 0_{R/I}$ y como este es dominio tenemos que o bien $a = 0_{R/I}$ o $b = 0_{R/I}$, por lo que $a \in I \vee b \in I$, como queríamos ver.

($\Leftarrow$) En primer lugar, como I es un ideal primo entonces $\exists a \in R$ tal que $a \notin I$, de modo que $\bar{a} \neq \bar{0}$ y así $(a+I)(0+I) = 0_{R/I}$ y el $0_{R/I}$ es divisor del cero. Ahora, dados $(a + I), (b + I) \in R/I$, entonces $(a + I)(b + I) = (ab) + I$. Como I es primo tenemos que, $ab + I = 0 + I \Leftrightarrow ab \in I \Leftrightarrow a \in I \vee b \in I \Leftrightarrow (a + I) = 0_{R/I} \vee (b + I) = 0_{R/I}$, de modo que $0_{R/I}$ es el único divisor del cero y R/I es dominio.

(II) Veamos que cuerpo sii maximal.

($\Rightarrow$) Como I es maximal, entonces $1 \notin I$ y en $R/I, \bar{0} \neq \bar{1}$. Ahora, sea $x \in R/I \backslash \{\bar{0}\}$, veamos que tiene inverso. Sabemos que $\exists a \in R$ tal que $\bar{a} = x$. Como $a \notin I, I \subseteq I + (a) = (1)$ por ser I maximal. Por tanto $1 \in I + (a)$ y podemos escribir $1 = t + ab$ con $t \in I, b \in R$. Así pues, tomando cocientes tenemos que $\bar{1} = \bar{t} + \bar{a}\bar{b} = x\bar{b}$ de modo que x tiene inverso.

($\Leftarrow$) Supongamos que $\exists J$ ideal tal que $I \subsetneq J$ y veamos que $J = (1)$. De la contención tenemos que $\exists a \in J \backslash I$, de modo que $\bar{a} \in R/I \backslash \{0\}$. Como R/I es cuerpo entonces $\exists \bar{b}$ tal que $\bar{a}\bar{b} = \bar{1}$, ie, $\exists t \in I$ con $1 = ab^{\in J} + t^{\in I \subsetneq J}$ y por tanto $1 \in J$, concluyendo que I es maximal.

■

Definición 2.2.9. Sea D un dominio, decimos que es de *factorización única* (DFU) si:

(I) Cada elemento no nulo y que no es unidad se puede escribir como producto de irreducibles en D

(II) si $p_1, \ldots, p_n$ y $q_1, \ldots, q_m$ son elementos irreducibles en D tales que

$$p_1, \ldots, p_n = q_1, \ldots, q_m$$

entonces $m = n$ y los elementos están asociados [2].

Observación 2.2.4. En un DFU, se verifica el recíproco entre primo e irreducible, de manera que todo elemento irreducible es primo cerrando la relación: a es primo $\iff a$ es irreducible.

Observación 2.2.5. En un DFU, introducimos los conceptos de gcd y lmc.

Definición 2.2.10. Diremos que un ideal I es *principal* si $\exists a \in R$ tal que $I = \{at \mid t \in R\}$ y lo denotamos como $(a) = a \cdot R$.

Ejemplo 2.2.1 (Ideal no principal)**.** $I = (x^2, 2x)$ en $R = \mathbb{Z}[x]$

Demostración. Supongamos que $\exists a \in \mathbb{Z}[x]$ con $(x^2, 2x) = (a)$. Como $x^2 \in (x^2, 2x), \exists r_1 \in \mathbb{Z}[x]$ tal que $x^2 = ar_1$. De manera análoga, existe un r_2 tal que $2x = ar_2$. Bien, tenemos entonces que: $\deg(ar_2) = 1$ y como $\mathbb{Z}$ es dominio, entonces $\deg(a) \in \{0, 1\}$. Si fuera 0 entonces, escribiendo $a = x^2p_1 + 2xp_2$ y evaluando en cero tendríamos que $a = 0\#$ Por otro lado, si es 1, entonces $a = ux + v$ con $u, v \in Z$. Sin embargo, como $\mathbb{Z}$ es DFU (ver propiedad 2.2.2), entonces existe gcd y entonces, como $a \mid x^2$ y $a \mid 2x$, necesariamente $a = 1$ (lo hemos descartado antes por el grado) o $a = x$. Pero si fuera así $x = x^2f(x) + 2xg(x) \Rightarrow 1 = xf(x) + 2g(x)$ y de nuevo, evaluando en 0 tenemos que $1 = 2g(0) \in \mathbb{Z}\#$. ■

Definición 2.2.11. Sea D un dominio de integridad, diremos que es de *ideales principales* (DIP) si todo ideal es principal.

Observación 2.2.6. Si $\mathbb{K}$ es un cuerpo entonces $\mathbb{K}[x]$ su anillo de polinomios es un DIP.

Teorema 2.2.2. *Sea $\mathbb{K}$ un cuerpo, entonces $\mathbb{K}[x]$ es un DIP con exactamente dos ideales primos, (0) y (x).*

[2] Técnicamente tenemos que existe $\sigma \in S_n$ tal que $\forall i \in \{1, \cdots, n\}$ se tiene que $p_i \sim q_{\sigma(i)}$ donde la relación $\sim$ es la de ser asociados, definida como que existe una unidad u tal que $p_i = u \cdot q_{\sigma(i)}$

Demostración. Sea I un ideal de $\mathbb{K}[x]$, si $I = (0)$ o $I = (1)$ entonces es principal. En otro caso consideramos el conjunto

$$A = \{n \in \mathbb{N} \mid \exists \sum_{i=n}^{\infty} a_i x^i \in I \backslash \{0\}, a_n \neq 0\}$$

Dado que $I \neq 0$ entonces $A \neq \emptyset$ y por tanto existe un $n \in \mathbb{N}$ tal que $n = \text{mín}(A)$. Veamos que $I = (x^n)$.

- Vemos en primer lugar que $(x^n) \subseteq I$, como $n = \text{mín}(A)$ entonces $\exists f \in I$ tal que $f = a_n x^n + a_{n+1} x^{n+1} + \cdots = x^n(a_n + a_{n+1}x + \cdots) = x^n g$ con $a_n \neq 0$. Como $a_n \in \mathbb{K}$ entonces es unidad y g lo es (ver ejercicio 3.1.10), de este modo $x^n = fg^{-1} \in I$ de modo que $(x^n) \subseteq I$ como queríamos ver.

- Para la otra contención, $I \subseteq (x^n)$, tomamos $f \in I \backslash \{0\}$, entonces

  $$f = a_k x^k + a_{k+1} x^{k+1} + \cdots$$

  con $a_k \neq 0$. De la definición de A y de n tenemos entonces que $n \leq k$ y por tanto $f = x^n(a_k x^{n-k} + a_{k+1} x^{n-(k+1)} + \cdots) \in (x^n)$.

■

Teorema 2.2.3. *Todo dominio de ideales principales es un dominio de factorización única.*

Demostración. Ver Teorema II.5.26 en [2]. ■

Para finalizar este repaso damos la relación entre estos conjuntos:

Propiedad 2.2.2.

$$\{\text{Cuerpos}\} \subseteq \{\text{DIPs}\} \subseteq \{\text{DFUs}\} \subseteq \{\text{Dominios}\} \subseteq \{\text{Anillos}\}$$

Capítulo 3: Ideales

Una vez hemos hecho una revisión a los conceptos introducidos en la asignatura de Estructuras algebraicas a modo de preámbulo, pasamos al plato fuerte de la asignatura: los *ideales*. Cómo se definen, propiedades, tipos y conjuntos que podemos definir a partir de ellos. Así pues, remarcamos también que a partir de ahora, consideraremos en todo caso que estamos trabajando con anillos *conmutativos* y *unitarios*, ya que de esto va la asignatura.

3.1. Algunos resultados

Empezamos el capítulo con esta sección en la que damos algunos resultados acerca de los ideales, homomorfismos, etc.

Lema 3.1.1. *Sea J un ideal de R. Si $n \in \mathbb{N}, a_1, \ldots, a_n \in J$, entonces $\sum_{i=1}^{n} a_i \in J$.*

Demostración. Apliquemos inducción en n.

($n = 1$): $\sum_{i=1}^{n} a_i = a_1 \in J$ por hipótesis.

Suponiendo cierto para $k > 0$ demostremos para $k + 1$.

($n = k + 1$): $\sum_{i=1}^{+1} a_i = \sum_{i=1}^{k} a_i + a_{k+1}$. Aplicando hipótesis de inducción al primer sumando y llamando $\sum_{i=1}^{k} a_i = y$ tenemos $y^{\in J} + a_{k+1}^{\in J}$, de modo que por la definición de ideal se tiene el resultado.

■

Proposición 3.1.1. *Sea $S \subseteq R$ un conjunto, existe el menor ideal I tal que $S \subseteq I$ y lo denotamos por (S) el ideal generado por S. Además éste tiene la siguiente forma:*

$$(S) = \{\sum_{i=1}^{n} a_i s_i \mid n \in \mathbb{N}, a_i \in R, s_i \in S, 1 \leq i \leq n\}.$$

Demostración. En primer lugar, observamos que $(S) \neq \emptyset$ porque $0 \in S$. Por otro lado, veamos que se cumplen las condiciones de que sea ideal.

- Si $a, b \in (S)$ entonces $a = \sum_{i=1}^{n} a_i s_i, a_i \in R, s_i \in S$ y $b = \sum_{j=1}^{m} b_j t_j, b_j \in R, t_j \in S$, entonces sumando vemos rápidamente que $a + b \in (S)$.
- $a \in S, c \in R$ entonces podemos escribir el producto como $\sum_{i=1}^{n} a_i s_i \cdot c = \sum_{i=1}^{n} (a_i \cdot c) s_i \in (S)$

Vemos que $S \subseteq (S)$ porque, dado $x \in S$ entonces $x = 1_R \cdot x \in (S)$. Por otro lado, para ver que es el más pequeño, supongamos que $\exists J$ tal que $S \subseteq J \subsetneq (S)$. Entonces sea $x \in (S) = \sum_{i=1}^{n} a_i s_i, a_i \in R, s_i \in S$, para cada $i \in \{1, \cdots, n\}$ tenemos que $s_i \in S \subseteq J \Rightarrow a_i s_i \in J$ concluyendo que $x \in J \Rightarrow J = (S)$ contradiciendo que sea uno más pequeño distinto. ■

Proposición 3.1.2. *Sean R y S dos anillos y $\varphi : R \longrightarrow S$ un homomorfismo de anillos, entonces $ker\varphi$ es un ideal de R*

Demostración. En primer lugar, como $\varphi(0_R) = 0_S$ tenemos que $ker\varphi$ es no vacío. Ahora:

- Si $x, y \in ker\varphi$, entonces $\varphi(x + y) = \varphi(x) + \varphi(y) = 0_S + 0_S = 0_S$.
- Si $x \in ker\varphi$ e $y \in R$ entonces $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = 0_S \cdot \varphi(y) = 0_S$ por lo que $x \cdot y \in ker\varphi$.

■

Ejemplo 3.1.1. Consideremos el siguiente homomorfismo:

$$\begin{aligned} \varphi :& \mathbb{R}[x, y] \longrightarrow \mathbb{R} \\ & f(x, y) \longmapsto f(1, 1) \end{aligned}$$

El $ker\varphi = \{f(x, y) \in \mathbb{R}[x, y] \mid f(1, 1) = 0\}$. Veamos entonces que el kernel de esta aplicación coincide con el ideal $I = (x - 1, y - 1)$.

$\subseteq$ Sea $f \in I$, entonces $\exists g, h \in \mathbb{R}[x, y]$ tales que $f = (x - 1)h + (y - 1)g$. Evaluando en el punto $(1, 1)$ tenemos que $f(1, 1) = 0 \Rightarrow f \in ker\varphi$

$\supseteq$ Sea $f \in ker\varphi$, tenemos que

$$f(x, y) = \sum_{(i,j)\in A} a_{i,j} \cdot x^i \cdot y^j = \sum_{(i,j)\in A} a_{i,j} \cdot (x - 1 + 1)^i \cdot (y - 1 + 1)^j$$

donde desarrollando por el binomio de Newton llegamos a que

$$f(x, y) = \sum Ctes \cdot (x - 1)^k \cdot (y - 1)^{\tilde{k}} \in (x - 1, y - 1)$$

Lema 3.1.2. *Si I es un ideal de R entonces I es un subrupo de $(R, +, 0_R)$*

Demostración. Veamos que se verifican la definición de subrupo: mismo elemento neutro, cerrado con la suma y todo elemento tiene inverso. Las propiedad asociativa se deduce de la contención de I en R.

- $0_R \in I$ porque dado $t \in I$ se cunmple que $0 \cdot t = 0 \in I$.
- Dados $a, b \in I$, por la definición de ideal tenemos que $a + b \in I$.
- Sea $a \in I$, tomamos el inverso aditivo de 1_R y entonces $-a = -1_R \cdot a \in I$.

■

Observación 3.1.1. Como R es un grupo conmutativo y todo ideal I es subgrupo podemos construir el grupo cociente, denotando a los elementos del cociente como: $[a], \bar{a}$ o $a + I$

Teorema 3.1.1. *Sea R un anillo, I un ideal de R, entonces el grupo cociente R/I es un anillo con el producto:*

$$\begin{aligned} \cdot : R/I \times R/I &\longrightarrow R/I \\ ([a],[b]) &\longmapsto [a \cdot b] \end{aligned}$$

Corolario 3.1.1. *Todo ideal I de R es núcleo de un homomorfismo de anillos*

Demostración. Consideramos la aplicación

$$\begin{aligned} \pi : R &\longrightarrow R/I \\ a &\longmapsto a + I \end{aligned}$$

Así, $a \in ker\pi \Leftrightarrow \pi(a) = a + I = 0 + I \Leftrightarrow a - 0 \in I \Rightarrow a \in I$. ■

Teorema 3.1.2. *Sea $\mathbb{K}$ un cuerpo y $T \subseteq \mathbb{K}$ infinito. Sea $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$. Si $\forall a \in T^n, f(a) = 0$ entonces $f(x) = 0$.*

Demostración. Apliquemos inducción en el número de variables:

- $(n = 1)$: Sea $f(x) \in \mathbb{K}[x]$, si $f(x) = 0$ lo tendríamos. En otro caso, $\deg(f(x)) \geq 1$. Por la regla de Ruffini y ser $\mathbb{K}[x]$ un DIP tenemos que $f(x) = (x - a_1) \cdots (x - a_n)$ tiene a lo sumo n raíces, contradiciendo que T sea infinito.

Suponiendo cierto para $k > 0$ demostremos para $k + 1$.

- $(n = k + 1)$: Sea $f(x_1, \ldots, x_{k+1}) \in \mathbb{K}[x_1, \ldots, x_{k+1}]$, observemos que si alguna de las variables no aparece en el desarrollo de $f(x)$ estaríamos en el caso anterior y por inducción se tendría. Por otro lado, si

  $$f(x_1, \ldots, x_{k+1}) = g_0(x_1, \ldots, x_{k+1}) + g_1(x_1, \ldots, x_{k+1})x + \cdots + g_{k+1}(x_1, \ldots, x_{k+1})x^{k+1}$$

  para cada $(a_1, \ldots, a_k) \in T^n$ evaluamos en $f(a_1, \ldots, a_k, x_{k+1})x^{k+1}$ de modo que

  $$f = g_0(a_1, \ldots, a_k, x_{k+1}) + \cdots + g_{k+1}(a_1, \ldots, a_k, x_{k+1})$$

  que es ahora un polinomio en una única variable, x_{k+1}. Este polinomio verifica que $\forall b \in T, f(a_1, \ldots, a_k, b) = 0$ y por el caso base, $f(a_1, \ldots, a_k, x_{k+1}) = 0$, i.e, todos sus coeficientes son nulos y como hemos tomado una tupla $a_1, \ldots, a_k \in T^n$ arbitraria entonces por hipótesis de inducción $g_0 = \cdots = g_k = 0$ y por ello $f(x_1, \ldots, x_{k+1}) = 0$.

■

Observación 3.1.2. Nótese que en el teorema 3.1.2, si consideramos en $\mathbb{R}^2$ la circunferencia $\mathbb{S}^1$ parece generar una contradicción pues en ella el polinomio $f(x) = x^2 + y^2 - 1$ se anula en infinitos puntos pero no es idénticamente nulo. Esto viene de no haber tomado un conjunto $T \subseteq \mathbb{K}$ (en nuestro caso $\mathbb{R}$) infinito tal que en T^n el polinomio se anula. Las raíces son infinitas pero no puedo escribir $\mathbb{S}^1 = T \times T$ tal que $\forall (a_1, a_2) \in T^2$ el polinomio se anule [3].

[3] Para comprobar que efectivamente $\mathbb{S}^1 \neq T \times T$ podemos hacer uso de sus grupos fundamentales. Sabemos que $\pi_1(\mathbb{S}^1) = \mathbb{Z}$, por otro lado es fácil ver que $T \times T \cong [0,1] \times [0,1]$ que es simplemente conexo y por tanto $\pi_1(T \times T) = \{0\}$. Por lo que como los grupos fundamentales son distintos, no pueden ser isomorfos.

Corolario 3.1.2. *Sea $\mathbb{K}$ un cuerpo infinito y $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ dos polinomios. consideramos las aplicaciones*

$$\begin{aligned} \tilde{f} : \mathbb{K}^n &\longrightarrow \mathbb{K} \\ a &\longmapsto f(a) \end{aligned}$$

$$\begin{aligned} \tilde{g} : \mathbb{K}^n &\longrightarrow \mathbb{K} \\ a &\longmapsto g(a) \end{aligned}$$

Si $\tilde{f} = \tilde{g}$ entonces $f = g$

Demostración. Sea $h = f - g$, tenemos entonces que $\tilde{h} = Cte_0$ y por el teorema anterior, $\forall a \in \mathbb{K}^n, h(a) = 0 \Rightarrow h \equiv 0 \Rightarrow f \equiv g$. ■

Para finalizar esta sección recogemos el siguiente resultado que relaciona la contención de ideales y cómo se comportan con el cociente.

Teorema 3.1.3. *Sea R un anillo, I un ideal de R, entonces:*

I Si J es un ideal de R tal que $I \subseteq J$, entonces I es un subgrupo de J (lema 3.1.2) y J/I es también subgrupo de R/I. Además, J/I es un ideal de R/I. En particular, $\forall a \in R, \bar{a} \in J/I \Leftrightarrow a \in J$.

II Todo ideal K de R/I se puede expresar como J/I para un único ideal J con $I \subseteq J$.

Demostración. Se deja al lector como ejercicio. ■

Ejemplo 3.1.2. Consideramos por ejemplo la siguiente proyección

$$\begin{aligned} \pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/(24) \\ t &\longmapsto \bar{t} \end{aligned}$$

Así, tomamos $6\mathbb{Z} \subseteq \mathbb{Z}$, y vemos que $\pi(6\mathbb{Z}) = \bar{6}\mathbb{Z}/(24)$, es decir que la imagen de los múltiplos de 6 en $\mathbb{Z}$ es el ideal generado por la clase de 6 en $\mathbb{Z}/(24)$. Demostremos este hecho rápidamente: Dado $n \in \pi(6\mathbb{Z})$ entonces $\exists v \in \mathbb{Z}$ tal que $n = \bar{6}v \Rightarrow n \in \bar{6}\mathbb{Z}/(24)$. Recíprocamente, si $n \in \bar{6}\mathbb{Z}/(24)$ entonces existe $x \in \mathbb{Z}/(24)$ con $n = \bar{6}x$ donde $x = \bar{y}$ para algún $y \in \mathbb{Z}$ de modo que $6y \in 6\mathbb{Z}$ concluyendo que $\pi(6y) = n \in \pi(6\mathbb{Z})$.

Para finalizar, enunciamos la siguiente proposición.

Proposición 3.1.3. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos e $I \subseteq S$ un ideal, entonces $\varphi^{-1}(I)$ es un ideal de R.*

Demostración. Basta verificar la definición de ideal junto a la hipótesis de que la imagen sí que lo es. ■

Corolario 3.1.3. *Sea $R \subseteq S$ un subanillo de S. Sea I un ideal de S entonces $R \cap I$ es un ideal de R.*

Demostración. Basta considerar la inclusión $i : R \hookrightarrow S$, de modo que $i^{-1}(I) = R \cap I$ que por la proposición anterior (3.1.3) es un ideal de R. ■

Observación 3.1.3. El recíproco de la proposición no es cierto, la imagen de un ideal por un homomorfismo de anillos no es un ideal necesariamente, basta considerar la inclusión:

$$\begin{aligned} i : \mathbb{Z} &\hookrightarrow \mathbb{Z}[i] \\ t &\longmapsto t \end{aligned}$$

donde podemos ver rápidamente que $(1) = \mathbb{Z}$ es un ideal en $\mathbb{Z}$ (el total) pero en los enteros de Gauss tenemos que $1 \in \mathbb{Z}, i \in \mathbb{Z}[i]$ y $1 \cdot i = i \notin \mathbb{Z}$.

3.1.1. Ejercicios

Ejercicio 3.1.1. Sea $(G, +, e)$ un grupo conmutativo. Sea $H = \mathrm{Hom}(G, G)$ el conjunto de todos los homomorfismos de grupo de G en G. En H definimos las operaciones de suma y composición:

$$\begin{aligned} + :& H \times H \longrightarrow H \\ & (f, g) \longmapsto (f + g) \end{aligned}$$

donde $f + g$ se definen a su vez como aplicación

$$\begin{aligned} f + g :& G \times G \longrightarrow H \\ & a \longmapsto f(a) + g(a) \end{aligned}$$

y del mismo modo para el producto

$$\begin{aligned} \circ :& H \times H \longrightarrow H \\ & (f, g) \longmapsto (f \circ g) \end{aligned}$$

y de nuevo $f \circ g$

$$\begin{aligned} f \circ g :& G \times G \longrightarrow H \\ & a \longmapsto g(f(a)) \end{aligned}$$

Demuestre que efectivamente $+$ y $\circ$ definen operaciones en H. Demuestre que $(H, +, \circ)$ es un anillo, donde el elemento neutro de la suma es el homomorfismo trivial constante, y el neutro del producto es el homomorfismo identidad Id_G.

Demostración. Se deja al lector, simplemente mirar que se verifican las definiciones. ■

Ejercicio 3.1.2. Sea R un anillo conmutativo. Sea $H = \mathrm{Hom}(R, R)$ el conjunto de homomorfismos de grupo de R en R con la suma, y consideremos en H la estructura de anillo dada en el ejercicio anterior. Demuestre que la aplicación:

$$\varphi : R \to H, \quad a \mapsto m_a : R \to R, \quad t \mapsto at$$

está bien definida y es un homomorfismo inyectivo de anillos.

Demostración. Se deja al lector, simplemente mirar que se verifican las definiciones. ■

Ejercicio 3.1.3. Sean $(R_1, +_1, *_1, 0_1, 1_1), \ldots, (R_n, +_n, *_n, 0_n, 1_n)$ anillos. Consideremos el producto cartesiano $T = R_1 \times \cdots \times R_n$. Definamos en T las operaciones:

$$+ : T \times T \to T, \quad ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) \mapsto (a_1 +_1 b_1, \ldots, a_n +_n b_n)$$

$$* : T \times T \to T, \quad ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) \mapsto (a_1 *_1 b_1, \ldots, a_n *_n b_n)$$

Demuestre que T es un anillo y que T es conmutativo si y solo si $R_1, \ldots, R_n$ lo son.

Demostración. Se deja al lector, simplemente mirar que se verifican las definiciones. ■

Ejercicio 3.1.4. Sea R un anillo conmutativo, demuestre que R es un cuerpo si y solo si tiene exactamente dos ideales, (0) y (1).

Demostración. Ver propiedad **??** ■

Ejercicio 3.1.5. Sea $\mathbb{K}$ un cuerpo y $\mathbb{K}[x, y]$ el anillo de polinomios en dos variables. Demuestre que el ideal $I = (x, y)$ no es un ideal principal.

Demostración. Supongamos que $\exists a$ tal que $(x, y) = (a)$. Tenemos por tanto que $\exists r_1, r_2 \in R[x]$ tales que $x = a \cdot r_1$ e $y = a \cdot r_2$. Lleguemos a un absurdo para x y de manera análoga llegaríamos a una contradicción por y. Si $x = a \cdot r_1$ entonces $\text{grad}(a \cdot r_1) = 1$ y como $\mathbb{K}[x, y]$ es dominio por ser $\mathbb{K}$ cuerpo ([2], Teorema II.4.4, pág. 71), entonces $1 = \text{grad}(a) + \text{grad}(r_1)$., de donde vemos que $\text{grad}(a) \in \{0, 1\}$. Si a fuera una constante entonces tendríamos que $(a) = (1)$ por ser $\mathbb{K}$ cuerpo pero $1 \notin (x, y)$. Entonces tenemos que $a = ux, u \in \mathbb{K}$, esto implica de manera directa que $a \in (x)$, pero por otro lado tendríamos que $y = uxr_2 \in (x)$, sin embargo, x e y son variables independientes por lo que llegamos a contradicción y concluimos que (x, y) no es principal. ■

Ejercicio 3.1.6. Determine las unidades, los divisores de cero y los elementos nilpotentes de $\mathbb{Z}/24\mathbb{Z}$.

Demostración. Veamos por partes cada uno de los tipos que nos pide el enunciado:

- Un elemento $\bar{a} \in \mathbb{Z}/24\mathbb{Z}$ será unidad si $\exists \bar{b} \in \mathbb{Z}/24\mathbb{Z}$ tal que $ab = \bar{1}$, ie, $(a + 24\mathbb{Z})(b + 24\mathbb{Z}) = 1 + 24\mathbb{Z}$. Esto sucede si $\text{gdc}(a, b) = 1$, por lo que las unidades serám $\{[1], [5], [7], [11], [13], [17], [19], [23]\}$.
- Los divisores del cero en $\mathbb{Z}/24\mathbb{Z}$ serán aquellos elementos que tengan un factor común con 24 de manera que, si $\text{gdc}((a, 24) = b \leq 23$ entonces $a \cdot b \in 24\mathbb{Z}$ y $[a \cdot b] = 0$. En este caso son $\{[2], [3], [4], [6], [8], [9], [10], [12], [14], [15], [16], [18], [20], [21], [22]\}$.
- Los nilpotentes serán aquellos elementos tales que exista un número natural mayor que cero de modo que $a^n \in 24\mathbb{Z}$, dicho de otra manera, $24 \mid a^n \Rightarrow 2 \cdot 3 \mid a$ de modo que los nilpotentes son $\{[6], [12], [18]\}$.

■

Ejercicio 3.1.7. Sea R un anillo conmutativo, sean $x, y \in R$. Describa qué queremos decir exactamente cuando decimos que la igualdad

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

es cierta para $n \in \mathbb{N}$. Demuéstrela.

Demostración. Se deja al lector como ejercicio. ■

Ejercicio 3.1.8. Use el ejercicio anterior para demostrar que, en un anillo conmutativo R, el conjunto de elementos nilpotentes es un ideal I de R.

Demostración. A partir del ejercicio anterior es simple probar este resultado. En primer lugar I es no vacío puesto que 0_R es nilpotente. Ahora, dados dos elementos $x, y \in I$ y $z \in R$ tenemos que:

- Si $n, m \in \mathbb{N}$ son los menores naturales para los que se verifica que x, y son nilpotentes, llamando $k = m + n$ tenemos que

$$(x+y)^k = \sum_{i=0}^{k} \binom{k}{i} x^{k-i} y^i = a_0 x^k + \ldots a_m x^{k-m} y^m + \ldots a_k y^k$$

  donde, para $i \leq m$ se da que $x^i = x^n \cdot x^{i-n} = 0$ y para $i \geq m, y^i = y^m \cdot y^{i-m} = 0$.

- El producto se da de manera directa considerando el máximo de las potencias.

■

Ejercicio 3.1.9. Sea $a \in R$ un elemento nilpotente. Demuestre que $1 + a$ es una unidad de R. Demuestre también que si $u \in R^*$ es una unidad de R, entonces $u + a$ es una unidad de R. Compare este resultado con el ejercicio 3.1.8.

Demostración. Haremos los dos apartados de una, haciendo el caso segundo para una unidad arbitraria ya que tomando $u = 1_R$ tenemos el primero. Para demostrarlo, buscamos $v \in R$ tal que $(u + a) \cdot v = 1_R$ u $v \cdot (u + a)$, consideramos

$$v = u^{-1} \sum_{k=0}^{n-1} (-1)^k a^k u^{-k-1}$$

donde u^{-1} es el elemento tal que $u \cdot u^{-1} = 1$ y $n \in \mathbb{N}_{\geq 1}$ el menor natural tal que $a^n = 0$.. Así pues desarrollando el producto por un lado (el otro se ve de manera análoga), tenemos que:

$$\begin{aligned} u \cdot v &= 1 - au^{-1} + a^2 u^{-2} + \cdots + (-1)^{n-1} a^{n-1} u^{n-1} \\ a \cdot v &= au^{-1} - a^2 u^{-2} + \cdots + (-1)^{n-2} a^{n-1} u^{n-1} + 0 \end{aligned}$$

De donde sumando vemos fácilmente que $u \cdot v + a \cdot v = 1$ como queríamos ver. ■

Ejercicio 3.1.10. Sea R un anillo y $R[x]$ el anillo de polinomios en una indeterminada sobre R. Sea

$$f = r_0 + r_1 x + \cdots + r_n x^n \in R[x].$$

1. Pruebe que f es unidad de $R[x]$ si y solo si r_0 es unidad de R y $r_1, \ldots, r_n$ son nilpotentes. (Pista: si $n > 0$, f es unidad y $a_0 + \cdots + a_m x^m$ es su inverso, demuestre por inducción que $r_n^{i+1} a_{m-i} = 0$ para cada $i = 0, \ldots, m$.)

2. Pruebe que f es nilpotente si y solo si $r_0, \ldots, r_n$ son nilpotentes.

3. Pruebe que f es divisor de cero si y solo si existe $c \in R \setminus \{0\}$ tal que $cf = 0$. (Si f es divisor de cero, escoja un $g = c_0 + \cdots + c_k x^k \in R[x]$, $g \neq 0$, de grado mínimo tal que $fg = 0$. Demuestre por inducción que $r_{n-i} g = 0$ para cada $i = 0, \ldots, n$.)

Demostración. Demostremos cada una de las partes que nos pide el enunciado:

1 $\Leftarrow$ Si $r_1, \ldots, r_n$, como forman un ideal, entonces $r_1 x + \cdots + r_x x^n = t$ es nilpotente y $\exists k \in \mathbb{N}_{\geq 1}$ tal que $t^n = 0$. Si r_0 es unidad, $f = r_0 + t$ es unidad por el ejercicio anterior, como queríamos ver.

$\Rightarrow$ Supongamos ahora que $f = r_0 + r_1x + \dots r_nx^n$ es unidad. Entonces existe un inverso $g = s_0 + s_1x + \cdots + s_mx^m$ tal que $f \cdot g = 1$. Igualando términos tenemos que $1 = r_0s_0 \Rightarrow r_0$ es unidad. Ahora, en el coeficiente de mayor grado tenemos que $r_n \cdot s_m = 0$, supongamos que $r_n^i s_{m-i} = 0, \forall i \leq k-1$ y veamos que se cumple para k. Por las relaciones, el coeficiente de x^{n+m-k} es $r_n s_{m-k} + r_{n-1}s_{m-k+1} + \cdots + r_{n-k}s_m = 0$. Multiplicando ahora por r_n^{k-1} llegamos a que $r_n^k s_{n-k} = 0$. Tenemos por tanto que r_n es nilpotente y r_0 unidad, por lo que $f - r_nx^n$ es unidad e iterando de nuevo para el resto de potencias llegaríamos al resultado que queremos

2 $\Leftarrow$ Se da de manera directa pues los nilpotentes forman un ideal

$\Rightarrow$ Por el ejercicio anterior (3.1.9), si f es nilpotente entonces $1 + f$ es unidad y por el apartado que acabamos de probar, $g = 1 + xf$ unidad sii 1 unidad y los coeficientes no constantes son nilpotentes, es decir, $r_0, \dots, r_n$ [4].

3 $\Leftarrow$ Trivial

$\Rightarrow$ Si f es divisor del 0, entonces $\exists g \neq 0, g = c_0 + \cdots + c_mx^m \in R[x]$ con grado mínimo tal que $f \cdot g$. Veamos que $r_i \cdot g = 0, \forall i \in \{1, \cdots, n\}$. Cuando $i = n$, entonces igualando coeficientes tenemos directamente que $r_n \cdot c_m = 0$ y por tanto $f \cdot (g \cdot r_n) = 0$ pero como $g \cdot r_n$ tiene grado menor que m, entonces necesariamente $g \cdot r_n = 0$, por ser g de grado mínimo. Suponiendo ahora que se verifica $\forall k + 1 \leq n$ veamos que se da para k. Tomando el coeficiente x^{n+m-k} tendríamos $r_nc_{m-k} + \cdots + r_{n-k}c_m = 0$, los coeficientes son todos cero por h.di, de manera que de nuevo estamos ante un polinomio de grado estrictamente menor que m y por tanto debe ser $r_{n-k} \cdot g = 0$. Por tanto tenemos que por inducción para cada coeficiente r_i se cumple que $r_i \cdot g = 0$, en particular, $r_i \cdot c_k = 0, \forall i \in \{1, \cdots, n\}$ y por tanto tomando $g = c_k \neq 0$ se da el resultado.

■

3.2. Operaciones con ideales

En esta sección vamos a empezar a definir una serie de operaciones entre ideales y las propiedades que cumplen. En primer lugar, parece razonable empezar por ver cómo se comportan dos o una cantidad arbitraria de ideales respecto de la unión y la intersección. Por ello tenemos:

Teorema 3.2.1. *Sea $\{I_j \mid j \in \Lambda\}$ un conjunto no vacío de ideales de un anillo R. Entonces $\bigcap_{j\in\Lambda} I_j$ es un ideal de R.*

Demostración. Tenemos que $\forall j \in \Lambda, 0_R \in I_j$ por lo que $0_R \in \bigcap_{j\in\Lambda} I_j$. Por otro lado, si $a, b \in \bigcap_{j\in\Lambda} I_j, \forall j \in \Lambda, a + b \in I_j$ por ser I_j ideal y por tanto $a + b \in \cap_{j\in\Lambda} I_j$. De manera análoga se prueba el producto. ■

Sin embargo, en general no se verifica la misma propiedad para la unión (ver ejercicio 3.2.2). Por ello introducimos la siguiente definición:

[4] Nótese aquí la necesidad de multiplicar por x, si no lo hiciéramos, por el apartado anterior tendríamos que $1 + r_0$ es unidad y $r_1, \dots, r_n$ son nilpotentes, no concluyendo el resultado que deseábamos.

Definición 3.2.1. Sea R un anillo y $\{I_j \mid j \in \Lambda\}$ un conjunto de ideales, definimos la suma de ideales como:

$$\sum_{j\in\Lambda} I_j = \Big(\bigcup_{j\in\Lambda} I_j\Big).$$

La suma de ideales es el ideal generado por la unión de ellos.

Hacemos a continuación una serie de observaciones acerca de la notación:

Observación 3.2.1. Si $\Lambda = \emptyset$ entonces $\sum_{j\in\Lambda} I_j = 0$

Observación 3.2.2. Si $\Lambda = \{1, 2\}$ entonces $\sum_{j\in\Lambda} I_j = I + J$

Observación 3.2.3. Si $\Lambda = \{1, \cdots, n\}$ entonces $\sum_{j\in\Lambda} I_j = I_1 + \cdots + I_n$

Cabe pensar, que si hemos aprovechado la intersección y la suma (como *sustituto* de la unión), por qué no *generalizar* estos conceptos para más operaciones. Así pues, sea R un anillo, I, J ideales de R entonces:

Definición 3.2.2. El *producto* viene dado como $I \cdot J = \Big(\{a \cdot b \mid a \in I, b \in J\}\Big)$

Definición 3.2.3. El *radical* será $\sqrt{I} = \{a \in R \mid \exists n \in \mathbb{N}_{\geq 1}, a^n \in I\}$

Definición 3.2.4. El *cociente* de dos ideales será $I : J = \{a \in R \mid \forall b \in J, a \cdot b \in I\}$

Son muy importantes en relación a estas propiedades los ejercicios de esta sección, que dan los generadores, equivalencias y más propiedades de estas operaciones con ideales. Ponemos a continuación unas pequeñas observaciones que pueden ser de utilidad, extraídas de estos ejercicios, de aquellas relaciones que podrían ser, si así se piensa, *más importantes*.

Observación 3.2.4. El radical de 0 es

$$\sqrt{(0)} = \{a \in R \mid \exists n \in \mathbb{N}_{\geq 1}, a^n \in (0)\} = \{\text{nilpotentes}\}.$$

Por lo que un elemento $a \in \sqrt{(0)} \iff a$ es nilpotente. Además, tenemos demostrado en el ejercicio 3.2.8 que el conjunto de los nilpotentes es un ideal de R, por lo que se verifica que $\sqrt{(0)}$ lo es.

No hemos probado como tal que el radical de un ideal sea un ideal. Pero, por la observación anterior, podemos fácilmente demostrarlo en el siguiente resultado.

Teorema 3.2.2. *Sea R un anillo e $I \subseteq R$ un ideal, entonces $\sqrt{I}$ es un ideal.*

Demostración. Tomamos $G = R/I$, entonces,

$$\bar{a} \text{ nilpotente} \iff \exists m \in \mathbb{N}_{\geq 1}, \bar{a}^m = \bar{0} \iff a^m \in I \iff a \in \sqrt{I}.$$

Ahora, claramente $0 \in \sqrt{I}$. Por otro lado, dados $a, b \in \sqrt{I}$ entonces $\bar{a}, \bar{b} \in \sqrt{(0_G)} \Rightarrow \bar{a} + \bar{b} \in \sqrt{(0_G)} \Rightarrow a + b \in \sqrt{I}$. De igual manera vemos que $a \in \sqrt{I}, b \in R$ entonces $\bar{a} \in \sqrt{(0)} \Rightarrow \bar{a}\bar{b} \in \sqrt{(0)} \Rightarrow ab \in I$. ■

Estamos en el mismo caso para el cociente de ideales, probemos que es un ideal.

Teorema 3.2.3. *Sea R un anillo, I, J ideales de R, entonces $I : J$ es un ideal de R*

Demostración. Observamos en primer lugar que $0_R \in I : J$ porque, $\forall b \in J, 0 \cdot b = 0 \in I$. Ahora veamos las otras dos condiciones.

(I) Sean $x, y \in I : J$ y $b \in J$ arbitrario, tenemos que $(x + y) \cdot b = x \cdot b + y \cdot b$, donde ambos están en I por estar en el cociente, de modo que la suma está en $I : J$.

(II) De manera análoga, dado $x \in I : J$, $c \in R$. Tenemos que $\forall b \in J, x \cdot b \in I$ y por ser I ideal entonces $x \cdot c \cdot b \in I$, concluyendo que $x \cdot c \in I : J$.

■

Pongamos ahora un ejemplo de lo que es el cociente de dos ideales, para poder visualizar la idea que hay detrás de esto.

Ejemplo 3.2.1. En $\mathbb{Z}$, consideramos $(108) : (1000)$, lo denotamos como $I : J$. Observamos que lo podemos escribir como $(2^2 \cdot 3^3) : (2^3 \cdot 5^3)$. En primer lugar $3^3 \in I : J$ porque

$$3^3 \cdot r_1 \cdot 2^3 \cdot 5^3 = 3^3 \cdot 2^2 \cdot r_2 \in (108)$$

Así, tenemos que $(108 \in I : J)$ y $27 \in (I : J)$. Como $\mathbb{Z}$ es un DIP entonces tenemos que $I : J = (d)$ y por tanto, si $108 \in (d), 27 \in (d) \Rightarrow d \mid 108, d \mid 27$. Vemos que $3^2 \notin (d)$ por lo que $I; J = (27)$. El ejercicio 3.2.11 clarifica más como encontrar los generadores de esta operación de ideales en el caso de DIPs.

Observación 3.2.5. Podemos expresar la suma de ideales como

$$I_1 + \cdots + I_n = \{a_1 + \cdots + a_n \mid a_i \in I_i, 1 \leq i \leq n\}.$$

Ver ejercicio 3.2.4.

Observación 3.2.6. Si tenemos dos ideales $I = (a_1, \ldots, a_n), J = (b_1, \ldots, b_m)$ finitamente generados, entonces:

- $I + J = (a_1, \ldots, a_n, b_1, \ldots, b_m)$.
- $I \cdot J = \Big(\{a_i \cdot b_j, 1 \leq i \leq n, 1 \leq j \leq m\}\Big)$.

Ver ejercicio 3.2.4.

Observación 3.2.7. El radical del radical es él mismo, es decir, $\sqrt{\sqrt{I}} = \sqrt{I}$. Ver ejercicio 3.2.8.

3.2.1. Ejercicios

Ejercicio 3.2.1. Demuestre que la intersección arbitraria (no vacía) de ideales es un ideal.

Demostración. Ver la demostración del teorema 3.2.1. ■

Ejercicio 3.2.2. Demuestre que la unión de ideales no es, en general, un ideal.

Demostración. Podemos encontrar numerosos contraejemplos en $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{K}[x,y]$. En particular consideramos en $\mathbb{Z}$ los ideales (2) y (3), de manera que $(2)\cup(3)$ no es ideal ya que $2+3=5\notin(2)\cup(3)$. ■

Ejercicio 3.2.3. Sea R un anillo e I, J ideales de R. Demuestre que:

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

Demuestre que si $I_1,\dots,I_n$ son ideales de R entonces:

$$I_1+\cdots+I_n=\{a_1+\cdots+a_n \mid a_i\in I_i, 1\leq i\leq n\}.$$

Ejercicio 3.2.4. Sea R un anillo, $I=(a_1,\dots,a_n)$, $J=(b_1,\dots,b_m)$ ideales finitamente generados. Demuestre que:

1. $I+J=(a_1,\dots,a_n,b_1,\dots,b_m)$.
2. $IJ=\{a_ib_j, 1\leq i\leq n, 1\leq j\leq m\}R$.

En particular, tanto $I+J$ como IJ son finitamente generados.

Ejercicio 3.2.5. Determine todos los ideales de $\mathbb{Q}[x]/(x^2-1)$ y de $\mathbb{Q}[x]/(x^2+1)$.

Demostración. Para $\mathbb{Q}[x]/(x^2-1)$ tenemos que los ideales serán $J/(x^2-1)$ con $(x^2-1)\subseteq J$. Como $\mathbb{Q}[x]$ es DIP, entonces $J=(a)$ con $a\mid x^2-1$ y entonces tomamos las clases de los divisores: $(\bar{1}), (\overline{x+1}), (\overline{x-1})$ y $(\overline{x^2-1})=(\bar{0})$. Por otro lado, como x^2+1 es irreducible en $\mathbb{Q}[x]/(x^2+1)=\mathbb{Q}[i]$ (Galois), es cuerpo y entonces sus ideales son $(\bar{0})$ y $(\bar{1})$ (**??**). También podríamos proceder como en el caso anterior de manera que, como los divisores de x^2+1 son el mismo y el 1 llegaríamos al mismo resultado. ■

Ejercicio 3.2.6. Sea $\mathbb{K}$ un cuerpo y $R=\mathbb{K}[x,y,z,t]$ el anillo de polinomios. Sea $I=(x,y)$ y $J=(z,t)$. Demuestre que el conjunto:

$$T=\{fg \mid f\in I, g\in J\}$$

no es un ideal de R. En particular, $IJ\neq\{fg \mid f\in I, g\in J\}$.

Demostración. Tenemos que $xz\in T$ y $ty\in T$ por lo que si fuera ideal la suma debería estar, es decir, $xz+yt\in T$. Ahora bien, $xz+yt$ es irreducible pero todo elemento de $T\backslash\{0\}$ es reducible, por lo que $xz+yt\notin T$, concluyendo. Para el segundo caso, tenemos por el ejercicio 3.2.4 que $IJ=(xz,xt,yz,yt)$, así de manera análoga al primer caso vemos que $xz\in IJ$ pero no es reducible de la manera que no está en T. ■

Ejercicio 3.2.7. Sea I un ideal, $I^n = I \cdots I$ (n veces). ¿Es cierto en general que $\sqrt{I^n} = \sqrt{I}$? Demuéstrelo o dé un contraejemplo.

Demostración. Sea $I \subseteq R$ entonces:

- $\supseteq$ Sea $x \in \sqrt{I}, \exists m \in \mathbb{N}_{\geq 1}$ tal que $x^m \in I \Rightarrow x^{n \cdot m} \in I^n \Rightarrow x \in \sqrt{I^n}$.
- $\subseteq$ Dado que $I^n \subseteq I \Rightarrow \sqrt{I^n} \subseteq \sqrt{I}$. Para ver la primera contención podemos generalizar por inducción el apartado 2 del ejercicio 3.2.8, tomando $I = J$.

■

Ejercicio 3.2.8. Demuestre las siguientes propiedades de las operaciones con ideales. En los casos en los que solo se dé una inclusión, busque un contraejemplo si no se cumple la igualdad:

1. $(IJ)K = I(JK)$
2. $IJ \subseteq I \cap J$
3. $I(J + K) = IJ + IK$
4. $IJ \subseteq I \cap J$
5. $\sqrt{\sqrt{I}} = \sqrt{I}$
6. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
7. $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$
8. $I \cap (J + K) = (I \cap J) + (I \cap K)$ siempre que $J \subseteq I$ o $K \subseteq I$
9. $(I + J)(I \cap J) \subseteq IJ$
10. $I \subseteq (I : J)$
11. $(I : J) : K = I : (JK) = (I : K) : J$
12. $(\bigcap_\lambda I_\lambda) : K = \bigcap_\lambda (I_\lambda : K)$
13. $I : (\sum_\lambda K_\lambda) = \bigcap_\lambda (I : K_\lambda)$

Demostración. Vayamos probando cada apartado en orden, dando un contraejemplo donde sea necesario.

1. La demostración se sigue de tomar la definición como conjunto y desarrollar las igualdades aplicando la propiedad distributiva.

$$\begin{aligned}(IJ)K &= \left\{\sum_{s=1}^{n} u_s k_s \mid n \in \mathbb{N}, u_s \in IJ, k_s \in K\right\} \\ &= \left\{\sum_{s=1}^{n}\left(\sum_{t=1}^{m_s} a_{st}b_{st}\right) k_s \mid n, m_s \in \mathbb{N}, a_{st} \in I, b_{st} \in J, k_s \in K\right\} \\ &= \left\{\sum_{s=1}^{n}\sum_{t=1}^{m_s}(a_{st}b_{st})k_s \mid a_{st} \in I, b_{st} \in J, k_s \in K\right\} \\ &= \left\{\sum_{s=1}^{n}\sum_{t=1}^{m_s} a_{st}(b_{st}k_s) \mid a_{st} \in I, b_{st} \in J, k_s \in K\right\} \\ &= \left\{\sum_{p=1}^{q} a_p v_p \mid q \in \mathbb{N}, a_p \in I, v_p \in JK\right\} \\ &= I(JK)\end{aligned}$$

2. Sea $x \in IJ$, por la definición de ideal producto entonces $x = abr, a \in I, b \in J, r \in R$. Pero observamos que por ser I, J ideales entonces $x = a^{\in I} \cdot br^{\in R} \in I$ (resp. $x = b^{\in J} \cdot ar^{\in R} \in J$) de modo que $x \in I \cap J$.

3. De manera similar al apartado 1, basta desarrollar por conjuntos y aplicar la distributiva:

$$\begin{aligned}I(J+K) = I\{a+b \mid a \in I, b \in J\} &= \{\sum_{i=1}^{n} t_i(a_i+b_i) \mid t_i \in I, a_i \in J, b_i \in K, n \in \mathbb{N}\} \\ &= \{\sum_{i=1}^{n} t_i a_i + \sum_{i=1}^{n} t_i b_i \mid t_i \in I, a_i \in J, b_i \in K\} \\ &= \{v+u \mid v \in IJ, u \in IK\} = IJ + IK\end{aligned}$$

4. Sea $x \in IJ$, entonces existen $a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in J$ tales que $x = a_1b_1 + \cdots + a_nb_n$. Por ser I ideal entonces $a_ib_i \in I$ y análogamente $a_ib_i \in J$ de modo que de manera directa vemos que $x \in I \cap J$.

   El contraejemplo lo podemos ver considerando en $\mathbb{Z}$ el ideal (2), consigo mismo tenemos que $(2)(2) = (4)$ y $(2) \cap (2) = (2)$, que no son iguales.

5. Sea $x \in \sqrt{I}$ trivialmente se verifica que $x \in \sqrt{\sqrt{I}}$. Para la otra contención, sea $x \in \sqrt{\sqrt{I}}$ entonces $\exists n \in \mathbb{N}_{\geq 1}$ tal que $x^n \in \sqrt{I}$ pero entonces de nuevo $\exists m \in \mathbb{N}_{\geq 1}$ tal que $x^{nm} \in I$ de manera que $x \in \sqrt{I}$ como queríamos ver.

6. Demostremos por contenciones, en primer lugar $\sqrt{IJ} \subseteq \sqrt{I \cap J}$ es directo por el apartado 4. de este ejercicio. Ahora hacia el otro lado es también directo, puesto que, dado $t \in \sqrt{I \cap J}, \exists n \in \mathbb{N}_{\geq 1}, t^n \in I \cap J \Rightarrow t^n \in I \wedge t^n \in J \Rightarrow t^{2n} \in IJ \Rightarrow t \in \sqrt{IJ}$. Ahora, la segunda igualdad se sigue de lo siguiente:

- $\subseteq$ Si $x \in \sqrt{I \cap J}, \exists n \in \mathbb{N}_{\geq 1}, x^n \in I \cap J \subseteq I \Rightarrow x \in \sqrt{I}$, análogamente $x \in \sqrt{J}$ y por tanto $x \in \sqrt{I} \cap \sqrt{J}$.
- $\supseteq$ Dado $x \in \sqrt{I} \cap \sqrt{J}$, entonces $\exists n, m \in \mathbb{N}_{\geq 1}$ tales que $x^n \in \sqrt{I} \wedge x^m \in \sqrt{J}$, por tanto $x^{n+m} \in I \cap J \Rightarrow x \in \sqrt{I \cap J}$.

Observación 3.2.8. El resultado es cierto para la intersección finita, podemos realizar la demostración por inducción. Sin embargo no lo es para el caso infinito, basta considerar $I_k = (2^k)$ de modo que:

$$\bigcap_k (2^k) = (0) \Rightarrow \sqrt{\bigcap_k I_k} = \sqrt{(0)} = 0$$
$$\sqrt{I_k} = (2) \Rightarrow \bigcap \sqrt{I_k} = \bigcap_k (2) = (2)$$

7. Veamos el resultado por doble contención

   - $\supseteq$ Sea $t \in \sqrt{\sqrt{I} + \sqrt{J}}$, entonces $\exists n \in \mathbb{N}_{\geq 1}$ tal que $t^n \in \sqrt{I} + \sqrt{J}$. Por el ejercicio 3.2.3 tenemos que $t^n = a + b, a \in \sqrt{I} \wedge b \in \sqrt{J}$. Por tanto a su vez $\exists p, q \in \mathbb{N}_{\geq 1}$ tales que $a^p \in I \wedge b^q \in J$. Por tanto tenemos que $t^{n\cdot(p+q)} = (a + b^{(p+q)}) = \sum_{k=0}^{p+q} \binom{p+q}{k} a^k b^{k-(p+q)}$, donde cada sumando está o bien en I o bien en J, de modo que $t^{n\cdot(p+q)} \in I + J \Rightarrow t \in \sqrt{I + J}$.
   - $\subseteq$ Sea $t \in \sqrt{I + J}$, entonces $\exists n \in \mathbb{N}_{\geq 1}$ tal que $t^n \in I + J$, por tanto tenemos que $t^n = a + b$. Despejando vemos que $t^n - b = a \in I$ y como naturalmente $a \in \sqrt{I}$ entonces $t^n - b \in \sqrt{I}$. De nuevo, como $b \in \sqrt{J}$, entonces $a + b \in \sqrt{I} + \sqrt{J} \Rightarrow t^n - b + b = t^n \in \sqrt{I} + \sqrt{J} \Rightarrow t \in \sqrt{\sqrt{I} + \sqrt{J}}$.

8. Veamos las dos contenciones, en la segunda de ellas haremos uso de la hipótesis adicional, la primera es general.

   - ($\supseteq$) Sea $x \in (I \cap J) + (I \cap K)$ entonces

     $$x = a + b, a \in (I \cap J), b \in (I \cap K) \Rightarrow a \in I, a \in J, b \in I, b \in K.$$

     Podemos observar por tanto que $x \in I$ por estar $a, b \in I$, del mismo modo como $a \in J, b \in K$ entonces $a + b \in J + K \Rightarrow x \in J + K$ y por tanto $x \in I \cap (J + K)$ como queríamos ver.
   - ($\subseteq$) Dado $x \in I \cap (J + K)$ entonces $x \in I, x = a + b, a \in J, b \in K$. Suponiendo que $J \subseteq I$ (de manera análoga se ve el otro caso), entonces $x - a = b \in I \subseteq K$ de modo que se verifica que $a \in I \wedge a \in J, b \in I, b \in K$ y vemos que $a \in I \cap J, b \in I \cap K \Rightarrow x = a + b \in (I \cap J) + (I \cap K)$.

Observación 3.2.9. En la segunda contención ha sido necesario suponer uno de los dos casos del enunciado, si no fuera así podemos plantear el siguiente contraejemplo: Tomamos en $\mathbb{Q}[x, y]$ los ideales $I = (x), J = (y), K = (x + y)$ tenemos entonces que:

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

donde que $(y) + (y + x) = (x, y)$ se puede probar fácilmente por doble contención, que $(x) \cap (y) = (xy)$ basta ver que son comaximales y aplicar el teorema 4.1.5 y finalmente que $(x) \cap (x + y) = (xy, x^2)$ y $(xy) + (xy, x^2) = (xy, x^2)$ se puede probar fácilmente por doble contención.

9. Veamos la contención, supongamos que tenemos un elemento $x \in (I+J)(I \cap J)$ entonces

$$\begin{aligned} x &= \sum_{i=1}^{n} (a_i + b_i)c_i, a_i \in I, b_i \in J, c_i \in I \cap J \\ &= \sum_{i=1}^{n} a_i c_i + \sum_{i=1}^{n} b_i c_i, a_i \in I, b_i \in J, c_i \in I \cap J \end{aligned}$$

Como $c_i \in I \cap J$ en particular en ambos conjuntos de manera que $a_i c_i \in IJ, b_i c_i \in IJ$, concluyendo que $x \in IJ$. Ahora, si tomamos por ejemplo, en $\mathbb{Q}[x,y]$ los ideales $I = (x), J = (y)$ entonces tenemos que, para el lado derecho trivialmente se verifica que $IJ = (xy)$. Para el otro lado tenemos que

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

Comparando ambos lados, tenemos $IJ = (xy)$ y $(I+J)(I \cap J) = (x^2y, xy^2)$ de modo que son distintos, bastaría ver que no podemos escribir un polinomio del conjunto de la izquierda como producto de los de la derecha por grados.

10. Esta contención es trivial, pues dado $x \in I$, como I es ideal, $\forall r \in R, xr \in I$ y en particular para J. Para ver la contención basta tomar $J = I$ de manera que $(I; I) = (1)$ pues $1 \cdot x \in I, \forall x \in I$ trivialmente y con $I = (2)$ en $\mathbb{Z}$ basta.

11. REVISAR

    Sea $r \in (I : J) : K$. Entonces, para todo $k \in K$, se tiene $rk \in (I : J)$, lo que implica $rkJ \subseteq I$. Luego $rJK \subseteq I$, es decir, $r \in I : (JK)$. Así, $(I : J) : K \subseteq I : (JK)$. El recíproco se prueba del mismo modo, por lo que $(I : J) : K = I : (JK)$.

    Análogamente, si $r \in I : (JK)$, entonces $rJK \subseteq I$, así que $rjK \subseteq I$ para todo $j \in J$, es decir, $rj \in (I : K)$ y por tanto $r \in (I : K) : J$. La recíproca se prueba de igual forma, lo que da $I : (JK) = (I : K) : J$.

    Así se concluye la igualdad:

$$(I : J) : K = I : (JK) = (I : K) : J.$$

12. Sea $r \in (\bigcap_\lambda I_\lambda) : K$. Entonces $rK \subseteq \bigcap_\lambda I_\lambda$, por lo que $rK \subseteq I_\lambda$ para todo λ, es decir, $r \in I_\lambda : K$ para todo λ, y por tanto $r \in \bigcap_\lambda (I_\lambda : K)$.

    Recíprocamente, si $r \in \bigcap_\lambda (I_\lambda : K)$, entonces $rK \subseteq I_\lambda$ para todo λ, lo que implica $rK \subseteq \bigcap_\lambda I_\lambda$, es decir, $r \in (\bigcap_\lambda I_\lambda) : K$.

    Por lo tanto,

$$\left(\bigcap_\lambda I_\lambda \right) : K = \bigcap_\lambda (I_\lambda : K).$$ ■

13. Veamos ambas implicaciones:

    $\subseteq$ Sea $t \in I : (\sum_\lambda K_\lambda)$ y λ_0 arbitrario, veamos que $t \in I : K_{\lambda_0}$. Por definición de división de ideales tenemos que $\forall b \in \sum_\lambda K_\lambda, b \cdot t \in I$, en particular para todo $b \in K_{\lambda_0}$ por lo que $t \in I : K_{\lambda_0}$. Así, como hemos tomado un λ_0 arbitrario concluimos que se cumple para todos y entonces $t \in \bigcap_\lambda (I : K_\lambda)$.

    $\supseteq$ Queremos ver que $\forall b \in \sum_\lambda K_\lambda$. Por definición de suma de ideales tenemos que $b = b_1 s_1 + \cdots + b_{\lambda_n} s_{\lambda_n}$ con $b_i \in K_{\lambda_i}, s_{\lambda_i} \in R$. Por tanto $t \cdot b = t \cdot b_1 s_1 + \cdots + t \cdot b_{\lambda_n} s_{\lambda_n}$ y como por hipótesis $t \in I : K_{\lambda_i}, \forall i$ entonces todos los productos están en I, como queríamos ver.

Ejercicio 3.2.9. Demuestre las siguientes propiedades:

1. $\sqrt{I} = (1) \Leftrightarrow I = (1)$
2. $\sqrt{I} + \sqrt{J} = (1) \Leftrightarrow I + J = (1)$
3. $I : J = (1) \Leftrightarrow J \subseteq I$

Demostración. Probemos cada una de las propiedades.

1. Trivial
2. La implicación de derecha a izquierda es directa puesto que si $(1) = I + J$ entonces existen $a \in I, b \in J$ tales que $1 = a + b$, ahora como a, b están en sus respectivos radicales entonces $1 = a + b \in \sqrt{I} + \sqrt{J}$ como queríamos. Por otro lado, si $\sqrt{I} + \sqrt{J} = (1)$ entonces existen $x \in \sqrt{I}, y \in \sqrt{J}$ tales que $x + y = 1$. Ahora, sean $n, m \in \mathbb{N}_{\geq 1}$ tales que $x^n \in I, y^m \in J$ entonces consideramos ahora $(x+y)^{n+m-1} = 1$ y desarrollando con el binomio de Newton el término de la izquierda vemos que tenemos todos los términos en $I + J$ de modo que $1 \in I + J$ como queríamos
3. La implicación de izquierda a derecha es directa puesto que, si $x \in I : J$ entonces $x \cdot y \in I, \forall J$, como $1 \in I : J$ entonces $1 \cdot y \in I, \forall y \in J$ concluyendo el resultado. Para la contención contraria basta ver que si $J \subseteq I$ entonces $x \cdot y \in I, \forall y \in J$ verificando que $x \in I : J$ como queríamos ver.

■

Ejercicio 3.2.10. (Se supone conocida la definición de ideal primo). Sea P un ideal primo y J un ideal arbitrario. Demuestre que:

$$P : J = P \quad \text{o} \quad P : J = (1)$$

Demostración. Realicemos la prueba por la definición de división de ideales. Sea $x \in P : J$ un elemento arbitrario, entonces tenemos que $x \cdot y \in P, \forall y \in J$. Dado que P es un ideal primo tenemos dos opciones, o bien $x \in P$ o $y \in P$ para cada producto.

- Supongamos en primer lugar que $x \notin P$, entonces $y \in P, \forall y \in J$ de modo que $1_R \in P : J$ llegando al segundo caso.
- Ahora, si para algún elemento de $J, y \notin P$ necesariamente $x \in P$ y como hemos tomado un elemento arbitrario entonces $P : J = P$.

■

Ejercicio 3.2.11. Sea D un dominio de ideales principales (DIP). Sean (a) y (b) ideales de D, distintos de (0) y (1). Entonces los ideales:

$$(a)+(b), \quad (a)\cap(b), \quad (a)(b), \quad \sqrt{(a)}, \quad (a):(b)$$

son principales. Describa un generador de cada uno en función de la factorización en irreducibles de a y b.

Ejercicio 3.2.12. Sea I un ideal de un anillo R, y sean J, K ideales de R que contienen a I. Para cada elección de ideal M, hallar el único ideal L de R con la propiedad de que $L \supseteq I$ y $L/I = M$.

1. $M = J/I + K/I$
2. $M = (J/I) \bigcap (K/I)$
3. $M = (J/I) : (K/I)$
4. $M = (J/I)^n$
5. $M = (J/I)(K/I)$
6. $M = (a_1 + I, \ldots, a_n + I)$

Demostración. Vayamos paso por paso.

1. El candidato es $L = (J+K)/I$, probemos ambas contenciones,
2. Como el anterior para $M = (J/I) \bigcap (K/I)$
3. Veamos que $L = J \cdot K + I$.
   - $\subseteq$ Sea $\bar{x} \in (J/I)\cdot(K/I)$, entonces $\bar{x} = \sum_h \bar{j_h} \cdot \bar{k_h}$ con $\bar{j_h} \in J/I, \bar{k_h} \in K/I$. Vemos que $\forall h, j_h \in J, k_h \in K$, por tanto $\sum_h j_h \cdot k_h \in J \cdot K \subseteq J \cdot K + I$ y concluimos que $\bar{x} \in (J \cdot K + I)/I$.
   - $\supseteq$ Sea $\bar{x} \in (J \cdot K + I)/I$, $x \in J \cdot K + I$, entonces $x = \sum j_h \cdot k_h + a, j_h \in J, k_h \in K, a \in I$ y por tanto tomando módulos vemos que $\bar{x} \in (J/I)\cdot(K/I)$
4. Tomamos $L = (J^n + I)$
5. $M = (J/I)(K/I)$
6. Probemos que $L = (a_1, \ldots, a_n) + I$

■

REVISAR CREO QUE CAMBIADOS DE ORDEN

Observación 3.2.10. Observamos que en (3) no podemos seguir el razonamiento de los dos primeros casos, basta ver que $(J/I) : (K/I) \neq (KJ/I)$, porque considerando $I = J = (x)$ entonces $(x) \subseteq (x)$ en ambos casos pero $(x) \not\subseteq (x^2)$. Ahora, para el resto sí que seguimos la lógica de tomar la solución *evidente* y sumarle el ideal por el que cocientamos.

Ejemplo 3.2.2. En $\mathbb{Z}/(49)$ tenemos que $(\bar{14}) \Leftrightarrow (14)+(49) = (7)$. Sin embargo $(\bar{7}) = (\bar{14})$, por lo que vemos que estudiar el ideal $(\bar{14})$ equivale a estudiar el (7) en $\mathbb{Z}$.

Por ejemplo, en el ejercicio 3.1.6 considerábamos $\mathbb{Z}/(24)$, y si tomamos el ideal (6) vemos que sí coincide, pero porque $(24) \subseteq (6)$.

Observación 3.2.11. Si $I \subseteq J$, consideramos la proyección y entonces $J/I = \big(\pi(J)\big)$. Si tomamos ahora $I \subseteq K$, del mismo modo $K/I = \big(\pi(K)\big)$. Ahora, en ambos casos tenemos que existen elementos en J y K respectivamente tales que $x = y + a$ o $x = y + a.$, $y \in J(K), a \in I$. Ahora, en el primer caso

$$x = y + a, y \in J, a \in I \Rightarrow x \in I + J$$

pero en el segundo tenemos que

$$x = y + a, y \in K, a \in I \subseteq K \Rightarrow x \in K.$$

Observación 3.2.12. En R/I, $I \subsetneq J, J/I = \big(\pi(J)\big)$ y entonces, vemos que $J/I = (J + I)/I$ y por tanto $(R/I)\Big/(J/I) \cong R\Big/(I + J)$

Capítulo 4: Ideales primos y maximales

Una vez hemos conocido las propiedades, operaciones y más relaciones básicas de los ideales, en este capítulo abordamos dos clases particulares de este: los ideales *primos* y los *maximales*. Estos ideales juegan un papel muy importante en toda la teoría de anillos por su relevancia a la hora de formar anillos cocientes con buenas propiedades, su relación la estructura del anillo en el que están y sus consecuencias en teoría de módulos, geometría algebraica y la descomposición de ideales. Así pues, recapitulando en los concepto básicos o ya introducidos previamente:

Definición 4.0.5. Sea R un anillo, diremos que:

1. Al ideal $R = (1)$ lo llamamos ideal *impropio*
2. Todo ideal $I \neq R$ lo llamamos *propio*

Y ahora, como parece razonable por el interés de este capítulo, recuperamos las definiciones 2.2.7 y 2.2.8, aunque podemos hacer un pequeño comentario acerca de esta segunda que nos será de más utilidad como definición de *maximal*.

Observación 4.0.13. Un ideal se dice *maximal* si lo es para la relación de contención $\subseteq$.

4.1. Existencia y relevancia

En esta sección abordaremos la existencia de ideales maximales, que por la 2.2.3, además nos dará la de ideales primos. Para introducir esta idea en ideales abstractos recurriremos al *Lema de Zorn* que es equivalente al *Axioma de elección*, la relevancia de este resultado aparece en numerosas demostraciones esenciales de distintas áreas de las matemáticas, tales como el teorema de *Hahn-Banach* en análisis funcional, el teorema de que todo espacio vectorial tiene una base y el teorema de *Tychonoff* en topología. Bajo este contexto nos cercionamos de la existencia de este tipo de ideales y obtenemos así los resultados posteriores.

Lema 4.1.1 (Lema de Zorn)**.** *Sea (Σ, Φ) un conjunto no vacío ordenado por Φ, tal que toda cadena de Σ tiene cota superior, entonces Σ tiene al menos un elemento maximal.*

A partir de este resultado enunciamos el siguiente teorema.

Teorema 4.1.1. *Sea $R \neq \{0\}$, un anillo no trivial, entonces R tiene al menos un ideal maximal*

Demostración. Sea $\Sigma = \{I \subsetneq R \mid I \text{ ideal}\}$ el conjunto de los ideales propios, como $R \neq \{0\}$, entonces $0R \in \Sigma \neq \emptyset$. Por otro lado, tenemos que Σ está ordenado por la relación de contención $\subseteq$, veamos que Σ tiene elementos maximales por el lema de Zorn. Sea $\{I_\lambda : \lambda \in A\} \subseteq \Sigma$ una cadena, es decir, si $\alpha, \beta \in A$ entonces $I_\alpha \subseteq I_\beta$ o $I_\beta \subseteq I_\alpha$, veamos que tiene cota superior. Tomamos $J = \cup_{\lambda \in A} I_\lambda$, veamos que es un ideal. Claramente es no vacío. Ahora, sean $a, b \in J$, veamos que $a + b \in J$. Como $a \in J$, entonces $\exists \alpha \in A$ con $a \in I_\alpha$ y análogamente $b \in I_\beta$. Como tenemos una cadena podemos asumir sin pérdida de generalidad que $I_\alpha \subseteq I_\beta$ y por tanto $a \in I_\beta$ de modo que $a + b \in I_\beta \subseteq J$. Ahora, si $1 \in J$ entonces $\exists \gamma \in A$ tal que $1 \in I_\gamma$ contradiciendo que $I_\gamma \in \Sigma$ pues no sería propio. De este modo vemos que J es una cota superior de la cadenas y por el lema de Zorn tenemos que Σ tiene elementos maximales. ■

Corolario 4.1.1. *Sea $R \neq \{0\}$ un anillo e I un ideal propio, entonces $\exists m$ ideal maximal con $I \subseteq m$.*

Podemos dar dos demostraciones a este corolario.

Demostración. (I) Aplicamos el lema de Zorn al conjunto $\Sigma = \{J \subseteq R \mid I \subsetneq J \subsetneq R\}$ ■

Demostración. (II) Como $I \subsetneq R$, entonces $R/I \neq \{0\}$ y por tanto el cociente tiene un maximal m/I. Ahora por la biyección de ideales de R/I en R tenemos que $I \subseteq m \subsetneq R$. ■

Ejemplo 4.1.1. Consideremos las funciones continuas $\mathscr{C}(\mathbb{R})$, el conjunto de sus unidades

$$\mathscr{C}(\mathbb{R})^* = \{f \in \mathscr{C}(\mathbb{R}) \mid \exists g \in \mathscr{C}(\mathbb{R}), f \cdot g = cte_1\} = \{f \in \mathscr{C}(\mathbb{R}) \mid \forall x \in \mathbb{R}, f(x) \neq 0\}$$

Ahora, si m es maximal en $\mathscr{C}(\mathbb{R})$ entonces tenemos que $\forall f \in m, \exists x$ tal que $f(x) = 0$, pues de no ser así, $f \in \mathscr{C}(\mathbb{R})^* \Rightarrow 1 \in m\#$. Ahora, consideremos por ejemplo las funciones f, g que son cte_0 y x en dos conjuntos disjuntos complementarios, de modo que $f \cdot g = cte_0$, entonces tenemos que $f \cdot g \in m$ y como por ser maximal es primo entonces $f \in m \vee g \in m$. Sin embargo ninguna de ellas es 0 y por tanto vemos a su vez que $\mathscr{C}(\mathbb{R})$ no es un dominio.

Por otro lado, consideramos ahora el ideal $m_a = \{g \in \mathscr{C}(\mathbb{R}) \mid g(a) = 0\}$ y el homomorfismo de evaluación φ_a. Por el primer teorema de isomorfía tenemos que $\mathscr{C}(\mathbb{R})/ker\varphi_a \cong \mathbb{R}$ que es cuerpo y por tanto, $ker\varphi_a = m_a$ es un ideal maximal. Es fácil probar que m_a es ideal y φ_a homomorfismo, aunque como más adelante demostraremos que el kernel es un ideal no hace demostramos que m_a sea un ideal.

Ya hemos probado la existencia de los ideales maximales en un anillo R. Por tanto, empecemos con los resultados de anillos relacionados con estos tipo de ideales.

Proposición 4.1.1. *Sea R un anillo y m maximal (P primo), $x \in R$ nilpotente, entonces $x \in m$ (P)*

Demostración. Para el caso de un ideal maximal, supongamos que $\exists x \notin m$ nilpotente, entonces

$$m + (x) = (1) \Rightarrow 1 = t + x \cdot y, t \in m, y \in R.$$

Así despejando $t = 1 - x \cdot y$, como $x \cdot y$ es nilpotente por el ejercicio 3.1.9, $t \in R^*\#$. Por otro lado, para P primo, tenemos que $x^n = 0 \in P$, por lo que por ser primo $x \cdot x^{n-1} \in P \Rightarrow x \in P \vee x^{n-1} \in P$. En el primer caso habríamos acabado y en el segundo, iterando llegaríamos al resultado. ■

Teorema 4.1.2. *Sea R un anillo, $R \neq \{0\}$, entonces* $\bigcup_{\substack{m \subseteq R \\ m \text{ máx}}} m = R \backslash R^*$.

Demostración. Veámos el resultado por doble contención.

- $\subseteq$ Si $x \in \bigcup_{\substack{m \subseteq R \\ m \text{ máx}}} m$ entonces $\exists I$ maximal con $x \in I$ tal que $x \notin R^*$ porque de no ser así $1 \in I$ y no sería maximal.
- $\supseteq$ Sea $x \in R \backslash R^*$, entonces $(x) \subsetneq (1)$ y como (x) es propio entonces $\exists I$ maximal tal que $(x) \in I \subseteq \bigcup_{\substack{m \subseteq R \\ m \text{ máx}}} m$.

■

Corolario 4.1.2. *Sea $R \neq \{0\}$ un anillo, entonces* $\bigcup_{P \text{ primo}} P = R \backslash R^*$

Demostración. La demostración es directa por la propiedad 2.2.3 y del teorema anterior (4.1.2):

$$R \backslash R^* = \bigcup_{m \text{ máx}} m \subseteq \bigcup_{p \text{ primo}} P \subseteq R \backslash R^*$$

■

Del mismo modo que hemos visto la relación entre un anillo y la unión de sus maximales podemos intentar ver como es la intersección. Introducimos previamente:

Definición 4.1.1. Sea $R \neq \{0\}$ un anillo, llamaremos *radical de Jacobson* a

$$Jac(R) := \bigcap_{m \text{ máx}} m$$

A partir de esta definición enunciamos el siguiente teorema.

Teorema 4.1.3. $Jac(R) = \{x \in R \mid \forall y \in R, 1 - xy \in R^*\}$

Demostración. Procedamos por doble contención:

- $\subseteq$ Sea $x \in Jac(R)$, sabemos por el teorema 4.1.2 que

  $$R^* = R \backslash (\bigcup_{m \text{ max}} m) = \bigcap_{m \text{ max}} (R, m)$$

  de modo que $1 - xy \in R^* \Leftrightarrow \forall m$ maximal , $1 - xy \notin m$. Si $1 - xy \in m$, como $x \in m$ entonces $(1 - xy) + xy \in m \Rightarrow 1 \in m\#$.
- $\supseteq$ Supongamos que $\forall y \in R$ se cumple $1 - xy \in R^*$. Vamos a probar que $x \in m$ para todo ideal maximal m, es decir, $x \in \text{Jac}(R)$. Supongamos, por el contrario, que existe un ideal maximal m tal que $x \notin m$. Como m es maximal, el ideal generado por x y m es todo R, es decir, $(x) + m = R \Rightarrow \exists r \in R, a \in m$ tal que $xr + a = 1 \Rightarrow 1 - xr = a \in m$. Pero esto contradice el hecho de que $1 - xr \in R^*$, porque tendríamos un elemento unidad en un maximal.

■

Teorema 4.1.4. *Si $I \subsetneq R$ es un ideal, entonces* $\sqrt{I} = \bigcap_{\substack{P \text{ primo} \\ I \subseteq P}} P$

Demostración. Vamos a demostrar la contención de izquierda a derecha. Sea $x \in \sqrt{I}$, P un ideal primo tal que $I \subseteq P$, entonces $\exists n \in \mathbb{N}_{\geq 1}$ tal que $x^n \in I \subseteq P$ y como P es primo entonces $x^n \in P \Rightarrow x \in P$ [5].

Para la otra contención tomemos un elemento $x \notin \sqrt{I}$ y veamos que $\exists J \subseteq P$ con $x \notin P$ y por ello no en su intersección. Consideremos el conjunto

$$\Sigma = \{J \subseteq R \mid J \text{ ideal}, I \subseteq J, x \notin \sqrt{J}\}.$$

que no es vacío porque estamos asumiendo que I lo verifica. Además Σ esta ordenado por la relación de contención y si tomamos J_λ una cadena sabemos que $H = \bigcup J_\lambda$ es un ideal. Por otro lado tenemos que $I \subseteq J_\lambda \subseteq H$ y si existiese $n \in \mathbb{N}_{\geq 1}$ tal que $x^n \in H$ entonces $x^n \in J_\lambda$ para algún λ lo que sería un absurdo, por lo que $\forall n \in \mathbb{N}_{\geq 1}, x^n \notin H$ y $H \in \Sigma$. En estas condiciones podemos aplicar el lema de Zorn, llamemos al elemento maximal P, que cumple que $I \subseteq P \wedge x^n \notin P$. Además, como es maximal tenemos que $\forall S, S \supseteq P, \exists n \in \mathbb{N}_{\geq 1}$ tal que $x^n \in S$. Veamos ahora que P es primo. Para ello probemos que dados dos elementos $a, b \notin P$ entones $ab \notin P$. Tomemos esos dos elementos, entonces

$$P \subseteq P + (a) = S_1 \tag{4.3}$$
$$P \subseteq P + (b) = S_2 \tag{4.4}$$

de modo que existen $n_1, n_2 \in \mathbb{N}_{\geq 1}, r_1, r_2 \in P, t_1, t_2 \in R$ tales que

$$x^{n_1} = r_1 + a \cdot t_1 \tag{4.5}$$
$$x^{n_2} = r_2 + b \cdot t_2 \tag{4.6}$$

multiplicando ahora ambas expresiones tenemos que

$$x^{n_1+n_2} = (r_1 r_2)^{\in P} + (r_1 b t_2)^{\in P} + (r_2 a t_1)^{\in P} + (ab t_1 t_2)^{\in (ab)}$$

de modo que $x^{n_1+n_2} \in P + (ab)$ y como $x^{n1+n2} \notin P$ y $ab \notin P$,si $x^{n_1+n_2} \in P$ entonces tendríamos que $ab \in P$ contradiciendo la hipótesis, por lo que concluimos que P es primo. ■

Observación 4.1.1. En particular, si $I = P$ primo entonces $\sqrt{I} = P$. Supongamos que $\exists \tilde{P}$ primo tal que $I \subseteq \tilde{P} \subsetneq P$. Dados $a, b \in R, ab \in \tilde{P}$ entonces por ser primo $a \in \tilde{P} \vee b \in \tilde{P}$, por contención entonces $a \in P \vee b \in P$ y por tanto $ab \in P$ contradiciendo que $\tilde{P} \subsetneq P$ y concluyen que efectivamente, por el resultado que P es el único primo que contiene a P y por tanto coincide con su radical.

Corolario 4.1.3. *En particular,* $\sqrt{(0)} = \bigcap_{P \text{ primo}} P$.

Demostración. Basta aplicar el teorema anterior y ver que efectivamente $(0) \subseteq I$ en general para todos los ideales por lo que en particular para todos los primos. ■

Ejemplo 4.1.2. *Hacemos aquí una mención honorífica al ejemplo del Sudoku.*

Definición 4.1.2. Un anillo R se dice *local* si tiene un único maximal m.

Ejemplo 4.1.3. Si $p \in \mathbb{Z}$ es un número primo, entonces $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ es un anillo local de maximal (p).

[5] Aquí estamos omitiendo el mismo procedimiento que en la demostración de la proposición 4.1.1

Lema 4.1.2. *Sea R un anillo, son equivalentes:*

(I) *R es un anillo local.*

(II) *$R\backslash R^*$ es un ideal de R.*

Demostración. Procedamos por doble implicación.

- $\Rightarrow$ Tenemos que por ser R un anillo local $\exists m \subseteq R$ ideal maximal único de R. Veamos que efectivamente $m = R\backslash R^*$. Dado $x \in R$, si fuera unidad $x \notin m$ de modo que $m \subseteq R\backslash R^*$. Por otro lado $x \in R\backslash R^*$, si $x \notin m$ entonces $m + (x) = R$ y (x) sería maximal, lo que contradice que m sea el único.
- $\Leftarrow$ Si $R\backslash R^*$ es un ideal entonces veamos que es único. Supongamos que $\exists I \neq R\backslash R^*$ maximal. Por tanto $\exists x \in I \subseteq R$. Rápidamente vemos que, si $x \in R^*$ entonces $1_R \in I \Rightarrow I = (1)$ y si por el contrario $x \in R\backslash R^* \Rightarrow I \subseteq R\backslash R^*$ contradiciendo que I es maximal.

■

Observación 4.1.2. Damos a continuación una demostración alternativa de este resultado.

Demostración. De nuevo por doble implicación:

$\Leftarrow$ Como R es local entonces tiene un único maximal y en virtud del teorema 4.1.2 tenemos que $R\backslash R^* = \bigcup_{I \text{ máx}} = m$, que es un ideal

$\Rightarrow$ Análogamente, sea m un ideal maximal, $m \subseteq R\backslash R^*$ y como $R\backslash R^*$ es propio entonces $m = R\backslash R^*$.

■

Observación 4.1.3. Si R es un anillo local, entonces su maximal asociado es precisamente $R\backslash R^*$. La prueba de esto es directa.

Proposición 4.1.2. *Sea R un anillo local entonces $Jac(R) = R\backslash R^*$*

Demostración. Para ver este resultado basta aplicar el teorema 4.1.2 y la definición de radical de Jacobson (4.1.1), pues al solo haber un maximal $m = R\backslash R^*$ se tiene que

$$R\backslash R^* = \bigcup_{m \text{ max}} m = m = \bigcap_{m \text{ max}} m = Jac(R)$$

■

Hemos estudiado ya las relaciones entre intersecciones de ideales, generadores de productos, etc. En relación a esta propiedad aparece la relevancia de los ideales maximales en el teorema chino del resto (una de sus versiones [6]). Previamente introducimos una definición y un teorema.

Definición 4.1.3. Dos ideales I, J se dicen *comaximales* si $I + J = (1)$

[6] En [3] y [4] pueden verse las distintas versiones junto con sus demostraciones.

Observación 4.1.4. Como particularidad, para estos ideales se verifica que $IJ = I \cap J$.

Demostración. La contención de izquierda a derecha siempre se cumple (ver ejercicio 3.2.8,4). Para el otro lado tenemos que, por ser comaximales existen $a \in I, b \in J$ tales que $1 = a + b$. Ahora, sea $x \in I \cap J$, entonces $x = ax + bx$ y entonces el primer sumando $a^{\in I}x^{\in J}$ y el segundo $b^{\in J}x^{\in I}$, por lo que vemos que $x \in IJ$. ■

Teorema 4.1.5. *Sean $I_1, \ldots, I_n$ ideales propios de R tales que $\forall i, j, i \neq j$ tales $I_i + I_j = (1)$ (comaximales dos a dos) entonces:*

(I) Para cada $j \in \{1, \cdots, n\}$ los ideales I_j y $\bigcap_{i \neq j} I_i$ son comaximales.

(II) $\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$

Demostración. (I) Sin pérdida de generalidad probemos que $\bigcap_{i=1}^{n-1} I_i + I_n = (1)$. Como para cada $j \in \{1, \cdots, n-1\}$ tenemos que I_j, I_n son comaximales entonces existen $a_j \in I_j$ y $b_j \in I_n$ tales que $a_j + b_j = 1$. Tenemos por tanto que $\forall j \in \{1, \cdots, n-1\}, a_j = 1 - b_j \in I_j$ y entonces

$$A = \prod_{j=1}^{n-1} a_j \in \prod_{j=1}^{n-1} I_j \subseteq \bigcap_{j=1}^{n-1} I_j.$$

Ahora, sustituyendo $a_j = 1 - b_j$:

$$A = \prod_{j=1}^{n-1} (1 - b_j) = 1 - B$$

donde $B = \sum$ factores b_j de modo que salvo el 1, todos los factores están en I_n y reordenando tenemos

$$1 = A + B \in \bigcap_{i=1}^{n-1} I_i + I_n$$

■

Demostración. (II) Apliquemos inducción.

- $n = 2$: Este caso se corresponde con la observacion 4.1.4.

Suponiéndolo cierto para todo $k \leq n - 1$ entonces:

- $n = k$: $\prod_{i=1}^{n} I_i = \prod_{i=1}^{n-1} I_i \cdot I_n$. Aplicando HDI tenemos $\bigcap_{i=1}^{n-1} I_i \cdot I_n$ y como por (I) son comaximales, aplicando el caso $n = 1$ se prueba el resultado.

■

Visualicemos un ejemplo de lo que nos dice este teorema en $\mathbb{Z}$.

Ejemplo 4.1.4. Dados $a, b \in \mathbb{Z}_{>0}$, $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \Leftrightarrow \gcd(a, b) = 1$. Entonces:

(I) Si tuviéramos $\gcd(a_1, \cdot, a_n) = 1$, coprimos entre sí, entonces $\gcd(\prod_{i=1}^{n-1} a_i, a_n) = 1$.

(II) Como $\gcd(a, b) = 1$ entonces $(a) \cap (b) = (ab)$. Sabemos por el ejercicio 3.2.11 que $(a) \cap (b) = (\text{lcm}(ab)) = ab$, verificándose lo que sabíamos.

Teorema 4.1.6 (Teorema chino del resto)**.** *Sea R un anillo no trivial, $I_1, \dots, I_n \subseteq R$ ideales comaximales dos a dos, entonces el homomorfismo $\varphi : R \longrightarrow R/I_1 \times \cdots \times R/I_n$ es sobreyectivo. Además, $ker\varphi = \bigcap_{i=1}^{n} I_i$ que por el teorema 4.1.5 es igual a $\prod_{i=1}^{n}$, de manera que por el primer teorema de isomorfía (teorema 2.1.1) se verifca que:*

$$R\Big/\prod_{i=1}^{n} I_i \cong \prod_{i=1}^{n}\Big(R/I_i\Big)$$

Demostración. Como los ideales son comaximales dos a dos. para cada $j \in \{1, \cdots, n\}$ se tiene que I_j y $\bigcap_{i\neq j} I_i$ son comaximales (teorema 4.1.5) y por tanto existen $a_j \in \bigcap_{i\neq j} I_i$ y $b_j \in I_j$ tales que $1 = a_j + b_j$. Tenemos entonces que $\varphi(a_j) = (\dots, \bar{1}^{(j)}, \dots)$ pues en R/I_j tenemos que $\bar{a_j} = \bar{1}$ porque $b_j = 1 - a_j \in I_j$. Así pues, tomando $(r_1 + I_1, \dots, r_n + I_n) \in R/I_1 \times \cdots \times R/I_n$, llamamos $x = a_1r_1 + \cdots + a_nr_n$ y tenemos que $\varphi(x) = (r_1 + I_1, \dots, r_n + I_n)$ concluyendo que es un homomorfismo sobreyectivo.

El resultado final se ve directamente, en R/I_j es claro que el kernel será I_j de modo que para el homomorfismo φ, $x \in ker\varphi \Leftrightarrow x \in I_j, \forall j \in \{1, \cdots, n\} \Leftrightarrow x \in \bigcap I_j$ que como hemos delantado en el enunciado conduce a lo que queremos. ■

Pongamos un ejemplo del funcionamiento de este teorema:

Ejemplo 4.1.5. Imaginemos que queremos resolver:

$$\begin{aligned} x &\equiv 2 \pmod{35}, \\ x &\equiv 7 \pmod{9}, \end{aligned}$$

Tenemos que:

$$\begin{aligned} 35 &= 35 \cdot (1) + 9 \cdot (0) \\ 9 &= 35 \cdot (0) + 9 \cdot (1) \\ 8 &= 35 \cdot (1) + 9 \cdot (-3) \\ 1 &= 35 \cdot (-1) + 9 \cdot (4) \end{aligned}$$

Entonces,

$$-173 = 35 \cdot (-1) \cdot (7) + 9 \cdot 4 \cdot (2)$$

y recordando que estamos en trabajando módulo llegamos a que

$$-173 \pmod{35 \cdot 9} = 35 \cdot (-1) \cdot 7 \pmod{9} + 9 \cdot 4 \cdot 2 \pmod{35}$$

$$142 = 35 \cdot 8 \cdot 7 + 9 \cdot 4 \cdot 2$$

siendo $x = 142$ la solución.

LLegamos ahora al teorema final de esta sección: el teorema de evitación de primos. La idea de este resultado es que, dado un ideal en una unión de ideales primos entonces está contenido completamente en uno de ellos. Comencemos con un resultado auxiliar.

Lema 4.1.3. *Sea R un anillo, $P \subseteq R$ primo y los ideales $I_1, \dots, I_n$ ideales de R, son equivalentes:*

(I) $\exists i \in \{1, \cdots, n\}$, $I_i \subseteq P$

(II) $\bigcap_{i=1}^{n} I_i \subseteq P$

(III) $\prod_{i=1}^{n} I_i \subseteq P$

Demostración. Tenemos que, para cada $k \in \{1, \cdots, n\}$, se verifica que

$$\prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i \subseteq I_k$$

por lo que (I) $\Rightarrow$ (II) $\Rightarrow$ (III).

Veamos ahora que (III) $\Rightarrow$ (I). Supongamos que es falso. Para cada $i \in \{1, \cdots, n\}, \exists a_i \in I_i \backslash P$, pero entonces, tenemos que $\prod_{i=1}^{n} a_i \in \prod_{i=1}^{n} I_i$ pero por hipótesis $\prod_{i=1}^{n} I_i \subseteq P$ concluyendo que $\prod_{i=1}^{n} a_i \in P$. Como P es primo entonces necesariamente $a_i \in P$ para algún i contradiciendo la hipótesis. ■

Corolario 4.1.4. *Sea P un ideal primo, $I_1, \ldots, I_n$ ideales. Si $P = \bigcap_{i=1}^{n} I_i$, entonces existe un $i \in \{1, \cdots, n\}$ con $P = I_i$.*

Demostración. Por el lema anterior (4.1.3), $\exists k$ con $I_k \subseteq P = \bigcap_{i=1}^{n} I_i \subseteq I_k$. ■

Con este lema auxiliar, probemos el teorema que pone fin a esta sección.

Teorema 4.1.7 (Teorema de evitación de primos)**.** *Sea R un anillo, $P_1, \ldots, P_n$ ideales primos e I un ideal arbitrario, si $I \subseteq \bigcup_{i=1}^{n} P_i$ entonces $\exists k \in \{1, \cdots, n\}$ con $I \subseteq P_k$.*

Demostración. Probemos el resultado por inducción para $n \geq 2$, el caso para $n = 1$ es trivial.

- $n = 2$: Supongamos $I \subseteq P_1 \bigcup P_2$. Si I no está contenido en ninguno entonces $\exists a \in I \backslash P_1$ y $\exists b \in I \backslash P_2$. Entonces, tenemos que $a + b \in I \subseteq P_1 \bigcup P_2$, donde, si $a + b \in P_1 (P_2)$ entonces contradice que $a \in P_1 (b \in P_2)$.

Supongamos que es cierto para n ideales y probemos para n+1 concluyendo la inducción

- $n + 1$: Supongamos que $I \subseteq \bigcup_{i=1}^{n+1} P_i$, si $\exists j \in \{1, \cdots, n+1\}$ tal que

$$I \subseteq \bigcup_{\substack{i \in \{1, \cdots, n+1\}, \\ i \neq j}} P_i$$

  por h.p.i tendríamos el resultado. Por lo contrario, si $\forall j \in \{1, \cdots, n+1\}$, $\exists a_j \in I \backslash \left(\bigcup_{k \neq j} P_k \right)$ (observemos que $a_j \in P_j$). Consideramos $b = a_1 \cdots a_n + a_{n+1} \in I$<Observamos que $\exists k, b \in P_k$ porque $b \in I \subseteq \bigcup_{i=1}^{n} P_1$, de este modo:

  - Si $k \in \{1, \cdots, n\}$, luego $a_k \in P_k$ y $a_{n+1} = b - a_1 \cdots a_n \in P_k$ #
  - Si $k = n + 1$ entonces $a_k \in P_k$ y $a_{n+1} - b = a_1 \cdots a_n \in P_{n+1}$ y como P_{n+1} es primo entonces llegamos a contradicción porque necesariamente $a_i \in P_{n+1}$ para algún $i \in \{1, \cdots, n\}$.

■

Observación 4.1.5. En la primera parte de la demostración no hemos hecho uso en ningún momento de que P_1, P_2 son primos, por lo que ese resultado es general para dos ideales arbitrarios. La necesidad de esta condición viene en el paso inductivo.

4.1.1. Extensión de anillos de polinomios a matrices

Definición 4.1.4. Sea $\mathbb{K}$ cuerpo, $A \in \mathcal{M}_{n\times n}$, definimos

$$\mathbb{K}[A] = \{\sum_{i=0}^{n} k_i A^i \mid n \in \mathbb{N}, k_i \in \mathbb{K}(A^0 = Id)\} \subseteq \mathcal{M}_{n\times n}(\mathbb{K})$$

.

Consideremos la siguiente aplicación:

$$\begin{aligned} \varphi : \mathbb{K}[x] &\longrightarrow \mathbb{K}[A] \\ f(x) &\longrightarrow f(A) \\ \sum_{i=0}^{n} k_i x^i &\longrightarrow \sum_{i=0}^{n} k_i A^i \end{aligned}$$

Observamos que es sobreyectiva por la defición de $\mathbb{K}[A]$ y además, $ker\varphi = \{f(x) \mid f(A) = (0)\}$, es decir $\exists g(x)$ de grado mínimo tal que $g(A) = 0$ y por el primer teorema de isomorfía $\mathbb{K}[x]/(g) \cong \mathbb{K}[A]$.

Ejemplo 4.1.6. Consideramos $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, el polinomio mínimo es $x^2 + 1$, de manera que podemos relacionar $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$ mediante la definición y la aplicación anterior:

$$\mathbb{R}[x]/(x^2+1) \cong \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} = \{a \cdot Id + b \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mid a, b \in \mathbb{R}\} = \mathbb{R}\left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right]$$

.

4.2. Ejercicios

Ejercicio 4.2.1. Demuestre que en $\mathbb{R}[x,y,z]$ el ideal $(x^2+y^2+z^2)$ es primo.

Demostración. Como $\mathbb{R}$ es cuerpo por la observación 2.2.6 tenemos que $\mathbb{R}[x,y,z]$ es un DIP y en particular DFU. Ahora bien, el polinomio $x^2+y^2+z^2$ es claramente irreducible en $\mathbb{R}[x,y,z]$, basta plantear una descomposición y ver que no tiene soluciones reales. Por lo que por la observación 2.2.4 tenemos que irreducible sii primo y entonces el ideal generado por un elemento primo es primo (observación 2.2.2). ■

Ejercicio 4.2.2. Sea P un ideal primo, demuestre que $\sqrt{P^m} = P$ para todo $m \geq 1$. ¿Es cierto el resultado si P no es un ideal primo?

Demostración. Veamos las dos contenciones

- $\subseteq$ Tenemos que $P^m \subseteq P$ y tomando radicales tenemos que $\sqrt{P^m} \subseteq \sqrt{P} = P$ por ser P primo (4.1.1)
- $\supseteq$ Esta contención es directa.

Si el ideal no es primo el resultado no es cierto, basta ver que hemos hecho uso de ello a la hora de concluir en la primera contención que $\sqrt{I} = I$. Como contraejemplo consideramos en $\mathbb{Z}$ el ideal (4), tenemos entonces que $\sqrt{(4)^m} = (2) \neq (4)$. ■

Ejercicio 4.2.3. Sea R un anillo no trivial. Demuestre que son equivalentes:

1. R tiene exactamente un ideal primo.
2. Todo elemento de R es o bien unidad o bien nilpotente.
3. $\sqrt{(0)}$ es maximal.

Demostración. Vayamos implicación por implicación.

- (II)⇒(III): Si se cumple (II) tenemos que necesariamente $R\backslash R^* = \sqrt{(0)}$ es un ideal por lo que R es un anillo local de maximal $\sqrt{(0)}$ (lema 4.1.2).
- (III)⇒(I): Sea $m = \sqrt{(0)}$ maximal entonces es primo. Ahora, sea Q otro ideal primo tal que $m \subseteq Q$, como m es maximal y $Q \neq (1)$ entonces necesariamente $Q = m$, concluyendo que solo hay un primo.
- (I)⇒(II): En virtud del lema 4.1.2 y la observación 2.2.3 tenemos que, si R tiene exactamente un primo entonces R es un anillo local (puesto que si hubiera dos maximales habría dos primos contradiciendo la hipótesis) y por tanto $P = R\backslash R^*$, asi que todo elemento o es unidad o está en P. Adicionalmente, por el teorema 4.1.4 tenemos que $\sqrt{(0)} = \bigcap_{\substack{(0)\subseteq P \\ P \text{ primo}}} P = P = R\backslash R^*$ de modo que el conjunto de los nilpotentes coincide con $R\backslash R^*$.

■

Ejercicio 4.2.4. Considere el homomorfismo $\varphi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ definido por:

$$\varphi(x) = (x + 5\mathbb{Z}, x + 13\mathbb{Z}).$$

Calcule una preimagen de $(3+5\mathbb{Z}, 10+13\mathbb{Z})$. ¿Cómo calcularía las preimágenes de un par arbitrario?

Demostración. Para calcular $\varphi^{-1}(3-5\mathbb{Z}, 10+13\mathbb{Z})$ aplicaremos un procedimiento similar al del ejemplo 4.1.5. Queremos resolver el sistema

$$\begin{aligned} x &\equiv 10 \pmod{13}, \\ x &\equiv 3 \pmod{5}, \end{aligned}$$

Tenemos que:

$$\begin{aligned} 13 &= 13 \cdot (1) + 5 \cdot (0) \\ 5 &= 13 \cdot (0) + 5 \cdot (1) \\ 3 &= 13 \cdot (1) + 5 \cdot (-2) \\ 2 &= 13 \cdot (-1) + 5 \cdot (3) \\ 1 &= 13 \cdot (2) + 5 \cdot (-5) \end{aligned}$$

Entonces,

$$-172 = 13 \cdot (2) \cdot (3) + 5 \cdot (-5) \cdot (10)$$

Y tomando módulos llegamos a que

$$-172 \mod 13 \cdot 5 = 13 \cdot (2) \cdot (3) \mod 5 + 5 \cdot (-5) \cdot (10) \mod 13$$

$$x = 23$$

Para un elemento arbitrario $(a+5\mathbb{Z}, b+13\mathbb{Z})$ procederíamos de la misma manera: Aplicamos el algoritmo de Euclides, ajustamos con los valores que queremos y tomamos módulos para obtener la solución. ■

Ejercicio 4.2.5. Sea $\mathbb{K}[x_1, \ldots, x_n]$ un anillo de polinomios en n variables con coeficientes en el cuerpo $\mathbb{K}$. Sean $a_1, \ldots, a_n \in \mathbb{K}$. Demuestre que la cadena:

$$(0) \subset (x_1 - a_1) \subset (x_1 - a_1, x_2 - a_2) \subset \cdots \subset (x_1 - a_1, \ldots, x_n - a_n)$$

es una cadena estricta de ideales primos.

Demostración. En primer lugar, denotando $I_k = (x_1 - a_1, \ldots, x_k - a_k)$ vemos rápidamente que:

$$\mathbb{K}[x_1, \ldots, x_n]/I_k \cong \mathbb{K}[x_{k+1}, \ldots, x_n]$$

y como $\mathbb{K}$ es cuerpo entonces $\mathbb{K}[x_{k+1}, \ldots, x_n]$ es un dominio (2.2.6), concluyendo que I_k es primo.

Ahora, para ver que es una cadena de desigualdades estricta probemos por inducción el resultado. El caso base $0 \subset (x_1 - a_1)$ es trivial, puesto que la igualdad se da sii $0 = x_1 - a_1 \Rightarrow x_1 = a_1$ de modo que que $(x_1 - a_1)$ es el polinomio nulo lo cual no es posible porque x_1 es una variable y en un cuerpo tenemos al menos dos elementos, $0_{\mathbb{K}}$ y $1_{\mathbb{K}}$. Supongamos entonces que el resultado es cierto para $k-1$ y probemos que se verifica para k.

$$I_{k-1} \subset I_k.$$

La contención no estricta es trivial, falta ver que efectivamente no pueden ser iguales. Supongamos que $(x_k - a_k) \subseteq I_{k-1}$, tomando de nuevo el cociente y operando como en la demostración inicial tenemos que:

$$\mathbb{K}[x_1, \ldots, x_n]/I_{k-1} \cong \mathbb{K}[x_k, \ldots, x_n]$$

pero por hipótesis tenemos que $\overline{(x_k - a_k)} = \bar{0}$ de modo que $(x_k - a_k) = 0 \in \mathbb{K}[x_k, \ldots, x_n]$ y de nuevo, como x_k es una variable esto no es posible, de manera que concluimos el resultado. ■

Ejercicio 4.2.6. Demuestre que en un anillo de polinomios univariados $R[x]$, el radical de Jacobson es igual al radical de cero.

Demostración. Veamos ambas implicaciones:

- ($\Rightarrow$) Si $f(x) \in \sqrt{Jac(R[x])}$ entonces $1 - f(x)h(x) \in R[x]^*, \forall h(x) \in R[x]$, en particular para$h(x) = x$ y por ello ello $1 - xf(x) \in R[x]^*$. Por el ejercicio 3.1.10 tenemos que si $f = f_0 + \ldots, f_n x^n$ entonces $f_0, f_1, \ldots, f_n$ son nilpotentes y entonces $f(x)$ es nilpotente. [7]

- ($\Leftarrow$) Para el otro caso, como todo ideal maximal es primo, tenemos que, por la definición de radical de Jacobson y la caracterización 4.1.3:

$$Jac(R[x]) = \bigcap_{m \text{ max}} m \subseteq \bigcap_{P \text{ primo}} P = \sqrt{(0)}$$

■

Ejercicio 4.2.7. Un anillo R se llama de Boole si, para todo $x \in R$, se cumple $x^2 = x$. Sea R un anillo de Boole, demuestre que:

1. $x + x = 0$
2. Todo ideal primo P es maximal y R/P es un cuerpo con dos elementos
3. Todo ideal finitamente generado es principal

Demostración. Demostremos cada una de las partes:

En primer lugar, como R es un anillo entonces consideramos $y = x + x$, por ser de Boole entonces sabemos que $y^2 = y \Rightarrow (x + x)^2 = x + x$, desarrollando el cuadrado tenemos que $4x^2 = 2x^2 \Rightarrow 2x^2 = 2x \Rightarrow x + x = 0$.

Para las dos siguientes, vemos lo siguiente. Como P es primo entonces R/P es un dominio, por lo que tomamos $\bar{x} \in R/P$. Por ser de Boole tenemos que $\bar{x}^2 = \bar{x} \Rightarrow \bar{x}(\bar{x}-1) = \bar{0}$. Por ser dominio tenemos que o bien $\bar{x} = \bar{0}$ o bien $\bar{x} = \bar{1}$. De este modo vemos que en R/P solo tenemos dos elementos y por tanto $R/P \cong \mathbb{Z}/2\mathbb{Z}$ que es cuerpo concluyendo así ambas afirmaciones.

■

Ejercicio 4.2.8. Sea (R, m) un anillo local. Demuestre que no existe ningún elemento $x \notin \{0, 1\}$ tal que $x^2 = x$.

Demostración. Supongamos que $\exists x$ tal que se cumple la hipótesis del enunciado. Entonces tenemos que $x - x^2 = 0 \Rightarrow x(1-x) = 0$. Supongamos ahora que $x \neq 0$ y entonces lleguemos a que necesariamente $x = 1$. Supongamos que $x \neq 0$, entonces o bien $x \in (R\backslash\{0\})\backslash R^*$ o bien $x \in R^*$. Si $x \in R^*$ entonces por la ley de cancelación (proposición 2.2.1) $x(x-1) = 0 \Leftrightarrow x(x-1) = 0x \Leftrightarrow (x-1) = 0 \Leftrightarrow x = 1$. Por otro lado, si $x \in R\backslash R^*$ entonces tenemos que $(1-x) \notin m$, de ser así $(1-x)^{\in m} + x^{\in m} = 1 \in m$. Pero entonces $1 - x \in R^*$ de manera que podemos cancelar como antes y llegar a que $x = 0$ #. ■

[7] Puede observarse que este último paso es similar a una de las demostraciones del ejercicio 3.1.10 y que si no tomamos x no concluimos el resultado porque tenemos $1 - f_0$ unidad, lo que no nos da información sobre este término.

Ejercicio 4.2.9. Sea R un anillo y supongamos que existe un número natural n tal que para todo $x \in R$, se cumple $x^n = x$. Demuestre que entonces todo ideal primo es maximal.

Demostración. Sea P un ideal primo de R, en virtud del teorema 2.2.1, probemos que R/P es cuerpo. Nótese que ya sabemos, por ese mismo teorema que es dominio. Para ello, tomamos $\bar{0} \neq \bar{x} \in R/P$. Sabemos entonces que $\exists x \in R \backslash P$ tal que $\bar{x} = x + P$, por hipótesis sabemos que existe un n tal que $x^n = x$ por lo que $\bar{x}^n = \bar{x}^{n-1}\bar{x} = \bar{x} \Rightarrow \bar{x}^{n-1}\bar{x} - \bar{x} = (\bar{x}^{n-1} - 1)\bar{x} = \bar{0}$. Por hipótesis tenemos que $\bar{x} \neq 0$ y como es dominio entonces necesariamente $\bar{x}^{n-1} = \bar{1} \Rightarrow \bar{x} \cdot \bar{x}^{n-2} = \bar{1}$, concluyendo que efectivamente existe inverso y por tanto R/P es cuerpo. ■

Ejercicio 4.2.10. Sea A un anillo no trivial. Sea Σ el conjunto de ideales $I \subseteq A$ tales que todo elemento de I es divisor de cero. Demuestre que Σ tiene elementos maximales y que estos son ideales primos. Deduzca que el conjunto de divisores de cero de un anillo es unión de ideales primos.

Demostración. En primer lugar veamos que $\Sigma \neq \emptyset$. Como A es no trivial entonces 0 es divisor de cero de manera que $I = (0) \in \Sigma$. Veamos ahora que toda cadena tiene cota superior en Σ. Consideramos $\{I_\lambda \mid \lambda \in \Lambda\}$ una cadena de ideales. Sabemos por la demostración del teorema 4.1.1 que $\bigcup I_\lambda = J$ es un ideal. Veamos que $J \in \Sigma$. Tenemos que si $t \in J$ entonces $\exists \lambda \in \Lambda$ tal que $t \in I_\lambda$ y como $I_\lambda \in \Sigma$ entonces t es divisor del cero. Por el lema de Zorn, entonces Σ tiene elementos maximales, nos falta ver que este, $P \in \Sigma$ es maximal de Σ y entonces es primo.

Supongamos que existen $a, b \in A \backslash P$ tales que $ab \in P$. Entonces $P + (a) \notin \Sigma$ por lo que $\exists x \in P + (a)$ que no es divisor del cero con $x = q + a \cdot t$, $q \in P$, $t \in A$. Análogamente llegamos a $y = p + b \cdot r$. Entonces $x \cdot y = q \cdot p + q \cdot b \cdot r + a \cdot t \cdot p + a \cdot b \cdot t \cdot r \in P$ de modo que $x \cdot y \in P \in \Sigma$ y $x \cdot y$ es divisor de cero #.

Finalmente, sea $T = \{P \in \Sigma \mid P \text{ es maximal de } \Sigma\}$, veamos que $\bigcup_{P \in T} P = \{x \in A \mid x \text{ divisor de cero}\}$.

- $\subseteq$ Trivial.
- $\supseteq$ Sea x divisor de cero, $I = (x)$, si $a \in I$ entonces existe $b \in A$ tal que $a = x \cdot b$. Como x es divisor del cero entonces $\exists y \neq 0$ tal que $x \cdot y = 0$, luego $a \cdot y = 0$ y entonces a es divisor de cero, de modo que $I \in \Sigma$. Ahora, sea $\bar{\Sigma} = \{I \in \Sigma \mid x \in I\} \subseteq \Sigma$ entonces, $\bar{\Sigma} \neq \emptyset$. Aplicando el lema de Zorn (lema 4.1.1), $\bar{\Sigma}$ tiene un elemento P maximal. Además P está en Σ, si suponemos que no fuera maximal aquí y hubiera $S \in \Sigma$ con $P \subseteq S$ y por tanto $x \in P \subseteq S$, entonces $S \in \bar{\Sigma}$ de modo que necesariamente $P = S$ y entonces P es primo, por lo que $x \in \bigcup_{P \in T} P$.

■

Capítulo 5: Primarios

Ahora, avanzamos un paso más allá en los ideales que forman nuestro anillos, los ideales *primarios*. Éstos nos permiten establecer una descomposición análoga o similar a la que tenemos por factores primos en $\mathbb{Z}$ pero dentro de un ámbito mucho más general. Relacionaremos este nuevo tipo de elementos con los primos y maximales.

5.1. Concepto

Introduzcamos en primer lugar lo que entendemos por ideal *primario.*. Este generaliza la idea de primo con una condición menos estricta, de manera que nos encontramos ante elementos *casi primos*, pero que nos será suficiente para descomponer ideales.

Definición 5.1.1. Sea R u anillo, $Q \subseteq R$ un ideal propio, entones decimos que Q es un ideal *primario* si:

$$\forall x, y \in R, x \cdot y \in Q \Longrightarrow x \in Q \vee y \in \sqrt{Q}$$

Como mencionábamos, es una condición más laxa que los primos puesto que nos basta con que uno de los elementos esté en el ideal o en su radical. A partir de esta definición damos el primer resultado.

Proposición 5.1.1. *Sea R un anillo, $Q \subseteq R$ un ideal, son equivalentes:*

(I) Q es primario

(II) R/Q es un anillo no trivial en el que todo divisor de cero es nilpotente

Demostración. Probemos ambas implicaciones

$\Rightarrow$ Como $Q \neq (1)$, R/Q es no trivial. Sea $t \in R/Q$ divisor de cero, entonces se tiene que $\exists s \in R/Q \backslash \{\bar{0}\}$ tal que $t \cdot s = \bar{0}$. Sean $a, b \in R$ con $\bar{a} = t$ y $\bar{b} = s$. Como $s \neq \bar{0}$ entonces $b \notin Q$, pero tenemos que $\overline{ab} = t \cdot s = \bar{0}$ luego $ab \in Q$. Así pues como Q es primario y $b \notin Q$ necesariamente por la definición (5.1.1) tenemos que $\exists n \in \mathbb{N}_{\geq 1}$ tal que $a^n \in Q$ y por tanto $t^n = \bar{0}$ concluyendo que t es nilpotente.

$\Leftarrow$ Sean Q ideal y R/Q tal que se cumple (II), como R/Q es no trivial entonces $Q \neq R$. Por otro lado, sean $x, y \in R$ tales que $x \cdot y \in Q$ entonces tenemos que $x \in Q \vee y \in \sqrt{Q}$. Supongamos que $x \notin Q$, entonces sabemos que $\overline{xy} = \bar{0}$ y como $\bar{x} \neq \bar{0}$ entonces $\bar{y}$ es un divisor del cero y por la hipótesis es nilpotente, de manera que $\exists n \in \mathbb{N}_{\geq 1}, y^n = 0$, concluyendo que Q es primario.

■

Observación 5.1.1. En la segunda implicación de la demostración vemos que no hay pérdida de generalidad en suponer que $x \notin Q$ frente a $y \notin Q$ puesto que estamos con elementos arbitrarios de manera que si $x = 5$ y $y = 3$ y el resultado se da al revés basta con renombrar $x = 3, y = 5$ y ya estaríamos en el caso que hemos demostrado.

Proposición 5.1.2. *Sea Q un ideal primario, entonces $\sqrt{Q}$ es un ideal primo.*

Demostración. Sean $x, y \in R$ tales que $x \cdot y \in \sqrt{Q}$, entonces tenemos que $\exists n \in \mathbb{N}_{\geq 1}$ tal que $(x \cdot y)^n = x^n \cdot y^n \in Q$. Como Q es primario por hipótesis entonces tenemos que o bien $x^n \in Q$ o $y^n \in \sqrt{Q}$. Si se da el el primer caso tenemos que $x^n \in Q \Rightarrow x \in \sqrt{Q}$ y habríamos acabado. En el segundo de los casos, si $y^n \in \sqrt{Q}$ entonces $\exists m \in \mathbb{N}_{\geq 1}$ tal que $(y^n)^m = y^{n \cdot m} \in Q$ de modo que $y \in \sqrt{Q}$, concluyendo que x o $y \in \sqrt{Q}$ y por tanto $\sqrt{Q}$ es primo. ■

Definición 5.1.2. Si Q es un ideal primario y $P = \sqrt{Q}$ es el ideal primo que genera el radical, diremos que P es el primo asociado a Q y Q es *P-primario.*

Observación 5.1.2. Todo ideal primo es primario y además coincide con su radical (4.1.1) por lo que P primo entones es $P-$primario

Ejemplo 5.1.1. En $\mathbb{C}[x]$, x es irreducible y (x^7) es un ideal $(x)-$primario.

Ejemplo 5.1.2. En un DFU, si f es un elemento irreducible entonces (f^n) es un ideal $(f)-$primario. Dados $a \cdot b \in (f^n)$ tenemos que $f^n \mid a \cdot b$. Si $f \not| a$ entonces $f^n \mid b$, es decir, que $a \in \sqrt{(f^n)} = (f)$ o $b \in (f^n)$ como queríamos ver.

Proposición 5.1.3. *Sea Q un ideal, si $\sqrt{Q}$ es maximal, entonces Q es primario.*

Demostración. Supongamos que no es primario, es decir, existen $x, y \in R$ tales que $x \cdot y \in Q$ pero $x \notin Q$ e $y \notin \sqrt{Q}$. Ahora bien, entonces $(y) + \sqrt{Q} = (1)$ luego,

$$(1) \subseteq (y) + \sqrt{Q} \subseteq \sqrt{(y)} + \sqrt{Q} \subseteq \sqrt{\sqrt{(y)} + \sqrt{Q}} \subseteq (1).$$

Así por el ejercicio 3.2.9 tenemos que:

$$(1) = \sqrt{\sqrt{(y)} + \sqrt{Q}} \Leftrightarrow (1) = \sqrt{(y)} + \sqrt{Q} \Leftrightarrow (y) + Q = (1)$$

De este modo existen $a \in Q, b \in R$ tales que:

$$1 = a + y \cdot b \Rightarrow x = a \cdot x + x \cdot y \cdot b \in Q$$

Contradiciendo la hipótesis inicial de que $x \notin Q$ y concluyendo que Q es primario. ■

Ejemplo 5.1.3. En $\mathbb{K}[x, y, z]$ el ideal $I = (x^3, y^4, z^7, xyz)$ es primario. Para comprobarlo calculamos su radical, $\sqrt{I} = (x, y, x)$ y como es maximal, por el resultado que precede I es primario. Esta condición es directa puesto que $\mathbb{K}[x, y, z]/(z, y, z) \cong \mathbb{K}$ que es cuerpo. Por otro lado, que el radical coindice con ese ideal lo vemos rápidamente. Dado que $x, y, z \in \sqrt{I} \Rightarrow (x, y, z) \in \sqrt{I}$ y por otro lado como $I \subseteq (x, y, z) \Rightarrow \sqrt{I} \subseteq \sqrt{(x, y, z)} = (x, y, z)$ porque maximal implica primo (2.2.3) y por tanto coincide con su radical (4.1.1).

Nos planteamos ahora, como parte final de esta sección, cómo se comportan los ideales primarios frente a los homomorfismos.

Lema 5.1.1. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos y $Q \subseteq S$ un ideal P-primario, entonces $Q^c = \varphi^{-1}(Q) \subseteq R$ es un ideal primario y $P^c = \varphi^{-1}(P) \subseteq R$ es su primo asociado.*

Demostración. Veamos en primer lugar que $Q^c \neq R$, lo cual es directo porque $\varphi(1_R) = 1_S \notin Q$ por ser este primario. Ahora supongamos que tenemos $a, b \in R$ tales que $a \cdot b \in Q^c$, asumamos que $a \notin Q^c$ y veamos que $b \in \sqrt{Q^c}$. Por un lado sabemos que $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \in Q$ y $\varphi(a) \notin Q$, por tanto como Q es primario tenemos que $\varphi(b) \in \sqrt{Q}$ de manera que $\exists n \in \mathbb{N}_{\geq 1}$ tal que $\varphi(b)^n = \varphi(b^n) \in Q$. De modo que $b^n \in Q^c$ y por tanto $b \in \sqrt{Q^c}$.

Por otro lado, comprobemos ahora que efectivamente Q^c es P^c-primario. Como antes, al ser P primo entonces $\varphi(1_R) = 1_S \notin P \Rightarrow P^c \neq R$. Ahora bien, dados $a, b \in R$ con $a \cdot b \in P^c$ entonces $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \in P$. Como P es primo tenemos que $\varphi(a) \in P$ o $\varphi(a) \in P$, por lo que $a \in P^c$ o $b \in P^c$. ■

Demostración. (Alternativa P^c es primo) Consideremos las aplicaciones

$$R \xrightarrow{\varphi} S \xrightarrow{\pi} S/P.$$

Como P es primo tenemos que S/P es dominio (2.2.1). Además, por el primer teorema de isomorfía (2.1.1) sabemos que $R/P^c \cong \mathrm{Im}(\pi\varphi) \subseteq S/P$. Como S/P es un dominio entonces R/P^c que está contenido es dominio y por tanto P^c es primo. Ahora, comprobamos rápidamente que, por la proposición 3.1.3 si I es un ideal de S entonces $I^c = \varphi^{-1}(I)$ es un ideal de R y por ello:

$$x \in \sqrt{I^c} \Leftrightarrow \exists n \in \mathbb{N}_{\geq 1} \mid x^n \in I^c \Leftrightarrow \exists n \in \mathbb{N}_{\geq 1} \mid \varphi(x)^n \in I \Leftrightarrow \varphi(x) \in \sqrt{I} \Leftrightarrow x \in \varphi^{-1}(\sqrt{I})$$

y en particular $\sqrt{Q^c} = \varphi^{-1}(\sqrt{Q}) = \varphi^{-1}(P) = P^c$ ■

A la luz de este resultado, y principalmente por cómo hemos hecho la segunda demostración, nos podemos preguntar cómo son los primarios (resp. primos)en el cociente R/I. Así pues enunciamos el siguiente corolario.

Corolario 5.1.1. *Hay una biyección entre los ideales primarios (resp. primos) de R/I y los ideales primarios (resp. primos) de R que contienen a I*

Demostración. Sean $A = \{T \subseteq R/I \mid T \text{ ideal}\}$ y $B = \{T' \subseteq R \mid I \subseteq T' \text{ ideal}\}$, definimos la siguiente aplicación:

$$\begin{aligned} \tilde{\pi} : A &\longrightarrow B \\ T &\longrightarrow \pi^{-1}(T) = \{x \in R \mid [x] \in T\} \end{aligned}$$

Así, si T es un ideal de R/I y $S = \pi^{-1}(T)$ ideal de R, que contiene a I, entonces:

$$T = S/I \Rightarrow^{2.1.3} (R/I)\Big/(S/I) \cong R/S.$$

De modo que:

$$T \text{ primo} \Leftrightarrow R/I\Big/T \text{ dominio} \Leftrightarrow R/S \text{ dominio} \Leftrightarrow S \text{ primo}$$

$$T \text{ primario} \Leftrightarrow R/I\Big/T \text{ Todo divisor de 0 es nilpotente} \Leftrightarrow S \text{ primario}$$

■

Pongamos un ejemplo que ilustre este resultado.

Ejemplo 5.1.4. Tomemos $\mathbb{R}[x,y,z], I = (x^2 - yz)$ y $T = \big([x],[y]\big)$. Por la definición de primo va a ser muy difícil, por lo que estudiamos $\big(\mathbb{R}[x,y,z]/I\big)\Big/\big([x],[y]\big)$. En primer lugar, $\pi^{-1}(T) = (x,y) + I = (x,y,x^2 - yz)$ donde observamos que $x^2 - yz = x \cdot x - yz \in (x,y)$ de modo que $\pi^{-1}(T) = (x,y)$. Ahora, utilizando el homomorfismo de evaluación $\varphi_{(0,0,z)}$ observamos que $\ker(\varphi_{(0,0,z)})$ es (x,y), de modo que claramente tenemos que (x,y) es primo ya que $\mathbb{R}[x,y,z]\Big/(x,y) \cong \mathbb{R}[z]$ que es dominio y por el resultado anterior (corolario 5.1.1) $T = ([x],[y])$ es primo.

En relación a la última equivalencia del corolario anterior (5.1.1) podemos enunciar la siguiente proposición

Lema 5.1.2. *Sea R un anillo, $Q_1, \ldots, Q_n$ ideales $P-$primarios ($n \in \mathbb{N}_{\geq 1}$), entonces $\bigcap_{i=1}^n Q_i$ es $P-$primario*

Demostración. Veamos que se cumplen las condiciones de ser un ideal $P-$primario.

- $\bigcap_{i=1}^n Q_i \subseteq Q_1 \subsetneq R$, luego $\bigcap_{i=1}^n Q_i$ es propio.
- $\sqrt{\bigcap_{i=1}^n Q_i} = \bigcap_{i=1}^n \sqrt{Q_i} = \bigcap_{i=1}^n P = P$
- Supongamos que $a \cdot b \in \bigcap_{i=1}^n Q_i$ pero $a \notin \bigcap_{i=1}^n Q_i$, veamos que $b \in P$. Como $a \notin \bigcap_{i=1}^n Q_i$ entonces $\exists j \in \{1, \cdots, n\}$ tal que $a \notin Q_j$, pero $a \cdot b \in Q_j$ de modo que por ser Q_j $P-$primario entonces $b \in P$ como queríamos ver.

■

El siguiente ejemplo ilustra un poco el comportamiento de este resultado.

Ejemplo 5.1.5. Consideremos el anillo de polinomios $\mathbb{R}[x,y,z]$ y en él los ideales

$$I = (x^3y, y^4, xz^5, x^4, z^6).$$

$$J = (y^7, x^4z^4, x^5, z^5).$$

Podemos ver rápidamente que $(x,y,z) \subseteq \sqrt{(I)}$ y como (x,y,z) es maximal y $1 \notin \sqrt{I}$ entonces $(x,y,z) = \sqrt{I}$. De manera análoga vemos que $\sqrt{J} = (x,y,z)$. Así, ambos son ideales $(x,y,z)-$primarios y por tanto $I \cap J$ es un ideal $(x,y,z)-$primario.

Lema 5.1.3. *Sea $Q \subseteq R$ un ideal $P-$primario, sea $a \in R$,*

I Si $a \in Q$ entonces $(Q : a) = (1)$

II Si $a \notin Q$ entonces $(Q : a)$ es $P-$primario.

III Si $a \notin P$, $(Q : a) = Q$

Demostración. Vayamos por casos.

- (I) Si $a \in Q$ entonces $1_R \cdot a \in Q$ y entonces $1_R \in (Q : a)$.

- (II) En primer lugar, dado que $a \notin Q$ entonces $1 \cdot a \notin Q$ por lo que $1 \notin (Q : a)$ es propio. Ahora, dado $b \in (Q : a)$, $b \cdot a \in Q$. Dado que $a \notin Q$, entonces necesariamente $b \in P$ y de aquí tenemos que $(Q : a) \subseteq P$. Ahora, $Q \subseteq (Q : a) \subseteq P$ y tomando radicales tenemos $P \subseteq \sqrt{(Q : a)} \subseteq P$, concluyendo que $\sqrt{(Q : a)} = P$. Ahora veamos que $(Q : a)$ es primario. Sean $x, y \in R$ tales que $x \cdot y \in (Q : a)$, entonces si $x \notin (Q : a), x \cdot y \cdot a \in Q$, como $x \cdot a \notin Q$ entonces como es $P-$primario tenemos que $y \in P$.

- (III) Si $a \notin P$, se da que siempre se verifica que $Q \subseteq (Q : a)$ y por otro lado, dado $x \in (Q : a), x \cdot a \in Q$, como $a \notin P$ y Q es $P-$primario entonces $x \in Q$, como queríamos demostrar.

■

Observación 5.1.3. El caso (I) es general, si $J \subseteq K$ entonces, por el mismo razonamiento, $(K : J) = (1)$.

El siguiente caso ilustra el funcionamiento de este lema.

Ejemplo 5.1.6. Consideremos el anillo $\mathbb{Q}[x, y, z]$ y en él los ideales $I = (x^3y, y^4, xz^5, x^4, z^6)$ y $J = (z-3)$. Observamos que todos los generadores de I se anulan en el $(0, 0, 0)$ mientras que J no. Por ello podemos ver que $(z - 3) \notin I$ y $(z - 3) \notin \sqrt{I}$. Por lo que $(I : z - 3) = I$

5.2. Descomposición

Vayamos ahora uno de los pilares por los que introducíamos los ideales primarios. Éstos nos van a permitir descomponer ideales en un anillo.

Definición 5.2.1. Sea $I \subseteq R$ un ideal, diremos que es un ideal *descomponible* si existen $Q_1, \ldots, Q_n \subseteq R$ ideales primarios tales que $I = Q_1 \cap \ldots, \cap Q_n$.

Proposición 5.2.1. *En un DIP, todo ideal propio (f) admite una representación por primarios, dada por sus los factores ireducibles f.*

Demostración. Sea R un anillo y $I = (f) \subsetneq R$, distinguimos dos casos.

- Si $f = 0$ entonces (0) es primo y por tanto primario, siendo él mismo su descomposición.

- Si $f \in R \backslash R^* \wedge f \neq 0$ entonces, como estamos en un DIP existe la factorización en irreducibles $f = p_1^{k_1} \cdot \cdots \cdot p_n^{k_n}$ de modo que $I = (f) = (p_1^{k_1}) \cap \cdots \cap (p_n^{k_n})$ donde hemos aplicado el ejercicio 3.2.11 para el ideal generado por el producto. Así pues, observamos que $\sqrt{(p_i^{k_i)}} = (p_i)$ maximal, con esto ya bastaría por prop. 5.3.2 pero lo demostramos igual, de manera que, dados $x, y \in R$ tales que $x \cdot y \in (p_i^{k_i})$ entonces, si $x \notin (p_i)$ tenemos que $p_i^{k_i} \mid x \cdot y$ y como p_i es primo entonces

$$\gcd(p_i, x) = 1 \Rightarrow \gcd(p_i^{k_i}, x) = 1 \Rightarrow p_i^{k_i} \mid y \Rightarrow y \in (p_i^{k_i})$$

■

Ahora, en ningún momento hemos especificado que la descomposición en ideales primarios sea única y esto puede acarrear un problema, pongamos un ejemplo de ello.

Ejemplo 5.2.1. En $\mathbb{Z}$ mismamente:

$$(36) = (2^2) \cap (3^2) = (2^2) \cap (3^2) \cap (3)$$

Ambas descomposiciones primarias con cantidades distintas. Por ilustrar otro caso en un anillo distinto, sea $\mathbb{K}[x, y]$, los ideales:

$$(x^4) = (x^4) \cap (x, y^3)$$
$$(x^2, xy, y^2) = (x^2, y) \cap (x, y^2)$$

donde nos encontramos un problema como el en ejemplo anterior.

Por ello introducimos:

Definición 5.2.2. Sea I un ideal descomponible, llamamos a una descomposición primaria: *minimal* $I = \bigcap_{i=1}^{n}$ si

$$\forall j \in \{1, \cdots, n\}, I \neq \bigcap_{\substack{i=1 \\ j \neq i}}^{n} Q_i$$

Y adicionalmente tenemos que los ideales primos asociados, $\sqrt{Q_1}, \ldots, \sqrt{Q_n}$, son todos distintos entre sí.

Proposición 5.2.2. *Todo ideal I descomponible admite una descomposición primaria minimal.*

Demostración. Como I es descomponible entonces existen $Q_1, \ldots, Q_n$ tales que

$$I = Q_1 \cap \cdots \cap Q_n.$$

Si existen $Q_{i_1}, \ldots, Q_{i_r}$ con $\sqrt{Q_{i_1}} = \cdots = \sqrt{Q_{i_r}}$, tomemos $Q = \bigcap_{k=1}^{r} Q_{i_k}$ que también es primario (lema 5.1.2) y por tanto $I = Q \cap \bigcap_{i=1}^{n} Q_i$. Podemos suponer entonces que $I = Q_1 \cap \cdots \cap Q_n$ con todos los primos asociados diferentes. Ahora bien, si tuviéramos para algún para $i, j \in \{1, \cdots, n\}, i \neq j$ dos ideales $Q_i = Q_j$ entonces los eliminamos e iterando llegaríamos a una descomposición primaria minimal ■

Antes dijimos que no habíamos mencionado nada de la unicidad de la descomposición, por lo que vamos a introducir ahora el primer teorema relacionado con ella.

Teorema 5.2.1 (Primer teorema de unicidad)**.** *Sea $I = Q_1 \cap \cdots \cap Q_n$ un descomposición primaria minimal, entonces $\{\sqrt{Q_1}, \ldots, \sqrt{Q_n}\}$ no depende de la descomposición y en particular n tampoco.*

Observación 5.2.1. Recordemos que, si $a \in R$, Q un ideal $P-$primario entonces:

$$(Q : a) = \begin{cases} (1) \text{ si } a \in Q \\ P - \text{primario si } a \in P \wedge a \notin Q \\ Q \text{ si } a \notin P \end{cases}$$

Adicionalmente, tenemos que $(\cap Q_i : a) = \cap (Q_i : a)$

Demostración. Sean $P_i = \sqrt{Q_i}, \forall i \in \{1, \cdots, n\}$, sabemos que $\forall j \in \{1, \cdots, n\}, I \neq \bigcap_{\substack{r=1 \\ j \neq r}}^{n} Q_r$ por lo que para todo i existe $t_i \in (\bigcap_{k \neq i} Q_k) \backslash I$ y por ello $t_i \notin Q_i$ pues si lo estuviera $t_i \in \bigcap Q_i = I$ absurdo y por ello llegamos a:

- Si $k \neq i$ entonces $(Q_k : t_i) = (1)$
- Si $k = i$ entonces $(Q_k : t_i)$ es P_k-primario de modo que $\sqrt{\cap(Q_k : t_i)} = P_k$. porque observamos que $\sqrt{(I : t_i)} = \sqrt{(\cap q_k : t_i)} = \sqrt{\cap(Qk : t_i)}$ y como son todos o unos o el correspondiente al primario entonces llego a $(I : t_i) = \sqrt{q_i}$ (creo que estoy suponiendo que el t_i esta en la intersección de los primarios entonces al hacer su radical te sale P_k y por ello llego a que el radical de $(I : i_k)$ es P_k)

  Una vez hecho eso puedo tomar $\{p1, ..., p_n\}$ contenido en $\{p \mid p \text{ primo}\}$ y existe un $a \in R$ con $\sqrt{(I : a)} = P$

  Si adicionalmente suponemos que $\sqrt{(I : a)} = P$ es primo yo puedo ver que $(\bigcap Q_i : a) = \bigcap (Q_i : a)$ y como cada uno de estos es o uno o P_i entonces $\sqrt{(I : a)} = \bigcap P_{i_1} \cdots P_{i_e}$ con $i_1, \ldots, i_e \subseteq \{1, \cdots, n\}$ y $\exists j$ con $P_{i_j} = \sqrt{(I : a)}$ y por tanto concluyo que los primarios de cualquier descomposición minimal son los primos de esa forma y los primos y en particular el numero de ellos que hay no dependen de la descomposición minimal. A esos radicales y P_{i_j} los llamo primos asociados a I o primos que pertenecen a I.

■

Del teorema de unicidad podemos dar resultados que nos permitan conocer o caracterizar los divisores de cero de un anillo, que en general es una tarea complicada.

En primer lugar, podemos enunciar que, sea $I \subseteq Q$, son equivalentes que:

- Q es primario en R
- Q/I es primario en R/I

Demostración. Sabemos por el tercer teorema de isomorfía (teorema 2.1.3) que

$$R/Q \cong R/I \Big/ R/Q$$

ahora, por la última cadena de desigualdades del corolario 5.1.1

$$Q \text{ primario} \Leftrightarrow div_0(R/a) = Nil(R/Q) \Leftrightarrow div_0(R/I \Big/ R/Q) \Leftrightarrow Q/I \text{ primario en } R/I$$

Concluyendo el resultado. ■

Del mismo modo, nos podemos plantear cómo se comportan el resto de elementos con el cociente.

Proposición 5.2.3. *Si en R, $I = Q_1 \cap \ldots, \cap Q_r$ es una descomposición primaria, entonces en R/I:*

$$(0) = (Q_1/I) \cap \cdots \cap (Q_r/I)$$

Recordamos ahora ciertas definiciones de la Sección 4.1. Sea R un anillo, entonces

- Los nilpotentes son
$$\sqrt{(0)} = \bigcap_{P \text{ primo}} P$$
- El radical de Jacobson
$$Jac(R) = \bigcap_{m \text{ maximal}} m$$

Teníamos como propiedad que $x \in Jac(R) \Leftrightarrow \forall y \in R, 1 - xy \in R^*$. Ahora también habíamos caracterizado

- Las unidades como $R \setminus \bigcup_{m \text{ maximal}} m$

Queremos ahora hacer lo mismo para los divisores de cero.

Sea $I = Q_1 \cap \dots Q_n$ una descomposición primaria minimal tales que $\sqrt{Q_1} = P_1, \dots, \sqrt{Q_n} = P_n$, sabemos que no depende de la descomposición.

$$P \in \{\sqrt{Q_1}, \dots, \sqrt{Q_n}\} \Leftrightarrow \exists a \in R \mid P = \sqrt{I : a}$$

Si $(0) = (Q_1/I) \cap \dots \cap (Q_r/I)$ entonces reescribimos como

$$P \in \{\sqrt{Q_1}, \dots, \sqrt{Q_n}\} \Leftrightarrow \exists a \in R \mid P = \sqrt{0 : a} = P$$

y por tanto $b \in (0 : a) \Leftrightarrow b \cdot a = 0$. De aquí vemos que tenemos divisores del cero y por qué lo vamos a utilizar para caracterizarlos.

Teorema 5.2.2. *Sea R un anillo no trivial, supongamos que (0) admite una descomposición primaria minimal $(0) = Q_1 \cap \dots \cap Q_n$. Sean ahora $\{P_1 = \sqrt{Q_1}, \dots, P_n = \sqrt{Q_n}\}$ los primos asociados, entonces:*

$$\sqrt{(0)} = P_1 \cap \dots \cap P_n$$
$$div_0(R) = P_1 \cup \dots \cup P_n$$

Demostración. Demostremos ambas igualdades.

1. Si $x \in \sqrt{(0)}$ entonces $\exists n \in \mathbb{N}_{\geq 1}$ con $x^n = 0 \in Q_1 \cap \dots \cap Q_n$ de modo que $x^n \in Q_i \Rightarrow x \in P_i$. Para el otro contenido, si $x \in P_1 \cap \dots \cap P_n$, entonces para cada $i, \exists m_i \in \mathbb{N}_{\geq 1}$ tal que $x^{m_i} \in Q_i$. Considerando $M = \text{máx}\{m_i\}$ tenemos que $x^M \in Q_i \forall i \Rightarrow x^M \in Q_1 \cap \dots \cap Q_n = 0 \Rightarrow x \in \sqrt{(0)}$.

2. Sea $a \in div_0(R)$ entonces existe un $b \neq 0$ tal que $a \cdot b = 0$. Dado que $b \neq 0$ entonces $b \notin Q_1 \cap \dots \cap Q_n$ y entonces $\exists Q_i \mid b \notin Q_i$, pero como todos ellos son primarios entonces $a \cdot b \in Q_i, b \notin Q_i \Rightarrow a \in P_i \subseteq P_1 \cup \dots \cap P_n$. Por otro lado, sea $a \in P_i$, si $a = 0$ ya esta. En otro caso, si $a \neq 0$, como P_i es un primo asociado, $\exists b \in R$ tal que $P_i = \sqrt{(0 : b)}$ y por tanto $a \in \sqrt{(0 : b)}$ donde vemos que $\exists M \in \mathbb{N}_{\geq 1} \mid a^M \in (a : b) \Rightarrow a^M \cdot b = 0$. Volvemos a distinguir dos casos, si $a \cdot b = 0$ hemos acabado (pues $b \neq 0$ porque $(0 : 0) = (1)$ y $P_i \subsetneq (1)$). En la otra situación, $\exists j \mid a^{j+1} \cdot b = 0, a^j \cdot b \neq 0$ y con esto ya tenemos que $a \cdot (a^j \cdot b) = 0$ y $a \in div_0(R)$

■

Ejemplo 5.2.2. Consideramos en $\mathbb{Z}, n = p_1^{q_1} \cdots p_n^{q_n} \in \mathbb{Z} \Rightarrow (n) = (p_1^{q_1}) \cap \cdots \cap (p_n^{q_n})$, donde observamos que como $p_i^{q_i}$ es primario entonces su primo asociado es $\sqrt{(p_i^{q_i})} = (p_i)$ que es maximal. Consideramos ahora $\mathbb{Z}/n\mathbb{Z}$ y $(\bar{0}) = (p_1^{\bar{q}_1}) \cap \cdots \cap (p_n^{\bar{q}_n})$. Además $\sqrt{(p_i^{\bar{q}_i})} = (\bar{p}_i) = P_i/n\mathbb{Z}$. De este modo vemos que

$$\sqrt{(\bar{0})} = (\bar{p_1}) \cap \cdots \cap (\bar{p_n}) = (\bar{p_1}) \cdots (\bar{p_n})$$
$$div_0 = (\bar{p_1} \cup \cdots \cup \bar{p_n})$$

donde se da la igualdad entre producto e intersección por ser los ideales $(\bar{p_i})$ maximales y distintos, de manera que son comaximales y podemos aplicar el teorema 4.1.5

Ejemplo 5.2.3. Busquemos los divisores de cero en $\mathbb{Q}[x,y,z]\Big/(xyx, x^2y^2, y^5)$. Descomponemos, por el ejercicio 5.3.15

$$(xyz, x^2y^2, y^5) = (xz, x^2y^2, y^5) \cap (y, x^2y^2, y^5)$$

Buscamos ahora reducir la descomposición, llegando a $(y) \cap (x, y^5) \cap (z, x^2, y^5) \cap (z, y^2)$ Entonces, aplicando lo visto tenemos que

$$div_0(R) = (\bar{y}) \cup (\bar{x}, \bar{y}) \cup (\bar{x}, \bar{y}, \bar{z}) \cup ((\bar{z}, \bar{y})) = (\bar{x}, \bar{y}, \bar{z})$$

que es maximal (esto es casual).

Ejemplo 5.2.4. Consideramos ahora $\mathbb{Q}[x,y]\Big/(x^2-1, y^2-1)$. No tenemos ningún algoritmo para calcular una descomposición primaria del ideal (x^2-1, y^2-1). Si bien, recordemos que la descomposición primaria puede estudiarse como las soluciones de un sistema de ecuaciones, en este caso con solución $x = \pm 1, y = \pm 1$, por lo que podemos sospechar que

$$(x^2-1, y^2-1) = (x-1, y-1) \cup (x-1, y+1) \cup (x+1, y-1) \cap (x+1, y+1)$$

que son primarios por ser maximales. No tenemos herramientas para ver la igualdad, si bien para algunos podemos calcular la intersección por ser maximales. Haremos uso de *Sage* porque en general no tenemos esta *suerte*. Usando este *software* vemos que coincide y entonces

$$div_0 = P_1/I \cup \cdots \cup P_4/I$$
$$\sqrt{(0)} = \bar{P}_1/I \cap \cdots \cap \bar{P}_4/I = (0)$$

por lo que no hay elementos nilpotentes. Podríamos utilizar también el teorema chino del resto.

5.3. Ejercicios

En esta hoja de ejercicios, además de los relacionados con la teoría expuesta en este capítulo se añaden una serie de conceptos y ejercicios que los trabajan que no son todos parte del temario.

5.3.1. Ideales monomiales

Definición 5.3.1. Sea $\mathbb{K}$ un cuerpo y $\mathbb{K}[x_1, \ldots, x_n]$ el anillo en n indeterminadas sobre $\mathbb{K}$. Dado $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$ denotamos por $x^a = x_1^{a_1} \cdots x_n^{a_n}$ el monomio asociado a a. Con esta definición, 1 es el monomio asociado a $(0, \ldots, 0)$ y 0 no es un monomio. Además, todo polinomio $f(x_1, \ldots, x_n)$ se puede expresar de manera *única* como $f = \sum_{a \in A} c_a x^a$, donde $A \subset \mathbb{N}^n$ es finito y $\forall a \in A, c_a \neq 0$.

El conjunto de monomios forma una base de $\mathbb{K}[x_1, \ldots, x_n]$ como $\mathbb{K}$-espacio vectorial. Los monomios de la forma x^a con $c_a \neq 0$ los llamamos los monomios de f.

Sea $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ un ideal. Diremos que I es un *ideal monomial* si existen monomios $x^{a_1}, \ldots, x^{a_t}$ tales que $I = (x^{a_1}, \ldots, x^{a_t})$. Es decir, I está generado por una cantidad finita de monomios.

A continuación se presentan una serie de ejercicios sobre ideales monomiales:

Ejercicio 5.3.1. Sean $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathbb{N}^n$ y x^a, x^b los monomios correspondientes. Demuestre que $x^a \mid x^b$ si y solo si existe un monomio x^c tal que $x^a x^c = x^b$, si y solo si $\forall i \in \{1, \ldots, n\}, a_i \leq b_i$.

Demostración. Vemoas en primer lugar las dos primeras implicaciones:

- $\Leftarrow$ Trivial
- $\Rightarrow$ Sabemos que si $x^a \mid x^b$ entonces $\exists f, x^a \cdot f = x^b$. Por la descomposición en monomiales podemos escribir $f = \sum_{i \in A} c_i x^i$ de donde desarrollando el producto tenemos que $A = \{i\}$,$c_i = 1$ y $x^a \cdot x^i = x^b$, como queríamos ver.

Para la segunda, la implicación de izquierda a derecha es trivial, del mismo modo que igualamos coeficientes observamos que $a_i + l_i = b_i$ y como $l_i \geq 0$ entonces $a_i \leq b_i, \forall \in \{1, \cdots, n\}$. De derecha a izquierda, si $a_i \leq b_i, \forall i \in \{1, \cdots, n\}$ entonces consideramos $x^L = \prod_{i=1}^n x^{b_i - a_i}$ y observamos rápidamente que este monomio verifica que $x^a \cdot x^L = x^b$. ■

Ejercicio 5.3.2. Sea x^a un monomio y $f \in \mathbb{K}[x_1, \ldots, x_n]$. Demuestre que $x^a \mid f$ si y solo si x^a divide a todos los monomios de f.

Demostración. Demostremos ambas implicaciones, considerando $f = \sum_{i \in A} c_i x^i$

- $\Leftarrow$ Supongamos que $\forall i \in A, x^a \mid x^i$, entonces por el ejercicio 5.3.1, $\exists x^d$ tal que $x^a \cdot x^d = x^i$, por lo que $x^a \mid f$
- $\Rightarrow$ Supongamos ahora que $x^a \mid f$, entonces $x^a \cdot g = f$, con $g = \sum_{i \in B} r_i x^i$. Ahora, $\sum_{i \in B} r_i x^{i+a} = \sum_{j \in A} r_j x^j$, de modo que igualando tenemos $r_i x^i x^a = x_j$ y por tanto $x^a \mid x^j, \forall j \in \{1, \cdots, n\}$.

■

Ejercicio 5.3.3. Sea $I = (x^{a_1}, \ldots, x^{a_t})$ un ideal monomial. Entonces, para cada monomio x^b, se tiene que $x^b \in I$ si y solo si existe $i \in \{1, \ldots, t\}$ con $x^{a_i} \mid x^b$.

Demostración. Veamos ambas implicaciones.

- $\Leftarrow$ Trivial
- $\Rightarrow$ Supongamos que existen $g_1, \ldots, g_j$ tales que $x^{a_1}g_1 + \cdots + x^{a_t}g_t = x^b$. Observamos que los monomios de $(x^{a_1}g_1 + \cdots + x^{a_t}g_t) \subseteq \bigcup \text{monomios}(x^{a_i}g_i)$. Por tanto debe existir g_i con x^b monomio de $x^{a_i}g_i$, de manera que $x^{a_j}x^j = x^b$.

■

Ejercicio 5.3.4. Sea $I = (x^{a_1}, \ldots, x^{a_t})$ un ideal monomial y $f = \sum_{b \in A} c_b x^b$ (con $c_b \neq 0$ para todo $b \in A$). Demuestre que:

$$f \in I \Leftrightarrow \forall b \in A, x^b \in I \Leftrightarrow \forall b \in A, \exists i \in \{1, \ldots, t\}, x^{a_i} \mid x^b.$$

Demostración. Demostremos ambas implicaciones.

- $\Leftarrow$ Trivial, si todos los monomios de f están en I entonces f es una combinación lineal de ellos y está en I
- $\Rightarrow$ Si $f \in I$, $\exists g_1, \ldots, g_t$ tal que $f = g_1 x^{a_1} + \cdots + g_t x^{a_t}$. Para cada monomio x^b de f, este aparece en el desarrollo anterior y por el ejercicio 5.3.3 entonces x^b es mútiplo de algún x^{a_i}.

■

Ejercicio 5.3.5. Demuestre que dos ideales monomiales $I = (x^{a_1}, \ldots, x^{a_t})$, $J = (x^{b_1}, \ldots, x^{b_s})$ son iguales si y solo si para cada $i \in \{1, \ldots, t\}$ existe $j \in \{1, \ldots, s\}$ con $x^{a_i} \mid x^{b_j}$ y para cada $u \in \{1, \ldots, s\}$ existe $v \in \{1, \ldots, t\}$ con $x^{b_u} \mid x^{a_v}$.

Demostración. dem ■

Ejercicio 5.3.6. Demuestre que los ideales $I = (x^2, x^5y, y^3)$ y $J = (x^2, y^3, xy^5) \subset \mathbb{K}[x, y, z]$ son iguales.

Demostración. Hagamos las dos implicaciones

- $\Leftarrow$ Para que $I = (x_{i_1}, \ldots, x_{i_r})$ observamos que es monomial. Sin pérdida de generalidad consideramos el homomorfismo

$$\begin{aligned} ev : &\mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}[x_1, \ldots, x_n] \\ &f \longmapsto f(0, \ldots, 0, x_{r+1}, \ldots x_n). \end{aligned}$$

  Y $ker(ev) = I$ de modo que la imagen es un dominio e I es primo. Ahoram sea I monomial y priom, si I es monomial ¿podemos afirmar que $(x^{a_1}, \ldots, x^{a_r})$ son variables? Pensemos en (x, y, xy), deberíamos a quitar los que sobran y eso es mucho lío. Analizamos x^{a_i}.

  - Si $x^{a_i} = x_{j_i}$ entonces no lo tocamos

- Si $x^{a_i} = x_{j_i}^{a_{j_i}} \cdots x_{j_n}^{a_{j_n}}$

▪ $\Rightarrow$

■

Ejercicio 5.3.7. Demuestre que un ideal monomial I es primo si y solo si admite un conjunto generador formado por variables.

Demostración. dem ■

Ejercicio 5.3.8. Sea $I = (x^{a_1}, \ldots, x^{a_t})$ un ideal monomial. Supongamos que $i \neq j$ son tales que $x^{a_i} \mid x^{a_j}$. Demuestre que $I = (x^{a_1}, \ldots, x^{a_{j-1}}, x^{a_{j+1}}, \ldots, x^{a_t})$. Concluya que podemos calcular, a partir de $\{x^{a_1}, \ldots, x^{a_t}\}$, un conjunto de generadores minimal para la inclusión.

Demostración. dem ■

Ejercicio 5.3.9. Sea I un ideal monomial. Sea A el conjunto formado por todos los conjuntos finitos de monomios que generan I. Demuestre que A tiene un mínimo para la inclusión. Es decir, existe un conjunto finito de monomios G tal que $I = (G)$ y si H es otro conjunto finito de monomios que genera I entonces $G \subset H$.

Demostración. dem ■

Ejercicio 5.3.10. Sea R un anillo e $I = (f, g)$ un ideal. Demuestre que para todo $h \in R$, $(f, g) = (f, g + fh)$.

Demostración. dem ■

Ejercicio 5.3.11. Sea $I = (x-y, y-z, z-2x) \subset \mathbb{R}[x, y, z]$. Demuestre que I es monomial.

Demostración. dem ■

Ejercicio 5.3.12. Sean $\ell_1 = a_{11}x_1 + \cdots + a_{1n}x_n, \ldots, \ell_m = a_{m1}x_1 + \cdots + a_{mn}x_n$ formas lineales. Consideramos el ideal $I = (\ell_1, \ldots, \ell_m) \subset \mathbb{K}[x_1, \ldots, x_n]$ y el subespacio vectorial $V = \{v \in \mathbb{K}^n \mid \ell_1(v) = \cdots = \ell_m(v) = 0\} \subset \mathbb{K}^n$. Demuestre que son equivalentes:

1. I es un ideal monomial.
2. Existen variables $x_{i_1}, \ldots, x_{i_s}$ tales que $I = (x_{i_1}, \ldots, x_{i_s})$.
3. Existen $e_{j_1}, \ldots, e_{j_{n-s}}$ vectores de la base canónica tales que $V = \langle e_{j_1}, \ldots, e_{j_{n-s}} \rangle$.

Demostración. dem. la idea de uno implica dos esque las sumas pertenecen al ideal monomial y una funcion pertenece a un ideal monomial si y solo si alguno de sus monomios devide a f es decir para cada xi algun x^a lo divide pero como son variables las sumas entonces los x^a son univariados y se tiene.

la de dos implica tres esque sin perdida de generalidad suponemos que son los s primeros entonces la base canonica de et con t mayor que s verifica que pertenezca a V.

y la de tres implica uno es que si es de esta forma entonces estamos evaluando en todas ceros menos una, si no fuera monomial es decir apareciese una suma entonces al evaluar en la base canonica me quedaria un coeficiente = 0 y veo que esos coeficientes me los quito y por ello em quedan monomios de las variables que no apparecen en la base canonica ■

Ejercicio 5.3.13. Sea $I = (x^{a_1}, \ldots, x^{a_t})$ un ideal monomial y supongamos que el conjunto de generadores es minimal, es decir, si $i \neq j$, entonces $x^{a_i} \nmid x^{a_j}$. Demuestre que I es primario si y solo si para cada generador $x_1^{c_1} \cdots x_n^{c_n}$ y cada índice i tal que $c_i > 0$, existe un N tal que $x_i^N \in I$. Demuestre entonces que existe un conjunto de variables $x_{i_1}, \ldots, x_{i_s}$ tal que

$$I = (x_{i_1}^{p_1}, \ldots, x_{i_s}^{p_s}, x^{b_1}, \ldots, x^{b_k}),$$

donde los monomios x^{b_u} sólo involucran a las variables $x_{i_1}, \ldots, x_{i_s}$.

Demostración. dem ■

Ejercicio 5.3.14. Demuestre que el ideal $I = (x^6, x^5y, x^4y^2, x^3y^3, x^2y^4, xy^5, y^6)$ es primario.

Demostración. dem ■

Ejercicio 5.3.15. Sean $I = (x^{a_1}, \ldots, x^{a_t})$, $J = (x^{b_1}, \ldots, x^{b_s})$. Demuestre que

$$I \cap J = (\text{mcm}(x^{a_i}, x^{b_j}) \mid 1 \leq i \leq t,\ 1 \leq j \leq s).$$

En particular, la intersección de ideales monomiales es monomial. ¿Es cierto que si $U = (f_1, \ldots, f_t)$ y $V = (g_1, \ldots, g_s)$ son ideales arbitrarios finitamente generados entonces $U \cap V = (\text{lcm}(f_i, g_j))$?

Demostración. dem ■

Ejercicio 5.3.16. Demuestre que si $I = (x^b, x^{a_1}, \ldots, x^{a_t})$, $J = (x^c, x^{a_1}, \ldots, x^{a_t})$, entonces

$$I \cap J = (\text{mcm}(x^b, x^c), x^{a_1}, \ldots, x^{a_t}).$$

Demostración. dem ■

Ejercicio 5.3.17. Exprese el ideal $I = (x^2, y^3x, zx^3y)$ como intersección de ideales monomiales primarios.

Demostración. dem ■

Ejercicio 5.3.18. Demuestre que si I es un ideal monomial entonces podemos expresar I como intersección finita de ideales primarios monomiales.

Demostración. dem ■

Ejercicio 5.3.19. En $\mathbb{R}^2$ dibuje la parábola $y = x^2 - x$.

1. Calcule la recta tangente a la parábola en el punto $(0, 0)$.
2. Calcule las soluciones del sistema $y = x^2 - x$, $x - y = 0$.
3. Calcule las soluciones del sistema $y = x^2 - x$, $x + y = 0$.
4. Demuestre que el ideal $I = (y - x^2 + x, x + y)$ es un ideal primario que no es primo. ¿Cuál es su radical?
5. Demuestre que $J = (y - x^2 + x, x - y) = (x, y) \cap (x - 2, y - 2)$ es una descomposición de J en ideales primarios que son primos.

Demostración. dem ■

5.3.2. Espectro de un anillo

Ejercicio 5.3.20. Sea X un conjunto y $C \subset \mathcal{P}(X)$ una familia de subconjuntos de X. Demuestre que C es el conjunto de cerrados de una topología en X si y solo si:

1. $\emptyset \in C$, $X \in C$.
2. Si $\{C_i \mid i \in I\} \subset C$ entonces $\bigcap_{i\in I} C_i \in C$.
3. Si $A, B \in C$ entonces $A \cup B \in C$.

Demostración. dem ■

Definición 5.3.2. Sea R un anillo no trivial. Denotamos por $\mathrm{Spec}(R) = \{P \subset R \mid P \text{ ideal primo}\}$ y por $\mathrm{Specm}(R) = \{m \subset R \mid m \text{ ideal maximal}\}$ el espectro y espectro maximal de R. Sea $I \subset R$ un ideal, definimos $V(I) = \{P \in \mathrm{Spec}(R) \mid I \subset P\}$.

Ejercicio 5.3.21. Sea R un anillo, $\{I_i \mid i \in \Lambda\}$ un conjunto de ideales de R, I, J ideales de R. Demuestre que:

1. $V(I) = V(\sqrt{I})$.
2. $V(0_R) = \mathrm{Spec}(R)$.
3. $V(1_R) = \emptyset$.
4. $V\left(\sum_{i\in\Lambda} I_i\right) = \bigcap_{i\in\Lambda} V(I_i)$.
5. $V(I \cap J) = V(IJ) = V(I) \cup V(J)$.

Concluya que $\{V(I) : I \text{ ideal de } R\}$ es el conjunto de cerrados de una topología en $\mathrm{Spec}(R)$: la topología de Zariski.

Demostración. Probemos cada una de las partes

1.
2.
3.
4. $P \in V(\sum_{i\in\Lambda} I_i) \Leftrightarrow \sum_{i\in\Lambda} I_i \subseteq P \Leftrightarrow \forall i \in \Lambda, I_i \subseteq P \Leftrightarrow \forall i \in \Lambda, P \in V(I_i) \Leftrightarrow P \in V((\bigcap_{i\in\Lambda} I_i)$
5. $P \in V(I \cap J) \Leftrightarrow I \cap J \subseteq P \Rightarrow I \subseteq P \wedge J \subseteq P \Leftrightarrow P \in V(I) \cup V(J)$

■

Ejercicio 5.3.22. Sea D un dominio de ideales principales (DIP) que no sea un cuerpo. Sabemos que los únicos ideales primos son (0) y (x) con x irreducible.

1. Demuestre que $\{(0)\}$ es un punto denso para la topología de Zariski en $\mathrm{Spec}(D)$.
2. Demuestre que si x es irreducible, entonces $\{(x)\}$ es un punto cerrado de $\mathrm{Spec}(D)$.
3. Demuestre que $\mathrm{Spec}(D)$ es un espacio T_0 pero no es T_1.

4. Demuestre que la topología inducida en $\mathrm{Specm}(D)$ es la topología cofinita.

Demostración. dem ■

Ejercicio 5.3.23. Sea R un anillo finito. Demuestre que $\mathrm{Spec}(R)$ es un conjunto finito y la topología de Zariski es la topología discreta.

Demostración. dem ■

Definición 5.3.3. Sea $\varphi : R \to S$ un homomorfismo de anillos. Si $P \in \mathrm{Spec}(S)$ es un ideal primo de S, entonces $P^c = \varphi^{-1}(P)$ es un ideal primo de R. Esto induce una aplicación en los espectros:

$$\varphi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$$

Dado un ideal $I \subset R$, denotamos por $I^e = \{\varphi(x) : x \in I\}S$ el ideal de S generado por $\varphi(I)$.

Ejercicio 5.3.24. Sea $\varphi : R \to S$ un homomorfismo de anillos. Demuestre que si φ es sobreyectivo entonces $\varphi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ es inyectiva.

Demostración. dem ■

Ejercicio 5.3.25. Sea $\varphi : R \to S$ un homomorfismo de anillos. Demuestre que si I es un ideal de R entonces

$$(\varphi^*)^{-1}(V(I)) = V(I^e) \subset \mathrm{Spec}(S).$$

Concluya que $\varphi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ es una aplicación continua.

Demostración. dem ■

Ejercicio 5.3.26. Sea R un anillo no trivial y $I \subset R$ un ideal propio. Sea $\pi : R \to R/I$. Demuestre que $\pi^* : \mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ es una aplicación inyectiva cuya imagen es $V(I)$, y que $\pi^* : \mathrm{Spec}(R/I) \to V(I)$ es un homeomorfismo (es decir, una inmersión topológica).

Demostración. dem ■

Ejercicio 5.3.27. Sea R un anillo no trivial y $f \in R$. Denotamos por $D_f = \{P \in \mathrm{Spec}(R) \mid f \notin P\}$. Demuestre que:

1. Si f es nilpotente, entonces $D_f = \emptyset$.
2. Si f es unidad, entonces $D_f = \mathrm{Spec}(R)$.
3. $\mathrm{Spec}(R) \setminus D_f = V(fR)$, por lo tanto D_f es abierto.
4. $D_{fg} = D_f \cap D_g$.
5. $\{D_f \mid f \in R\}$ es una base de la topología de Zariski en $\mathrm{Spec}(R)$.
6. Demuestre que $\mathrm{Spec}(R)$ es compacto.

Demostración. dem ■

Definición 5.3.4. Sea $\mathbb{K}$ un cuerpo. Para cada punto $a = (a_1, \ldots, a_n) \in \mathbb{K}^n$ le asociamos el ideal maximal $m_a = (x_1 - a_1, \ldots, x_n - a_n) \in \operatorname{Specm}(\mathbb{K}[x_1, \ldots, x_n])$.

Ejercicio 5.3.28. Demuestre que la aplicación

$$\varphi : \mathbb{K} \to \operatorname{Specm}(\mathbb{K}[x])$$

dada por $a \mapsto (x - a)$ es biyectiva si y solo si $\mathbb{K}$ es algebraicamente cerrado.

Demuestre que si $\mathbb{K}$ es algebraicamente cerrado y $f(x) \in \mathbb{K}[x]$ es un polinomio de grado estrictamente positivo, entonces φ induce una biyección entre el conjunto de raíces de f y $V(f)$.

Demostración. dem ■

Ejercicio 5.3.29. Sea $\mathbb{K}$ un cuerpo e $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideal finitamente generado $I = (f_1, \ldots, f_r)$. Sean:

$$A = \{p \in \mathbb{K}^n \mid f_1(p) = \cdots = f_r(p) = 0\}, \quad B = \{p \in \mathbb{K}^n \mid \forall g \in I,\ g(p) = 0\}$$

Demuestre que $A = B$.

Demuestre que $p = (p_1, \ldots, p_n) \in A$ si y solo si $m_p = (x_1 - p_1, \ldots, x_n - p_n) \in V(I)$. Así, hay una biyección entre:

- Las soluciones del sistema $f_1 = \cdots = f_r = 0$.
- Los elementos de $V(I) \cap \operatorname{Specm}(\mathbb{K}[x_1, \ldots, x_n])$ de la forma m_p.
- Los elementos de $\operatorname{Specm}(\mathbb{K}[x_1, \ldots, x_n]/I)$ de la forma $m_p/I = ([x_1 - p_1], \ldots, [x_n - p_n])$.

Demostración. dem ■

5.3.3. Ejercicios

Ejercicio 5.3.30. Demuestre que son equivalentes:

1. R es un dominio.
2. $R[x]$ es un dominio.
3. $xR[x]$ es un ideal primo de $R[x]$.

Demostración. dem ■

Ejercicio 5.3.31. Sea

$$I[x] = \left\{ \sum_{i=0}^{n} c_i x^i \in R[x] \;\middle|\; c_i \in I,\ 0 \leq i \leq n \right\}.$$

Demuestre que $I[x]$ es un ideal de $R[x]$.

Demuestre que $I[x] = IR[x]$, el menor ideal de $R[x]$ que contiene a $I \subset R \subset R[x]$.

Demostración. dem ■

Ejercicio 5.3.32. Demuestre que

$$(R/I)[x] \cong R[x]/I[x].$$

Demostración. dem ■

Ejercicio 5.3.33. Demuestre que I es un ideal primo de R si y solo si $I[x]$ es un ideal primo de $R[x]$. Dé un contraejemplo de que esta equivalencia es falsa para ideales maximales.

Demostración. dem ■

Ejercicio 5.3.34. Demuestre que I es un ideal primario de R si y solo si $I[x]$ es un ideal primario de $R[x]$.

Demostración. dem ■

5.3.4. Lema de Gauss, DFU

Esta sección demuestra que si D es un DFU entonces $D[x]$ es un DFU. Las demostraciones son estándar, pero trataremos de reescribirlas con el lenguaje propio de la asignatura

Definición 5.3.5. Sea R un anillo y $f(x) \in R[x]$ un polinomio. Si $f = \sum_{i=0}^{n} a_i x^i$ llamamos contenido de f al ideal $\text{cont}_I(f) = (a_0, \ldots, a_n)$. Un polinomio se dice primitivo si su contenido es (1).

En el contexto de dominios de factorización única y, sobre todo, en $\mathbb{Z}$, el contenido de un polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$ se suele definir como $\gcd(a_0, \ldots, a_n)$. Para no complicar la notación, si $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$ y D es un DFU, escribiremos $\text{cont}_I(f) = (a_0, \ldots, a_n) \subset D$ y $\text{cont}(f) = \gcd(a_0, \ldots, a_n) \in D$.

Ejercicio 5.3.35. (Lema de Gauss, parcialmente resuelto). Sean $f, g \in R[x]$. Sean I el contenido de f, J el contenido de g y K el contenido de fg. Demuestre que:

$$K \subset IJ \subset I \cap J \subset \sqrt{K}$$

Pistas y esbozos:

1. Todo coeficiente de fg es suma de productos de coeficientes de f y g.
2. El segundo contenido es el Ejercicio 6.2 de la Hoja 2.
3. Si P es un primo que contiene a K, entonces en $R[x]/K^e$ se tiene $fg = 0$. Como este anillo es un dominio (ver Ejercicio 32), entonces $f = 0$ o $g = 0$. Concluya que los primos que contienen a K también contienen a $I \cap J$, por lo que $\sqrt{K} = \sqrt{I \cap J}$.

Demostración. dem ■

Ejercicio 5.3.36. Interprete el ejercicio anterior cuando $K = (1)$, por lo que no existen primos P verificando $K \subset P$.

Demostración. dem ■

Ejercicio 5.3.37. Demuestre que en $R[x]$ los polinomios f y g son primitivos si y solo si fg es primitivo.

Demostración. dem ■

Ejercicio 5.3.38. Sea D un DFU y $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$ no constante. Sea $c = \gcd(a_1, \ldots, a_n)$. Demuestre que $\text{cont}_I(f) \subset (c)$. Por tanto, si f tiene contenido 1 en nuestra definición, también lo tiene en la definición alternativa. Dé un ejemplo que muestre que el recíproco es falso: que $\gcd(a_1, \ldots, a_n) = 1$ no implica $\text{cont}_I(f) = (1)$.

Demostración. dem ■

Teorema 5.3.1. *Sea D un DFU, $\mathbb{K}$ su cuerpo de fracciones. Consideremos un polinomio $f(x) = \sum_{i=0}^{n} f_i x^i \in D[x]$, con $\deg(f) > 0$ y $\gcd(f_0, \ldots, f_n) = 1$. Entonces, $f(x)$ es reducible como polinomio en $D[x]$ si y sólo si es reducible como polinomio en $\mathbb{K}[x]$.*

Esbozo de la demostración. ($\Rightarrow$) Si $f(x)$ es reducible en $D[x]$, entonces existen $g(x), h(x) \in D[x]$, no unidades, tales que $f(x) = g(x)h(x)$. Como $f(x)$ no es constante, se sigue que $\deg(g), \deg(h) > 0$. Por lo tanto, $f(x)$ también es reducible en $\mathbb{K}[x]$.

($\Leftarrow$) Supongamos que existen $g(x), h(x) \in \mathbb{K}[x]$, polinomios no constantes, con $f(x) = g(x)h(x)$. Escribamos

$$g(x) = \sum_{i=0}^{r} \frac{a_i}{b_i} x^i, \quad \text{con } \gcd(a_i, b_i) = 1,\ a_i \in D,\ b_i \in D \setminus \{0\}.$$

Sea $c = \text{lcm}(b_1, \ldots, b_r) \in D$. Entonces $cg(x) \in D[x]$ y los coeficientes de $cg(x)$ tienen $\gcd = 1$ (demuestralo). Análogamente, existe $d \in D$ tal que $dh(x) \in D[x]$ con coeficientes primitivos (i.e., $\gcd = 1$).

Entonces

$$cdf(x) = (cg(x))(dh(x)) \in D[x].$$

Es fácil ver que el gcd de los coeficientes de $cdf(x)$ es cd (demuéstralo). Supongamos que c no es unidad. Como D es DFU, existe un irreducible $p \in D$ tal que $p \mid c$. Entonces, en el anillo D/p, $(cg)(dh) \equiv 0$, por lo que uno de los factores debe ser cero módulo p, implicando que p divide todos los coeficientes de cg o de dh, contradiciendo su construcción. Lo mismo aplica a d. Por tanto, c y d son unidades en D, y se sigue que

$$f(x) = (cd)^{-1}(cg(x))(dh(x)) \in D[x],$$

lo que implica que $f(x)$ es reducible en $D[x]$. ■

Ejercicio 5.3.39. Demuestre que si D es un DFU, entonces $D[x]$ también es un DFU. Siga el siguiente razonamiento:

1. Si $c \in D$ es irreducible, entonces c es irreducible en $D[x]$. (Use el comportamiento del grado del producto de polinomios).

2. Todo $c \in D$ se factoriza en $D[x]$ como producto de irreducibles.

3. Si $f(x) \in D[x]$ no es constante, entonces $f(x) = c \cdot g(x)$ con $c \in D$ y el gcd de los coeficientes de g igual a 1.

4. Si el gcd de los coeficientes de $f(x)$ es 1, y $f(x) = g_1 \cdots g_t$ es la factorización en irreducibles de f en $\mathbb{K}[x]$, entonces esta también es una factorización en irreducibles de $f(x)$.

5. Todo $f \in D[x]$ se puede expresar como un producto de irreducibles de la forma $cg_1(x) \cdots g_t(x)$ donde $c \in D$ es el gcd de los coeficientes y cada g_i es primitivo (coeficientes coprimos).

6. Si
$$f = c_1 \cdots c_k g_1(x) \cdots g_s(x) = d_1 \cdots d_u h_1(x) \cdots h_t(x)$$
son dos descomposiciones de f en irreducibles, entonces:

   a) $c_1 \cdots c_k$ y $d_1 \cdots d_u$ son asociados en D, por lo que $k = u$ y la factorización es única salvo unidades y permutación.

   b) $f = cg_1 \cdots g_t = dh_1 \cdots h_t$ son factorizaciones en $\mathbb{K}[x]$, donde c, d son unidades, así que $s = t$ y los factores son únicos salvo asociados y permutación.

   c) Si g_i y h_j son asociados en $\mathbb{K}[x]$, entonces también lo son en $D[x]$, usando que sus coeficientes tienen gcd = 1.

Demostración. dem ■

Ejercicio 5.3.40. Demuestre por inducción que si D es un DFU, entonces el anillo de polinomios $D[x_1, \ldots, x_n]$ también lo es.

Demostración. dem ■

Capítulo 6: Anillos noetherianos

6.1. Anillos noetherianos

Seguimos profundizando en la estructura de los anillos conmutativos, esta vez centrándonos en una clase especialmente bien comportada: los *anillos noetherianos*. Estos anillos se caracterizan por una propiedad de finitud en sus ideales que, lejos de ser una restricción, nos permite controlar y entender mejor su comportamiento. Esta condición nos proporcionará un marco adecuado para resultados fundamentales como el *Teorema de la base de Hilbert*.

6.2. Introducción

Comencemos dando la definición.

Definición 6.2.1. Un anillo R se dice *noetheriano* si todo ideal de R admite un conjunto finito de generadores, es decir.

$$\forall I \subseteq R, \exists a_1, \ldots, a_n \in R \text{ tales que } I = (a_1, \ldots, a_n)$$

Observación 6.2.1. Si R es un anillo finito entonces todo ideal es finito y por tanto R es noetheriano.

$$\text{Finito} \Rightarrow \text{Noetheriano}$$

Observación 6.2.2. Si $\mathbb{K}$ es un cuerpo los ideales son (0) o (1) y por tanto es noetheriano.

$$\text{Cuerpo} \Rightarrow \text{Noetheriano}$$

Observación 6.2.3. Si R es un DIP entonces todo ideal está generado por un elemento lo que implica directamente que R es noetheriano.

$$\text{DIP} \Rightarrow \text{Noetheriano}$$

Estudiemos ahora como se comporta un anillo noetheriano respecto del cociente por uno de sus ideales.

Proposición 6.2.1. *Sea R un anillo noetheriano e $I \subseteq R$ un ideal, entones R/I es noetheriano.*

Demostración. Sea $J \subseteq R/I$ un ideal, por la biyectividad entre los ideales de R/I y los que contienen a I tenemos que

$$K = \{x \in R \mid \bar{x} \in J\}$$

es un ideal de R tal que $I \subseteq K$. Como R es noetheriano entonces sabemos que existen $a_1, \dots, a_n \in R$ tales que $K = (a_1, \dots, a_n)$.

Probemos ahora que efectivamente $J = (\bar{a_1}, \dots, \bar{a_n})$. Por la definición del ideal K tenemos que $(\bar{a_1}, \dots, \bar{a_n}) \in J$. Ahora, si $b \in J$ entonces $\exists c \in K$ tal que $\bar{c} = b$. Dado que $K = (a_1, \dots, a_n)$ entonces $c = a_1c_1 + \cdots + a_nc_n$ con $c_i \in R$. Tomando clases tenemos que $\bar{b} = \bar{a_1}\bar{c_1} + \cdots + \bar{a_n}\bar{c_n}$ llegando al resultado. ■

Una vez visto esto, vamos a dar un teorema de equivalencias que nos permite establecer definiciones alternativas de la noción de anillo noetheriano.

Teorema 6.2.1 (Caracterización o definiciones alternativas)**.** *Sea R un anillo, son equivalentes:*

(I) $\forall I \subseteq R$ *ideal,* $\exists a_1, \dots, a_n \in R$ *con* $I = (a_1, \dots, a_n)$*, es decir, R es noetheriano.*

(II) Si $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ *es una cadena ascendente de ideales de R entonces es estacionaria, ie,* $\exists k \in \mathbb{N}$ *tal que* $I_k = I_{k+1} = \cdots$*.*

(III) Si $\Sigma \neq \emptyset$ *es un conjunto cualquiera de ideales de R, Σ contiene elementos maximales para la relación de inclusión.*

Observación 6.2.4. El enunciado (III) recuerda al Lema de Zorn (4.1.1) pero sin la hipótesis de que necesitamos cotas.

Demostración. Probemos las distintas implicaciones.

- (I) $\Rightarrow$ (II) Sea $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ una cadena de ideales ascendente entonces $J = \bigcup_{i=1}^{\infty} I_i$ es un ideal (ver la demostración del *Lema de Zorn* 4.1.1). Por (I) tenemos que $\exists a_1, \dots, a_n$ que generan J y por tanto, como $\forall a_i, i \in \{1, \cdots, n\}, a_i \in J$ entonces $\exists t_i$ tal que $a_i \in I_{t_i}$. Tomando $t = \max t_i$ tenemos que

$$a_1, \dots, a_n \in I_t \Rightarrow J = I_t \Rightarrow I_t = I_{t+s}, s \in \mathbb{N}.$$

- $\neg$(III) $\Rightarrow$ $\neg$(II) Supongamos que $\exists \Sigma \neq \emptyset$ un conjunto de ideales sin maximal para la inclusión. Entonces, como Σ es no vacío entonces $\exists I_1 \in \Sigma$. Consideramos $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n$. Como I_n no es maximal entonces existe $I_{n+1} \in \Sigma$ tal que $I_n \subsetneq I_{n+1}$, concluyendo $\neg$(II).

- $\neg$(I) $\Rightarrow$ $\neg$(III). Supongamos que existe un ideal que no está finitamente generado, podemos entonces considerar

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \cdots (a_1, \dots, a_n) \subsetneq I$$

  con $a_i \in I$. Tomando $\Sigma = \{(a_1), \dots, (a_1, \dots, a_n), \dots\}$ observamos que no tiene maximal, porque de tenerlo entonces generaría I, contradiciendo la hipótesis.

■

Ejemplo 6.2.1. Consideremos el anillo $R = \mathbb{R}[x_1, \dots, x_n, \dots]$. Observamos rápidamente que $\mathbb{R}[x_1] \subseteq R[x_1, x_2] \subseteq \cdots \subseteq \mathbb{R}[x_1, \dots, x_n]$. Ahora vemos también que

$$R = \bigcup_{i=1}^{\infty} \mathbb{R}[x_1, \dots, x_i].$$

donde cada polinomio tiene una cantidad finita de variables. Veamos que $I = (x_1, \dots, x_n, \dots)$ no es finitamente generado, lo cual lo podemos ver si

$$(x_1) \subsetneq (x_1, x_2) \cdots \subsetneq (x_1, \dots, x_i) \subsetneq \cdots .$$

Supongamos para ello que sí que es finitamente generado, entonces existen

$$f_1(x_1, \dots, x_{i_1}), \dots, f_n(x_1, \dots, x_{i_n}).$$

tales que

$$I = (f_1(x_1, \dots, x_{i_1}), \dots, f_n(x_1, \dots, x_{i_n})).$$

Asumimos sin pérdida de generalidad que $i_1 \leq \cdots \leq i_n$ y comprobemos que $x_{i_n+1} \in I \backslash (f_1, \dots, f_n)$. De no ser así existirían polinomios $g_1(x_1, \dots, j_1), \dots, g_n(x_1, \dots, j_n) \in R$ de modo que podemos escribir $x_{i_n+1} = f_1 g_1 + \cdots + f_n g_n$, donde observamos que esta igualdad si cumple en el anillo $\mathbb{R}[x_1, \dots, \text{máx}\{i_{n+1}, j_1, \dots, j_n\}]$, llamando al máximo N, consideramos el homomorfismo de evaluación, donde observamos lo siguiente:

$$\begin{aligned} ev :& \varphi([x_1, \dots, x_N]) \to \mathbb{R} \\ & h(x_1, \dots x_N) \mapsto h(0, \dots, 1^{(i_n+1)}, 0 \dots, 0) \\ & f_i \longmapsto 0 \\ & x_{i_n+1} \longmapsto 1 \end{aligned}$$

de modo que $1 = 0\#$.

Teorema 6.2.2. *Sea R un anillo no trivial, si todo ideal primo de R es finitamente generado entonces R es un anillo noetheriano.*

Demostración. Por contrarrecíproco, supongamos que R no es noetheriano, entonces sea

$$Z = \{I \subseteq R \mid I \text{ no finitamente generado } \}$$

sabemos que $Z \neq \emptyset$, si lo fuera directamente sería Noetheriano. Sea ahora $\{I_j \mid j \in \Lambda\}$ una cadena de Σ (para $\subseteq$), entonces $\bigcup_{j\in\Lambda} I_j = K$ es un ideal. Si fuera finitamente generado entonces $K = (a_1, \dots, a_n)$ de modo que para cada a_i existe I_j tal que $a_i \in I_j$ de modo que tomando el máximo de los $\{I_{j_1}, \dots, I_{j_n}\}$, tomando por ejemplo sin pérdida de generalidad que este es I_{j_n} entonces $I_{j_n} = K$ contradiciendo que $I_{j_n} \in \Sigma$. Así pues K no puede estar finitamente generado y por el lema de Zorn (4.1.1) Σ tiene elementos maximales, lo llamamos P.

Como R no es noetheriano entonces existe P ideal tal que

(I) P no es finitamente generado

(II) $P \subsetneq Q$, con Q ideal finitamente generado

Probemos por tanto que es primo. Suponemos que no lo es, es decir, $\exists x, y \in R \backslash P$ tales que $x \cdot y \in P$. Ahora, como $x \notin P$, $P \subsetneq P + (x)$ este debe ser finitamente generado, es decir, existen $f_1, \dots, f_r \in P, g_1, \dots, g_r \in R$ tales que

$$P + (x) = (f_1 + xg_1, \dots, f_r + xg_r)$$

Como $x \in P + (x)$ entonces

$$(f_1 + xg_1 \ldots, f_r + xg_r) = (f_1 + xg_1, \ldots, f_r + xg_r, x) = (f_1, \ldots, f_r, x)$$

Tomamos por tanto $(P : (x))$ y como sabemos que $y \in (P : x)$ y ya que $x \cdot y \in P$ tendremos $y \notin P$, $P \subsetneq (P : x)$ y por tanto

$$P \subseteq (P + (y)) \subseteq (P : x)$$

. Por la maximalidad de P en Σ entonces $(P : x) = (h_1, \ldots, h_s)$ con $h_i \in (P : x)$ de modo que $h_i \cdot x \in P$ luego $(f_1, \ldots, f_r, h_1x, \ldots, h_sx) \subseteq P$. Falta ver la otra contención para concluir. Sea $z \in P \subseteq P + (x)$ entonces podemos escribir

$$z = f_1q_1 + \cdots + f_rq_r + xq \Rightarrow xq = z - f_1q_1 \cdots \in P$$

de modo que $q \in (P : x)$ y por tanto $q = h_1u_1 + \cdots h_su_s$ con $u_i \in R$. Ahora,

$$xq = (h_1x)u_1 + \cdots + (h_sx)u_s \in (f_1, \ldots, f_r, h_1x, \ldots, h_rx)$$

y así $P = (f_1, \ldots, f_r, h_1x, \ldots, h_rx)\#$ pues P no estaba finitamente generado y concluimos la demostración. ■

Lema 6.2.1. *Sea R un anillo, $I \subseteq R[x]$ un ideal. Sea $n \in \mathbb{N}$, entonces el conjunto*

$$J_n = \{a \in R \mid \exists a_0, \ldots, a_{n-1}, a_0 + \cdots + a_{n-1}x^{n-1} + ax^n \in I\}.$$

es un ideal de R.

Demostración. Para la demostración veamos que se cumple la definición de ideal:

- En primer lugar, $0 = 0 + 0x + \cdots + 0x^n \in I$, por lo que $0 \in J_n \neq \emptyset$.
- Si $u, v \in J_n$ entonces existen $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in R$ tales que:

  $$a_0 + \cdots + a_{n-1}x^{n-1} + ux^n \in I$$

  $$b_0 + \cdots + b_{n-1}x^{n-1} + vx^n \in I$$

  directamente se observa que sumando $(u + v) \in J_n$.
- Para el producto se desarrolla de forma parecida a la suma y se llega trivialmente al resultado.

■

Lema 6.2.2. *En las condiciones anteriores, $\forall n, J_n \subseteq J_{n+1}$*

Demostración. Sea $a \in J_n$, entonces $\exists a_0, \ldots, a_{n-1} \in R$ con $a_0 + \cdots + a_{n-1}x^{n-1} + ax^n \in I$. Como I es ideal entonces podemos multiplicar por x, de modo que

$$a_0x + \cdots + a_{n-1}x^n + ax^{n+1} \in I.$$

luego se verifica que $a \in J_{n+1}$. ■

Teorema 6.2.3 (Teorema de la base de Hilbert)**.** *Sea R un anillo noetheriano, entonces $R[x]$ su anillo de polinomios es una variable es noetheriano.*

Demostración. Veamos para la demostración que todo ideal I de $R[x]$ es finitamente generado. Por el lema anterior (6.2.2) sabemos que $J_0 \subseteq \cdots \subseteq J_n \cdots \subseteq R$, pero como este es noetheriano entonces $\exists N$ a partir del cual la cadena estaciona. Para cada $0 \leq i \leq N$ tenemos que $J_i = (a_{i_0}, \ldots, a_{i_t})$ es finitamente generado en R y por tanto existen $f_{i_0}, \ldots, f_{i_t} \in I$ tales que $\deg(f_{i_j}) = i$ donde los coeficientes $a_{i_j} \neq 0$. Afirmamos que

$$I = (f_{0_0}, \ldots, f_{0_{t_0}}, \ldots, f_{N_0}, \ldots, f_{N_{t_N}})$$

veamos ambas contenciones

- Por la definición de los f_{i_j} se da $\supseteq$
- Probemos por inducción en el grado. En primer lugar vemos que si $\deg(f) = 0$ entonces tenemos que $f \in I \Rightarrow f \in J_0$ y $f = a_0 b_1 + \cdots + a_{0_{t_0}} b_{t_0}$ con $b_{t_i} \in R, f_{0_j} = a_{0_j} x^0 \in I$ de modo que

  $$f = f_{0_1} b_1 + \cdots + f_{0_{t_0}} b_{t_0} \in (f_{i_j})$$

  Supongamos ahora el resultado cierto para $\deg(f) < n$ y probemos el caso n. Distinguimos dos casos:

  - Si $n \leq N$ entonces tenemos que $a_n \in J_n = (a_{n_1}, \ldots, a_{n_{t_n}})$ de modo que existen $b_1, \ldots, b_{t_n}$ con $a_n = a_{n_1} b_1 + \cdots + a_{n_{t_n}} b_{t_n}$ y el polinomio $g = f_{n_1} b_1 + \cdots + f_{n_{t_n}} b_{t_n} \in I$ porque $f_{i_j} \in I$. Así pues

    $$g = a_n x^n + g_{n-1} x^{n-1} + \cdots + g_0 \Rightarrow f - g \in I \wedge \deg(f - g) < n$$

    aplicando hipótesis de inducción tenemos que $f - g \in (f_{i_j}) \Rightarrow f = (f - g) + g \in (f_{i_j})$
  - Para el caso $n > N$, si $a_n \in J_n = J_N = (a_{N_1}, \ldots, a_{N_{t_N}})$. Operando como en el caso anterior tenemos que:

    $$a_n = a_{N_1} b_1 + \cdots + a_{N_{t_N}} b_{t_N}$$

    para ciertos coeficientes b_j. Del mismo modo definimos un polinomio

    $$g = (x^{n-N} f_{N_1}) b_1 + \cdots + (x^{n+N} f_{N_{t_N}}) b_{t_N} \in f_{i_j}$$

    Vemos de nuevo que $g = g_0 + \cdots + a_n x^n$ y entonces restando podemos aplicar h.d.i concluyendo el resultado.

■

Corolario 6.2.1. *Si R es noetheriano entonces $R[x_1, \ldots, x_n]$ es noetheriano y en particular $\mathbb{K}[x_1, \ldots, x_n]$ es noetheriano.*

Demostración. Basta aplicar inducción. ■

Observación 6.2.5. Si R es noetheriano entonces R/I también,

Teorema 6.2.4. *Sea $R \neq \{0\}$ un anillo noetheriano entonces todo ideal $I \subseteq R$, $I \neq (1)$ admite una descomposición primaria.*

Demostración. Supongamos que $R \neq \{0\}$ es noetheriano, por reducción al absurdo supongamos que hay un ideal no descomponible. Sea

$$\Sigma = \{I \subsetneq R \mid I \text{ no es descomponible}\}$$

tenemos que $\Sigma \neq \emptyset$.

Por ser R noetheriano, tenemos que existe $I \in \Sigma$ maximal en Σ para la relación de contención $\subseteq$.

- I no es descomponible
- $I \subsetneq J \subsetneq R$, J es descomponible

I no puede ser primario (porque no es descomponible), entonces $\exists a, b \in R$ tales que $a \cdot b \in I$ pero $a \notin I, b \notin \sqrt{I}$. Consideremos ahora:

$$I \subseteq (I : b) \subseteq (I : b^2) \subseteq \cdots \subseteq (I : b^n) \subseteq \ldots$$

que es una cadena porque si $x \in I : b^i$ entonces $x \cdot b^{i+1} = x \cdot b^i \cdot b \in I \Rightarrow x \in I : b^{i+1}$. Además, como es noetheriano la cadena es estacionaria y $\exists k \in \mathbb{N}$ con $(I : b^k) = (I : b^{k+1})$. Ahora, sea $J = I + (a)$, como $a \notin I$, entonces $I \subsetneq J$. Si se diera que $J = (1)$ existirían $x \in I$ y $c \in R$ tales que $1 = x + c \cdot a$, donde multiplicando por b.

$$b = b \cdot x + c \cdot ab \in I \subseteq \sqrt{I}\#.$$

Por maximalidad existen primarios $Q_1, \ldots, Q_t$ tales que $Q_1 \cap \cdots \cap Q_t = J$. Ahora, sea $T = I : b^k$ tal que se estaciona la cadena, entonces $b \neq 0$ porque si $I = (I : b)$ entones $a \cdot b \in I$, $a \in (I : b)\#$. Por lo que $I \subsetneq T$. Ahora si $T = (1)$, $b^k = 1 \cdot b^k \in I$, pero por tanto $b \in \sqrt{I}\#$, luego $I \subsetneq T \subsetneq (1)$ y existen primarios $U_1, \ldots, U_s$ con

$$T = I : b^k = U_1 \cap \cdots \cap U_s$$

Finalmente, sea $H = I + (b^k)$, vemos que $I \subsetneq I + (b^k)$ porque $b^k \in I + (b^k)$ pero como $b \notin \sqrt{I}$ entonces $b^k \notin I$. Por otro lado, $I + (b^k) \neq (1)$, si lo fuera tendríamos que $1 = x + b^k \cdot c, x \in I, c \in R$ y multiplicando por a llegamos a que $a = (a \cdot x)^{\in I} + (a \cdot b^k \cdot c)^{\in I} \in I\#$.

Por tanto existen $V_1, \ldots, V_r$ primarios con $I + (b^k) = V_1 \cap \cdots \cap V_r$. Veamos que $I = \Big(I + (a)\Big) \bigcap \Big(I + (b^k)\Big)$.

$\subseteq$ Trivial puesto que $I \subseteq I + (a)$ y $I \subseteq I + (b^k)$

$\supseteq$ Sea $x \in \Big(I + (a)\Big) \bigcap \Big(I + (b^k)\Big)$, existen $y \in I, z \in R$ tales que $x = y + a \cdot z$ y existen $p \in I, q \in R$ con $x = p + b^k \cdot q$. De modo que multiplicando por b, entonces:

$$xb = yb + (ab)z = pb + b^{k+1}q, \quad yb, ab \in I$$

Y por tanto $xb = yb + abz = pb + qb^{k+1} \in I$ así

$$xb - pb = qb^{k+1} \in I$$

y de aquí deducimos que $q \in (I : b^{k+1}) = (I : b^k)$ de modo que $q \cdot b^k \in I$ luego $x = p + q \cdot b^k \in I$.. Tenemos que

$$I = Q_1 \cap \cdots \cap Q_t \cap V_1 \cap \cdots \cap V_r\#$$

contradicción con que $\Sigma \neq \emptyset$ de modo que todo ideal debe ser descomponible.

■

Ejemplo 6.2.2. Sea $I = (2^4 \cdot 3^5 \cdot 7^2 \cdot 11) \subseteq \mathbb{Z}$. Tenemos que $\sqrt{I} = (2 \cdot 3 \cdot 7 \cdot 11)$. Ahora consideramos $a = 2^4 \cdot 3^5 \cdot 7^2$ y $b = 11$. Sabemos que $a \notin I, b \notin \sqrt{I}$ pero que $a \cdot b \in I$. Así pues, consideramos el ideal que utilizamos en el teorema anterior (6.2), $J = I + (2^4 \cdot 3^5 \cdot 7^2) = (2^4 \cdot 3^5 \cdot 7^2)$. Por otro lado, por el ejercicio 3.2.11 que $(I : b) = (2^4 \cdot 3^5 \cdot 7^2)$ y $(I : b^k) = (2^4 \cdot 3^5 \cdot 7^2)$. Así pues $I = \Big(I + (a)\Big) \bigcap \Big(I + (b^k)\Big) = (2^4 \cdot 3^5 \cdot 7^2) \cap (11)$.

Consideremos ahora $a_1 = 2^4 \cdot 3^5$ y $b_1 = 7^2$. Se verifican las mismas condiciones de antes: $a_1 \notin I, b_1 \notin \sqrt{I}$ pero que $a_1 \cdot b_1 \in I$ y por otro lado $J_1 = I_1 + (2^4 \cdot 3^5), (I : b_1) = (2^4 \cdot 3^5)$ e $I = \Big(I + (a)\Big) \bigcap \Big(I + (b^k)\Big) = (2^4 \cdot 3^5) \cap (7^2) \cap (11) = (2^4) \cap (3^5) \cap (7^2) \cap (11)$, que es en particular una descomposición en primarios minimal.

Observación 6.2.6. La potencia de un primo no es necesariamente primario. Ahora, si el radical de un ideal es maximal sí que es primario (teorema 5.1.3) que es lo que hemos utilizado en la segunda parte del ejemplo

Proposición 6.2.2. *Sea $\mathbb{K}[x_1, \ldots, x_n]$ un anillo de polinomios, sean*

$$\tilde{I} = \begin{cases} f_1 = 0 \\ \ldots \\ f_r = 0 \end{cases}$$

$$\tilde{J} = \begin{cases} g_1 = 0 \\ \ldots \\ g_s = 0 \end{cases}$$

Entonces, $H = (f_1, \ldots, f_r) \cap (g_1, \ldots, g_s) = (h_1, \ldots, h_t)$ y el sistema:

$$\tilde{H} = \begin{cases} h_1 = 0 \\ \ldots \\ h_t = 0 \end{cases}$$

Las soluciones de $\tilde{H}$ = soluciones de $\tilde{I}$ $\bigcup$ soluciones de $\tilde{J}$

Demostración. Demostremos por doble contención.

- $\supseteq$ Sea a solución de $\tilde{I}$, entonces $f_1(a) = \cdots = f_r(a) = 0$. Ahora sea h_j un generador de $H \subseteq (f_1, \ldots, f_r)$, entonces $\exists u_1, \ldots, u_r$ tales que $h_j = u_1 f_1 + \cdots + u_r f_r$ y por tanto $h_j(a) = 0, \forall j \in \{1, \cdots, t\}$. De manera análoga se prueba para una solución de $\tilde{J}$
- $\subseteq$ Sea a con $h_1(a) = \cdots = h_t(a) = 0$. Si $a \in \text{Sol}(\tilde{I})$ hemos acabado. Por otro lado si $a \notin \text{Sol}(\tilde{I})$ entonces $\exists f_i(a) \neq 0 . i \in \{1, \cdots, r\}$. Ahora, $f_i \cdot g_j \in H$ para todo j y existen coeficientes $v_1, \ldots, v_t$ tales que $f_i \cdot g_j = v_1 h_1 + \cdots + v_t h_t$ y por tanto $f_t(a) \cdot g_j(a) = 0$ para todo j y como estamos en un cuerpo entonces $g_j(a) = 0$ y $a \in \text{Sol}(\tilde{J})$

■

Observación 6.2.7. Dados $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_n]$ saber si hay solución o no:

- $\mathbb{C}$ Teorema de los ceros de Hilbert, $(f_1, \ldots, f_r) = (1)$

$\mathbb{R}$ Hay algoritmos pero son muy complicados

$\mathbb{Q}$ Problema abierto.

$\mathbb{Z}$ No puede haber algoritmo (está demostrada la indecibilidad). Cualquier algoritmo que tome como *input* un sistema de ecuaciones hay ciertos sistemas que hacen que el algoritmo de como *output* una solución errónea o no progrese el algoritmo.

En base a esta observación, enunciamos el teorema del caso en $\mathbb{C}$, en una versión más débil.

Teorema 6.2.5. *Sea $\mathbb{K} \subseteq \mathbb{L}$ una extensión de cuerpos. Sea $a \in \mathbb{L}$. Son equivalentes:*

(I) *a es algebraico sobre $\mathbb{K}$.*

(II) *$\mathbb{K}[a]$ es un espacio vectorial de dimensión finita sobre $\mathbb{K}$.*

(III) *$\mathbb{K}[a]$ es un cuerpo.*

Demostración. Es un resultado clásico de teoría de Galois.

- (I) $\Rightarrow$ (II): Si a es algebraico de grado n, entonces $\{1, a, \ldots, a^{n-1}\}$ es una base de $\mathbb{K}[a]$, por lo que tiene dimensión finita.
- (II) $\Rightarrow$ (I): Si $\mathbb{K}[a]$ tiene dimensión finita, entonces la sucesión infinita $1, a, a^2, \ldots$ debe ser linealmente dependiente. Luego existe una combinación lineal no trivial $a^n = b_0 + b_1 a + \cdots + b_{n-1} a^{n-1}$, lo que implica que a satisface un polinomio no trivial, y por tanto es algebraico.
- $\neg$(I) $\Rightarrow$ $\neg$(III): Si a es trascendente, $\mathbb{K}[a]$ es un anillo de polinomios y no puede ser un cuerpo.
- (I) $\Rightarrow$ (III): Sea $F(x)$ el polinomio mínimo de a. Dado $b \in \mathbb{K}[a] \setminus \{0\}$, existe un polinomio $B(x)$ tal que $B(a) = b$. Como F es irreducible, $\gcd(F, B) = 1$, y por el teorema de Bézout existen U, V con $FU + BV = 1$. Evaluando en a, se obtiene $b \cdot V(a) = 1$, es decir, b es invertible.

■

Teorema 6.2.6. *Sea $\mathbb{K} \subseteq \mathbb{L}$ una extensión de cuerpos. Sean $a \in \mathbb{L}$, $b \in \mathbb{K}[a] \setminus \{0\}$. Si $\mathbb{K}[a, 1/b]$ es un cuerpo, entonces a es algebraico sobre $\mathbb{K}$.*

Demostración. Si $b \in \mathbb{K}$, entonces $\mathbb{K}[a, 1/b] = \mathbb{K}[a]$, y por el teorema anterior, a es algebraico. Supongamos entonces $b \in \mathbb{K}[a] \setminus \mathbb{K}$. Entonces existe un polinomio $B(x) \in \mathbb{K}[x] \setminus \mathbb{K}$ con $b = B(a)$.

- Sea $G(x) = B(x)x + 1 \in \mathbb{K}[x]$. Si $G(a) = 0$, entonces a es algebraico.
- Si $G(a) \neq 0$, entonces $G(a)^{-1} \in \mathbb{K}[a, 1/b]$. Hay un polinomio $H(x, y) \in \mathbb{K}[x, y]$ tal que $H(a, 1/b) = G(a)^{-1}$. Escribimos $H(x, 1/B(x)) = F(x)/B(x)^n$.

  ** Entonces:

  $$F(x)G(x) - B(x)^n \in \mathbb{K}[x]$$

  y se anula al evaluar en a. Si este polinomio fuera nulo, tendríamos $B(x)^n = F(x)(B(x)x + 1)$, lo cual implica que un factor de $B(x)x + 1$ divide a $B(x)^n$, y por tanto dividiría a 1, contradicción. Luego, el polinomio no es nulo y se anula en a, luego a es algebraico.

■

Teorema 6.2.7 (Lema de Zariski)**.** *Sea $\mathbb{K} \subseteq \mathbb{L}$ una extensión de cuerpos. Sean $a_1, \ldots, a_n \in \mathbb{L}$. Si $\mathbb{K}[a_1, \ldots, a_n]$ es un cuerpo, entonces la extensión $\mathbb{K} \subseteq \mathbb{K}[a_1, \ldots, a_n]$ es algebraica.*

Demostración. Procedemos por inducción sobre n. Para $n = 1$ es el Teorema anterior.

Supongamos que vale para $n - 1$. Tenemos:

$$\mathbb{K}(a_1)[a_2, \ldots, a_n] = \mathbb{K}[a_1, \ldots, a_n]$$

que es un cuerpo. Por hipótesis de inducción, $\mathbb{K}(a_1) \subseteq \mathbb{K}[a_1, \ldots, a_n]$ es una extensión algebraica. Basta probar que a_1 es algebraico sobre $\mathbb{K}$. Para cada $i \geq 2$, a_i es algebraico sobre $\mathbb{K}(a_1)$. Sea $d_i = [\mathbb{K}(a_1, a_i) : \mathbb{K}(a_1)]$. Existe un polinomio $F_i(x) \in \mathbb{K}[a_1][x]$ que se anula en a_i. Cualquier potencia a_i^j puede escribirse como combinación lineal de menores potencias con coeficientes en $\mathbb{K}[a_1, 1/b_i]$, donde b_i es el coeficiente principal de F_i. Un elemento $c \in \mathbb{K}[a_1, \ldots, a_n]$ se puede escribir como:

$$c = \sum_{j_2=0}^{d_2-1} \cdots \sum_{j_n=0}^{d_n-1} c_{j_2,\ldots,j_n} a_2^{j_2} \cdots a_n^{j_n}, \quad \text{con } c_{j_2,\ldots,j_n} \in \mathbb{K}[a_1, 1/(b_2 \cdots b_n)]$$

.

El conjunto $\{a_2^{j_2} \cdots a_n^{j_n}\}$ genera $\mathbb{K}[a_1, \ldots, a_n]$ como espacio vectorial sobre $\mathbb{K}(a_1)$, por lo que tiene una base finita $\{v_1 = 1, \ldots, v_\ell\}$. Cada coeficiente se puede expresar con denominadores, de modo que todos los elementos de $\mathbb{K}[a_1, \ldots, a_n]$ se expresan como:

$$c = c_1 + c_2 v_2 + \cdots + c_\ell v_\ell, \quad \text{con } c_i \in \mathbb{K}[a_1, 1/b]$$

para un cierto $b \in \mathbb{K}[a_1]$. En particular, si $c \in \mathbb{K}(a_1)$, esta expresión obliga a que $c_i = 0$ para $i \geq 2$, luego $c \in \mathbb{K}[a_1, 1/b]$, por lo tanto:

$$\mathbb{K}[a_1, 1/b] = \mathbb{K}(a_1)$$

y como $\mathbb{K}[a_1, 1/b]$ es un cuerpo, por el Teorema anterior, a_1 es algebraico sobre $\mathbb{K}$. ■

Teorema 6.2.8 (Teorema de los ceros de Hilbert)**.** *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Sea $\mathbb{K}[x_1, \ldots, x_n]$ el anillo de polinomios en n variables, si $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ es un ideal maximal entonces existe $a_1, \ldots, a_n \in K$ con $I = (x_1 - a_1, \ldots, x_n - a_n)$.*

Demostración. Sea $\mathbb{L} = \mathbb{K}[x_1, \ldots, x_n]/I$, sabemos que es cuerpo porque I es maximal, consideramos la extensión

$$\mathbb{K} \hookrightarrow \mathbb{K}[x_1, \ldots, x_n] \hookrightarrow \mathbb{L}$$

tenemos que $\mathbb{K}$ es un subcuerpo de $\mathbb{L} = \mathbb{K}[\bar{x_1}, \ldots, \bar{x_n}]$ y por el lema de Zariski 6.2.7 tenemos que $\mathbb{K} \subseteq \mathbb{K}[\bar{x_1}, \ldots, \bar{x_n}]$ es algebraico, además $\mathbb{K}$ es algebraicamente cerrado (todo polinomio no nulo en $\mathbb{K}$ tiene al menos una raíz en $\mathbb{K}$) y por tanto $\mathbb{K} = \mathbb{K}[\bar{x_1}, \ldots, \bar{x_n}]$, existen por ello $a_1, \ldots, a_n \in \mathbb{K}$ con $\bar{x_1} = a_1, \ldots, \bar{x_n} = a_n$, pues cada $\bar{x_1}$ estaba ya en $\mathbb{K}$, entonces $(x_1 - a_1, \ldots, x_n - a_n) \subseteq I$, por tanto, $(x_1 - a_1, \ldots, x_n - a_n)$ maximal y es igual a I ■

Corolario 6.2.2 (Versión débil)**.** *Sea $\mathbb{K}$ algebraicamente cerrado y $\mathbb{K}[x_1, \ldots, x_n]$ anillo de polinomios. Sean $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ son equivalentes:*

(I) $\{a \in \mathbb{K}^n \mid f_1(a) = \cdots = f_s(a) = 0\} = \emptyset$ *(sistema incompatible)*

(II) $\exists g_1, \cdots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ *con* $1 = g_1 f_1 + \cdots + g_s f_s$

(III) $I = (f_1, \ldots, f_s) = (1)$

Demostración. Vayamos demostrando ciertas implicaciones:

- En primer lugar $(II) \Leftrightarrow (III)$ es trivial puesto que es cierto en general, no solo si $\mathbb{K}$ es algebraicamente cerrado.
- $(II) \Rightarrow (I)$: Si se cumple (II) tenemos que $\forall a, f_1(a) = \cdots = f_s(a) = 0$ y por tanto si $1 = 0\#$.
- $(I) \Rightarrow (II)$ Veamos el contrarrecíproco, si no se cumple (II) entonces el ideal $I = (f_1, \ldots, f_s) \neq (1)$ (ya demostramos este sii), por tanto existe un maximal m con $I \subseteq m$. Como $\mathbb{K}$ es algebraicamente cerrado existen $a_1, \ldots, a_n \in \mathbb{K}$ con $m = (x_1 - a_1, \ldots, x_n - a_n)$. Así pues, $\forall i, 1 \leq i \leq s$ tenemos que $f_i = h_1^i(x_1 - a_1) + \cdots + h_n^i(x_n - a_n)$ de manera que $f_i(a_1, \ldots, a_n) = 0$ y tenemos un sistema compatible.

■

Observación 6.2.8. Este corolario se puede ver como una generalización del *Teorema de Rouché-Fröbenius* para un sistema de ecuaciones con polinomios o del *Teorema Fundamental del Álgebra* para polinomios en varias variables.

En el contexto de anillos Noetherianos y con los resultados expuestos al final de la Sección 5.2, podemos hacer de nuevo ciertos ejercicios como el 4.2.10. Se da a continuación una versión de ese ejercicio con su demostración análoga a la que se hizo en él, aunque no el teorema 5.2.2 el resultado es trivial, ya que la prueba es ese mismo teorema.

Ejercicio 6.2.1 (4.2.10 anillos noetherianos)**.** Si A es noetheriano, y $(0) = Q_1 \cap \cdots \cap Q_n$ intersección de primarios. Entonces

$$div_0(A) = \sqrt{Q_1} \cup \cdots \cup \sqrt{Q_n}$$

Por otro lado, concluir que $div_0(A)$ es unión de ideales primos.

Demostración. Como $A \neq \emptyset$, definimos el conjunto

$$\Sigma = \{I \subseteq A \mid I \text{ ideal}, \forall t \in I, t \in div_0(A)\}$$

Observamos que Σ tiene elementos maximales y estos son ideal primos. Aplicar el Lema de Zorn

- $\Sigma \neq \emptyset$, como $A \neq \{0\}$ entonces $0 \in div_0(A) \Rightarrow (0) \in \Sigma$
- Sea L una cadena en Σ, $J = \bigcup_{I \in L} I$ es un ideal (visto en 4.1.1). Entonces $\forall t \in J, \exists I \in L, t \in I$ y como $I \in \Sigma, t \in div_0(A)$. Por lo que $J \in \Sigma$ y toda cadena de Σ admite cota superior en Σ y por el lema de Zorn (4.1.1) Σ tiene maximales.

  Sea P un maximal de Σ queremos ver que P es primo supongamos que $a \cdot b \in P$ y $a, b \notin P$. Por reducción al absurdo veamos que P es primo. Tenemos entonces que:

$$P \subsetneq P + (a)$$

$$P \subsetneq P + (b)$$

de modo que existen $q_1, q_2 \in P, r_1, r_2 \in A$ con:

$$t = q_1 + ar_1 \notin div_0(A)$$

$$s = q_2 + br_2 \notin div_0(A)$$

Multiplicando ambas expresiones tenemos que

$$t \cdot s = q_1(q_2 + br_2) + ar_2q_2 + abr_1r_2 \in P$$

de modo que el producto $t \cdot s \in div_0(A)$, lo que es el absurdo porque si el producto de dos cosas es divisor del cero una de las dos es divisor del cero.

Para la segunda parte, nuestro objetivo es demostrar que si $a \in div_0(A)$ entonces existe un ideal P primos con $a \in P \subseteq div_0(A)$. Tenemos dos opciones de demostración:

1. Tomamos $\Sigma_a = \{I \text{ ideal} \mid I \subseteq div_0(A), a \in I\}$ y repetimos la demostración. Para ver que $\Sigma_a \neq \emptyset$ basta ver que $(a) \subseteq div_a(A)$ y repetimos.

2. Si $a = 0$ tomo P_a cualquier maximal de Σ. Si en otro caso $a \neq 0$ tomo $B = A/(a)$ y por lo que acabamos de probar $\exists Q$ primo de B con $Q \subseteq div_0(B)$. Ahora consideramos
$$P = \pi^{-1}(Q) = \{x \in A \mid \bar{x} \in Q\}$$
Observamos ahora que:
   - $a \in P$
   - P ideal primo
   - $P \subseteq div_0(A)$

   Sea $x \in P$ tal que $\bar{x} \in Q$ entonces $\exists \bar{r} \neq \bar{0}$ con $\bar{x}\bar{r} = \bar{0}$ y $\exists r \notin (a)$ con $xr \in (a) \subseteq P$.

$\forall a \in div_0(a), \exists P_a$ primo tal que $a \in P_a \subseteq div_0(A)$ y por tanto

$$div_0(A) = \bigcup_{a \in div_0(A)} \{a\} \subseteq \bigcup_{a \in div_0(A)} P_a \subseteq div_0(A)$$

■

6.3. Hoja 5

Definición 6.3.1. Sean $R \subseteq S$, $R_1 \subseteq T$ anillos donde R y R_1 son isomorfos por $\sigma : R \to R_1$. Diremos que un homomorfismo $\phi : S \longrightarrow T$ es un R-homomorfismo (resp. R-isomorfismo) si es un homomorfismo (resp. isomorfismo) que extiende a σ. Es decir, si para todo $c \in R$, $\phi(c) = \sigma(c)$.

Es muy común que, en el caso de tener una inyección canónica $i : R \hookrightarrow S$, identificar (por abuso de notación) R con $i(R)$ y escribir $R \subseteq S$. Por ejemplo, cuando $\mathbb{Q} \subseteq \mathbb{Q}[x]$ o, más $\mathbb{Q} \subseteq \mathbb{Q}[x]/(x^2 + 1)$. En este contexto, si $i_S : R \hookrightarrow S$ y $i_T : R \to T$ son inyecciones canónicas, diremos simplemente que un R-homomorfismo $\phi : S \to T$ es un homomorfismo en el que $\forall c \in R, \phi(c) = c$. Donde, si nos ponemos muy técnicos, deberíamos decir que

$\forall c \in i_S(R)$, $\phi(c) = i_T(i_S^{-1}(c))$.

El siguiente resultado nos dice que, si $\mathbb{K} \subseteq \mathbb{L}$ es una extensión de cuerpos, con $\mathbb{L}$ algebraicamente cerrado, entonces toda extensión algebraica finita $\mathbb{K} \subseteq \mathbb{K}_1$ de $\mathbb{K}$ se puede considerar, sin pérdida de generalidad, como un subcuerpo de $\mathbb{L}$, $\mathbb{K} \subseteq \mathbb{K}_1 \subseteq \mathbb{L}$. El resultado es cierto para toda extensión algebraica, pero solo necesitaremos el caso de extensiones finitas.

Teorema 6.3.1. *Sea $\mathbb{K}$ un cuerpo, $\mathbb{K} \subseteq \mathbb{L}$ con $\mathbb{L}$ algebraicamente cerrado. Si $\mathbb{K} \subseteq \mathbb{K}[a_1, ..., a_n]$ es una extensión algebraica finita de cuerpos, entonces existe un homomorfismo (necesariamente inyectivo):*

$$\phi : \mathbb{K}[a_1, ..., a_n] \longrightarrow \mathbb{L}$$

tal que para todo $c \in \mathbb{K}$, $\phi(c) = c$.

Demostración. Por inducción en n. Si $n = 1$, sea $\mathbb{K} \subseteq \mathbb{K}[a_1]$ algebraica. Sea $f(x) \in \mathbb{K}[x]$ el polinomio mínimo de grado d_1 de a_1 sobre $\mathbb{K}$. Como $\mathbb{L}$ es algebraicamente cerrado, existe $\beta \in \mathbb{L}$ con $f(\beta) = 0$. Como f es irreducible en $\mathbb{K}[x]$, es también el polinomio mínimo de β sobre $\mathbb{K}$. Por tanto:

$$\mathbb{K}[a_1] \simeq \mathbb{K}[x]/(f(x)) \simeq \mathbb{K}[\beta] \subseteq \mathbb{L}$$

De donde el homomorfismo buscado es:

$$\begin{array}{rccc} \phi : & \mathbb{K}[a_1] & \longrightarrow & \mathbb{K}[\beta] \subseteq \mathbb{L} \\ & \sum_{i=0}^{d_1-1} c_i a_1^i & \mapsto & \sum_{i=0}^{d_1-1} c_i \beta^i \end{array}$$

Supongamos cierto el resultado para todo cuerpo y toda extensión algebraica con $n-1$ generadores y consideremos $\mathbb{K} \subseteq \mathbb{K}[a_1, ..., a_n]$. Por hipótesis de inducción existe un homomorfismo $\psi : \mathbb{K}[a_1, ..., a_{n-1}] \longrightarrow \mathbb{L}$ que es constante en $\mathbb{K}$. Sea $f = \sum_{i=0}^{d_n} c_i x^i$ el polinomio mínimo de a_n sobre $\mathbb{K}[a_1, ..., a_{n-1}]$, de donde $c_i \in \mathbb{K}[a_1, ..., a_{n-1}]$, $0 \leq i \leq d_n$. Es fácil ver que:

$$\mathbb{K}[a_1, ..., a_{n-1}][x] \simeq \mathbb{K}[\psi(a_1), ..., \psi(a_{n-1})][x]$$

donde el isomorfismo, que viene dado por $\sum_j p_j x^j \mapsto \sum_j \psi(p_j) x^j$ (si $p_j \in \mathbb{K}[a_1, \ldots, a_{n-1}]$), es un K-isomorfismo. Sea $g = \sum_{i=0}^{d_n} \psi(c_i) x^i \in \mathbb{L}[x]$. De nuevo, existe $\beta \in \mathbb{L}$ con $g(\beta) = 0$. Además, como f es irreducible en $\mathbb{K}[a_1, ..., a_{n-1}][x]$, g es irreducible en $\mathbb{K}[\psi(a_1), ..., \psi(a_{n-1})][x]$. De nuevo:

$$\mathbb{K}[a_1, ..., a_n] \simeq \mathbb{K}[a_1, ..., a_{n-1}][x]/(f(x)) \simeq$$

$$\mathbb{K}[\psi(a_1), ..., \psi(a_{n-1})][x]/(g(x)) \simeq \mathbb{K}[\psi(a_1), ..., \psi(a_{n-1}), \beta] \subseteq \mathbb{L}$$

donde todos los isomorfismos son constantes en $\mathbb{K}$. ■

Observación 6.3.1. El isomorfismo no es único, como ya sabemos por la teoría de Galois, pero dos isomorfismos están relacionados por un K-automorfismo de $\mathbb{K}[a_1, ..., a_n]$, como indica la Teoría de Galois. Por ejemplo $(x^2 - 2, y^2 - 3) \subseteq \mathbb{Q}[x, y]$ es un ideal maximal de $\mathbb{Q}[x, y]$ (los ejercicios de esta hoja están motivados para comprobar esta afirmación), por tanto $R = \mathbb{Q}[x, y]/(x^2 - 2, y^2 - 3)$ es Q-isomorfo a un subcuerpo de $\mathbb{C}$, $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Pero

tenemos cuatro Q-homomorfismos:

$$\begin{aligned}\phi_1 : R &\longrightarrow \mathbb{C} \\ \bar{x} &\mapsto \sqrt{2} \\ \bar{y} &\mapsto \sqrt{3}\end{aligned} \qquad \begin{aligned}\phi_2 : R &\longrightarrow \mathbb{C} \\ \bar{x} &\mapsto -\sqrt{2} \\ \bar{y} &\mapsto \sqrt{3}\end{aligned}$$

$$\begin{aligned}\phi_3 : R &\longrightarrow \mathbb{C} \\ \bar{x} &\mapsto \sqrt{2} \\ \bar{y} &\mapsto -\sqrt{3}\end{aligned} \qquad \begin{aligned}\phi_4 : R &\longrightarrow \mathbb{C} \\ \bar{x} &\mapsto -\sqrt{2} \\ \bar{y} &\mapsto -\sqrt{3}\end{aligned}$$

En todos los casos, el conjunto imagen es $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Esto ocurre porque la extensión $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ es de Galois. Si tomamos una extensión que no sea normal, por ejemplo $\mathbb{Q} \subseteq R = \mathbb{Q}[x]/(x^3 - 2)$, los homomorfismos son:

$$\begin{aligned}\phi_1 : R &\longrightarrow \mathbb{C} \\ \bar{x} &\mapsto \sqrt[3]{2}\end{aligned} \qquad \begin{aligned}\phi_2 : R &\longrightarrow \mathbb{C} \\ \bar{x} &\mapsto \sqrt[3]{2}(-1 + \sqrt{-3})/2\end{aligned}$$

$$\begin{aligned}\phi_3 : R &\longrightarrow \mathbb{C} \\ \bar{x} &\mapsto \sqrt[3]{2}(-1 - \sqrt{-3})/2\end{aligned}$$

donde $\phi_1(R) = \mathbb{Q}[\sqrt[3]{2}] \neq \mathbb{Q}[\sqrt[3]{2}(-1 + \sqrt{-3})/2] = \phi_2(R)$, a pesar de ser cuerpos Q-isomorfos.

Definición 6.3.2. Denotamos por $\mathbb{Q}^{alg}$ la clausura algebraica de $\mathbb{Q}$ en $\mathbb{C}$. Es decir el subcuerpo de $\mathbb{C}$ formado por todos los elementos algebraicos sobre $\mathbb{Q}$. Se supone conocido que $\mathbb{Q}^{alg}$ es algebraicamente cerrado.

6.4. Ejercicios

Ejercicio 6.4.1. Sean $f_1, ..., f_r \in \mathbb{Q}[x_1, ..., x_n]$. Son equivalentes:

1. $\{f_1, ..., f_r\}\mathbb{Q}[x_1, ..., x_n] \neq \mathbb{Q}[x_1, ..., x_n]$.
2. $\{f_1, ..., f_r\}\mathbb{Q}^{alg}[x_1, ..., x_n] \neq \mathbb{Q}^{alg}[x_1, ..., x_n]$.
3. Existe $a = (\alpha_1, ..., \alpha_n) \in (\mathbb{Q}^{alg})^n \subseteq \mathbb{C}^n$ con $f_1(a) = \cdots f_r(a) = 0$.

Demostración. En primer lugar, si existen $g_1, \ldots, g_r \in \mathbb{Q}^{\text{alg}}[x_1, \ldots, x_n]$ con $g_1 f_1 + \cdots + g_r f_r = 1$ entonces existen $h_1, \ldots, h_r \in \mathbb{Q}[x_1, \cdots, x_r]$ con $h_1 f_1 + \cdots + h_r f_r = 1$. Vemos que esto es equivalente a (I)⇔(II). Probemos por tanto.

- $\neg$(I) $\Rightarrow \neg$(II): Si $\{f_1, \ldots, f_r\}\mathbb{Q}[x_i] = (1)$ entonces existen $g_1, \ldots, g_r \in \mathbb{Q}[x_1, \ldots, x_n] = \mathbb{Q}[x]$ tales que $g_1 f_1 + \cdots + g_r f_r = 1 \Rightarrow \{f_1, \ldots, f_r\}\mathbb{Q}^{\text{alg}}[x] = (1)$
- (II) $\Leftrightarrow$ (III): Teorema de los ceros de Hilbert (6.2.3).

- (I) $\Rightarrow$ (III): Supongamos que $\{f_1, \ldots, f_r\}\mathbb{Q}[x] \neq (1)$. Por tanto $\exists m$ maximal en $\mathbb{Q}[x]$ con $(f_1, \ldots, f_r) \subseteq m$. De este modo el cociente $\mathbb{Q}[x]/m$ es un cuerpo y por el lema de Zariski (6.2.7) es algebraico sobre $\mathbb{Q}$. Por el teorema 6.3.1 existe

$$\begin{aligned} \psi : \mathbb{Q}[x]/m &\longrightarrow \mathbb{Q}^{\text{alg}} \\ \bar{x_i} &\longmapsto \alpha_i \end{aligned}$$

  Tenemos que $\forall i \in \{1, \cdots, n\}, f_i \in m$ y $f = \sum e_i x^{i_1} \cdots x_n^{i_n}$ de manera que

$$0 = \psi(0) = \psi(\bar{f}) = f(\alpha_1, \ldots, \alpha_n)$$

  y tenemos 3.

■

Ejercicio 6.4.2. Sea $I \subseteq \mathbb{Q}[x_1, ..., x_n]$ un ideal maximal del anillo de polinomios. Entonces existe $a = (\alpha_1, ..., \alpha_n) \in (\mathbb{Q}^{alg})^n$ que cumple $\forall f \in I, f(a) = 0$.

Demostración. Estoy en Noetheriano por lo que puedo pensarlo como anillo finito y por ello si I es maximal como noetheriano puede ser generado por un conjunto finito f1,...,fn y es distinto del (1) por lo que trivialmente como antes tenemos que (f1,...,fn) distinto del total y existen los alphas buscados (III). ■

Ejercicio 6.4.3. Sea $I \subseteq \mathbb{Q}[x_1, ..., x_n]$ un ideal maximal del anillo de polinomios. Sea $a = (\alpha_1, ..., \alpha_n) \in \mathbb{Q}^{alg}$ tal que $\forall f \in I, f(a) = 0$. Sea $f_1(x_1) \in \mathbb{Q}[x_1]$ el polinomio mínimo de α_1 sobre $\mathbb{Q}$. Para cada $i \geq 2$ sea $f_i(\alpha_1, ..., \alpha_{i-1}, x_i)$ el polinomio mínimo de α_i sobre $\mathbb{Q}[\alpha_1, ..., \alpha_{i-1}]$. Demuestre que $I = (f_1(x_1), f_2(x_1, x_2), ..., f_n(x_1, ..., x_n))$.

Indicación: Pruebe que $(f_1(x_1), f_2(x_1, x_2), ..., f_n(x_1, ..., x_n))$ es el núcleo del homomorfismo de evaluación en $(\alpha_1, ..., \alpha_n)$. Para uno de los contenidos, divida un polinomio g sucesivamente entre $f_n, ..., f_1$ teniendo en cuenta que f_i es mónico en x_i.

Demostración. Consideramos el homomorfismo de evaluación en $a = (a_1, \ldots, a_n)$:

$$\begin{aligned} \varphi_a : \mathbb{Q}[x_1, \ldots, x_n] &\longrightarrow \mathbb{Q}[a_1, \ldots, a_n] \\ f(x_1, \ldots, x_n) &\longmapsto f(a_1, \ldots, a_n) \end{aligned}$$

En primer lugar, vemos que $I \subseteq ker\varphi_a$ de manera directa pues $f(a) = 0, \forall f \in I$. Y por otro lado, $\varphi_a(1) = 1 \neq 0$ por lo que $ker\varphi_a \neq (1)$ y por ser I un ideal maximal entonces necesariamente $ker\varphi_a = I$. Tengamos en cuenta ahora que tenemos la siguiente sucesión de extensiones:

$$\mathbb{Q} \hookrightarrow \mathbb{Q}[a_1] \hookrightarrow \cdots \hookrightarrow \mathbb{Q}[a_1, \ldots, a_n]$$

Llamemos $J = \Big(f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\Big)$, observamos también de manera sencilla que:

- $f_1(a_1) = 0$ porque f_1 es el polinomio mínimo de a_1 sobre $\mathbb{Q}$ y por contención en las extensiones tenemos que se anula (no es el polinomio mínimo) en $\mathbb{Q}[a_1, \ldots, a_n]$ de modo que $\varphi(f_1) = 0$
- De manera análoga vemos que en general $f_i(a_1, \ldots, a_i) = 0, \forall i \in \{2, \ldots, n\}$.

Así hemos demostrado que $J \subseteq ker\varphi$.

HASTA AQUÍ QUE ES LA PRIMERA CONTENCIÓN ESTÁ BIEN

Para la inclusión $I \subseteq J$, tomamos un polinomio $g \in I$. Aplicamos divisiones sucesivas para expresar g en términos de los f_i y los residuos. En este contexto, asumimos que estamos en un escenario donde el algoritmo de la división es aplicable para reducir el grado de g con respecto a cada variable x_i mediante f_i. Esto lleva a una serie de expresiones: $g = q_n f_n + r_n$, donde $\deg_{x_n}(r_n) < \deg(f_n)$. Luego, $r_n = q_{n-1}f_{n-1} + r_{n-1}$, con $\deg_{x_{n-1}}(r_{n-1}) < \deg(f_{n-1})$, y así sucesivamente hasta $r_1 = q_1 f_1 + r_0$, donde r_0 es un elemento constante de $\mathbb{Q}$ (o del cuerpo base $\mathbb{K}$).

Dado que $g(\alpha) = 0$ y cada $f_i(\alpha) = 0$, al evaluar sucesivamente las expresiones en α, obtenemos $r_k(\alpha) = 0$ para todo k. En particular, $r_0(\alpha) = 0$. Como r_0 es una constante, esto implica que $r_0 = 0$.

Sustituyendo $r_0 = 0$ de vuelta en las ecuaciones, podemos expresar g como una combinación lineal de los f_i: $g = q_n f_n + r_n = q_n f_n + (q_{n-1}f_{n-1} + r_{n-1}) = \cdots = \sum_{i=1}^{n} q_i f_i$. Dado que $q_i \in \mathbb{K}[x_1, \ldots, x_n]$, esto demuestra que $g \in J$. Por lo tanto, $I \subseteq J$.

Considerando que la otra contención $J \subseteq I$ es trivial por la definición de J

■

Observación 6.4.1. Sabemos que la contracción de un ideal maximal es primo, pero hemos visto ejemplos de que esto falla para maximales. Veamos el caso de anillos de polinomios sobre $\mathbb{Q}$.

Ejercicio 6.4.4. Sea $\mathbb{Q}[x_1, ..., x_n] \subseteq \mathbb{Q}[x_1, ..., x_n, y_1, ..., y_m]$ anillos de polinomios. Demuestre que si Q es un ideal maximal de $\mathbb{Q}[x_1, ..., x_n, y_1, ..., y_m]$, entonces $Q^c = Q \cap \mathbb{Q}[x_1, ..., x_n]$ también es maximal en $\mathbb{Q}[x_1, ..., x_n]$.

Bibliografía

[1] Fernando. Etayo Gordejuela. *Apuntes de la asignatura: Teoría Global de Superficies*. Universidad de Cantabria. 2024-2025.

[2] J. Javier. Jiménez Garrido. *Notas del curso: Estructuras algebraicas*. Tercera edición. Universidad de Cantabria. 2023.

[3] Yifan Liu y Tianqi Liu. «Research and Application of Chinese Remainder Theorem». En: *ResearchGate* (2023). URL: https://www.researchgate.net/publication/375603865_Research_and_application_of_Chinese_remainder_theorem.

[4] Piotr Schwarz. «The Chinese Remainder Theorem, Its Proofs and Its Generalizations». En: *Silesian University of Technology, Institute of Informatics* (2009). URL: https://inf.ug.edu.pl/~schwarzw/papers/slgr09a.pdf.