Universidad de Valladolid

Facultad de Ciencias

Grado en matemáticas

TRABAJO DE FIN DE GRADO:

CÁLCULOS EFECTIVOS EN ÁLGEBRA CONMUTATIVA. NORMALIZACIÓN.

AUTOR:
Beatriz Jiménez Garmón
TUTOR:
Santiago Encinas Carrión

Julio 2024

Resumen

En el presente trabajo se estudia la normalización de Noether. Definiendo los conceptos de dependencia entera para anillos, explicaremos como se construye su clausura entera, así como la noción de anillo normal. Por último daremos un algoritmo para el cálculo de la normalización y el lugar geométrico no normal para un anillo. Además se presentarán unos ejemplos concretos para el cálculo de la normalización de una cúspide y del paraguas de Whitney.

Palabras clave

Dependencia entera.
Anillo noetheriano.
Anillo normal.
Clausura entera.
Normalización de un anillo.

Abstract

In this work we study the Noether normalization. Defining the concepts of integral dependence for rings, we will explain how its integral closure is constructed, as well as the notion of a normal ring. Finally we will give an algorithm for computing the normalization and the non-normal locus for a ring. In addition, some concrete examples will be presented for the computation of the normalization of a cusp and the Whitney umbrella.

Keywords

Integral dependence.
Normal ring.
Noetherian ring.
Integral closure.
Ring normalization.

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer a Santiago Encinas por su esfuerzo, sus correcciones y su ayuda a lo largo del trabajo que han hecho posibles esta memoria.

En segundo lugar, me gustaría agradecer a todos mis profesores, tanto universitarios como preuniversitarios, su contribución en mi formación con especial mención a Manuel, mi profesor del colegio, por su pasión por la matemáticas y por la forma que las imparte. Gracias a él, empece a admirar las matemáticas de una forma diferente y decidí comenzar esta carrera tan bonita.

En tercer lugar, me gustaría agradecer a todos mis compañeros con los que he tenido el placer de compartir mi etapa como estudiante, sobre todo este último año de Erasmus que era algo diferente.

Finalmente me gustaría agradecer a todos mis familiares, en especial a mis padres y mi hermano por todo su apoyo incondicional a lo largo de estos años.

Valladolid, 10 de Junio de 2024

Índice general

Capítulo 1

Introducción

El álgebra conmutativa es el campo de estudio de los anillos conmutativos, sus ideales, módulos y álgebras. Se considera que el fundador real de la materia, en la época en la que se llamaba *teoría de ideales* es David Hilbert, quien al parecer pensó sobre esta cuestión como un enfoque alternativo a la entonces de moda teoría de funciones complejas. El concepto adicional de módulo, presentado de alguna manera en el trabajo de Kronecker, es técnicamente un paso adelante si se compara con trabajar siempre directamente en el caso especial de los ideales. Este cambio se atribuye a la influencia de Emmy Noether. Hilbert influyó fuertemente en Emmy Noether, quien reformuló muchos resultados anteriores en términos de una condición de cadena ascendente, ahora conocida como la condición Noetheriana y los objetos que la satisfacen se denominan noetherianos en su honor.

En este trabajo vamos a centrarnos en el lema de normalización de Noether. Este lema se le atribuye a Emmy Noether, y fue presentado en el árticulo *Idealtheorie in Ringbereichen* (La teoría de ideales en los anillos) en 1921.
Haciendo un inciso, quiero darle especial importancia a Emmy Noether. Fue una matemática alemana del siglo XX y es considerada por David Hilbert, Albert Einstein y otros personajes relevantes como la mujer más importante en la historia de las matemáticas. Aunque también tuvo una importante aportación en el mundo de la física, con lo que cierne a las matemáticas, Noether transformó la teoría de ideales en los anillos conmutativos en una poderosa herramienta matemática con aplicaciones muy variadas. Revolucionó la teoría de anillos, teoría de cuerpos y la de K-álgebras.

Para entender la normalización de Noether desarrollaremos previamente conceptos como bases de Gröbner, cadenas, anillos noetherianos, elementos enteros, clausura entera... Todos ellos conceptos nuevos al no haber cursado

álgebra conmutativa durante el grado.

El segundo capítulo introducirá los conceptos previos para desarrollar la teoría de extensiones enteras. En particular las nociones de módulos y submódulos y algunas operaciones con ellos. Presentaremos el concepto de orden monomial para poder más tarde hablar de bases de Gröbner y bases estándar de ideales y módulos e introduciremos una primera versión del teorema de la base de Hilbert. Por último hablaremos de algunos ideales especiales como es el ideal cociente y el radical junto con algunas de sus propiedades.

En el capítulo siguiente hablaremos ya elementos enteros y de extensiones finitas y enteras junto con sus operaciones y equivalencias, como puede ser la propiedad de transitividad de la dependencia entera, el criterio sobre la dependencia entera, el criterio de finitud, compatibilidad con el paso a anillos cocientes. Presentaremos el teorema de Cayley Hamilton clave para algunas de las demostraciones de este capítulo. También introduciremos la clausura entera para anillos. Hablaremos de conjuntos multiplicativamente cerrados, cuerpos de fracciones y localización, todos ellos conceptos no estudiados durante el grado. Esto será relacionado con el concepto de anillo entero dando lugar a la propiedad de compatibilidad con la localización.

En el capítulo 4, retomaremos el concepto de clausura entera pero esta vez para ideales. Introduciremos las cadenas y las condiciones de cadenas ascendentes y descendentes para poder definir los anillos artinianos y noetherianos. Hablaremos del teorema del ascenso y del descenso para cadenas de ideales primos. Y nos centraremos más tarde en algunas proposiciones relacionadas con anillos noetherianos. Volveremos a presentar el teorema de Hilbert pero en vez de para anillos de polinomios, para anillos noetherianos en general. Y por último hablaremos de la normalización de un anillo, que es la clausura entera de A en el anillo total de fracciones de A, con una breve observación sobre lo que ocurre cuando A es un dominio de integridad, caso sobre el que basaremos nuestros ejemplos en el capítulo 7.

En el capítulo 5 daremos una breve introducción sobre la teoría de la dimensión, aunque este ámbito sea mucho más extenso de lo presentado en este capítulo con definiciones importantes como la dimensión de Krull. Se hablará de longitud de una cadena, altura de un ideal para definir la dimensión de un anillo y de un ideal e introduciremos la noción de anillo reducido.

En el capítulo 6 introduciremos la normalización de Noether para el caso de cuerpos finitos e infinitos y hablaremos también de anillos graduados.

En el último capítulo la idea principal es dar un algoritmo para calcular la normalización de un anillo. Haremos una breve introducción a los espectros, aunque se puede encontrar mucho más desarrollado en los apéndices del libro [4]. Introduciremos el lugar geométrico no normal, el conductor de un anillo A y daremos un criterio para la normalidad de un anillo. Se presentarán la sizigias (sin profundizar en estte concepto), que serán necesarias para el algoritmo de normalización. Por último se calculará la normalización de una cúspide y del paraguas de Whitney, este último también en SINGULAR un programa de ordenador para cálculos algebraicos.

Capítulo 2

Conceptos previos

En este capitulo, introduciremos conceptos básicos con los que trabajaremos constantemente durante esta memoria. Se presentarán los conceptos de módulos, submódulos y operaciones con ellos, la noción de finitamente generado y módulo libre. Además exponemos el concepto de orden monomial en general y orden total, para mas tarde definir orden modular. Por último explicaremos algunos conceptos como bases estándar y de Gröbner con sus propiedades.

2.1. Módulos y submódulos

Definición 2.1.1. Sea A un anillo. Sea un conjunto M, con dos operaciones $+ : M \times M \to M$ (suma) ,$\cdot : A \times M \to M$ (multiplicación por escalares) se dice que es un A-*modulo* si verifica las siguientes propiedades:

1. $(M, +)$ es un grupo abeliano
2. $(a + b) \cdot m = a \cdot m + b \cdot m$
   $a \cdot (m + n) = a \cdot m + a \cdot n$
   $(ab) \cdot m = a \cdot (b \cdot m)$
   $1 \cdot m = m$, para cada $\forall a, b \in A$ y $m, n \in M$

Veamos algunos ejemplos de A-módulos

Ejemplo 2.1.2.

1. Un ideal I de A es un A-módulo. En particular, el mismo A es un A-módulo
2. Si A es un cuerpo K, entonces un A-módulo es cualquier K-espacio vectorial

3. Si $A = \mathbb{Z}$ entonces un $\mathbb{Z}$-módulo es cualquier grupo abeliano. Pues por definición de $\mathbb{Z}$-módulo obviamente es un grupo abeliano, y para la implicación contraria bastaría definir la aplicación

$$\begin{array}{rccl} \cdot_{\mathbb{Z}}: & \mathbb{Z} \times G & \longrightarrow & G \\ & (n, g) & \longmapsto & ng = \underbrace{g + g + \ldots + g}_{\text{(n)}} \end{array}$$

Definición 2.1.3. Sean M, N dos A-módulos. Una aplicación $f : M \to N$ es un homomorfismo de A-módulos (o es A-lineal) si $f(x + y) = f(x) + f(y)$, $f(ax) = af(x)$ $\forall a \in A$

Si A es un cuerpo, un homomorfismo de A-módulo es lo mismo que una transformación lineal de espacios vectoriales.

Para cada módulo M existe un isomorfismo natural $Hom(A, M) \cong M$ cada homomorfismo de A-módulos $f : A \to M$ está unívocamente determinada por $f(1)$, que puede ser un elemento cualquiera de M.

Definición 2.1.4. Sea M un A-módulo. Un submódulo N de M es un subgrupo no vacío de M que es cerrado respecto al producto por elementos de A, es decir, para cada $m, n \in N$ y $a \in A$ verifica:

1. $m + n \in N$
2. $a \cdot m \in N$

Definición 2.1.5. Sea M un A-módulo y sea $\{M_i\}_{i \in I}$ una familia de submódulos de M. Su suma $\sum M_i$ es el conjunto de todas las sumas (finitas($\sum x_i$, donde $x_i \in M_i$ para todo, $i \in I$, y donde casi todas las x_i (todas salvo un numero finito) son cero.

$\sum M_i$ es el menor submódulo de M que contiene a todos los M_i

La intersección $\cap M_i$ es a su vez un submódulo de M.

No se puede, en general, definir el producto de dos submódulos pero se puede definir el producto $I \cdot M$, donde I es un ideal y M es un A-módulo. Se define como el conjunto de todas las sumas finitas $\sum a_i x_i$, con $a_i \in I, x_i \in M$, que es un submódulo de M.

Definición 2.1.6. Si N, P son submódulos de M, se define (N:P) como el conjunto de todos los $a \in A$ tales que $aP \subset N$, es un ideal de A.

En particular, (0:M) es el conjunto de todos los $a \in A$ tales que $aM = 0$, este ideal se denomina el anulador de M y se indica por $Ann(M)$.
Un A-módulo M es fiel si $Ann(M) = 0$.

Definición 2.1.7. Sea M un A-módulo y $M_i \subset M$ submódulos, con $i \in I$. Definimos la suma de los M_i como

$$\sum_{i\in I} M_i := \left\{ \sum_{i\in I} m_i \;\middle|\; m_i \in M_i, m_i \neq 0 \text{ solo para un numero fnito de i} \right\}$$

Definición 2.1.8. Sea $J \subset A$ un ideal y sea M un A-módulo. Definimos JM como

$$JM := \left\{ \sum_{i\in I} a_i m_i \;\middle|\; I \text{ finito},\ \ a_i \in J,\ \ m_i \in M \right\}$$

Definición 2.1.9. Se dice que un A-módulo M es finitamente generado si $M = \sum_{i=1}^{n} A \cdot m_i$ para $m_1, ..., m_n \in M$. Cuando esto ocurre escribimos $M = \langle m_1, \ldots, m_n \rangle$ y se dice que $m_1, \ldots, m_n$ son los generadores de M. Un módulo generado solo por un elemento se llama módulo cíclico.

Definición 2.1.10. Sea M un A-módulo. M se llamará módulo libre si $M \cong \bigoplus_{i\in I} A$.

2.2. Orden monomial

Un polinomio se puede representar de manera única, solo hasta un orden de sumandos, como combinación lineal de monomios. Sin embargo, podemos hacer que este orden sea único eligiendo un orden total en el conjunto de los monomios.

Definición 2.2.1. Un orden total u orden lineal en un conjunto X, es una relación binaria sobre X que es: reflexiva, transitiva, antisimétrica y total, esto es si se denota por $\leq$ la relación, para cualquier $a, b, c \in X$ se verifican las siguientes propiedades:

- Si $a \in X$, entonces $a \leq a$ (reflexiva)
- Si $a \leq b$ y $b \leq c$, entonces $a \leq c$ (transitiva)
- Si $a \leq b$ y $b \leq a$, entonces $a = b$ (antisimétrica)
- $a \leq b$ o $b \leq a$ (totalidad o completitud)

Esta última propiedad es equivalente a decir que todo par de elementos es comparable bajo la relación.
Un conjunto dotado de un orden total se denomina conjunto totalmente ordenado.

Definición 2.2.2. Un orden monomial es un orden total (o lineal) $>$ en el conjunto de los monomios $Mon_n = \{x^\alpha |\ \alpha \in \mathbb{N}^n\}$ en n variables que satisface

$$x^\alpha > x^\beta \Longrightarrow x^\gamma x^\alpha > x^\gamma x^\beta$$

para cada $\alpha, \beta, \gamma \in \mathbb{N}^n$.También decimos que $>$ que es un orden monomial en $A[x_1, \ldots, x_n]$, con A cualquier anillo, es decir que $>$ es un orden monomial en Mon_n

Definición 2.2.3. Sea $>$ un orden monomial fijado. Escribimos $f \in K[x], f \neq 0$, de una única forma como suma de termino no nulos

$$f = a_\alpha x^\alpha + a_\beta x^\beta + \cdots + a_\gamma x^\gamma, \quad x^\alpha > x^\beta > \cdots > x^\gamma,$$

y $a_\alpha, a_\beta, \cdots, a_\gamma \in K$. Definimos:

1. $\mathrm{LM}(f) := x^\alpha$ que llamaremos monomio líder.
2. $\mathrm{LE}(f) := \alpha$ que llamaremos exponente líder.
3. $\mathrm{LT}(f) := a_\alpha x^\alpha$ que llamaremos término líder.
4. $\mathrm{LC}(f) := a_\alpha$ que llamaremos coeficiente líder.
5. $tail(f) := f - a_\alpha x^\alpha = a_\beta x^\beta + \cdots + a_\gamma x^\gamma$ que llamaremos cola.

Definición 2.2.4. Sea $>$ un orden monomial en $\{x^\alpha |\ \alpha \in \mathbb{N}^n\}$

1. $>$ se dice que es un orden global si $x^\alpha > 1$ para todo $\alpha \neq (0, \ldots, 0)$,
2. $>$ se dice que es un orden local si $x^\alpha < 1$ para todo $\alpha \neq (0, \ldots, 0)$,
3. $>$ se dice que es un orden mixto si no es ni global ni local.

Proposición 2.2.5. *Sea $>$ un orden monomial, son equivalentes las siguientes condiciones:*

1. *$>$ está bien ordenado*
2. *$x_i > 1$ para $i = 1, \ldots, n$.*
3. *$x^\alpha > 1$ para cada $\alpha \neq (0, \ldots, 0)$, es decir, $>$ es global.*

4. $\alpha \geq_{nat} \beta$ *y* $\alpha \neq \beta$ *implica* $x^\alpha > x^\beta$. *La ultima condición significa que* $>$ *es un refinamiento del orden natural parcial en* $\mathbb{N}^n$ *definido por*

$$(\alpha_1, \ldots, \alpha_n) \geq_{nat} (\beta_1, \ldots, \beta_n) \Longleftrightarrow \alpha_i \geq \beta_i$$

para cada i

Demostración. (1)⇒(2): Si $x_i < 1$ para algún i, entonces $x_i^p < x_i^{p-1} < 1$, lo que produce un conjunto de monomios sin el elemento mas pequeño, lo cual lleva a una contradicción pues que suponíamos que está bien ordenado y por tanto cada subconjunto no vacío tiene un elemento más pequeño.
(2)⇒(3): Escribimos $x^\alpha = x^{\alpha'} x_j$ para algún j y usamos inducción.
(3)⇒(4): Sea $(\alpha_1, \ldots, \alpha_n) \geq_{nat} (\beta_1, \ldots, \beta_n)$ y $\alpha \neq \beta$. Entonces $\gamma := \alpha - \beta \in \mathbb{N}^n \setminus \{0\}$,tendríamos que $x^\gamma > 1$ y en consecuencia $x^\alpha = x^\beta x^\gamma > x^\beta$.
(4)⇒(1): Sea M un conjunto no vacío de monomios. Por el lema de Dickson que veremos en 2.2.11, existe un subconjunto finito $B \subset M$ tal que para casa $x^\alpha \in M$ hay un $x^\beta \in B$ con $\beta \geq_{nat} \alpha$. Asumiendo que $x^\beta < x^\alpha$ o $x^\beta = x^\alpha$, esto es que B contiene un elemento más pequeño de M con respecto a $>$, es decir que está bien ordenado como se quería.

□

Definición 2.2.6. Consideramos $>_1$ un orden monomial sobre $Mon(x_1, \ldots, x_n)$ y $>_2$ un orden monomial sobre $Mon(y_1, \ldots, y_m)$. Entonces el orden de productos o de bloques $>$. también se denota como $(>_1, >_2)$ sobre $Mon(x_1, \ldots, x_n, y_1, \ldots, y_m)$ se define como

$$x^\alpha y^\beta > x^{\alpha'} y^{\beta'} \Leftrightarrow x^\alpha >_1 x^{\alpha'} \text{ o } (x^\alpha = x^{\alpha'} \text{ y } y^\beta >_2 y^{\beta'}).$$

Si $>_1$ es un orden global, entonces el orden de productos cumple la propiedad que los monomios que contienen un x_i son siempre mayores que los monomios que no contienen x_i. Si los ordenes especiales $>_1$ sobre $Mon(x_1, \ldots, x_n)$ y $>_2$ sobre $Mon(y_1, \ldots, y_m)$ son irrelevantes, para el orden de productos sobre $Mon(x_1, \ldots, x_n, y_1, \ldots, y_m)$ escribiremos solamente $x \gg y$.

Definición 2.2.7. El orden lexicográfico es una relación de orden, definida sobre el producto cartesiano de conjuntos ordenados. Sean $(A, \leq_A)$ y $(B, \leq_B)$ dos conjuntos parcialmente ordenados por las relaciones $\leq_A$ y $\leq_B$ respectivamente. Entonces un orden lexicográfico es una relación de orden parcial $\leq_{A,B}$ definida como sigue :

$$\forall (a, b), (a', b') \in A \times B : (a, b) \leq_{A,B} (a', b') \Leftrightarrow a < a' \text{ o } a = a' \text{ y } b \leq b'$$

Si $(A, \leq_A)$ y $(B, \leq_B)$ son ordenes totales, $\leq_{A,B}$ también es un orden total.

Definición 2.2.8. Definimos el módulo libre $K[x]^r = \oplus_{i=1}^r K[x]e_i$ donde $e_i = (0, \ldots, 1, \ldots, 0) \in K[x]^r$ Llamamos $x^\alpha e_i = (0, \ldots, x^\alpha, \ldots, 0) \in K[x]^r$ un monomio

Definición 2.2.9. Sea $>$ un orden monomial:

1. Para $f \in K[x]_>$ elegimos $u \in K[x]$ tal que $\mathrm{LT}(u) = 1$ y $uf \in K[x]$. Definimos
$$\mathrm{LM}(f) := \mathrm{LM}(uf),$$
$$\mathrm{LC}(f) := \mathrm{LC}(uf),$$
$$\mathrm{LT}(f) := \mathrm{LT}(uf),$$
$$\mathrm{LE}(f) := \mathrm{LE}(uf),$$
y $tail(f) := f - \mathrm{LT}(f)$

2. Para cada subconjunto $G \subset K[x]_>$ se define el ideal
$$L_>(G) := L(G) := \langle \mathrm{LM}(g) \mid g \in G \setminus \{0\} \rangle_{K[x]}.$$
$L(G) \subset K[x]$ se llama ideal líder de G

Definición 2.2.10. Sea $I \subset R$ un ideal.

1. Un conjunto finito $G \subset R$ se llama base estándar de I si
$$G \subset I, \text{ y } L(I) = L(G).$$
Esto es que G es base estándar si el monomio líder de los elementos de G que generan el ideal líder de I.

2. Si $>$ es global, una base estándar se la llama base de Gröbner.

3. Si solamente decimos que G es una base estándar, nos referimos a que G es una base estándar del ideal $\langle G \rangle_R$ generado por G.

Introduciremos ahora un lema que sobre el que nos apoyaremos más adelante para demostrar algunos conceptos.

Lema 2.2.11. ***(Lema de Dickson)*** *Sea $I = \langle x^\alpha | \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$ un ideal monomial. Entonces I se puede escribir de la forma $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, donde $\alpha(1), \ldots, \alpha(s) \in A$. En particular, I tiene una base finita.*

La demostración de este lema se puede encontrar en el libro [2].

2.3. Bases de Gröbner y bases estándar para módulos

Trasladando las ideas que hemos expuesto anteriormente pero esta vez con un orden modular y módulos y submódulos, damos las definiciones de bases de Gröbner y bases estándar para módulos, que usaremos la mayor parte de las veces.

Definición 2.3.1. Sea $>$ un orden monomial en $K[x]$. Un orden modular en $K[x]^r$ es un orden total $>_m$ en el conjunto $\{x^\alpha e_i |\ \alpha \in \mathbb{N}^n, i = 1, \ldots, r\}$ que es compatible con la estructura $K[x]$-modular incluyendo el orden $>$, es decir, satisface

1. $x^\alpha e_i >_m x^\beta e_j \Longrightarrow x^{\alpha+\gamma} e_i >_m x^{\beta+\gamma} e_j$
2. $x^\alpha > x^\beta \Longrightarrow x^\alpha e_i >_m x^\beta e_j$ para cada $\alpha, \beta, \gamma \in \mathbb{N}^n, i, j = 1, \ldots, r$.

Si $x^\alpha e_i > x^\beta e_j \Longleftrightarrow i < j$ o $(i = j$ y $x^\alpha > x^\beta)$, donde se da prioridad a las componentes, y se denota por $(c, >)$.

Si $x^\alpha e_i > x^\beta e_j \Longleftrightarrow x^\alpha > x^\beta$ o $(x^\alpha = x^\beta$ y $i < j)$, donde se da prioridad a los monomios en $K[x]$ y se denota por$(>, c)$.

Se dice que $>_m$ está bien ordenado en $K[x]^r$ si y solo si $>$ lo es también en $K[x]$. Igualmente diremos que $>_m$ es global, local o mixto si lo es $>$.

Fijamos un orden modular $>_m$ y lo denotaremos por $>$. Como cualquier vector $f \in K[x]^r \setminus \{0\}$ se puede escribir de forma única como

$$f = cx^\alpha e_i + f^*$$

con $c \in K \setminus \{0\}$ y $x^\alpha e_i > x^{\alpha^*} e_j$ para cualquier termino no nulo $c^* x^{\alpha^*} e_j$ de f^* podemos definir como antes

$$\mathrm{LM}(f) := x^\alpha e_i$$

$$\mathrm{LC}(f) := c,$$

$$\mathrm{LT}(f) := cx^\alpha e_i$$

Podemos llamarlos monomio principal, coeficiente principal y término principal respectivamente de f. Y $tail(f) := f - \mathrm{LM}(f)$ se llama cola de f.
Además para $G \subset K[x]^r$ llamamos

$$L_>(G) := L(G) := \langle \mathrm{LM}(g) |\ g \in G \setminus \{0\} \rangle_{K[x]} \subset K[x]^r$$

el submódulo de $\langle G \rangle$ principal.

Definición 2.3.2.

1. Sea $I \subset R^r$ un submódulo. Un conjunto finito $G \subset I$ se llama bases estándar de I si y solo si $L(G) = L(I)$, en otras palabras, para cada $f \in I \setminus \{0\}$ existe un $g \in G$ tal que $\mathrm{LM}(g)|\mathrm{LM}(f)$.

2. Si el orden está bien ordenado entonces la base estándar G se llama base de Gröbner. En este caso $R = K[x]$ y por tanto, $G \subset I \subset K[x]^r$.

Daremos ahora una definición equivalente de base estándar y de Gröbner, que es más fácil de usar para la demostración del teorema de existencia de base de Gröbner.

Definición 2.3.3. Fijado un orden monomial en el anillo de polinomios $K[x_1, \ldots, x_n]$, un subconjunto finito $G = \{g_1, \ldots, g_t\}$ de un ideal $I \subset K[x_1, \ldots, x_n]$ diferente de $\{0\}$ se dice que es una base de Gröbner (o base estándar) si

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$$

Usando el convenio de que $\langle \emptyset \rangle = \{0\}$, definimos $\emptyset$ como la base de Gröbner de ideal cero $\{0\}$.

Introduciremos ahora un teorema muy importante, y cuya demostración nos servirá para construir una base de Gröbner. Más adelante volveremos a enunciarlo de otra forma relacionandolo con nuevos conceptos vistos.

Teorema 2.3.4. ***(Algoritmo de división en*** $K[x_1, \ldots, x_n]$***)*** *Sea* $>$ *un orden monomial sobre* $\mathbb{Z}^n_{\geq 0}$ *y sea* $F = (f_1, \ldots, f_s)$ *una s-upla de polinomios ordenada en* $K[x_1, \ldots, x_n]$*. Entonces todo* $f \in K[x_1, \ldots, x_n]$ *se puede escribir como*

$$f = q_1 f_1 + \ldots + q_s f_s + r,$$

donde $q_i, r \in K[x_1, \ldots, x_n]$ *y* $r = 0$ *o es una combinación lineal, con coeficientes en* K*, de monomios, ninguno de ellos es divisible por cualquier* $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$*.*
Llamaremos r *al resto de* f *al dividirlo por* F*.*

La demostración de este teorema se encuentra en el libro [2].

Teorema 2.3.5. ***(Teorema de la base de Hilbert)*** *Todo ideal* $I \subset K[x_1, \ldots, x_n]$ *tiene un conjunto finito que lo genera. En otras palabras,* $I = \langle g_1, \ldots, g_t \rangle$ *para algún* $g_1, \ldots, g_t \in I$*.*

Demostración. Si $I = \{0\}$ tomamos con el conjunto que lo genera a $\{0\}$, que obviamente es finito. Si I contiene algún polinomio distinto de cero, entonces el conjunto generador $g_1, \ldots, g_t$ para I se puede construir de la siguiente forma.
Primero seleccionamos un orden monomial particular para usar en el algoritmo de división descrito previamente y para calcular el término líder. Entonces I tiene un ideal formado por términos lideres $\langle \mathrm{LT}(I) \rangle$ y además sabemos que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ por el Lema de Dickson visto 2.2.11, que nos concluía que un ideal monomial está finitamente generado. Afirmamos que $I = \langle g_1, \ldots, g_t \rangle$.
Para probar esto, es claro que $\langle g_1, \ldots, g_t \rangle \subset I$ puesto que $g_i \in I$. Por otro lado, sea $f \in I$ un polinomio. Si aplicamos el algoritmo de división para dividir f por $(g_1, \ldots, g_t)$ obtenemos una expresión de la siguiente forma

$$f = q_1 g_1 + \ldots + q_t g_t + r$$

donde ningún término de r es divisible por ningún $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Podemos asegurar que $r = 0$.
Supongamos por reducción al absurdo que no lo fuera, tenemos

$$r = f - q_1 g_1 - \ldots - q_t g_t \in I$$

Si $r \neq 0$ entonces $\mathrm{LT}(r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, y entonces se sigue que $\mathrm{LT}(r)$ deberá ser divisible por algún $\mathrm{LT}(g_i)$, lo cual es una contradicción y por tanto $r = 0$.
Luego $f = q_1 g_1 + \ldots q_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle$, lo que demuestra la otra inclusión que queríamos $I \subset \langle g_1, \ldots, g_t \rangle$, y por tanto se da la igualdad. □

Corolario 2.3.6. *Fijado un orden monomial, todo ideal $I \subset K[x_1, \ldots, x_n]$ tiene una base de Gröbner. Es más, todo base de Gröbner para un ideal I, es base de I.*

Demostración. Dado un ideal no nulo, el conjunto $G = \{g_1, \ldots, g_t\}$ construido de la misma forma que en la demostración del teorema anterior, es po definición una base de Gröbner. Para lo segundo, notemos que si $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, entonces el argumento dado en el teorema anterior muestra que $I = \langle g_1, \ldots, g_t \rangle$, y por tanto G es una base de I. □

2.4. Algunos ideales especiales

Observación 2.4.1. Recordaremos brevemente las definiciones de ideal, ideal primo y de ideal maximal para que nos quede mas claro la demostración del siguiente lema.

Un subconjunto $I \in A$ se llama ideal si verifica las siguientes propiedades:

$$f, g \in I \Rightarrow f + g \in I$$

$$f \in I,\ a \in A \Rightarrow af \in I$$

Diremos que I es un ideal primo si $I \neq A$ y para cada $a, b \in A$ tal que $ab \in I$ entonces se debe cumplir que o bien $a \in I$ o bien $b \in I$.

Diremos que I es un ideal maximal si $I \neq A$ y si es maximal con respecto a la inclusión, es decir, que si I' es un ideal con $I' \subsetneq A$ y $I \subset I'$ entonces solo puede ser $I = I'$.

Observación 2.4.2. Recordaremos también esta definición muy básica.
Se dice que A es un dominio de integridad si $A \neq 0$ y si no tiene ningún divisor de cero.

Definición 2.4.3. Si I, J son ideales en el anillo A, su ideal cociente es

$$(I : J) = \{x \in A : xJ \subset I\}$$

que es un ideal.
En particular, $(0 : J)$ se denomina el anulador de J y se indica por $Ann(J)$ es el conjunto de todos los $x \in A$ tales que $xJ = 0$.
Con esta notación, el conjunto de todos los divisores de cero en A es $D = \cup_{x \neq 0} Ann(x)$.
Algunas propiedades son:

- $I \subset (I : J)$.
- $(I : J)J \subset I$.
- $((I : J) : L) = (I : JL) = ((I : L) : J)$.
- $(\cap_i I_i : J) = \cap_i (I_i : J)$.
- $(I : \sum_i J_i) = \sum_i (I : J_i)$.

Definición 2.4.4. Llamaremos nilradical de A al ideal $\mathcal{N}$ que es el conjunto formado por todos los elementos nilpotentes en un anillo A. Recordemos que un elemento $x \in A$ es nilpotente si $\exists n > 0$ con $x^n = 0$.

Proposición 2.4.5. *El nilradical de A es la intersección de todos los ideales primos de A.*

La demostración se puede encontrar en el libro [1].

Definición 2.4.6. Sea A un anillo y $I \subset A$ un ideal.
El radical de I, denotada como $\sqrt{I}$ o como $rad(I)$ es el ideal

$$\sqrt{I} = \{a \in A \mid \exists d \in \mathbb{N} \text{ tal que } a^d \in I\},$$

que contiene a I. Se dice que I es reducido o que es el ideal radical si $I = \sqrt{I}$.
Si $\varphi : A \to A/I$ es el homomorfismo canónico entonces $rad(I) = \varphi^{-1}(\mathcal{N}_{A/I})$ y como $\mathcal{N}_{A/I}$ es un ideal, tenemos que $rad(I)$ también lo es.
Algunas propiedades son:

- $I \subset rad(I)$.
- $rad(I) = rad(rad(I))$.
- $rad(IJ) = rad(I \cap J) = rad(I) \cap rad(J)$.
- $rad(I) = (1) \Leftrightarrow I = (1)$.
- $rad(I + J) = rad(rad(I) + rad(J))$.
- Si p es un ideal primo, $rad(p^n) = p \ \forall n > 0$.

Proposición 2.4.7. *El radical de un ideal I es la intersección de los ideales primos que contienen a I*

La demostración se encuentra en el libro [1].

Sea $f : A \to B$ un homomorfismo de anillos. Si I es un ideal de A, $f(I) = \{f(i) : i \in I\}$ no es necesariamente un ideal de B.

Definición 2.4.8. Se define la extensión I^e de I como el ideal $B \cdot f(I)$ generado por $f(I)$ en B. En forma mas explícita, se puede definir I^e como el conjunto de todas las sumas $\sum y_i f(x_i)$, donde $x_i \in I$ e $y_i \in B$.
Si J es un ideal de B, entonces $f^{-1}(J)$ es siempre un ideal de A, llamado la contracción J^c de J.
Probemos que es siempre un ideal. Sean $a, b \in f^{-1}(J)$ entonces $f(a), f(b) \in J$. Además $f(\lambda a + \mu b) = \lambda f(a) + \mu f(b) \in J \ \forall \lambda, \mu \in A$ luego $\lambda a + \mu b \in f^{-1}(J) \ \forall \lambda, \mu \in A$. Y por tanto se puede concluir que $f^{-1}(J)$ es un ideal.
Algunas propiedades son:

- $I \subset I^{ec}, J \supset J^{ce}$.
- $J^c = J^{cec}, I^e = I^{ece}$.

- Si C es el conjunto de los ideales contraídos en A y E es el conjunto de los ideales extendidos en B, entonces $C = \{I : I^{ec} = I\}$ y $E = \{J : J^{ce} = J\}$ y $I \to I^e$ es una aplicación biyectiva de C en E cuya inversa es $J \to J^c$.

Capítulo 3

Extensiones finitas y enteras

En este capítulo introduciremos las primeras definiciones básicas sobre elemento entero o extensiones finitas y enteras. Posteriormente se probarán algunas de las proposiciones más importantes relativas a estos conceptos como pueden ser el criterio de la dependencia entera o el criterio de finitud. Estos criterios permiten hacer cálculos efectivos para comprobar si un elemento es entero o si un morfismo es finito.

Definición 3.0.1. Sea $A \subset B$ anillos.

1. $b \in B$ se llama elemento entero sobre A si existe un polinomio mónico $f \in A[x]$ tal que $f(b) = 0$, es decir, b satisface una ecuación de grado p,
$$b^p + a_1 b^{p-1} + \cdots + a_p = 0,\ a_i \in A$$
para algún $p > 0$.
Esta idea ya la conocíamos, pues si se estuviese hablando sobre cuerpos en vez de anillos sería un elemento algebraico, puesto que la raíz de un polinomio es también la raíz de un polinomio mónico si se divide por el coeficiente principal.

2. B se dice que es entero sobre A o que es una extensión entera de A si para todo $b \in B$ es un elemento entero sobre A.
Al igual que antes podemos hacer el mismo comentario sobre cuerpos y sería una extensión algebraica

3. B se llama extensión finita de A si B es un A-módulo finitamente generado.

4. Si $\varphi : A \to B$ es un homomorfismo de anillos, entonces φ se llama extension entera si cumple para el subanillo $\varphi(A) \subset B$

Observación 3.0.2. Es evidente que cada elemento de A es un elemento entero sobre A, dado que si $a \in A$, entonces a es raíz del polinomio mónico $x - a$ con coeficientes en A.

Ejemplo 3.0.3. Sean $A = \mathbb{Z}$, $B = \mathbb{Q}$. Si un número racional $x = \frac{r}{s}$ es entero sobre $\mathbb{Z}$, donde r y s no tiene ningún factor común, se verifica que

$$\left(\frac{r}{s}\right)^n + a_1\left(\frac{r}{s}\right)^{n-1} + \ldots + a_{n-1}\left(\frac{r}{s}\right) + a_n = 0 \text{ con } a_i \in \mathbb{Z}\ \forall i.$$

Multiplicando la igualdad anterior por s^n:

$$r^n + a_1 r^{n-1}s + \ldots + a_{n-1}rs^{n-1} + a_n s^n = 0.$$

Despejando obtenemos: $r^n = -s(a_1 r^{n-1} + \ldots + a_{n-1}rs^{n-2} + a_n s^{n-1})$. Luego s divide a r^n y puesto que r y s no tienen ningún factor común, solo puede ser que $s = \pm 1$, es decir, $x = \pm r \in \mathbb{Z}$
Como veremos más adelante cuando demos la definición de forma formal, esto quiere decir que $\mathbb{Z}$ es íntegramente cerrado en $\mathbb{Q}$.

Introduciremos este teorema, puesto que este resultado se utilizará en la demostración de la siguiente proposición

Teorema 3.0.4. ***(Teorema Cayley-Hamilton, Determinantal trick)*** *Sea M un A-módulo generado por n elementos, es decir, finitamente generado y $\phi : M \to M$ un endomorfismo del A-módulo M. Supongamos que I es un ideal de A tal que $\phi(M) \subset IM$. Entonces, ϕ satisface una ecuación de la forma*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0 \ , \text{ donde } a_i \in I^i \ \forall i$$

Demostración. Sea $\{x_1, \cdots, x_n\}$ un conjunto de generadores de M. Puesto que $\phi(x_i) \in IM \ \forall i$, podemos escribir

$$\phi(m_i) = \sum_{j=1}^{n} a_{ij}x_j$$

con $a_{ij} \in I \ \ \leq i \leq n$. Es decir,

$$\sum_{j=1}^{n} \underbrace{(\phi\delta_{ij} - a_{ij}I)}_{\Delta_{ij}} x_j = 0 \quad \text{donde } \delta_{ij} \text{ es la delta de Kronecker.}$$

$$\underbrace{\begin{pmatrix} \phi - a_{11}Id & -a_{12}Id & \dots & -a_{1n}Id \\ -a_{12}Id & \phi - a_{22}Id & \dots & -a_{2n}Id \\ \vdots & & & \\ -a_{nn}Id & -a_{n2}Id & \dots & \phi - a_{nn}Id \end{pmatrix}}_{\Delta} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{3.0.4.1}$$

Multiplicando Δ por la izquierda por su adjunta $adj\Delta$, tenemos que

$$\begin{pmatrix} det\Delta & & \\ & \ddots & \\ & & det\Delta \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{3.0.4.2}$$

Resumiendo tendríamos, $det(\Delta)(x_i) = 0 \ \ \forall i \in \{1, \dots, n\}$ con $\{x_i\}_{i=1}^n$ que genera M, y en consecuencia $det(\Delta)$ es el endomorfismo cero de M.
Desarrollando el determinante, se obtiene una expresión de la forma:

$$\phi^n + a_1\phi^{n-1} + \dots + a_{n-1}\phi + a_nId$$

□

Esta proposición resume muy bien las relaciones que existen entre los nuevos conceptos introducidos previamente.

Proposición 3.0.5. *Las siguientes proposiciones son equivalentes:*

1. *$x \in B$ es entero sobre A.*
2. *$A[x]$ es un A-módulo con generación finita.*
3. *$A[x]$ está contenido en un subanillo C de B tal que C es un A-módulo con generación finita.*
4. *Existe un $A[x]$-módulo fiel M que es de generación finita como A-módulo.*

Observación 3.0.6. Aunque ya habíamos visto este concepto en la definición 2.1.6, recordemos que M es un $A[x]$-módulo fiel, si $p(x)M = 0 \Rightarrow p(x) = 0$ con $p(x) \in A[x]$.

Demostración. (1)⇒ (2). Si $x \in B$ es entero sobre A, se tiene que

$$x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0 \quad \text{con } a_i \in A \ \ \forall i$$

Entonces $x^n = -(a_1x^{n-1} + \ldots + a_{n-1}x + a_n)$, y multiplicando por x tenemos que $x^{n+1} = -(a_1x^n + \ldots + a_{n-1}x^2 + a_nx)$. Por tanto se deduce que $A[x]$ es un A-módulo generado por $\{1, x, \ldots, x^{n-1}\}$.
(2)⇒ (3). Basta tomar $C = A[x]$
(3)⇒ (4). Tomamos $M = C$, de manera que M es un A-módulo con generación finita, y además M es fiel. Si $p \in A[x]$, de $pM = 0$ con $1 \in M$ se deduce que $p1 = 0$, luego debe ser $p = 0$.
(4)⇒ (1). Consideramos

$$\begin{array}{rccc} \phi\colon & M & \longrightarrow & M \\ & m & \longmapsto & x\,m \end{array}$$

e $I = A$ de manera que $\phi(M) \subset AM$ y

$$\begin{array}{rccc} \phi^n\colon & M & \longrightarrow & M \\ & m & \longmapsto & x^n\,m \quad \forall n \in \mathbb{N} \end{array}$$

Utilizando el teorema anterior, se verifica que:

$$\phi^n + a_1\phi^{n-1} + \ldots + a_nI = 0 \quad \text{con } a_i \in A \ \forall i.$$

$\Rightarrow (\phi^n + a_1\phi^{n-1} + \ldots + a_nI)\, m = 0 \ \forall m \in M$ que es equivalente a $(x^n + a_1x^{n-1} + \ldots + a_n)\, m = 0$.
Tenemos que $(x^n + a_1x^{n-1} + \ldots + a_n)\, M = 0$ con M un A[x]-módulo fiel, por tanto usando la definición tenemos que $x^n + a_1x^{n-1} + \ldots + a_n = 0 \quad \text{con } a_i \in A \ \forall i$. En conclusión $x \in B$ es elemento entero sobre A. □

Este lema es básico y se usará constantemente a lo largo de este capítulo

Lema 3.0.7. *Si N es de generación finita como B-módulo y B es de generación finita como A-módulo, entonces N es de generación finita como A-módulo.*

Demostración. Sean $y_1, \ldots, y_n$ un sistema de generadores de N sobre B, y sean $x_1, \ldots, x_m$ un sistema de generadores de B como A-módulo. Consideramos $h \in N$ entonces $h = b_1y_1 + \ldots + b_ny_n$ donde cada $b_i \in B$; además $b_i = a_{i1}x_1 + \ldots + a_{im}x_m$ con $a_{ij} \in A$. Entonces $h = (a_{11}x_1 + \ldots + a_{1m}x_m)y_1 + \ldots + (a_{n1}x_1 + \ldots + a_{nm}x_m)y_n$; es decir que los mn productos x_iy_j generan N sobre A. Por tanto N es de generación finita como A-módulo. □

Corolario 3.0.8. *Sean x_i con $1 \leq i \leq n$ elementos de B, cada uno de ellos entero sobre A. Entonces el anillo $A[x_1, \ldots, x_n]$ es un A-módulo con generación finita.*

Demostración. Razonaremos por inducción sobre n. Para $n = 1$ es la implicación (1)⇒(2) de la proposición anterior. Supongamos ahora que se cumple para $n > 1$, y sea $A_r = A[x_1, \ldots, x_r]$ $\forall r \in \{1, \ldots, n\}$.
Por hipótesis de inducción, A_{n-1} es un A-módulo con generación finita. Por el caso $n = 1$, dado que x_n es entero sobre A_{n-1} (por se entero sobre A) se tiene que $A_n = A_{n-1}[x_n]$ es un A_{n-1}-módulo con generación finita.
Aplicando ahora el lema anterior tenemos que A_n es un A-módulo con generación finita que es lo que queríamos probar. □

Definición 3.0.9. Sea $f : A \to B$ un homomorfismo de anillos. Si $a \in A$ y $b \in B$, se define un producto

$$ab = f(a)b.$$

Esta definición de multiplicación escalar convierte el anillo B en un A-módulo. De esta forma B tiene estructura de A-módulo y de anillo, estas dos estructuras son compatibles. El anillo B dotado de esta estructura de A-módulo, se denomina A-álgebra. Así, un A-álgebra es por definición un anillo B junto con un homomorfismo de anillos $f : A \to B$.

Definición 3.0.10. Si $f : A \to B$ y $g : A \to C$ son dos homomorfismos de anillos, entonces un homomorfismo de A-álgebras $h : B \to C$ es un homomorfismo de anillos que también es un homomorfismo de A-módulos y que verifica $h \circ f = g$.
Un homomorfismo $f : A \to B$ es de tipo finito, y B es una A-álgebra con generación finita, si existe un homomorfismo de A-álgebras de un anillo de polinomios $A[t_1, \ldots, t_n]$ sobre B

Proposición 3.0.11. *Sean A, B anillos.*
Si $\varphi : A \to B$ es una extension finita, entonces es entera. Más generalmente, si $I \subset A$ es un ideal y M es un B-módulo finitamente generado, entonces cualquier $b \in B$ con $bM \subset IM$ cumple una relación

$$b^p + a_1 b^{p-1} + \cdots + a_p = 0,\ a_i \in I^i \subset A$$

Demostración.
Remplazando A por la imagen de A, podemos asumir que $A \subset B$. Cada $b \in B$ define un endomorfismo de $B \to B$, la multiplicación por b. Recordemos que B es un A-módulo finitamente generado, puesto que $A \to B$ es extensión finita. El polinomio característico de este endomorfismo define una relación entera para b, por el *Teorema de Cayley-Hamilton o "determinantal trick"*3.0.4. En términos más concretos, sean $b_1, \ldots, b_k$ un sistema de generadores de B como A-módulo. Entonces $b \cdot b_i = \sum_{j=1}^{k} a_{ij} b_j, 1 \leq i \leq k$, para un

apropiado $a_{ij} \in A$. Esto implica, llamando E_n a la matriz unidad de tamaño $n \times n$:

$$(b \cdot E_n - (a_{ij})) \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} = 0, \tag{3.0.11.1}$$

por tanto, usando la Regla de Crammer, $det(b \cdot E_n - (a_{ij})) \cdot b_i = 0$, para $i = 1, \ldots, k$. Pero, puesto que $1 = \sum_i e_i b_i \in B$ para adecuados $e_1, \ldots, e_k$, obtenemos $det(bE_n - (a_{ij})) = 0$, que es la ecuación que queríamos demostrar para b.
En el caso general, visto ya en 3.0.4, para un M cualquiera que sea un B-módulo finitamente generado y para $I \subset A$ ideal, sean $b_1, \ldots, b_k$ un sistema de generadores de M como A-módulo. Podemos elegir los a_{ij} de I y por tanto el coeficiente de b^{k-i} en $det(bE_n - (a_{ij}))$ es la suma de los menores $i \times i$ de (a_{ij}) y en consecuencia están contenidos en I^i.

□

Corolario 3.0.12. *Si x_1, $x_2 \in B$ son enteros sobre A, entonces $x_1 + x_2$ y $x_1 \cdot x_2$ son enteros sobre A.*

Demostración. Por el corolario 3.0.8, sabemos que en este caso $A[x_1, x_2]$ es un A-módulo finitamente generado. Puesto que $A[x_1 + x_2] \subset A[x_1, x_2]$ y $A[x_1 \cdot x_2] \subset A[x_1, x_2]$ usando (3)⇒(1) de la proposición 3.0.5 podemos concluir que $x_1 + x_2$ u $x_1 \cdot x_2$ son enteros sobre A. □

Definición 3.0.13. El conjunto $C = \{b \in B |\ b$ es entero sobre A$\}$ se denomina la clausura entera de A en B o el cierre entero de B en A.
Si $C = A$, se dice entonces que A es íntegramente cerrado en B.
Si $C = B$, el anillo B se dice que es entero sobre A.

Observación 3.0.14. Mas adelante en el capítulo 4, cuando definamos la clausura para ideales, en vez de poner solo C escribiremos $C(A, B)$

Corolario 3.0.15. *El conjunto C de elementos de B que son enteros sobre A es un subanillo de B que contiene a A.*

Demostración. La idea es unir dos corolarios precedentes y sería una consecuencia directa. Sin embargo daremos la demostración para que quede claro. Si $x, y \in C$ entonces $A[x, y]$ es un A-módulo finitamente generado por el corolario 3.0.8. Por tanto $x \pm y$ y $x \cdot y$ son enteros sobre A como ya demostramos en el corolario 3.0.12, es decir, $x \pm y, x \cdot y \in C$. Y con esto se prueba

lo que queríamos, pues por definición C es subanillo de B, y obviamente C contiene A pues como ya dijimos en la observación 3.0.2 todo elemento de A es también entero sobre A y como $A \subset B$ se verifica lo que pedíamos. □

Corolario 3.0.16. ***(Transitividad de la dependencia entera)*** *Si $A \subset B \subset C$ son anillos y si B es entero sobre A y C es entero sobre B, entonces C es entero sobre A*

Demostración. Sea $x \in C$. Entonces se tiene una ecuación $x^n + b_1 x^{n-1} + \ldots + b_n = 0$, con $b_i \in B$ para cada $i \in \{1, \ldots, n\}$.
El anillo $B' = A[b_1, \ldots, b_n]$ es un A-módulo con generación finita y en virtud del corolario 3.0.8, gracias a que B es entero sobre A. Además de la relación anterior se sigue que x es entero sobre B', y en consecuencia, $B'[x]$ es un B'-módulo con generación finita.
Aplicando ahora el lema 3.0.7 mencionado anteriormente se tiene que $B'[x]$ es un A-módulo con generación finita, y aplicando (3)⇒(1) de la proposición 3.0.5 (gracias a que $A[x] \subset B'[x]$) podemos concluir que x es entero sobre A. □

Corolario 3.0.17. *Sean $A \subset B$ anillos y sea C la clausura entera de A en B. Entonces C es íntegramente cerrado en B.*

Demostración. $C = \{x \in B |\ x$ es entero sobre A$\}$
Queremos probar que C coincide con su clausura entera en B, es decir, que $C = \{x \in B |\ x$ es entero sobre C$\}$
$\boxed{\subseteq}$ Esta contención es trivial.
$\boxed{\supseteq}$ Sea $x \in B$ entero sobre C. Como C es entero sobre A, del corolario 3.0.16 se deduce que x es entero sobre A, y por tanto, $x \in C$ □

Una vez introducidos estos nuevos conceptos, nos centraremos en los resultados más importantes.

Proposición 3.0.18. ***(Criterio sobre la dependencia entera)*** *Sean $b, f_1, \ldots, f_k \in K[x], I = \langle g_1, \ldots, g_s \rangle \subset K[x]$ un ideal y nuevas variables $t, y_1, \ldots, y_k$. Consideramos el ideal*

$$M = \langle t - b, y_1 - f_1, \ldots, y_k - f_k, g_1, \ldots, g_s \rangle \subset K[x_1, \ldots, x_n, t, y_1, \ldots, y_k] \ .$$

Sea $>$ un orden en $K[x, t, y]$ con $x \gg t \gg y$, y sea G una base estándar de M con respecto a ese orden.
Entonces b es entero sobre $K[f] = K[f_1, \ldots, f_k]$ mod I si y solo si G contiene un elemento g con monomio principal $\mathrm{LM}(g) = t^p$ para algún $p > 0$. Es más, cualquier g de este tipo define una relación entera para b sobre $K[f]$ mod I.

Observación 3.0.19. Recordemos que $\gg$ se definió en 2.2.6.

Demostración. Si $\mathrm{LM}(g) = t^p$ entonces g debe ser de la forma

$$g(t,y) = a_0 t^p + a_1(y)t^{p-1} + \ldots + a_p(y) \in K[t,y], \;\; a_0 \in K \setminus \{0\}.$$

Supongamos que $a_0 = 1$. Puesto que $g \in M$, tendríamos que $y - f \in M$, $t - b \in M$ por definición del ideal, junto con $g(t,y) \in M$ tenemos que $g(b,f) \in I$. Luego, g define una relación entera para b sobre $K[f]$ *mod* I.
Por el contrario, si b es entero, entonces existe $g \in K[t,y]$ como se indicó anteriormente. Usando la fórmula de Taylor para polinomios en varias variables, recordemos que si queremos el desarrollo de orden 1 en el punto (b,f) la fórmula tendría la siguiente forma

$$g(t,y) = g(b,f) + \frac{\partial g(b,f)}{\partial t}(t-b) + \sum_{i=1}^{k} \frac{\partial g(b,f)}{\partial y_i}(y_i - f_i)$$

y si denotamos por $b_0 = \frac{\partial g(b,f)}{\partial t}$ y $b_i = \frac{\partial g(b,f)}{\partial y_i}$ obtendríamos la expresión $g(t,y) = g(b,f) + b_0 \cdot (t-b) + \sum_{i=1}^{k} b_i \cdot (y_i - f_i)$ para algunos $b_i \in K[t,y]$, $i = 0, \ldots, k$. Por tanto, $g \in M$ y $t^p = \mathrm{LM}(g) \in L(M)$. Como G es una base estándar, t^p es divisible por el monomio principal de algún elemento de G con lo que se concluye el resultado.

□

Observación 3.0.20. Recordaremos que en 2.2.7 habíamos ya definido el orden lexicográfico, este orden será importante en la próxima proposición.

Proposición 3.0.21. ***(criterio de finitud)***
Sea K un cuerpo, y sean $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_m)$ dos conjuntos de variables. Además, sea $I \subset K[x]$, $J = \langle h_1, \ldots, h_s \rangle \subset K[y]$ ideales y $\varphi : K[x]/I \to K[y]/J$ un homomorfismo, definido como $\varphi(x_i) := f_i$. Definamos

$$M := \langle x_1 - f_1, \ldots x_n - f_n, h_1, \ldots, h_s \rangle \subset K[x,y],$$

y sea $>$ un orden de bloques en $K[x,y]$ tal que $>$ es orden lexicográfico para $y, y_1 > \ldots > y_m$ y $y \gg x$. Sea $G = \{g_1, \ldots, g_t\}$ una base estándar de M con respecto a este orden.
Entonces φ es finito si y solo si para cada $j \in \{1, \ldots, m\}$ existe algún $g \in G$ tal que $\mathrm{LM}(g) = y_j^{\nu_j}$ para algún $\nu_j > 0$.

Demostración. Si $g_{s_j} = y_j^{\nu_j} + \sum_{\nu=0}^{\nu_j - 1} a_{j\nu}(x, y_{j+1}, \ldots, y_m) \cdot y_j^{\nu} \in M$ se tiene que

$$g_{s_j}|_{x=f} := g_{s_j}(f_1(y), \ldots, f_n(y), y_{j+1}, \ldots, y_m) \in J$$

para $j = 1, \ldots, m$ y donde $\{s_1, \ldots, s_m\} = \{1, \ldots, m\}$. Por tanto, y_m mod J es entero sobre $K[x]/I$. Usando la inducción y la transitividad entera, obtenemos que y_j mod J es entero sobre $K[x]/I$ y en consecuencia, $K[y]/J$ es finito sobre $K[x]/I$ por la proposición 3.0.11 (2).
Para demostrar ahora la implicación contraria, usaremos que la finitud de φ garantiza otra vez por la proposición 3.0.11, una relación entera de la forma

$$g = y_j^{\nu_j} + \sum_{\nu=0}^{\nu_j - 1} a_{j\nu}(f_1(y), \ldots, f_n(y)) \cdot y_j^{\nu} \in J \quad \text{para apropiados } a_{j\nu} \in K[x].$$

Usando ahora la fórmula de Taylor, si obtenemos el desarrollo de g de orden 1 en f obtendríamos una fórmula del tipo

$$g = g(f) + \sum_{i=1}^{n} \frac{\partial g(f)}{\partial x_i}(x_i - f_i)$$

es decir, un desarrollo con términos que pertenecen al ideal M y por tanto como se probó en la demostración de la proposición 3.0.18 obtenemos

$$y_j^{\nu_j} + \sum_{\nu=0}^{\nu_j - 1} a_{j\nu}(x_1, \ldots, x_n) \cdot y_j^{\nu} \in M,$$

y , entonces el monomio principal, $y_j^{\nu_j}$, es un elemento de L(M). □

Lema 3.0.22. *Sea $\varphi : A \to B$ un homomorfismo de anillos.*

1. *Si $P \subset B$ es un ideal primo, entonces $\varphi^{-1}(P) \subset A$ es un ideal primo.*
2. *Si φ es una extensión entera, y si $\varphi(x)$ es una unidad en B, entonces $\varphi(x)$ es también una unidad en el anillo $\varphi(A)$.*
3. *Sea φ una extensión entera, B es dominio de integridad. Entonces B es un cuerpo si y solo si $A/Ker(\varphi)$ es un cuerpo.*
4. *Si φ es una extensión entera y $M \subset B$ es un ideal maximal, entonces φ^{-1} es un ideal maximal en A.*

Para un homomorfismo de anillos $\varphi : A \to B$ y un ideal $I \subset B$, el ideal $\varphi^{-1} \subset A$ se llama contracción de I. Para $A \subset B$ la contracción de I es $I \cap A$.

Demostración. (1) Sean $a, a' \in A$ tal que $aa' \in \varphi^{-1}(P)$. Es decir, $\varphi(aa') \in P$. Puesto que φ es un homomorfismo de anillos, por definición se tiene que $\varphi(aa') = \varphi(a)\varphi(a')$. Y por tanto $\varphi(a)\varphi(a') \in P$. Ahora usaremos que P es

un ideal primo en B, luego $\varphi(a)$ o $\varphi(a')$ pertenece a P, es decir que a o a' pertenecen a $\varphi^{-1}(P)$ que es la definición de ideal primo. En conclusión, $\varphi^{-1}(P)$ es un ideal primo contenido en A.
(2) Para probar esto, sea $\varphi(x) \cdot y = 1$ para algún $y \in B$. Puesto que B es entero sobre A, podemos elegir $a_0, \ldots, a_{n-1} \in A$ tal que

$$y^n + \varphi(a_{n-1})y^{n-1} + \ldots + \varphi(a_0) = 0.$$

Multiplicando por $\varphi(x)^{n-1}$ obtenemos

$$y = y^n\varphi(x)^{n-1} = -\varphi(a_{n-1} + a_{n-2}x + \ldots + a_0x^{n-1}) \in \varphi(A).$$

(3) es una consecuencia de (2). Para la probar que si $A/Ker(\varphi)$ es un cuerpo, entonces B es cuerpo basta elegir una relación integral como en (2) de grado mínimo y usas que B es entero. La implicación contraria se verifica pues el cociente es isomorfo a la imagen de φ, por la primera versión del teorema de isomorfía, y también sabemos que la imagen es un subanillo de B, que a la vez por hipótesis es cuerpo.
(4) es una consecuencia de (3) ya que $A/\varphi^{-1}(M) \subset B/M$ es otra vez una extensión entera. □

3.1. Conjuntos multiplicativamente cerrados y cuerpos de fracciones

Definición 3.1.1. Si A es un dominio de integridad, la construcción del cuerpo de fracciones de A consiste en tomar todos los pares ordenados (a, s) donde $a, s \in A$ y $s \neq 0$ y establecer una relación de equivalencia entre estos pares: $(a, s) \sim (b, t) \Leftrightarrow at - bs = 0$
Sea A un anillo. Un subconjunto multiplicativamente cerrado de A es un subconjunto S de A tal que $1 \in S$ y S es cerrado respecto a la multiplicación: $s, s' \in S \Rightarrow s \cdot s' \in S$.
Se define una relación de equivalencia $\sim$ en $A \times S$ como sigue:

$$(a, s) \sim (b, t) \Leftrightarrow \exists u \in S \text{ tal que } (at - bs)u = 0$$

- $\sim$ es reflexiva.
- $\sim$ es simétrica.
- $\sim$ es transitiva: Supongamos que $(a, s) \sim (a', s')$ y que $(a', s') \sim (a'', s'')$. Entonces existen $t, t' \in S$ tales que $(as' - a's)t = 0$ y $(a's'' - a''s')t' = 0$

Tenemos $as't = a'st$ y multiplicando por t' obtenemos la siguiente igualdad $as'tt' = a'stt'$. Ahora multiplicando por s'' tendríamos $as'tt's'' = a'stt's'' = a's''t'st = a''s't'st$. Sacando factor común en la igualdad llegamos a $as''(s'tt') = a''s(s'tt')$ con $s'tt' \in S$ porque S es multiplicativamente cerrado. Luego llegamos a que $(a, s) \sim (a'', s'')$.

Así se tiene una relación de equivalencia. Se indica por $\frac{a}{s}$ la clase de equivalencia de (a, s), y sea $S^{-1}A$ el conjunto de las clases de equivalencia. Se da un estructura de anillo a $S^{-1}A$ definiendo una suma y un producto de estas "fracciones" $\frac{a}{s}$ de la misma manera que en álgebra elemental:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Se tiene también un homomorfismo de anillos

$$\begin{array}{rccc} f\colon & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & \frac{a}{1} \end{array}$$

que no es inyectivo en general.

Observación 3.1.2. Si A es un dominio de integridad y $S = A \setminus \{0\}$, entonces $S^{-1}A = Fr(A)$ es el cuerpo de fracciones de A. En este caso

$$\frac{a}{s} = \frac{a'}{s'} \Leftrightarrow \exists t \neq 0 \text{ tal que } t(as' - a's) = 0$$

y puesto que A es un dominio, usando la definición tenemos que tendría que $as' - a's = 0$.

Definición 3.1.3. El anillo $S^{-1}A$ se denomina el anillo de fracciones de A con respecto a S.

Definición 3.1.4. Sea p un ideal primo de A. Entonces $S = A \setminus p$ es multiplicativamente cerrado.

Proposición 3.1.5. *$A \setminus p$ es multiplicativamente cerrado $\Leftrightarrow$ p es primo.*

Demostración. $\boxed{\Rightarrow}$ Recordemos que en 2.4.1 ya revisamos la definición de ideal primo. Sean $x, y \in A$ tal que $x \cdot y \in p$. Veamos que $x \in p$ o $y \in p$. Supongamos que $x \cdot y \in p$ entonces $x \cdot y \notin A \setminus p$ y como $A \setminus p$ es multiplicativamente cerrado, si por absurdo suponemos que $x \in A \setminus p$ y que $y \in A \setminus p$ por definición $x \cdot y \in A \setminus p$ lo que conduce a un absurdo. Por tanto se tiene $x \notin A \setminus p$ o $y \notin A \setminus p$. Luego $x \in p$ o $y \in p$ y por tanto p es primo por definición.

$\boxed{\Leftarrow}$ Supongamos que $x, y \in A \setminus p$, veamos que $x \cdot y \in A \setminus p$. Tenemos entonces $x, y \notin p$ y puesto que p es primo esto implica que $x \cdot y \notin p$ pues si no fuese así se debería dar $x \in p$ o $y \in p$, en contra de lo que habíamos supuesto. Por tanto, dado que obviamente $x \cdot y \in A$ se tiene $x \cdot y \in A \setminus p$ y en conclusión $A \setminus p$ es multiplicativamente cerrado.

En este caso denotamos $A_p = S^{-1}A$
Los elementos $\frac{a}{s}$ con $a \in p$ forman el ideal $p \cdot A_p$ en A_p.
El proceso de pasar de A a A_p se denomina localización en p. □

3.2. Extensión y contracción de ideales en anillos de fracciones

Sea A un anillo y S un subconjunto multiplicativamente cerrado de A y $f : A \to S^{-1}A$ el homomorfismo natural definido por $f(a) = \frac{a}{a}$. Sea C el conjunto de todos los ideales contraídos en A y sea E el conjunto de todos los ideales extendidos en $S^{-1}A$. Si I es un ideal de A, su extensión I^e en $S^{-1}A$ es $S^{-1}I$ (pues cada $y \in I^e$ es de la forma $\sum \frac{a_i}{s_i}$ donde $a_i \in I$ y $s_i \in S$; reduciendo estas fracciones a común denominador).
Introduciremos esta proposición a la que más tarde haremos referencia al usarla en la proposición 4.1.17, sin embargo, no la demostraremos pues se acabaría extendiendo mucho esta sección. La demostración se puede encontrar en el libro [1].

Proposición 3.2.1.

1. *Cada ideal en $S^{-1}A$ es un ideal extendido.*
2. *Si I es un ideal en A, entonces $I^{ec} = \cup_{s \in S}(I : s)$. Por tanto, $I^e = (1) \Leftrightarrow I$ interseca S, es decir que $S \cap I \neq \emptyset$.*
3. *$I \in C \Leftrightarrow$ ningún elemento de S es divisor de cero en A/I.*
4. *Los ideales primos de $S^{-1}A$ están en correspondencia biyectiva con los ideales primos de A que no cortan S*

Introduciremos algunos lemas y definiciones nuevas que se usaran durante la demostración de la próxima proposición, un resultado también muy destacable de este capítulo.

Lema 3.2.2. ***(Compatibilidad con el paso a anillos cocientes)*** *Si $I \subset B$ es un ideal y B es entero sobre A, entonces B/I es entero sobre $A/(I \cap A)$*

Demostración. Sea $x \in B$ con $\overline{x} \in B/I$. Como B es entero sobre A, se tiene $x^n + a_1x^{n-1} + \ldots + a_n = 0$ con $a_i \in A \ \forall i$. Si reducimos esta ecuación módulo I, se tiene que

$$\overline{x}^n + \overline{a_1}\,\overline{x}^{n-1} + \ldots + \overline{a_n} = 0 \text{ con } \overline{a_i} \in A/(I \cap A)$$

Por tanto, $\overline{x}$ es entero sobre $A/(I \cap A)$. □

Lema 3.2.3. ***(Compatibiliadad con la localización)*** *Si S es una parte multiplicativamente cerrada en A y B es entero sobre A, entonces $S^{-1}B$ es entero sobre $S^{-1}A$.*

Demostración. Sea $\frac{x}{s} \in S^{-1}B$, con $x \in B$ y $s \in S$. Si dividimos la relación de dependencia entera de x sobre A entre s^n, obtenemos

$$\left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{r}{x}\right)^{n-1} + \ldots + \frac{a_n}{s^n} = 0 \ \text{ con } \frac{a_i}{s^i} \in S^{-1}A \ \forall i.$$

En consecuencia, $\frac{x}{s}$ es entero sobre $S^{-1}A$. □

Definición 3.2.4. Un anillo A se dice que es local si tiene exactamente un ideal maximal m. A/m se llama cuerpo residual de (A, m). Anillos con un número finito de ideales maximales se llaman semi-locales. Denotamos a los anillos locales por (A, m) o (A, m, K) donde $K = A/m$.

Capítulo 4

Clausura entera

Definición 4.0.1. Sea $A \subset B$ una extension de anillos. Sea $I \subset A$ un ideal. Llamaremos clausura entera débil de I sobre B al conjunto de elementos pertenecientes a B que son enteros sobre I.

$$C(I, B) = \{b \in B \mid b \text{ entero sobre } I\}$$

Si además, los coeficientes del polinomio para el cual el elemento es raíz cumplen que $a_i \in I^i$, decimos que b es un elemento entero fuerte sobre I y podemos definir

$$C_s(I, B) = \{b \in B \mid b \text{ elemento entero fuerte sobre } I\}$$

La clausura entera fuerte de I sobre B.

Observación 4.0.2. Recordemos que ya habíamos definido una clausura entera en 3.0.13 cuando $I = A$

4.1. Anillos Noetherianos y condiciones de cadena

Antes de presentar las proposiciones y teoremas de este capítulo, necesitamos conocer las nociones básicas de anillos noetherianos y sus propiedades. Estas ideas serán totalmente nuevas puesto que no he cursado álgebra conmutativa.

Proposición 4.1.1. *Sea A un conjunto parcialmente ordenado por una relación $\leq$. Las siguientes condiciones en A son equivalentes:*

1. *Cada sucesión creciente*

$$x_1 \leq x_2 \leq x_3 \leq \ldots \leq x_k \leq \ldots$$

en A es estacionaria, esto es, que existe algún j_0 tal que $x_j = x_{j_0}$ para todo $j \geq j_0$.

2. *Cada conjunto no vacío en A tiene un elemento maximal.*

Demostración. (1)⇒(2) Supongamos que existe un conjunto no vacío B en A que no tiene elemento maximal. Sea $x_1 \in B$, con x_1 no maximal, luego existe $x_2 \in B$ tal que $x_1 < x_2$. Puesto que por hipótesis x_2 tampoco es maximal, existirá $x_3 \in B$ tal que $x_2 < x_3$.
Así construimos una sucesión $x_1 < x_2 < x_3 < \ldots < x_n < \ldots$ en B tal que $x_n \neq x_{n+1}$, $\forall n$, lo que va en contra de (1).
(2)⇒(1) Dada una sucesión $x_1 \leq x_2 \leq \ldots$ en A. Sea $B = \{x_n\}_{n\geq 1}$. En virtud de (2), B tiene un elemento maximal. Sea x_{n_0} dicho elemento, entonces $x_n \leq x_{n_0} \forall n$ y $x_{n_0} \leq x_m \forall m \geq n_0$, lo que implica que $x_n = x_{n_0} \forall n \geq n_0$. Lo que prueba que la sucesión de partida es estacionaria. □

Definición 4.1.2. Si A es el conjunto de submódulos de un módulo M, ordenado por la relación de inclusión; es decir, $A_1 \subset A_2 \subset \ldots \subset A_n \subset \ldots$ entonces (1) se denomina la condición de cadena ascendente (c.c.a) y (2) la condición maximal. Un módulo M que satisface una de estas dos condiciones equivalentes se denomina noetheriano.
Si A esta ordenado por $\supseteq$; es decir, $A_1 \supset A_2 \supset \ldots \supset A_n \supset \ldots$ entonces (1) es la condición de cadena descendente (c.c.d) y (2) la condición minimal. Un módulo M que satisface estas condiciones se denomina artiniano.

Un anillo A se dice que es noetheriano, si lo es como un A-módulo, es decir, si satisface c.c.a en ideales.

Ejemplo 4.1.3.

- Un grupo finito (como $\mathbb{Z}$-módulo) satisface a la vez c.c.a y c.c.d .
- El anillo $\mathbb{Z}$ (como $\mathbb{Z}$-módulo) satisface c.c.a:
  Sea $I_1 \subset I_2 \subset \ldots$ una cadena de ideales de $\mathbb{Z}$. Como $\mathbb{Z}$ es un dominio de ideales principales podemos escribir la cadena como $(n_1) \subset (n_2) \subset \ldots$.
  Si la cadena no es estacionaria, existe una subcadena $(n_{11}) \subsetneq (n_{12}) \subsetneq (n_{13}) \subsetneq \ldots$. Por tanto, podemos suponer $(n_1) \subsetneq (n_2) \subsetneq (n_3) \subsetneq \ldots$.
  Si $n_1 = p_1^{r_1} \ldots p_s^{r_s}$ y denotamos $k = \sum_{i=1}^{s} r_i$, tras k pasos tendremos que $n_k = 1$ y por tanto $(n_k) = (n_{k+1}) = (n_{k+2}) = \ldots$ y la sucesión es estacionaria. En consecuencia $\mathbb{Z}$ es noetheriano.

- Por la versión del teorema de la base de Hilbert que demostraremos más adelante 4.1.19, A noetheriano $\Rightarrow A[x]$ noetheriano. Como K es noetheriano (sus únicos ideales son (0) y (1)), tenemos que $K[x_1, \ldots, x_n]$ es noetheriano.
- El anillo de polinomios $K[x_1, \ldots, x_n, \ldots]$ en un número infinito de indeterminadas x_n no satisface ninguna condición de cadena en los ideales. $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \ldots$ no es estacionaria y por tanto no es anillo noetheriano.

Los teoremas importantes "going up" o del ascenso y "lying over" o del descenso tambien tienen una versión para cadenas de ideales primos.

Proposición 4.1.4. *Sea $A \subset B$ dominios de integridad, B entero sobre A. Entonces B es un cuerpo si y solo si A es un cuerpo.*

Demostración. Supongamos que A es un cuerpo. Sea $y \in B$, $y \neq 0$. Sea

$$y^n + a_1 y^{n-1} + \ldots + a_n = 0 \quad (a_i \in A)$$

una ecuación de dependencia entera para y de menor grado posible. Puesto que B es un dominio de integridad tenemos que $a_n \neq 0$, y entonces $y^{-1} = -a_n^{-1}(y^{n-1} + a_1 y^{n-2} + \ldots + a_{n-1}) \in B$. Y por tanto llegamos a que B es un cuerpo.
Para la implicación contraria, supongamos ahora que B es un cuerpo. Sea $x \in A$, $x \neq 0$. Entonces $x^{-1} \in B$, luego es entero sobre A y tendremos la siguiente ecuación

$$x^{-m} + a'_1 x^{-m+1} + \ldots + a'_m = 0 \quad (a'_i \in A).$$

De donde se sigue que $x^{-1} = -(a'_1 + a'_2 x + \ldots a'_m x^{m-1}) \in A$, y por tanto A es un cuerpo. □

Proposición 4.1.5. *Sean $A \subset B$ anillos, B entero sobre A; sea q un ideal primo de B y sea $p = q \cap A$. Entonces q es maximal si y solo si p es maximal.*

Demostración. Por 3.2.2 sabemos que B/p es entero sobre A/p, y ambos anillos son dominios de integridad. Ahora usando 4.1.4 podemos concluir, puesto que sabemos que es equivalente que B/q sea cuerpo a que $q \subset B$ sea un ideal maximal. □

Teorema 4.1.6. *Sea $A \subseteq B$ anillo, con B entero A; y sea p un ideal primo de A. Entonces existe un ideal primo q de B tal que $q \cap A = p$.*

Demostración. Por 3.2.2 sabemos que B_p es entero sobre A_p, y el diagrama

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A_p & \longrightarrow & B_p \end{array}$$

(en el cual las lineas horizontales son aplicaciones inyectivas) es conmutativo. Sea n un ideal maximal de B_p, entonces $m = n \cap A_p$ es maximal por 4.1.5, y por tanto es el único ideal maximal de anillo local A_p. Si $q = \beta^{-1}(n)$, entonces q es primo y tendremos $q \cap A = \alpha^{-1}(m) = p$.

□

Teorema 4.1.7. ***(Going up o del ascenso)*** *Sean $A \subset B$ anillos, con B entero sobre A. Sea $p_1 \subseteq \ldots \subseteq p_n$ una cadena de ideales primos de A y sea $q_1 \subseteq \ldots \subseteq q_m$,con $m < n$,una cadena de ideales primos de B tales que $q_i \cap A = p_i \;\; 1 \leq i \leq m$. Entonces la cadena $q_1 \subseteq \ldots \subseteq q_m$ se puede extender a una cadena $q_1 \subseteq \ldots \subseteq q_n$ tal que $q_i \cap A = p_i \;\; 1 \leq i \leq n$*

Demostración. Por inducción, podemos limitarnos solo al caso $m = 1, n = 2$. Sea $\overline{A} = A/p_1, \overline{B} = B/q_1$; entonces $\overline{A} \subseteq \overline{B}$, y $\overline{B}$ es entero sobre $\overline{A}$ por el lema 3.2.2. Entonces usando el teorema anterior, sabemos que existe un ideal primo $\overline{q}_2$ de B tal que $\overline{q}_2 \cap \overline{A} = \overline{p}_2$, la imagen de $\overline{p}_2$ en $\overline{A}$. Llevando de vuelta $\overline{q}_2$ a B, tenemos ahora q_2 un ideal primo con las propiedades que queríamos. Si tenemos ahora $q_1 \subseteq \ldots \subseteq q_m$ y $p_1 \subseteq \ldots \subseteq p_m \subseteq p_{m+1} \subseteq \ldots \subseteq p_n$, tomando entonces $B' = B/q_{m-1}$ y $A' = A/p_{m-1}$ y aplicando sucesivamente el caso anterior habremos terminado. □

Ahora daremos la versión del teorema lying over o del descenso, sin embargo debemos introducir algún lema para que resulte más fácil la demostración.

Lema 4.1.8. *Sea C el cierre entero de A en B y sea I^e la extensión de I en C. Entonces el cierre entero de I en B es el radical de I^e (y por tanto es cerrado respecto a la adición y la multiplicación).*

Demostración. Queremos ver que

$$\sqrt{I^c} = \{ \text{ elementos de B que son enteros sobre I } \}$$

$\boxed{\supseteq}$ Si $x \in B$ es entero sobre I, se tiene una ecuación de la forma $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, con $a_1, \ldots, a_n \in I$.
Como I es un ideal de A, se tiene que x es entero sobre A. Luego $x \in C$ y además $x^n \in I^e$ ya que $x^n = -(a_1 x^{n-1} + \ldots + a_n)$. Entonces $x \in \sqrt{I^e}$.

$\boxed{\subseteq}$ Sea $x \in \sqrt{I^e}$. Entonces existe $n > 0$ tal que $x^n = \sum a_i x_i$ donde $a_i \in I$ y $x_i \in C$ para cada i.
Puesto que cada x_i es entero sobre A, del corolario 3.0.8 se deduce que $M = A[x_1, \ldots, x_n]$ es un A-módulo con generación finita. También se tiene que $x^n M \subseteq IM$.
Si aplicamos ahora el teorema 3.0.4, tomando ϕ como la multiplicación por x^n se ve que x^n es entero sobre I, y por tanto x es entero sobre I. □

Proposición 4.1.9. *Sean $A \subset B$ dominios de integridad, A íntegramente cerrado y sea $x \in B$ entero sobre un ideal I de A. Entonces x es algebraico sobre el cuerpo de fracciones K de A, y si su polinomio mínimo es $t^n + a_1 t^{n-1} + \ldots + a_n$ entonces $a_1, \ldots, a_n \in \sqrt{I}$.*

Demostración. Es claro que x es algebraico sobre K.
Sea L un cuerpo de extensión de K que contiene todos los conjugados $x_1, \ldots, x_n$ de cada x. Cada x_i satisface la misma ecuación de dependencia entera que x, luego cada x_i es entero sobre I. Los coeficientes del polinomio mínimo de x sobre K son polinomios en x_i, y como el cierre entero de I en B es cerrado respecto a la adición y la multiplicación en virtud del lema anterior, resulta que estos coeficientes también son enteros sobre I.
Puesto que A es íntegramente cerrado, aplicando el lema anterior con $C = A$ podemos concluir que dichos coeficientes pertenecen a $\sqrt{I}$ □

Teorema 4.1.10. ***(Lying over o del descenso)*** *Sean $A \subset B$ dominios de integridad, A íntegramente cerrado y B entero sobre A. Sea $p_1 \supseteq \ldots \supseteq p_n$ una cadena de ideales primos de A, y sea $q_1 \supset \ldots \supseteq q_m$,con $m < n$, una cadena de ideales primos de B tales que $q_i \cap A = p_i \;\; 1 \leq i \leq m$. Entonces la cadena $q_1 \supset \ldots \supseteq q_m$ puede extenderse a una cadena $q_1 \supset \ldots \supseteq q_n$ tal que $q_i \cap A = p_i \;\; 1 \leq i \leq n$*

Para demostración de este teorema la idea es la misma que en 4.1.7, es decir, limitarnos al caso $m = 1, n = 2$ para más tarde razonar por inducción. Queremos probar que p_2 es la contracción de un ideal primo de B_{q_1}, o equivalentemente que $(p_2 B_{q_1}) \cap A = p_2$.
$\boxed{\supseteq}$ Cierto siempre.

$\boxed{\subseteq}$ Sea $x \in (p_2 B_{q_1}) \cap A$, entonces $\frac{x}{1} = \frac{y}{s}$ con $y \in p_2 B$ y $s \notin q_1$, es decir, $s \in B \setminus q_1$
Veamos que y no solo es entero sobre A sino que es entero sobre p_2.
$y \in p_2 B$ luego $y = pb$ con $p \in p_2$ y $b \in B$. b es entero sobre A y se cumple que $b^n + a_1 b^{n-1} + \ldots + a_n = 0$ con $a_i \in A \;\; \forall i$.

Multiplicando la ecuación anterior por p^n

$$(pb)^n + \underbrace{a_1 p}_{\in p_2}(bp)^{n-1} + \ldots \underbrace{a_n p^n}_{\in p_2} = 0,$$

luego $y = pb$ es entero sobre p_2.
Aplicando la proposición anterior tenemos que y es algebraico sobre $Fr(A) = K$ (el cuerpo de fracciones de A) y su ecuación mínima es de la forma $y^r + u_1 y^{r-1} + \ldots + u_r = 0$ con $u_1, \ldots, u_r \in \sqrt{p_2} = p_2$.
Dividiendo la ecuación anterior entre x^r

$$\left(\frac{y}{r}\right)^r + \frac{u_1}{x}\left(\frac{y}{x}\right)^{r-1} + \ldots + \frac{u_r}{x^r} = 0$$

$$s^r + \frac{u_1}{x}s^{r-1} + \ldots + \frac{u_r}{x^r} = 0,$$

lo que nos proporciona una ecuación mínima para s sobre K. Podemos reescribir esta ecuación como $s^r + v_1 s^{r-1} + \ldots + v_r = 0$ con $v_i = \frac{u_i}{x^i}$ para cada i. s es entero sobre A, luego aplicando la proposición anterior con $I = (1)$ tenemos que $v_i \in A \ \forall i$.
$u_i = \underbrace{v_i}_{\in A} x^i \in p_2$ y como p_2 es primo, tenemos dos opciones:

- Si $x \in p_2$ ya estaría.
- Si $x \notin p_2$, entonces $v_i \in p_2 \ \forall i$, luego $s^r \in p_2 B \subseteq p_1 B \subseteq q_1$ lo cual es absurdo.

Proposición 4.1.11. *M es un A-módulo noetheriano $\Leftrightarrow$ Cada submódulo de M es de generación finita.*

Demostración.
$\boxed{\Rightarrow}$ Sea N un submódulo de M. Sea $\Sigma' := \{$ submódulos de N finitamente generados$\}$. $\Sigma' \neq \emptyset$ porque $(0) \in \Sigma'$. Como M es noetheriano, Σ' tiene un elemento maximal N_0, si $N_0 \neq N$, $\exists x \in N$ tal que $x \notin N_0$. Definimos $N_1 = N_0 + Ax$, que es un submódulo de N. N_1 es de generación finita y $N_0 \subsetneq N_1$, lo cual es absurdo. Por tanto $N = N_0$ es de generación finita.
$\boxed{\Leftarrow}$ Sea $M_1 \subset M_2 \subset M_3 \subset \ldots$ una cadena de submódulos de M. Sea $M_0 = \cup_{i \geq 1} M_i$ que es un submódulo de M y por tanto de generación finita. $M_0 = \langle m_1, \ldots, m_r \rangle$. Si $m_i \in M_{n_i}$ para cada $i \in \{1, \ldots, r\}$, entonces para casa $n \geq sup\{n_i : 1 \leq i \leq r\}$ se tiene que $M_0 \subset M_n$.
Como, además, $M_n \subset M_0 \ \forall n \in \mathbb{N}$ podemos concluir que $M_0 = M_n$ para cada $n \geq sup\{n_i : 1 \leq i \leq r\}$ y por tanto la cadena es estacionaria. $\square$

Ejemplo 4.1.12.

- Un cuerpo es a la vez noetheriano y artiniano.
- Un DIP es noetheriano (cada ideal es de generación finita).
- $K[x_1, x_2 \dots]$ no es noetheriano, pero es un dominio de integridad y por lo tanto tiene un cuerpo de fracciones. Así, un subanillo de un anillo noetheriano no es necesariamente noetheriano.

Estas dos proposiciones no las demostraremos pues se necesita algún resultado previo pero podemos encontrar su demostración en

Proposición 4.1.13. *Sea A un anillo noetheriano, M un A-módulo finitamente generado. Entonces M es noetheriano.*

Proposición 4.1.14. *Sea A un anillo noetheriano, I un ideal de A. Entonces A/I es un anillo noetheriano.*

Corolario 4.1.15. *Si A es noetheriano y $\varphi : A \to B$ es un homomorfismo sobreyectivo, entonces B es noetheriano.*

Demostración. Tenemos que $B \cong A/Ker\varphi$ pues es un homomorfismo sobreyectivo, y puesto que A es noetheriano y $Ker\varphi$ es un ideal, podemos aplicar la proposición anterior. Concluimos que B es un anillo noetheriano. □

Corolario 4.1.16. *Sea A un subanillo de B. Se supone que A es noetheriano y que B es de generación finita como A-módulo. Entonces B es noetheriano (como anillo).*

Demostración. Por la proposición 4.1.13, sabemos que B es noetheriano como A-módulo. Veamos que B es un anillo noetheriano probando que cada ideal en B es de generación finita.
Sea I un ideal de B. Entonces I es un subconjunto de B que es un subgrupo aditivo y es cerrado para el producto por elementos de B. Como $A \subset B$, I es también cerrado para el producto por elementos de A, y por tanto un A-submódulo de B. I es de generación finita porque B es noetheriano como A-módulo. En consecuencia, B es un anillo noetheriano. □

Proposición 4.1.17. *Si A es noetheriano y S es un subconjunto cualquiera multiplicativamente cerrado de A, entonces $S^{-1}A$ es noetheriano.*

Demostración. Lo demostraremos de dos formas diferentes para que quede más claro.
1) Sea J un ideal de $S^{-1}A$. Por la proposición 3.2.1 sabemos que todo ideal

de $S^{-1}A$ es un ideal extendido, luego $J = IS^{-1}A$, donde I es un ideal de A. Como A es noetheriano, I es finitamente generado $I = \langle a_1, \ldots, a_n \rangle$. Entonces vamos a ver que si $IS^{-1}A = \langle \frac{a_1}{a}, \ldots, \frac{a_n}{1} \rangle$, y por tanto J es finitamente generado lo cual implica que $S^{-1}A$ es noetheriano.
Sea $\frac{a}{s} \in IS^{-1}A$, de manera que $a \in I$ y por tanto $a = \lambda_1 a_1 + \ldots + \lambda_n a_n$ con $\lambda_i \in A$.

$$\frac{a}{s} = \frac{\lambda_1 a_1 + \ldots + \lambda_n a_n}{s} = \frac{\lambda_1}{s}\frac{a_1}{1} + \ldots + \frac{\lambda_n}{s}\frac{a_n}{1}, \quad \text{donde } \frac{\lambda_i}{s} \in S^{-1}A \ \forall i.$$

$\frac{a}{s} \in \langle \frac{a_1}{a}, \ldots, \frac{a_n}{1} \rangle$ y por tanto $IS^{-1}A \subset \langle \frac{a_1}{a}, \ldots, \frac{a_n}{1} \rangle$.
La otra contención es trivial y podemos concluir la igualdad.
2) Sea $J_1 \subset J_2 \subset \ldots \subset J_n \subset \ldots$ una cadena de ideales de $S^{-1}A$. Por la proposición 3.2.1, todos estos son ideales extendidos $J_i = I_i^e$, donde I_i es un ideal de A. Además por las propiedades vistas de extensión y contracción de ideales, estos ideales están en correspondencia biyectiva que conserva el orden con los ideales I_i^{ec} de A, lo que da lugar a una cadena $I_1^{ec} \subset I_2^{ec} \subset \ldots \subset I_n^{ec} \subset \ldots$ de ideales de A. Como A es noetheriano, $\exists\, n_0 \,/\, I_n^{ec} = I_{n+1}^{ec} \ \forall n \geq n_0$. Por tanto, $J_n = I_n^e = I_n^{ece} = I_{n+1}^{ece} = I_{n+1}^e = J_{n+1} \ \forall n \geq n_0$. Luego $S^{-1}A$ es noetheriano. □

Corolario 4.1.18. *Si A es noetheriano y p es un ideal primo de A, entonces A_p es noetheriano.*

Ahora daremos otro enunciado para este teorema tan importante para el álgebra conmutativa que ya habíamos visto en 2.3.5 y otra demostración similar con otra notación, aunque al fin y al cabo estamos probando lo mismo. La diferencia es que en el anterior lo hemos probado para A siendo un anillo de polinomios.

Teorema 4.1.19. ***(Teorema de la base de Hilbert)*** *Si A es un anillo noetheriano entonces el anillo de polinomios $A[x_1, \ldots, x_n]$ es noetheriano.*

Demostración. Necesitamos demostrar el teorema solo para $n = 1$, pues el caso general se sigue por inducción.
Razonaremos por reducción al absurdo. Supongamos que existe un ideal $I \subset A[x]$ que no es finitamente generado. Elijamos polinomios

$$f_1 \in I, \ \ , f_2 \in I \setminus \langle f_1 \rangle, \ldots, \ \ f_{k+1} \in I \setminus \langle f_1, \ldots, f_k \rangle, \ \ \ldots$$

del mínimo grado posible. Si $d_i = deg(f_i)$,

$$f_i = a_i x^{d_i} + \text{ terminos menores de x },$$

entonces $d_1 \leq d_2 \leq \ldots$ y $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \ldots$ es una cadena ascendente de ideales en A. Sabemos que es estacionaria, puesto que A es noetheriano, esto es que $\langle a_1, \ldots, a_k \rangle = \langle a_1, \ldots, a_{k+1} \rangle$ para algún k, por tanto $a_{k+1} = \sum_{i=1}^{k} b_i a_i$ para apropiados $b_i \in A$. Consideramos el polinomio

$$g = f_{k+1} - \sum_{i=1}^{k} b_i x^{d_{k+1}-d_i} f_i = a_{k+1} x^{d_{k+1}} - \sum_{i=1}^{k} b_i a_i x^{d_{k+1}} + \text{ terminos más pequeños } .$$

Puesto que $f_{k+1} \in I \setminus \langle f_1, \ldots, f_k \rangle$, se sigue que $g \notin \langle f_1, \ldots, f_k \rangle$ y $g \in I$ es un polinomio de grado menor que d_{k+1} lo cual es una contradicción por la elección de f_{k+1}. □

Observación 4.1.20. También es cierto que A noetheriano implica que $A[[x]]$ es noetheriano. La demostración es análoga a la del teorema anterior, excepto que se emplea con los términos de menor grados en las series de potencias que pertenecen a I. Y en consecuencia también se tiene que si A es noetheriano, $A[[x_1, x_2, \ldots, x_n]]$ es noetheriano. Para probar estos veamos que $A[[x_1]][[x_2]] = A[[x_1, x_2]]$ y se tendría por inducción. La primera contención es obvia, así que probaremos la implicación contraria. Sea $\sum_{i_1,i_2} \lambda_{i_1,i_2} x^{i_1} x^{i_2} \in K[[x_1, x_2]]$. Desarrollando tenemos $\sum_{i_1,i_2} \lambda_{i_1,i_2} x^{i_1} x^{i_2} = \lambda_{00} + (\lambda_{10} x_1 + \lambda_{01} x_2) + \ldots + (\sum_{i_1+i_2=n} \lambda_{i_1 i_2} x^{i_1} x^{i_2}) + \ldots = (\lambda_{00} + \lambda_{10} x_1 + \lambda_{20} x_1^2 + \ldots + \lambda_{n0} x_1^n + \ldots) + (\lambda_{01} + \lambda_{11} x_1 + \ldots + \lambda_{n1} x_1^n + \ldots) x_2 + \ldots = \sum_{m \geq 0} (\sum_{m \geq 0} \lambda_{mn} x_1^m) x_2^n \in K[[x_1]][[x_2]]$.

Proposición 4.1.21. *Sea A un anillo noetheriano, $A \subset B$ extensión de anillos y $I \subset A$ un ideal. Además, sea $S \subset A$ una parte multiplicativamente cerrada. Entonces:*

1. *$C(A, B)$ es un subanillo de B conteniendo a A y $C(I, B)$ es un $C(A, B)$-ideal.*
2. *$S^{-1}C(A, B) = C(S^{-1}A, S^{-1}B)$.*
3. *$IC(A, B) \subset C_s(I, B) \subset C(I, B) = \sqrt{IC(A, B)}$.*

Demostración. (1) En verdad lo primero ya se demostró en 3.0.15. El segundo resultado se sigue de la expresión de $C(I, B)$ en (3).
(2) Sea $\frac{b}{s} \in S^{-1}B$ entero sobre $S^{-1}A$. Entonces se tiene una ecuación de la forma:

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s_1}\left(\frac{b}{s}\right)^{n-1} + \ldots + \frac{a_n}{s_n} = 0 \text{ con } s_i \in S,\ a_i \in A\ \forall i.$$

Sea $t := \prod_i s_i \in S$ y multiplicando la ecuación previa por $(ts)^n$, obtenemos

$$t^n b^n + a_1 s s_1^{n-1}(s_2 \dots s_n)^n b^{n-1} + \dots + a_n s^n s_n^{n-1}(s_1 \dots s_{n-1})^n = 0$$

$$(tb)^n + \frac{a_1}{s_1} \cdot s \cdot t \cdot (bt)^{n-1} + \dots + \frac{a_n}{s_n}(ts)^n = 0, \text{ donde } \frac{a_i}{s_i}(st)^i \in A \text{ para cada } i \in \{1, \dots, n\}$$

Entonces hemos obtenido una ecuación de dependencia entera para $bt \in B$ luego es entero sobre A, eso es que $bt \in C(A, B)$ y por tanto $\frac{b}{s} = \frac{b \cdot t}{s \cdot t} \in S^{-1}C(A, B)$.
Para la otra inclusión, como $C(A, B) \subset B$ es entero sobre A, por el lema 3.2.3, $S^{-1}C(A, B) \subset S^{-1}B$ es entero sobre $S^{-1}A$.
(3) Sea $x \in IC(A, B)$ entonces por la Proposición 3.0.11 aplicada a $A \subset C(A, B)$ implica que $x \in C_s(I, B)$, y por tanto $IC(A, B) \subset C_s(I, B)$. Si $x \in \sqrt{IC(A, B)}$, tenemos que $x^n \in IC(A, B)$ para algún n, luego $x^n \in C_s(I, B)$ lo que implica obviamente que $x \in C(I, B)$. Por el contrario, sea $x \in C(I, B)$ y $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$, $a_i \in I$. Entonces $x \in C(A, B)$ y en consecuencia, $x^n = -\sum_{\nu=0}^{n-1} a_\nu x^\nu \in IC(A, B)$. Lo que implica que $C(I, B) \subset \sqrt{IC(A, B)}$ como se quería probar. □

La proposición muestra que el $C(A, B)$-ideal $C(I, B)$ se puede computar si $C(A, B)$ es computable, puesto que el radical es computable. Este es el caso si $B = Q(A)$ es el anillo total de fracciones de A.
La clausura integral fuerte $C_s(I, B)$ es de gran interés cuando $B = A$. En este caso tenemos $I \subset C_s(I, A) \subset C(I, A) = \sqrt{I}$. En particular, si $I = \sqrt{I}$ entonces $I = C_s(I, A)$.

Definición 4.1.22. Sea A un anillo reducido. La clausura entera $\overline{A}$ de A es la clausura entera de A en el anillo total de fracciones $Q(A)$, tal que,

$$\overline{A} = C(A, Q(A)).$$

$\overline{A}$ también se llama normalización de A. A se dice que es íntegramente cerrado, o normal si $A = \overline{A}$.

Definición 4.1.23. En particular si A es un dominio de integridad y sea $Q(A)$ su cuerpo de fracciones, la normalización de A en $Q(A)$ se llama simplemente la normalización de A. Si A coincide con su normalización, se dice que A es un dominio normal.Es decir, un dominio de integridad se dice que es íntegramente cerrado (sin otra especificación) si es íntegramente cerrado en su cuerpo de fracciones.

Por ejemplo, como vimos anteriormente $\mathbb{Z}$ es íntegramente cerrado. El mismo razonamiento muestra que cada dominio de factorización única es

íntegramente cerrado. En particular, un anillo de polinomios $K[x_1, \ldots, x_n]$ sobre un cuerpo y cualquier cuerpo (coincide con su cuerpo de fracciones) son íntegramente cerrados.

Proposición 4.1.24. *Sea A un anillo noetheriano, las siguientes condiciones son equivalentes:*

1. *A es normal.*
2. *A_P es normal para todo ideal primo $P \subset A$.*
3. *A_M es normal para todo ideal maximal $M \subset A$.*

Demostración. Por la Proposición 4.1.21 se tiene que (1) implica (2). Que (2) implica (3) es obvio, pues sabemos que un ideal maximal es también un ideal primo (el recíproco no es siempre cierto). Para probar que (3) implica (1), sea $C := C(A, Q(A))$. Por hipótesis y por la proposición 4.1.21, tenemos $A_M = C_M$ para todos los ideales maximales $M \subset A$.
Supongamos que $C \supsetneq A$ y sea $c \in C \setminus A$. Definimos $I := \{s \in A | cs \in A\}$ que es un ideal propio en A. Existe un ideal maximal $M \subset A$ tal que $I \subset M$. Pero $A_M = C_M$ y en consecuencia existe un $s \in A \setminus M$ tal que $sc \in A$. Pero esto es una contradicción por la definición de I y la elección de M. □

Lema 4.1.25. *Sea A un anillo noetheriano y $A \subset B$ es íntegramente cerrado, entonces $A[x] \subset B[x]$ es íntegramente cerrado.*

Demostración. Sea $f \in B[x]$ entero sobre $A[x]$, es decir que pertenece a la clausura entera $C(A[x], B[x])$. Por definición para ver que $A[x]$ es íntegramente cerrado en $B[x]$, basta probar que $C(A[x], B[x]) = A[x]$. Obviamente como vimos en 3.0.15 se tiene que $A[x] \subset C(A[x], B[x])$. Por tanto solo falta probar la otra inclusión para demostrar la igualdad, y por tanto que es íntegramente cerrado. Para esto último usaremos inducción sobre $n := deg(f)$ para probar que $f \in A[x]$. Primero de todo, definimos $M := A[x][f]$ que un $A[x]$-módulo finitamente generado. Sea $M_0 \subset B$ el A-módulo generado por todos los coeficientes de las potencias de x para todos los elementos de M, considerados como elementos de $B[x]$. M_0 es un A-módulo finitamente generado (generado por los coeficientes de $1, f, \ldots f^{m-1}$ si $f^m + \sum_{\nu=0}^{m-1} a_\nu f^\nu = 0, \ \ a_\nu \in A[x]$).
Si $f = \sum_{\nu=0}^{n} b_\nu x^\nu, \ \ b_n \neq 0$, entonces $A[b_n] \subset M_0$ es un A-módulo finito. Esto implica que b_n es entero sobre A, y por tanto $b_n \in A$. Ahora $g := f - b_n x^n$ es entero sobre $A[x]$. Si $n = 1$ esto implica que b_0 es entero y asumimos que $b_0 \in A$. En este caso, obtenemos $f \in A[x]$. Si $n > 1$ entonces $g \in A[x]$ por hipótesis de inducción y otra vez $f \in A[x]$. □

Ejemplo 4.1.26. Sea K un cuerpo, entonces el anillo de polinomios $K[x_1, \ldots, x_n]$ es normal

Demostración. Lo probaremos por inducción en n. Para $n = 1$, sean $f, g \in K[x_1]$ tal que $mcd(f, g) = 1$. Consideramos un relación entera para f/g,

$$\left(\frac{f}{g}\right)^m + a_{m-1}\left(\frac{f}{g}\right)^{m-1} + \ldots + a_0 = 0 \text{ con } a_i \in K[x_1]\ \forall i.$$

Esto implica que $g|f^m$ lo que contradice que $mcd(f, g) = 1$. Para el siguiente paso de la inducción usaremos el lema 4.1.25. Para $n > 1$, obtenemos por hipótesis de inducción que $K[x_1, \ldots, x_{n-1}] \subset K(x_1, \ldots, x_{n-1})$ es íntegramente cerrado y por tanto por el lema, $K[x_1, \ldots, x_n] \subset K(x_1, \ldots, x_{n-1})[x_n]$ es íntegramente cerrado. El caso $n = 1$ muestra que $K(x_1, \ldots, x_{n-1})[x_n] \subset K(x_1, \ldots, x_n)$ es íntegramente cerrado. El resultado sigue de la transitividad de la dependencia entera 3.0.16. □

Definición 4.1.27. El cuerpo de escisión de un polinomio $p(x)$ sobre un cuerpo K, es una extensión L de K sobre el cual p se factoriza en factores lineales

$$p(x) = c\prod_{i=1}^{degp}(x - a_i)$$

donde $c \in K$ y para cada i tenemos que $x - a_i \in L[x]$ con a_i no necesariamente distintos y tal que las raíces a_i generan L sobre K. Y no hay otro cuerpo más pequeño donde p se factorice como antes, es decir, es minimal.

Lema 4.1.28. *Sea $A \subset B$ un extensión de anillos donde A y B son noetherianos, A normal y B entero sobre A. Sea $x \in B$ entero sobre el ideal $I \subset A$ y $f = t^n + \sum_{\nu=0}^{n-1} a_\nu t^\nu \in Q(A)[t]$, sea el polinomio mínimo de x. Entonces $a_\nu \in \sqrt{I}$ para $\nu = 0, \ldots, n-1$.*

Demostración. Sea L el cuerpo de escisión de f sobre el cuerpo $Q(A)$ y sean $x_1 := x, x_2, \ldots, x_n \in L$ las raíces de f. Entonces todas las x_i son enteras sobre I porque f divide al polinomio que define la relación entera de x sobre I.
Los polinomios simétricos elementales en $x_1, \ldots, x_n$ son los coeficientes de f, y por tanto, los coeficientes son enteros sobre I, es decir, en $C(I, Q(A))$. Pero A es íntegramente cerrado, por lo tanto es igual a $C(A, Q(A))$, y en consecuencia por la Proposición 4.1.21, estos coeficientes están en $\sqrt{I}$. □

Ahora daremos otra versión para el teorema del descenso, pero esta vez pidiendo que A sea normal.

Teorema 4.1.29. ***(going down, teorema del descenso)*** *Sea $A \subset B$ un extensión de anillo del dominios enteros noetherianos, A normal y B entero sobre A. Sea $Q \subset B$ un ideal primo, $P = Q \cap A$ y $P' \subset P$ un ideal primo en A. Entonces existe un ideal primo $Q' \subset Q$ en B tal que $Q' \cap A = P'$.*

Demostración. Es suficiente con probar que $P'B_Q \cap A = P'$. Es decir, sea $S' = A \setminus P'$, entonces $P'S'^{-1}B_Q$ es un ideal propio, ya que $P'S'^{-1}B_Q = S'^{-1}B_Q$ implicaría que $s' \in P'B_Q$ para algún $s' \in S'$ lo que contradice que $P'B_Q \cap A = P'$. Sea $M \supset P'S'^{-1}B_Q$ un ideal maximal de $S'^{-1}B_Q$ entonces $P' = M \cap A$, porque $P' \subsetneq M \cap A$ implicaría que $s' \in M$ para algún $s' \in S'$, y M sería el anillo entero. Definiendo $Q' = M \cap B$ tenemos $Q' \subset Q$ y $Q' \cap A = P'$.
Tenemos que ver la inclusión $P'B_Q \cap A \subset P'$. Sea $x \in P'B_Q \cap A$ entonces $x = y/s$, para algún $s \in B \setminus Q$ e $y \in P'B \subset \sqrt{P'B} = C(P', B)$. Esto implica que y es entero sobre P' y usando el Lema 4.1.28, que los coeficientes a_ν del polinomio (mónico) mínimo $f = t^n + \sum_{\nu=0}^{n-1} a_\nu t^\nu$ de y sobre $Q(A)$ ya están en P'. Entonces $f(y) = 0$ implica

$$\left(\frac{y}{x}\right)^n + \frac{a_{n-1}}{x}\left(\frac{y}{x}\right)^{n-1} + \ldots + \frac{a_0}{x^n} = 0.$$

El polinomio $g := t^n + \sum_{\nu=0}^{n-1} \left(a_\nu / x^{n-\nu}\right) \cdot t^\nu$ es un polinomio en $Q(A)[t]$ porque $x \in A$ por suposición. Puesto que $y/x = s$, tenemos que $g(s) = 0$.
Pero entonces g es el polinomio mínimo de s, ya que de otro modo f no sería el polinomio mínimo de y. Esto implica, usando el Lema 4.1.28 con $I = A$, que $a_\nu / x^{n-\nu} \in A$ para $\nu = 0, \ldots, n-1$.
Ahora $(a_\nu / x^{n-\nu}) \cdot x^{n-\nu} = a_\nu \in P'$. Si $x \notin P'$ entonces obtenemos que $a_\nu / x^{n-\nu} \in P'$ para todo ν, lo que implica que $s^n \in P'B \subset PB \subset Q$. Esto lleva a una contradicción por la elección de s, y por tanto se prueba que $x \in P'$. □

Capítulo 5

Dimensiones

En este capítulo, usaremos cadenas de ideales primos para definir la dimensión de un anillo.

Definición 5.0.1. Tenemos una cadena de submódulos de un módulo M que es una sucesión $\{M_i\}(0 \leq i \leq n)$ de submódulos de M tal que $M_0 = M \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots \supsetneq M_n = (0)$.
Diremos que M es una cadena maximal si no se le pueden insertar otro submódulos, y esto es equivalente a decir que cada cociente $M_i/M(1 \leq i \leq n)$ es simple, es decir, no tiene submódulo distintos de (0) y el mismo. A esto lo llamaremos serie de composición.
La longitud de la cadena es n, que se corresponde con la idea del número de "eslabones", aunque ahora daremos una definición más formal.

Definición 5.0.2. Sea A un anillo.

1. Sea $\mathcal{C}(A)$ el conjunto de todas las cadenas de ideales primos en A, es decir,

$$\mathcal{C}(A) := \{\mathfrak{p} = (P_0 \subsetneq \ldots \subsetneq P_m \subsetneq A) | P_i \text{ ideal primos } \}.$$

2. Si $\mathfrak{p} = (P_0 \subsetneq \ldots \subsetneq P_m \subsetneq A) \in \mathcal{C}(A)$, definimos la $longitud(\mathfrak{p}) := m$.

3. La *dimensión* de A se define como $dim(A) = sup\{longitud(\mathfrak{p}) | \mathfrak{p} \in \mathcal{C}(A)\}$.

4. Para $P \subset A$ ideal primo sea

$$\mathcal{C}(A, P) = \{\mathfrak{p} = (P_0 \subsetneq \ldots \subsetneq P_m) \in \mathcal{C}(A) | P_m = P\}$$

que denota el conjunto de las cadenas de ideales primos que terminan en P. Definimos *altura* de P como $ht(P) = sup\{longitud(\mathfrak{p}) | \mathfrak{p} \in \mathcal{C}(A, P)\}$.

5. Para un ideal arbitrario $I \subset A$, $ht(I) = inf\{ht(P)|P \supset I \text{ primo }\}$ se llama *altura* de I y $dim(I) := dim(A/I)$ se llama *dimensión* de I.

Proposición 5.0.3. *En el anillo de polinomios $K[x_1, \ldots, x_n]$ sobre el cuerpo K todas las cadenas maximales de ideales primos tienen longitud n. Aquí una cadena de ideales primos se llama maximal si no puede refinarse.*

Demostración. Usaremos inducción sobre n, para el caso $n = 0$ es trivial. Sea $\langle 0\rangle = P_0 \subsetneq \ldots \subsetneq P_m \subsetneq A$ una cadena de ideales maximales en $\mathcal{C}(A)$ donde $A = K[x_1, \ldots, x_n]$. Elijamos $f \in P_1$ irreducibles y las coordenadas $y_1, \ldots, y_{n-1}$ tal que $K[x_1, \ldots, x_n]/\langle f\rangle \supset K[y_1, \ldots, y_{n-1}]$ es finito. Entonces, claramente, la cadena

$$\langle 0\rangle = P_1/\langle f\rangle \subsetneq P_2/\langle f\rangle \subsetneq \ldots \subsetneq P_m/\langle f\rangle$$

es también maximal. Usando el lema 5.0.14 y el teorema de la normalización de Noether 6.1.10, esta cadena induce una cadena maximal en $K[y_1, \ldots y_{n-1}]$ que por hipótesis de inducción tiene longitud $n - 1$ □

Corolario 5.0.4. *Sea $A \subset B$ una extensión entera. Entonces $Q \mapsto Q \cap A$ define una aplicación sobreyectiva de $\mathcal{C}(B) \to \mathcal{C}(A)$ conservando la longitud de las cadenas. En particular $dim(A) = dim(B)$.*

Demostración. Usando la proposición **??** se ve que la aplicación es sobreyectiva. Luego solo queda ver que se conservan las longitudes. Sean $Q \subsetneq Q'$ ideales primos en B, y asumimos que $Q \cap A = Q' \cap A = P$.
Ahora $A_P \subset B_P$ es una extensión entera, y A_P es local con ideal maximal PA_P. Además, $QB_P \subset Q'B_P$ son ideales primos en B_P cumpliendo la propiedad $QB_P \cap A_P = Q'B_P \cap A_P = PA_P$. Usando el lema 3.2.3 (3), QB_P y $Q'B_P$ son maximales, luego por tanto $QB_P = Q'B_P$. Lo que implica que $Q = Q'$. □

Definición 5.0.5. Sea A un anillo y $I \subset A$ un ideal. Un ideal primo P con $I \subset P$ se llama ideal primo minimal asociado a I , si para cualquier ideal primo $Q \subset A$ con $I \subset Q \subset P$ tenemos que $Q = P$. El conjunto de ideales primos minimales asociados a I se denota por $minAss(I)$.

Lema 5.0.6. *Sea A un anillo, $I \subset A$ un ideal tal que $I : \langle a\rangle = I : \langle a^2\rangle$ para algún $a \in A$. Entonces $I = (I : \langle a\rangle) \cap \langle I, a\rangle$.*

Demostración. Sea $f \in (I : \langle a\rangle) \cap \langle I, a\rangle$ y sea $f = g + xa$ para algún $g \in I$. Entonces $af = ag + xa^2 \in I$, y por tanto, $xa^2 \in I$. Esto es que $x \in I : \langle a^2\rangle = I : \langle a\rangle$, lo que implica que $xa \in I$ y en consecuencia $f \in I$. □

Proposición 5.0.7. *Sea A un anillo noetheriano y $I \subset A$ un ideal. Entonces $minAss(I) = \{P_1, \ldots, P_n\}$ es finito y*

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

En particular, $\sqrt{I}$ es la intersección de todos los ideales primos que contienen a I. Aunque esto ya lo habíamos afirmado previamente en la proposición 2.4.7, en la cual su demostración se dejaba para el lector.

Demostración. Obviamente tenemos que $minAss(I) = minAss(\sqrt{I})$ y por tanto podemos asumir que $I = \sqrt{I}$.
Si I es primo, el resultado es trivial. Luego podemos asumir que existen $a, b \notin I$ con $ab \in I$, es decir, que no es primo. Demostramos que $\sqrt{I : \langle a \rangle} = I : \langle a \rangle = I : \langle a^2 \rangle \supsetneq I$. Es decir, si $f \in \sqrt{I : \langle a \rangle}$ implica que $f^p \in I : \langle a \rangle$ para un adecuado p. Por tanto, $af^p \in I$ y $(af)^p \in I$, lo que implica que $af \in \sqrt{I} = I$, esto es que, $f \in I : \langle a \rangle$. Por otro lado, si $f \in I : \langle a^2 \rangle$ implica que $a^2 f \in I$ y $(af)^2 \in I$, esto es que $af \in \sqrt{I} = I$ y por tanto $f \in I : \langle a \rangle$. Y puesto que dabemos que $I : \langle a \rangle \subset I : \langle a^2 \rangle$ y que $I : \langle a \rangle \subset \sqrt{I : \langle a \rangle}$ se darán las igualdades. Por último, $b \in I : \langle a \rangle$ pero $b \notin I$. Ahora usando el lema previo, obtenemos $I = (I : \langle a \rangle) \cap \langle I, a \rangle$. En particular, tenemos

$$I = \sqrt{I} = \sqrt{(I : \langle a \rangle)} \cap \sqrt{\langle I, a \rangle} = (I : \langle a \rangle) \cap \sqrt{\langle I, a \rangle}.$$

Si $I : \langle a \rangle$ o $\sqrt{\langle I, a \rangle}$ no son primos, podemos continuar con estos ideales como hemos hecho con I. Este proceso tiene que terminar en algún momento puesto que A es noetheriano, y por tanto obtendríamos que $I = \cap_{i=n}^{n} P_i$ con P_i primo. Podemos suponer que $P_i \not\subset P_j$ para $i \neq j$ eliminando los primos innecesarios. En este caso tenemos que $minAss(I) = \{P_1, \ldots, P_n\}$. Si $P \supset I$ es un ideal primo, entonces $P \supset \cap_{i=n}^{n} P_i$, y por tanto, existe un j tal que $P \supset P_j$lo que prueba la proposición. □

Definición 5.0.8. Al anillo A se le llama reducido si no tiene ningún elemento nilpotente excepto el 0 , esto es que $\sqrt{\langle 0 \rangle} = \langle 0 \rangle$. Para cualquier anillo, el anillo cociente $A_{red} = A/\sqrt{\langle 0 \rangle}$ se llama reducción de A y el anillo reducido asociado a A.

Lema 5.0.9. *Sea A un anillo y sea $A_{red} := A/\sqrt{\langle 0 \rangle}$ la reducción de A. Entonces*

$$dim(A) = dim(A_{red}) = max_{P \in minAss(\langle 0 \rangle)}\{dim(A/P)\}$$

Proposición 5.0.10. *Sea A un anillo tal que cumple las dos condiciones siguientes:*

1. *Para cada ideal maximal M de A, la localización A_M es noetheriana.*
2. *Para cada $x \neq 0$ en A el conjunto de ideales maximales de A que contiene a x es finito.*

Entonces A es noetheriano.

Observación 5.0.11. Es posible para un dominio de integridad noetheriano que la dimensión sea infinita. Sea K un cuerpo y sea $A = K[x_1, x_2, \dots]$ un anillo de polinomios en un número contable de indeterminadas. Sea $(\nu_j)_{j\geq 1}$ una sucesión estrictamente creciente de enteros positivos tal que $(\nu_{j+1} - \nu_j)_{j\geq 1}$ es también creciente. Sea $P_i := \langle x_{\nu_{i+1}}, \dots, x_{\nu_{i+1}} \rangle$ y $S = A \setminus \cup_i P_i$. Entonces $S^{-1}A$ es un dominio de integridad noetheriano. Pero $ht(S^{-1}P_i) = \nu_{i+1} - \nu_i$ implica que $dim(S^{-1}A) = \infty$.

Observación 5.0.12. Observamos que el anillo de la observación anterior no es local. En general, todos los anillos noetherianos locales tienen dimensión finita. En particular, esto implica (usando la localización) que en un anillo noetheriano la altura de un ideal es siempre finita.

Observación 5.0.13. Para anillos graduados, aunque no nos dará tiempo a verlo en este trabajo, se puede dar otra descripción de la dimensión como el grado del polinomio de Hilbert. Esta será la base para calcular la dimensión debido al hecho de que para un ideal $I \subset K[x_1, \dots, x_n]$

$$dim(K[x_1, \dots, x_n]/I) = dim(K[x_1, \dots, x_n]/L(I)),$$

donde $L(I)$ es el ideal líder de I.
Por tanto, después de el cálculo de una base de Gröbner, el cálculo de la dimensión se reduce a un problema puro de combinatoria.

Lema 5.0.14. *Sea A un anillo tal que para cada ideal primo $P \subset A$ existe un dominio de integridad notheriano normal $C \subset A$ con $C \subset A/P$ siendo finito. Entonces se cumple lo siguiente:*
Si $A \subset B$ es un extensión de anillo finita entonces la aplicación $\mathcal{C}(B) \to \mathcal{C}(A)$ inducida por la contracción $P \mapsto P \cap A$ asigna cadenas maximales a cadenas maximales.

Demostración. Sea $\langle 0 \rangle = Q_0 \subset Q_1 \subset \dots \subset Q_n$ una cadena maximal de ideales primos en B y consideramos $\langle 0 \rangle = Q_0 \cap A \subset Q_1 \cap A \subset \dots \subset Q_n \cap A$. Tenemos que probar entonces que esta cadena es maximal. Asumimos que $Q \subset Q' \subset B$ son dos ideales primos y que existe un ideal primo $P \subset A$ tal que $Q \cap A \subsetneq P \subsetneq Q' \cap A$. Elegimos para $Q \cap A$ un dominio de integridad noetheriano íntegramente cerrado A' tal que $A' \subset A/(Q \cap A)$ sea finito.

Observemos que los ideales $\langle 0\rangle, P/(Q\cap A)\cap A', Q'/(Q\cap A)\cap A'$ son dos a dos diferentes puesto que $A'\subset A/(Q\cap A)$ es finito. Además, B/Q también es finito sobre A', y podemos aplicar el teorema "going down"4.1.29 para encontrar un ideal primo $\overline{P}'\neq\langle 0\rangle$ en B/Q, $\overline{P}'\subset Q'/Q$ tal que $\overline{P}'\cap A' = P\cap A'$. Entonces, $\overline{P}'\subsetneq Q'/Q$. Esto implica que existe un ideal primo P', con $Q\subsetneq P'\subsetneq Q'$ lo que prueba el lema. Para el caso $Q'\cap A\subsetneq P$ se razonaría de manera análoga. □

Observación 5.0.15. Es una consecuencia del teorema de la normalización de Noether 6.1.10 que todos los anillo de tipo finito sobre un cuerpo K tienen la propiedad requerida asumida por el lema.

Lema 5.0.16. *Sean A, B cumpliendo las hipótesis del teorema "going down" 4.1.29. Si $Q\subset B$ es un ideal primo entonces $ht(Q) = ht(Q\cap A)$.*

Demostración. Usando el corolario 5.0.4, sabemos que la aplicación $\mathcal{C}(B)\to\mathcal{C}(A)$ inducida por $P\mapsto P\cap A$, induce otra aplicación $\mathcal{C}(B,Q)\to\mathcal{C}(A,Q\cap A)$, que conserva la longitud de las cadenas de ideales primos. Para ver que esta aplicación es sobreyectiva, sea $Q\cap A = P_s\supsetneq P_{s-1}\supsetneq\ldots\supsetneq P_0$ una cadena de ideales primos en A. Empezando con P_{s-1}, y usando s veces el teorema "going down", obtenemos una cadena$Q = Q_s\supsetneq Q_{s-1}\supsetneq\ldots\supsetneq Q_0$ de ideales primos en B, con lo que se prueba el lema. □

Capítulo 6

Normalización de Noether

Sea K un cuerpo, $A = K[x_1, \ldots, x_n]$ el anillo de polinomios y $I \subset A$ un ideal. La normaliación de Noether es una herramienta en la teoría de K-álgebras afines, esto es, en álgebras del tipo A/I. Es la base para muchas aplicaciones de los teoremas de los capítulos previos, porque nos proporciona un anillo de polinomios $K[x_{s+1}, \ldots, x_n] \subset A/I$ tal que la extensión sea finita.

Definición 6.0.1. Sea $I \subset A = K[y_1, \ldots, y_n]$ un ideal. Una aplicación finita e inyectiva $K[y_{s+1}, \ldots, y_n] \to A/I$ se dice que es una normalización de Noether de A/I. Además, si I contiene $g_1, \ldots, g_s$ con

$$g_j = y_j^{e_j} + \sum_{k=0}^{e_j - 1} \xi_{j,k}(y_{j+1}, \ldots, y_n) \cdot y_j^k$$

cumpliendo $e_j \geq deg(\xi_{j,k}) + k$ para $k = 0, \ldots, e_j - 1$, se llama normalización de Noether general.

El lema de normalización de Noether nos dice que siempre podemos expresar $A \supset I$ de esta forma.

6.1. Anillos y módulos graduados

Definición 6.1.1. Un anillo graduado A es un anillo junto con una descomposición en forma de suma directa $A = \oplus_{\nu \geq 0} A_\nu$, donde A_ν son grupos abelianos que cumplen que $A_\nu A_\mu \subset A_{\nu+\mu}$ para todo $\nu, \mu \geq 0$.
Los A_ν se llaman componentes homogéneas y los elementos de A_ν se llaman elementos homogéneos de grado ν.

Definición 6.1.2. Sea $A = \oplus_{\nu \geq 0} A_\nu$ un anillo graduado. Un A-módulo M, junto con la descomposición en suma directa de grupos abelianos $M =$

$\oplus_{\nu\in\mathbb{Z}} M_\mu$ se dice que es un A-módulo graduado si $A_\nu M_\mu \subset M_{\nu+\mu}$ para todo $\nu \geq 0$ y $\mu \in \mathbb{Z}$.
Los elementos de M_ν se dicen que son homogéneos de grado ν. Si $m = \sum_\nu m_\nu$, con $m_\nu \in M_\nu$ entonces m_ν se llama la parte homogénea de grado ν de m.

La demostración de este lema se puede encontrar en el libro [4]. Sin embargo, debemos introducir estas equivalencias para poder definir el concepto de ideal homogéneo que aparecerá en nuestro teorema.

Lema 6.1.3. *Sea $M = \oplus_{\nu\in\mathbb{Z}} M_\nu$ un A-módulo graduado y $N \subset M$ un submódulo. Las siguientes condiciones son equivalentes:*

1. *N es graduado de la forma $N = \oplus_{\nu\in\mathbb{Z}}(M_\nu \cap N)$.*
2. *N está generado por elementos homogéneos.*
3. *Sea $m = \sum m_\nu$ con $m_\nu \in M_\nu$. Entonces $m \in N$ si y solo si $m_\nu \in N$ para todo ν.*

Definición 6.1.4. Un submódulo $N \subset M$ cumpliendo las condiciones equivalentes del lema precedente, se llama un submódulo graduado o submódulo homogéneo. Un submódulo graduado de un anillo graduado se llama ideal graduado o ideal homogéneo.

Observación 6.1.5. Aunque esta noción es muy básica, recordemos que se dice que un polinomio es homogéneo cuando cada uno de sus términos también llamados monomios tienen siempre el mismo grado.

Observación 6.1.6. Recordemos otra definición clave. Dado un cuerpo K y una extensión L/K, se dice que un elemento $\alpha \in L$ es algebraico sobre K si y solo si existe un polinomio $p \in K[X]$, que pertenece al anillo de polinomios con coeficientes en K, tal que $p(\alpha) = 0$. En caso contrario se dirá que es trascendente. Un subconjunto S de un cuerpo$L$ es algebraicamente independiente sobre un subcuerpo K si los elementos de S no satisfacen ninguna ecuación polinómica no trivial con coeficientes en K. Esto significa que para toda secuencia finita $\alpha_1, \ldots, \alpha_n$ de elementos de S, y todo polinomio distinto de cero $P(x_1, \ldots, x_n)$ con coeficientes en K, tenemos $P(\alpha_1, \ldots, \alpha_n) \neq 0$. Por otro lado, también se usará la noción de K-álgebra introducida ya en 3.0.9

Definición 6.1.7. Sea $f = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ un polinomio irreducible, donde K es un cuerpo. Se dice que f es separable, si f tiene solo raíces simples en $\overline{K}$, que es la clausura algebraica de K.
Una extensión algebraica sobre un cuerpo $K \subset L$ se dice que es separable si

todo elemento $a \in L$ es separable sobre K, esto es, que el polinomio mínimo de a sobre K es separable. Se dice que K es un cuerpo perfecto, si todo polinomio irreducible $f \in K[x]$ es separable.

Ahora introduciremos el lema de normalización de Noether. Este lema se puede presentar de muchas formas aparentemente distintas, pero en verdad todas con la misma idea. Primero presentaremos la forma general, para después refinarlo un poco más y centrarnos en la del libro [4]

Teorema 6.1.8. *Sea K un cuerpo y sea $A \neq 0$ una K-álgebra finitamente generada. Entonces existen elementos $y_1, \ldots, y_r \in A$ que son algebraicamente independientes sobre K y tales que A es entero sobre $K[y_1, \ldots, y_r]$.*

Demostración. Para la demostración del teorema distinguiremos el caso en que K es infinito y el caso en que es finito.

1. Supongamos que K es infinito. Por definición de álgebra finitamente generada, existe un homomorfismo sobre K-módulos que es sobreyectiva $\phi : K[x_1, \ldots, x_n] \to A$. A partir de ahora identificaremos $\phi(x_i)$ por x_i para ahorrar notación. Llamaremos $x_1, \ldots x_n$ a sus generados como clases en A, y reenumeremos estos generadores para que $x_1, \ldots, x_r$ sean algebraicamente independientes sobre K y que cada $x_{r+1}, \ldots x_n$ sean algebraicos sobre $K[x_1, \ldots, x_r]$. Ahora razonaremos por inducción sobre $n - r$. Si $n - r = 0$ entonces $n = r$ y los y_i del enunciado coinciden con los x_i. Supongamos ahora que $n - r > 0$ es decir que $n > r$ y que el resultado es cierto para $n - 1$ generadores.
   Como x_n es algebraico sobre $k[x_1, \ldots, x_n]$, existe un polinomio $f \neq 0$ en n variables tal que $f(x_1, \ldots, x_n) = 0$. Sea F la parte homogénea de mayor grado en f es decir, si tenemos que $f = \sum_{j=0}^{M} f_j(x_1, \ldots, x_n)$ donde f_j es homogéneo de grado j, entonces $F := f_M$. Puesto que K es infinito, existen $\lambda_1, \ldots \lambda_{n-1} \in K$ tal que $F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Para ver esto último, escribamos $F = \sum_{j=0}^{M} g_j x_n^j$ con $g_j \in K[x_1, \ldots, x_{n-1}]$ que son homogéneos de grado $M - j$. Entonces $G(x_1, \ldots x_{n-1}) := F(x_1, \ldots, x_{n-1}, 1) = \sum_{j=0}^{M} g_j$ que es distinto de cero si F es distinto de cero. Por tato $Z(G) \neq K^{n-1}$, dado que solo el polinomio que tiene K^{n-1} como conjunto de soluciones es el polinomio nulo, por el lema 6.1.9. En consecuencia podemos encontrar estos lambdas. Una vez probado eso, pongamos $x_i' = x_i - \lambda_i x_n$ para $i \in \{1, \ldots, n-1\}$. Entonces, si tenemos $F = \sum_{\alpha \in \mathbb{N}^n, |\alpha| = m} c_\alpha x^\alpha$ donde $x^\alpha = \prod_{i=1}^{n} x_i^{\alpha_i}$,

$$F = \sum_{\alpha \in \mathbb{N}^n, |\alpha| = m} c_\alpha x^\alpha = \sum_{\alpha \in \mathbb{N}^n, |\alpha| = m} c_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} = \sum_{\alpha \in \mathbb{N}^n, |\alpha| = m} c_\alpha x_n^{\alpha_n} \prod_{i=1}^{n-1} (x_i' + \lambda_i x_n)^{\alpha_i}.$$

Por tanto, los coeficientes de x_n^{degF} en F es $F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Para probar esto último, veamos que el término $\lambda_i x_n$ tiene una potencia α_i lo que da una forma $\prod_{i=1}^{n} x_i^{\alpha_i}$ en F cambiado con $x_i = \lambda_i$. Por tanto, escribiendo $C = F(\lambda_1, \ldots, \lambda_{n-1}, 1)$ y dividiendo $f(x'_1 + \lambda_1, \ldots, x'_{n-1} + \lambda_{n-1}, x_n$ por C, podemos obtener polinomio mónico con respecto a x_n; puesto que F es la parte de mayor grado de f dividiendo por C da un término mónico x_n^{degF}, que es el termino mayor en $f(x'_1 + \lambda_1, \ldots, x'_{n-1} + \lambda_{n-1}, x_n)$. Luego, $f(x'_1 + \lambda_1, \ldots, x'_{n-1} + \lambda_{n-1}, x_n) = 0$, ya que, $x_i = x'_i - \lambda_i x_n$; y podemos pensar $f(x'_1 + \lambda_1, \ldots, x'_{n-1} + \lambda_{n-1}, x_n)$ como un elemento en $K[x'_1, \ldots, x'_{n-1}][x_n]$. Entonces x_n es entero sobre $A' := K[x'_1, \ldots, x'_{n-1}]$. Esto implica que A es entero sobre $A'[x_n]$, y por tanto por la transitividad de la dependencia entera, A es entero sobre A'. Entonces por la hipótesis de inducción, A' tiene elementos $y_1, \ldots, y_r \in A'$ que son algebraicamente independientes sobre K y tal que A' es entero sobre $K[y_1, \ldots, y_r]$ Puesto que A es entero sobre A', tenemos por la transitividad de la dependencia entera que A es entero sobre $K[y_1, \ldots, y_r]$.

2. Supongamos ahora que K es finito. Igual que antes tenemos el homomorfismo sobreyectivo ϕ, los generadores $x_1, \ldots, x_n$, de la forma que los r primeros son independientes sobre K y los restantes son algebraicos sobre $K[x_1, \ldots, x_r]$. Y razonamos otra vez por inducción sobre $n-r$. El caso trivial $n-r = 0$ se razona como para el caso infinito y supongamos ahora que $n-r > 0$ y que el resultado es cierto para $n-1$ generadores. Como x_n es algebraico sobre $k[x_1, \ldots, x_n]$, existe un polinomio $f \neq 0$ en n variables tal que $f(x_1, \ldots, x_n) = 0$. Sea $d > deg(f)$, y $x'_i = x_i - x_n^{d^i}$ para $i = 1, \ldots, n-1$. Entonces escribimos $g(x'_1, \ldots, x'_{n-1}, x_n) := f(x'_1 + x_n^{d^1}, \ldots, x'_{n-1} + x_n^{d^{n-1}}, x_n) = 0$. Si $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$, entonces cada monomio en g tiene la forma $c_\alpha \prod_{i=1}^{n-1} (x'_i + x_m^{d^i})^{\alpha_i}$. Por tanto su término potencia de x_n tiene un exponente

$$\alpha_n \sum_{i=1}^{n-1} \alpha_i d^i$$

Puesto que d está elegido mayor que cualquier α_i, cada α tiene una término potencia distinto de x_n. Sea β el exponente tal que sus términos potencia de x_n sea los mayores. Entonces, dividiendo g por c_β podemos obtener un polinomio mónico de x_n sobre $A' = K[x'_1, \ldots, x'_{n-1}]$. Por consiguiente, x_n es entero sobre A' y por hipótesis de inducción, A' es entero sobre $K[y_1, \ldots, y_r]$ para algunos elementos algebraicamente independientes y_i. En conclusión, $A'[x_n]$ es entero sobre $K[y_1, \ldots, y_r]$ ya que $A'[x_n] = A$.

□

Lema 6.1.9. ***(Teorema de anulación del polinomio)*** *Sea K un cuerpo infinito, es decir, tiene infinitos elementos distintos y sea $f \in K[x_1, \ldots, x_n]$. Entonces $f = 0$ si y solo si $f : K^n \to K$ es la función nula.*

Demostración. Es obvio que el polinomio nulo es la función nula. Así que supongamos que f es un polinomio en $K[x_1, \ldots, x_n]$ para el cual $f : K^n \to K$ es la función nula. Probaremos el enunciado por inducción.
Para el caso $n = 1$, asumiremos que f es de grado m. Si f no fuera el polinomio nulo, entonces tendría como mucho m raíces distintas en K. Y puesto que K es infinito, habrá $b \in K$ para el cual $f(b) \neq 0$, pero esto no se puede dar ya que f es la función nula. Luego f es el polinomio nulo.
Supongamos que es cierto para $n - 1$. Reuniendo las diversas potencias de x_n, podemos escribir f de la forma

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^j,$$

donde cada $g_i \in K[x_1, \ldots, x_{n-1}]$. Ahora, para un punto $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ (fijado),

$$h(x_n) := f(b_1, \ldots, b_{n-1}, x_n) = \sum_{i=0}^{N} g_i(b_1, \ldots, b_{n-1}) x_n^j$$

está en $K[x_n]$. Como f es la función nula en K^n, h es la correspondiente función nula en K. La demostración para el caso $n = 1$ demuestra ahora que h es el polinomio nulo en $K[x_n]$, esto significa que cada coeficiente $g_i(b_1, \ldots b_{n-1}) = 0$. Puesto que la elección de $(b_1, \ldots b_{n-1})$ es arbitraria, se tiene que cada g_i es la función nula en K^{n-1} y por hipótesis de inducción, cada g_i es el polinomio nulo en $K[x_1, \ldots, x_{n-1}]$, lo que completa la demostración.
□

Teorema 6.1.10. ***(Normalización de Noether)*** *Sea K un cuerpo, y sea $I \subset K[x_1, \ldots, x_n]$ un ideal. Entonces existe un entero $s \leq n$ y también un isomorfismo*

$$\varphi : K[x_1, \ldots, x_n] \to A := K[y_1, \ldots, y_n],$$

tal que:

1. *La aplicación canónica $K[y_{s+1}, \ldots, y_n] \to A/\varphi(I)$, $y_i \mapsto y_i \, mod \varphi(I)$ es inyectiva y finita.*

2. *Ademas, φ se puede elegir tal que, para $j = 1, \ldots, s$ existen polinomios*

$$g_j = y_j^{e_j} + \sum_{k=0}^{e_j-1} \xi_{j,k}(y_{j+1}, \ldots, y_n) \cdot y_j^k$$

cumpliendo $e_j \geq deg(\xi_{j,k}) + k$ para $k = 0, \ldots, e_j - 1$.

3. *Si I es homogéneo, entonces los g_j se pueden elegir también homogéneos. Si I es un ideal primo, los g_j se pueden elegir irreducibles.*

4. *Si K es perfecto entonces el morfismo φ se puede elegir tal que además $Q(A/\varphi(I)) \supset Q(K[y_{s+1}, \ldots, y_n])$ es una extensión de cuerpos separable y también si K es infinito entonces $Q(A/\varphi(I)) = Q(K[y_{s+1}, \ldots, y_n])[y_s]/\langle g_s \rangle$.*

5. *Si K es infinito entonces φ se puede elegir lineal, $\varphi(x_i) = \sum_j m_{ij} y_j$ con $M = (m_{ij}) \in \mathrm{GL}(n, K)$.*

Demostración. Probaremos primero este teorema para cuerpos infinitos. Para el caso $I = \langle 0 \rangle$ es trivial, así que podemos suponer que $I \neq \langle 0 \rangle$. Y ahora procedemos a razonar por inducción en n. Sea $n = 1$, y sea $I = \langle f \rangle$, con f un polinomio de grado d. Entonces $K[x_1]/I = K + x_1 K + \ldots + x_1^{d-1} K$ es un K-espacio vectorial de dimensión finita; y el teorema se cumple con $s = 1$. Asumimos ahora que el teorema está probado para $n - 1 \geq 1$ y sea $f \in I$ un polinomio de grado $d \geq 1$. Si I es homogéneo, podemos elegir f para que sea homogéneo. Sea $f = \sum_{\nu=0}^{d} f_\nu$ la descomposición de f en partes homogéneas f_ν de grado ν, y sea $M_1 = (m_{ij}) \in \mathrm{GL}(n, K)$,

$$M_1 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. \tag{6.1.10.1}$$

Entonces obtenemos

$$\begin{aligned} f_d(x_1, \ldots, x_n) &= f_d\left(\sum_{j=1}^{n} m_{1j} y_j, \ldots, \sum_{j=1}^{n} m_{nj} y_j\right) \\ &= f_d(m_{11}, \ldots, m_{n1}) \cdot y_1^d + \text{ términos en } y_1. \end{aligned} \tag{6.1.10.2}$$

Ahora la condición para M_1, se convierte en $f_d(m_{11}, \ldots, m_{n1}) \neq 0$, la cual se puede cumplir puesto que K es infinito. Entonces, obviamente $K[y_2, \ldots, y_n] \to A/\langle f \rangle$ es inyectiva y finita por la proposición , ya que y_1 es cumple una relación entera y $\widetilde{g}_1 := f(M_1 y)$ tiene, después de normalizar, la propiedad pedida en (2).

Observemos que $K[y_2,\dots,y_n]/(I\cap K[y_2,\dots,y_n])\to A/I$ es inyectiva y también finita (escribimos I en vez de $\varphi(I)$). Si $I\cap K[y_2,\dots,y_n]=\langle 0\rangle$ entonces no hay nada que probar.
De no ser así, sea $I_0 := I\cap K[y_2,\dots,y_n]$. Por la hipótesis de inducción existe alguna matriz $M_0\in \mathrm{GL}(n-1,K)$ tal que para,

$$M_0\cdot\begin{pmatrix} z_2\\ \vdots\\ z_n\end{pmatrix}=\begin{pmatrix} y_2\\ \vdots\\ y_n\end{pmatrix}, \tag{6.1.10.3}$$

y algún $s\le n$, la aplicación $K[z_{s+1},\dots,z_n]\to K[y_2,\dots,y_n]/I_0$ es inyectiva y finita. Además, para $j=2,\dots,s$ existen polinomios

$$g_j = z_j^{e_j}+\sum_{k=0}^{e_j-1}\xi_{j,k}(z_{j+1},\dots,z_n)\cdot z_j^k$$

cumpliendo $e_j\ge deg(\xi_{j,k})+k$ para $k=0,\dots,e_j-1$. Además, los g_j se pueden elegir homogéneos si I es homogéneo.
Esto implica que $K[z_{s+1},\dots,z_n]\to A/I$ es inyectiva y finita. El teorema esta probado para

$$M = M_1\cdot\begin{pmatrix} 1 & 0 & \cdots & 0\\ 0 & & & \\ \vdots & & M_0 & \\ 0 & & & \end{pmatrix} \tag{6.1.10.4}$$

y $g_1 := \widetilde{g}_1(y_1, M_0 z), g_2,\dots,g_s\in K[y_1,z_2,\dots,z_n]$.
Si I es primo y si algún g_j de divide en factores irreducibles, entonces alguno de los factores tiene que estar en I. Podemos tomar este factor que tiene la forma que queremos.
Para el caso general, la demostración se encuentra en el documento [3]
(5) ya se probó en (1).

□

Observación 6.1.11. La demostración de este teorema lleva nos lleva a observar algunas conclusiones.

- El teorema lo hemos visto para M de la forma 6.1.10.4, sin embargo, también es valido para un M arbitrario elegido en:
  - algún subconjunto denso y abierto $U\subset \mathrm{GL}(n,K)$.

  - algún subconjunto denso y abierto U' en el conjunto de todas las matrices triangulares inferiores con 1's en la diagonal.

- La demostración también es valida para cuerpos finitos, si la característica del cuerpo es grande.

- Para un cuerpo con característica pequeña, el teorema también se cumple cuando se reemplaza el cambio linear de coordenadas $M \cdot y = x$ por el cambio de coordenadas del tipo $x_i = y_i + h_i(y)$ con $deg(h_i) \geq 2$.

La demostración de estos dos últimos casos se encuentra en el teorema general 6.1.8

Analizando también la demostración se puede obtener el siguiente algoritmo para realizar un normalización de Noether. Este algoritmo funciona bien para cuerpos con característica 0 o con característica grande.

Proposición 6.1.12. *Introducimos nuestro ideal I generado de esta forma $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, con $x = (x_1, \ldots, x_n)$.*
Obtendremos como resultado de realizar los pasos siguiente que daremos a continuación la normalización de Noether, es decir, un conjunto $\{x_{s+1}, \ldots, x_n\}$ y una aplicación $\varphi : K[x] \to K[x]$ tal que $K[x_{s+1}, \ldots, x_n] \subset K[x]/\varphi(I)$ es una normalización de Noether.

1. *Realizamos un cambio aleatorio de coordenadas lineales triangular inferior, esto es,*

$$\varphi(x) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad (6.1.12.1)$$

2. *Calcular una base estándar reducida $\{f_1, \ldots f_r\}$ de $\varphi(I)$ con respecto al orden lexicográfico con $x_1 > \ldots > x_n$, y ordenamos los f_i tal que $\mathrm{LM}(f_r) > \ldots > \mathrm{LM}(f_1)$;*

3. *elegimos s como el máximo tal que $\{f_1, \ldots, f_r\} \cap K[x_{s+1}, \ldots, x_n] = \emptyset$;*

4. *Para cada $i = 1, \ldots, s$ comprobamos si $\{f_1, \ldots, f_r\}$ contiene polinomios con monomio líder $x_i^{\rho_i}$ para algún ρ_i;*

5. *Si la comprobación es cierta, para todo i devolvemos φ y $x_{s+1}, \ldots x_n$. Hay que tener en cuenta que en este caso $K[x_{s+1}, \ldots, x_n] \subset K[x_1, \ldots, x_n]/\varphi(I)$ es finito.*

Y aquí acabaría el algoritmo.

Capítulo 7

Algoritmo para calcular la normalización

El objetivo de este capítulo es dar un criterio para la normalidad que es la base de un algoritmo para calcular la normalización de un anillo y el lugar geométrico no normal para un anillo, en particular para K-álgebras afines. En esta sección supondremos siempre que A es un anillo noetheriano reducido y que $\overline{A}$ es su normalización, es decir, que es la clausura integral de A en $Q(A)$, que es el anillo total de fracciones de A. A es normal si y solo si $A = \overline{A}$. La idea de calcular $\overline{A}$ es alargar el anillo A por el módulo de homomorfismo $A' = Hom_A(J, J)$, que es un A-módulo y también un anillo; para un adecuado J ideal tal que $A' \subset \overline{A}$. Repitiendo este proceso con A' en lugar de A, continuamos hasta que el criterio de normalidad nos permita parar.

7.1. Espectro y esquemas afines

Introduciremos ahora algunas definiciones nuevas que nos servirán para más tarde poder enunciar los teoremas importantes y algunos ejemplos básicos sobre el criterio de la normalidad.

Definición 7.1.1. Un anillo A que es isomorfo al anillo cociente $K[x_1, \ldots, x_n]/I$, donde I es un ideal, se llama anillo afín sobre K.

Definición 7.1.2. Sea A un anillo. Definimos el espectro primo de A como

$$Spec(A) := \{P \subset A \mid P \text{ ideal primo}\}.$$

Podemos convertir a $Spec(A)$ en un espacio topológico dotándolo de la denominada topología de Zariski, creando así un puente entre álgebra y topología. En muchos casos , se usará $Spec(A)$ simplemente como un conjunto, pero de vez en cuando, consideraremos el espectro afín $Spec(A)$ en lugar del anillo A y la variedad $V(I) \subset Spec(A)$ en lugar del ideal I. La mayoría de los ejemplos tratan de anillos afines sobre un cuerpo K.

Observación 7.1.3. Se puede encontrar la definición de la topología de Zariski sobre un espacio afín n-dimensional sobre K en el apéndice A.2 del libro [4].

Definición 7.1.4. Sea A un anillo y sea M un A-módulo. El soporte de M que denotaremos por $supp(M)$ se define como

$$supp(M) := \{P \subset A \text{ ideal primo } | M_P \neq \langle 0 \rangle\}.$$

Definición 7.1.5. Para $X = Spec(A)$ y $I \subset A$ un ideal

$$V(I) := \{P \in X | P \supset I\}$$

Lo llamaremos el conjunto de ceros de I en X. Observemos que $V(I) = supp(A/I)$, pues $supp(A/I) = \{P \in Spec(A) \mid (A/I)_P \neq 0\}$. Pero sabemos que $(A/I)_P = A_P/I_P$, y a su vez sabemos que este cociente no es nulo si y solo si $I_P \neq A_P$ lo cual ocurre si y solo si $I \subset P$. Por tanto $supp(A/I) = \{P \in Spec(A) \mid I \subset P\} = V(I)$.

Observación 7.1.6. Para cualquier ideal I de A, se define $V(I)$ como el conjunto de ideales primos que contienen a I. Se puede establecer una topología en $Spec(A)$ definiendo que una colección de conjuntos cerrados sea $\{V(I) : I \text{ es un ideal de } A\}$. Esta topología se denomina topología de Zariski. Una base para esta topología se puede construir de la siguiente manera. Para $f \in A$ se define D_f como el conjunto de ideales primos de A que no contienen a f. Entonces, cada D_f es un subconjunto abierto de $Spec(A)$, $\{D_f : f \in A\}$ es una base para la topología de Zariski. Usando las siguientes propiedades podemos definir también la topología de Zariski:

- $V(\langle 1 \rangle) = \emptyset$, $V(\langle 0 \rangle) = A$.
- $\cup_{i=1}^{k} V(I_i) = V(\cap_{i=1}^{k} I_i)$.
- $\cap_{\lambda \in \Lambda} V(I_\lambda) = V(\cup_{\lambda \in \Lambda} I_\lambda) = V(\sum_{\lambda \in \Lambda} I_\lambda)$.

Definición 7.1.7. Sea $X = Spec(A)$ u sea $Y \subset X$ cualquier subconjunto. El ideal

$$I(Y) := \cap_{P \in Y} P$$

se llama el ideal (anulador) de Y en X.

Observación 7.1.8. Observemos que si tenemos $Y \subset Z \subset X$, obtendremos que $I(Z) \subset I(Y)$ por construcción de este ideal. Pues $I(Y) := \cap_{P \in Y} P$, pero a la vez sabemos que $P \in Y \subset Z$, y por tanto al hacer la intersección en un conjunto mas grande estará contenido, es decir, $I(Y) := \cap_{P \in Y} P \supset \cap_{P \in Z} P := I(Z)$.

Teorema 7.1.9. *Sea $X = Spec(A)$ y sea $I \subset A$ un ideal. Entonces*

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

Demostración. El resultado es cierto gracias a las siguientes igualdades

$$I(V(I)) = \cap_{P \in V(I)} P = \cap_{P \in Spec(A), P \supset I} P = \sqrt{I}$$

donde la última igualdad se deduce de algo que ya sabíamos de la proposición 2.4.7, que el radical de un ideal es la intersección de todos los ideales primos que contienen a ese ideal. □

Lema 7.1.10. *Sea A un anillo, $S \subset A$ un subconjunto multiplicativamente cerrado y M un A-módulo finitamente generado. Entonces $Annn(S^{-1}M) = S^{-1}Ann(M)$.*

La demostración de este lema se puede encontrar en el capítulo 3 del libro [1].

Lema 7.1.11. *Sea A un anillo y M un A-módulo finitamente generado. Entonces*

$$supp(M) = \{P \subset A \text{ ideal primo } \mid P \supset Ann(M)\} =: V(Ann(M)).$$

Demostración. Supongamos que $Ann(M) \not\subset P$, entonces existe algún $s \in Ann(M)$ que a la vez $s \notin P$. Sea $m \in M$, entonces $sm = 0$. Lo que implica que $m/1 = sm/s = 0$ en M_P, y en consecuencia, $M_P = \langle 0 \rangle$.
Por otro lado, si $M_P = \langle 0 \rangle$, entonces $A_P = Ann(M_P) = (Ann(M))_P$ por el lema anterior que implicará que $Ann(M) \not\subset P$. □

7.2. Criterio de normalidad

Lema 7.2.1. *Sea A un anillo noetheriano reducido y sea $J \subset A$ un ideal que contiene un elemento x de A que no es divisor de cero. Entonces existe una inclusión natural de anillos*

$$A \subset Hom_A(J, J) \cong \frac{1}{x} \cdot (xJ : J) \subset \overline{A}.$$

Demostración. Para $a \in A$, sea $m_a : J \to J$ que será la multiplicación por a, es decir, $m_a(x) = a \cdot x$. Si $m_a = 0$, entonces $m_a(x) = ax = 0$ y por tanto $a = 0$, puesto que por hipótesis x no es un divisor de cero. Entonces, $a \mapsto m_a$ es una aplicación inyectiva y por tanto para cada elemento de A se puede definir un homomorfismo m_a, luego se define una inclusión $A \subset Hom_A(J, J)$. Es fácil ver que para $\varphi \in Hom_A(J, J)$, el elemento $\varphi(x)/x \in Q(A)$ es independiente de x: para cualquier $a \in J$ tenemos que $\varphi(a) = (1/x) \cdot \varphi(xa) = a \cdot \varphi(x)/x$, puesto que φ es A-lineal. Tendremos que $\varphi(a)$ está determinado por el valor de $\varphi(x)$.
Por tanto $\varphi \mapsto \varphi(x)/x$ define una inclusión $Hom_A(J, J) \subset Q(A)$ que envía $x \cdot Hom_A(J, J)$ en $xJ : J = \{b \in A | bJ \subset xJ\}$. La última aplicación también es sobreyectiva, ya que para cualquier $b \in xJ : J$ define, vía multiplicación por b/x, $\varphi(j) = \frac{b}{x}j$, un elemento $\varphi \in Hom_A(J, J)$ con $\varphi(x) = b$. Ya que x no es un divisor de cero, obtenemos el isomorfismo $Hom_A(J, J) \cong (1/x) \cdot (xJ : J)$. De la proposición 3.0.11 identificando $I = x$ y $M = J$, se sigue que cualquier $b \in xJ : J$, es decir, $bJ \subset xJ$ satisface una relación entera $b^p + a_1 b^{p-1} + \ldots + a_0 = 0$ con $a_i \in \langle x^i \rangle$. Dividiendo toda la ecuación por x, tendremos que b/x es entero sobre A, lo que demuestra que $(1/x) \cdot (xJ : J) \subset \overline{A}$. □

Por la proposición 4.1.24, A es normal si y solo si A_P es normal para cada ideal primo $P \subset A$.

Definición 7.2.2. El lugar geométrico no normal de A se define como

$$N(A) = \{P \in Spec\ A \mid A_P \text{ no es normal } \}$$

Lema 7.2.3. *Sea* $C = Ann_A(\overline{A}/A) = \{a \in A \mid a\overline{A} \subset A\}$ *el conductor de* A *en* $\overline{A}$. *Entonces*

$$N(A) = V(C) = \{P \in Spec\ A \mid P \supset C\}.$$

En particular, $N(A)$ *es cerrado en* $Spec(A)$.

Demostración. Si $P \in N(A)$ entonces $A_P \neq \overline{A}_P$ y en consecuencia se tiene que $C_P = Ann_{A_P}(\overline{A}_P/A_P) \subsetneq A_P$ entonces está contenido en algún ideal maximal de A_P, pero el único que hay es $P \cdot A_P$. Luego $C_P \subset PA_P$ y por tanto $P \supset C$ ya que si $c \in C$, tenemos que $\frac{c}{1} \in C_P \subset PA_P$, y se puede escribir también como $\frac{c}{1} = \frac{cs}{s}$ donde $s \notin P$ y $cs \in P$. Como sabemos que P es un ideal primo, solo puede ser que $c \in P$, lo que demuestra que $C \subset P$ como queríamos. Para ver la inclusión contraria, observemos que $C = \cap_{h \in \overline{A}} C_h$, donde $C_h := \{a \in A | ah \in A\}$. Luego, solo tenemos que ver que $V(C_h) \subset N(A)$, pues usando la propiedad $V(C) = V(\cap_{h \in \overline{A}} C_h) = \cup_{h \in \overline{A}} V(C_h)$, está

claro que si $V(C_h) \subset N(A)$ para todo $h \in \overline{A}$ también lo estará la unión de estos. Sea $P \notin N(A)$, entonces $A_P = \overline{A}_P$ y en consecuencia $h = p/q$ para adecuados $p, q \in A$, $q \notin P$, pues recordamos que $A_P = S^{-1}A$ donde $S = A \setminus P$. Esto implica que $qh \in A$, es decir, $q \in C_h$ por definición del conjunto. Entonces $C_h \not\subset P$ y $P \notin V(C_h)$. □

Lema 7.2.4. *Sea $J \subset A$ un ideal que contiene un elemento que no es divisor de cero de A.*

1. *Existe una inclusión natural de A-módulos*

$$Hom_A(J, J) \subset Hom_A(J, A) \cap \overline{A} \subset Hom_A(J, \sqrt{J}).$$

2. *Si $N(A) \subset V(J)$ entonces $J^d\overline{A} \subset A$ para algún d.*

Demostración. 1. La inmersión de $Hom_A(J, A)$ en $Q(A)$ viene dada por $\varphi \mapsto \varphi(x)/x$, donde x es el elemento que no es divisor de cero de J tal y como habíamos visto en 7.2.1. Tendremos que $a\varphi(x) = \varphi(ax) = x\varphi(a)$ por ser un homomorfismo de A-módulos y en consecuencia $\varphi(a) = a \cdot \frac{\varphi(x)}{x}$. Con esta misma identificación obtenemos

$$Hom_A(J, A) = A :_{Q(A)} J = \{h \in Q(A) | hJ \subset A\}$$

pues si tomamos $\varphi \equiv \frac{\varphi(x)}{x} \in Hom_A(J, J) \subset Q(A)$ y lo multiplicamos por un elemento cualquiera α de J, tendremos $\frac{\varphi(x)\alpha}{x} = \varphi(\alpha) \in A$ como queríamos para demostrar la primera inclusión de la igualdad. Sea ahora $h \in A :_{Q(A)} J$, tendremos que $hJ \subset A$. Luego $\varphi = m_h$, la multiplicación por h, define un homomorfismo en $Hom_A(J, A)$ pues envía $\alpha \in J$ en $h\alpha \in A$. Podemos hacer las mismas identificaciones para $Hom_A(J, J)$ y $Hom_A(J, \sqrt{J})$, que serán $h \in Q(A)$ tal que $hJ \subset J$, respectivamente $hJ \subset \sqrt{J}$. Por tanto la primera inclusión se sigue del lema 7.2.1 pues $Hom_A(J, J) \subset \overline{A}$ y también tenemos ahora que $Hom_A(J, J) \subset Hom(J, A)$ luego al hacer la intersección se verifica lo que queríamos.
Para la segunda inclusión, sea $h \in \overline{A} \cap Hom_A(J, A)$, por tanto cumple que $hJ \subset A$ por definición de $Hom_A(J, A)$. Consideramos una relación entera $h^n + a_1h^{n-1} + \ldots + a_n = 0$ con $a_i \in A$, ya que $h \in \overline{A}$ es decir que era entero sobre A. Queremos ver que $hJ \subset \sqrt{J}$. Tomamos $g \in J$ y multipliquemos la ecuación anterior por g^n. Entonces tendremos

$$(hg)^n + ga_1(hg)^{n-1} + \ldots + g^n a_n = 0.$$

Puesto que $g \in J$, tenemos que $hg \in A$ y por tanto $(hg)^n \in J$ ya que el resto de los sumandos de la relación entera estaban en $\langle g \rangle \subset J$ y en consecuencia

$hg \in \sqrt{J}$, lo que demuestra la segunda inclusión.
2. Por hipótesis, y por el lema 7.2.3, tenemos que $V(C) \subset V(J)$. Usando la observación 7.1.8 obtendremos que $I(V(C)) \supset I(V(J))$ y en consecuencia $\sqrt{J} \subset \sqrt{C}$ por el teorema 7.1.9 ya que $I(V(C)) = \sqrt{C}$ y $I(V(J)) = \sqrt{J}$. Luego $J \subset \sqrt{C}$ que es equivalente a decir $J^d \subset C$ para algún d que demuestra lo que queríamos probar. Para probar esta última equivalencia basta observar que si $J \subset \sqrt{C}$, entonces para cada $j \in J$, existe algún entero n tal que $j^n \in C$. Si consideramos d como el máximo de estos n para todos los generadores $j_1, j_2, \ldots, j_k$ de J. Entonces $(j_1 j_2 \ldots j_k)^d \in C$ lo que implica que $J^d \subset C$. Por otro lado si $J^d \subset C$ para algún $d \geq 1$, entonces para cualquier $j \in J$ tenemos $j^d \in C$. Y por definición del radical significa que $j \in \sqrt{C}$ luego se dará la otra inclusión. □

El siguiente criterio para la normalidad se debe a Grauert y Remmert

Proposición 7.2.5. ***(Criterio para la normalidad)*** *Sea A un anillo noetheriano reducido y se $J \subset A$ un ideal que cumple:*

1. *J contiene un elemento que no es divisor de cero de A,*
2. *J es un ideal radical,*
3. *$N(A) \subset V(J)$.*

Entonces A es normal si y solo si $A = Hom_A(J, J)$.

Demostración. Si $A = \overline{A}$ entonces $Hom_A(J, J) = A$ por el lema 7.2.1. Para ver la implicación contraria, elegimos $d \geq 0$ minimal tal que $J^d\overline{A} \subset A$ (Lema 7.2.4 (2)), luego queremos ver que $d = 0$. Razonemos por reducción al absurdo. Si $d > 0$, tenemos que $J^{d-1}\overline{A} \not\subset A$ pues sino d no sería minimal. Por tanto existe algún $a \in J^{d-1}$ y $h \in \overline{A}$ tal que $ah \notin A$. Pero $ah \in \overline{A}$ y $ah \cdot J \subset hJ^d \subset A$ ya que $a \in J^{d-1}$. Por el lema 7.2.4 sabemos que $Hom_A(J, A) = \{h \in Q(A) \mid hJ \subset A\}$, como $(ah)J \subset A$ tenemos $ah \in Hom_A(J, A) \cap \overline{A} \subset Hom_A(J, \sqrt{J}) = Hom_A(J, J)$ usando la cadena de inclusiones de 7.2.4 (1) y que por hipótesis hemos pedido $J = \sqrt{J}$ como condición para el ideal J. Puesto que ahora tenemos que $A = Hom_A(J, J)$ obtenemos $ah \in A$, con lo que llegamos a un absurdo. Por tanto podemos concluir que $d = 0$ y en consecuencia $A = \overline{A}$. □

Observación 7.2.6. Un ideal J cumpliendo las propiedades pedidas en la proposición anterior se dice que es un ideal test para la normalidad. No es difícil ver que el conductor ideal C es un ideal test. Pero C no puede calcularse mientras no conozcamos $\overline{A}$. En capítulo 5 del libro [4] se ve que un ideal test es el que da el lugar singular y que puede ser calculado. También

será importante en ese capítulo el radical del ideal generado por los menores $n-r$, llamado ideal Jacobiano, que va a ser un ideal test.

En caso de que A no sea normal, $A \subsetneq Hom_A(J,J) =: A'$ y continuamos con A' en lugar de A. Para hacer esto, necesitamos presentar A' con un A-álgebra de tipo finito.

Ahora introduciremos la definición de sizigias, pues se usará para el lema 7.2.9, el cual describe la estructura de A-álgebra de $Hom_A(J,J)$.

Definición 7.2.7. Una sizigia o una relación entre k elementos $f_1,\dots,f_k$ de un R-módulo M es una k-upla $(g_1,\dots,g_k) \in R^k$ que cumple

$$\sum_{i=1}^{k} g_i f_i = 0.$$

El conjunto de todas las sizigias entre $f_1,\dots,f_k$ es un submódulo de R^k. Además es el núcleo del homomorfismo de anillos

$$\varphi : F_1 := \oplus_{i=1}^{k} R\epsilon_i \longrightarrow M \ , \quad \epsilon_i \longmapsto f_i,$$

donde $\{\epsilon_1,\dots,\epsilon_k\}$ es la base canónica de R^k. φ es sobreyectiva en el R-módulo $I := \langle f_1,\dots,f_k\rangle_R$ y

$$syz(I) := syz(f_1,\dots,f_k) := Ker(\varphi)$$

se llama módulo de sizigias de I con respecto a los generadores $f_1,\dots,f_k$.

Observación 7.2.8. Hay métodos efectivos para calcular el módulo de sizigias, se puede encontrar esto en el libro [4]. La clave es que $syz(I) \subset R^k$ es un submódulo finitamente generado. Esta idea la usaremos en 7.2.9.

Lema 7.2.9. *Sea A un anillo noetheriano reducido, sea $J \subset A$ un ideal y sea $x \in J$ un elemento que no es divisor de cero. Entonces*

1. *$A = Hom_A(J,J)$ si y solo si $xJ : J = \langle x\rangle$.*

   Además, sea $\{u_0 = x, u_1,\dots,u_s\}$ un sistema de generadores para el ideal $xJ : J$. Entonces podemos escribir

2. $$u_i \cdot u_j = \sum_{k=0}^{s} x\xi_k^{ij} u_k \text{ para adecuados } \xi_k^{ij} \in A, \quad 1 \le i \le j \le s.$$

Sea $(\eta_0^{(k)}, \ldots, \eta_s^{(k)}) \in A^{s+1}$, $k = 1, \ldots, m$ *que generan* $syz(u_0, \ldots, u_s)$ *y sea* $I \subset A[t_1, \ldots, t_s]$ *el ideal*

$$I := \langle \{t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k | 1 \leq i \leq j \leq s\}, \{\sum_{\nu=0}^{s} \eta_\nu^{(k)} t_\nu | 1 \leq k \leq m\} \rangle,$$

donde $t_0 := 1$. *Entonces*

3. *La asignación* $t_i \mapsto u_i/x$, $i = 1, \ldots, s$ *define un isomorfismo*

$$A[t_1, \ldots, t_s]/I \xrightarrow{\cong} Hom_A(J, J) \cong \frac{1}{x} \cdot (xJ : J) :$$

Demostración. 1. Usaremos lema 7.2.1. En general tenemos que $A \subset \frac{1}{x}(xJ : J) \subset Q(A)$. Pero también sabemos que $\frac{1}{x}(xJ : J) \cong Hom_A(J, J)$. Luego si tenemos la igualdad $A = \frac{1}{x}(xJ : J)$ multiplicando por x tendremos $\langle x \rangle = (xJ : J)$.
2. Dado que u_i y u_j son elementos del ideal $xJ : J$, $u_i \in (xJ : J)$, esto quiere decir que $u_i J \subset xJ$ y en particular $u_i u_j \in xJ = \langle xu_0, \ldots, xu_s \rangle$. Por tanto existe $\xi_k^{ij} \in A$ tal que $u_i u_j = \sum_{k=0}^{s} \xi_k^{ij} x u_k$ como queríamos.
3. Definimos el homomorfismo de anillos $\phi : A[t_1, \ldots, t_s] \to (1/x) \cdot (xJ : J)$ como $t_i \mapsto u_i/x$ con $i = 1, \ldots, s$. Veamos que $I = Ker(\phi)$ y por tanto por el primer teorema de isomorfía tendremos que $\phi : A[t_1, \ldots, t_s]/I \to (1/x) \cdot (xJ : J)$ es un isomorfismo, dado que esta claro que la imagen de ϕ es $(1/x) \cdot (xJ : J)$. Obviamente $I \subset Ker(\phi)$. Consideramos un elemento general de I

$$t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k$$

Aplicando el homomorfismo ϕ a este elemento tenemos que

$$\phi(t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k) = \frac{u_i}{x} \cdot \frac{u_j}{x} - \sum_{k=0}^{s} \xi_k^{ij} \cdot \frac{u_k}{x}$$

Y usando la igualdad del apartado anterior obtenemos que ϕ anula los generadores de I con lo que tenemos la inclusión querida. Si ahora tomásemos un generador de la forma $\sum_{\nu=0}^{s} \eta_\nu^k t_\nu$, aplicando el homomorfismo obtendríamos $\sum_{\nu=0}^{s} \eta_\nu^k \frac{u_\nu}{x}$ y por definición de syzigia tenemos que $\sum_{\nu=0}^{s} \eta_\nu^k u_\nu = 0$. Luego este generador estará también en el núcleo de ϕ. Por otro lado, sea $h \in Ker(\phi)$. Entonces, usando las relaciones $t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k$, $1 \leq i \leq j \leq s$, podemos escribir $h \equiv h_0 + \sum_{i=1}^{s} h_i t_i \mathrm{mod}\ I$, para algún $h_0, h_1, \ldots, h_s \in A[t_1, \ldots, t_s]$. Ahora $\phi(h) = 0$ implica que $h_0 + \sum_{i=1}^{s} h_i \cdot (u_i/x) = 0$, entonces $(h_0, \ldots, h_s)$ es una sizigia de $u_0 = x, u_1, \ldots, u_s$, y en consecuencia $h \in I$ por la definición del ideal I. □

7.3. Algoritmos

Ahora usando la proposición 7.2.5 y el lema 7.2.9 obtenemos un algoritmo para calcular la clausura integral. Describimos un algoritmo par el caso en que $A = K[x_1, \ldots, x_n]/I$ es un dominio de integridad donde K es un cuerpo de característica 0. Recordemos que A es dominio si y solo si I es ideal, que es equivalente a I primo. Sea $I = \langle f_1, \ldots, f_m \rangle$ y $r = dim(A)$. Para poder aplicar la proposición 7.2.5, necesitamos encontrar un ideal J tal que $V(J)$ contiene un lugar geométrico no normal para el anillo A.
El conductor será un candidato, pero no lo podemos calcular sin conocer $\overline{A}$. Nos basta el ideal que define el lugar singular.
Ahora estamos preparados para dar un algoritmo de normalización. Nos restringiremos al caso de dominios de integridad afines $A = K[x_1, \ldots, x_n]/I$.

Proposición 7.3.1. *Calcularemos la normalización de I (NORMALIZACIÓN(I).*
Como ***Input*** *tendremos $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$ un ideal primo y $x = (x_1, \ldots, x_n)$.*
Como ***Output*** *tendremos un anillo de polinomios $K[t]$, con $t = (t_1, \ldots, t_N)$, un ideal primo $P \subset K[t]$ y $\pi : K[x] \to K[t]$ tal que induce la aplicación $\pi : K[x]/I \to K[t]/P$ que es la normalización de $K[x]/I$. ($\overline{A} = K[t]/P$).*

- *Si $I = \langle 0 \rangle$ el algoritmo devolverá como* ***output*** *$(K[x], \langle 0 \rangle, id_{K[x]})$;*
- *Calculamos $r := dim(I)$;*
- *Si sabemos que el lugar singular de I es $V(x_1, \ldots, x_n)$ entonces $J := \langle x_1, \ldots, x_n \rangle$; sino calcularemos $J :=$ el ideal de los $(n-r)$-menores de la matriz jacobiana de I. (El primer caso ocurre en curvas, cuando $r = 1$);*
- *J es el radical de $I + J$;*
- *Elijamos $a \in J \setminus \{0\}$. (Como $K[x]/I$ es dominio, la clase de a será no divisor de cero);*
- *Si $aJ : J = \langle a \rangle$ entonces devolveremos $(K[x], I, id_{K[x]})$;*
- *Calcularemos un sistema de generadores $u_0 = a, u_1, \ldots, u_s$ para $aJ : J$;*
- *Calcularemos un sistema de generadores $\{(\eta_0^{(1)}, \ldots, \eta_s^{(1)}), \ldots, (\eta_0^{(m)}, \ldots, \eta_s^{(m)})\}$ para el módulo de sizigias $syz(u_0, \ldots, u_s) \subset (K[x]/I)^{s+1}$;*

- *Calcularemos* ξ_k^{ij} *tal que* $u_i \cdot u_j = \sum_{k=0}^{s} a \cdot \xi_k^{ij} u_k$ *con* $i, j = 1, \ldots, s$;
- *Cambiaremos el anillo a* $K[x_1, \ldots, x_n, t_1, \ldots, t_s]$ *y el conjunto (con* $t_0 := 1$*)*

$$I_1 := \langle \{t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k\}_{0 \leq i \leq j \leq s}, \{\sum_{\nu=0}^{s} \eta_\nu^{(k)} t_\nu\}_{1 \leq k \leq m} \rangle + IK[x,t];$$

  Todos estos últimos pasos, calcular un sistema de generadores de $aJ : J$*, calcular un sistema de generadores para el módulo de sizigias y calcular los escalares* ξ_k^{ij}*; son posibles con el programa SINGULAR.*

- *Y devolveremos la NORMALIZACIÓN(*I_1*).*

Observemos que I_1 *sigue siendo un ideal primo ya que*

$$K[x_1, \ldots, x_n, t_1, \ldots, t_s]/I_1 \cong Hom_A(J, J) \subset Q(A)$$

es un dominio de integridad.

Sabemos que este algoritmo anterior es correcto debido a la proposición 7.2.5 y la terminación se deriva del siguiente teorema que solo enunciamos.

Teorema 7.3.2. *(E. Noether) Sea* $P \subset K[x_1, \ldots, x_n]$ *un ideal primo y sea* $A = K[x_1, \ldots, x_n]/P$*. Entonces la normalización* $\overline{A} \supset A$ *es un A-módulo finito*

La demostración del teorema requiere de otros lemas sobre los que apoyarse, pero se puede ver en el libro [4]

La proposición 7.2.5 y el lema 7.2.9 también nos da la posibilidad de calcular el lugar geométrico no normal.

Corolario 7.3.3. *Sea* A *y sea* J *como en la proposición 7.2.5, entonces el ideal* $Ann_A(Hom_A(J, J)/A) \subset A$ *define el lugar geométrico no normal. Además,*

$$Ann_A(Hom_A(J, J)/A) = \langle x \rangle : (xJ : J)$$

para cualquier elemento que no sea divisor de cero $x \in J$*.*

Podemos tomar la primera parte del algoritmo de normalización para calcular el lugar geométrico no normal:

Proposición 7.3.4. *Calcularemos el lugar geométrico no normal de I, NON-NORMALLOCUS(I).*
Como **Input** *tendremos $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$ un ideal primo y $x = (x_1, \ldots, x_n)$.*
Como **Output** *tendremos un ideal $NN \subset K[x]$, que define el lugar geométrico no normal en $V(I)$.*

- *Si $I = \langle 0 \rangle$ devolveremos como* **output** *$(K[x])$;*
- *Calcularemos $r = dim(I)$;*
- *Calcularemos J el ideal de los $(n-r)$ menores de la matriz jacobiana de I;*
- *J será el radical de $I + J$;*
- *Elegimos $a \in J \setminus \{0\}$;*
- *Devolveremos $(\langle a \rangle : (aJ : J))$.*

7.4. Ejemplos cálculo normalización

7.4.1. Cúspide

Primero veremos el ejemplo de normalización la cúspide $x^2 - y^3$.
Sea $A := K[x,y]/\langle x^2 - y^3 \rangle$ y sea $J := \langle x, y \rangle \subset A$ un ideal. Recordemos que tal y como habíamos definido en el algoritmo 7.3.1, J es resultado de obtener el ideal J' de los $(n-r)$ menores de la matriz jacobiana, en este caso serán las derivadas parciales $\frac{\partial x^2-y^3}{\partial x} = 2x$ y $\frac{\partial x^2-y^3}{\partial y} = -3y^2$. Y por último debemos hacer el radical del ideal J', con lo cual llegamos a que $J = \langle x, y \rangle$. Ahora tomamos $x \in J$ que es no es un divisor de cero en A, aunque también nos valdría tomar y puesto que en este caso A es un dominio, ya que el polinomio $x^2 - y^3$ es irreducible. Realizamos $xJ : J = x\langle x, y \rangle : \langle x, y \rangle = \langle x^2, xy \rangle : \langle x, y \rangle = \langle x, y^2 \rangle$ pues tenemos la relación $x^2 = y^3$ en este anillo. Si ahora usamos el lema 7.2.1 que nos dice $Hom_A(J, J) \cong \frac{1}{x} \cdot (xJ : J)$ tenemos para nuestro caso que $Hom_A(J, J) = \langle 1, y^2/x \rangle$. Ahora usaremos la notación del lema 7.2.9. Definimos $u_0 := x, u_1 := y^2$. Obtenemos que $u_1^2 = y^4 = y \cdot y^3 = x^2 y$ de la fórmula del punto 2 del lema 7.2.9, con $\xi_0^{11} = y$ y $\xi_1^{11} = 0$. Usando ahora la fórmula del lema 7.2.9 calculamos el ideal I. Observemos que en este caso nos reduciremos a t, pues al hacer el producto $t_i t_j$ tenemos $1 \leq i \leq j \leq s$ con $s = 1$. Luego de la primera parte, sustituyendo para los valores que

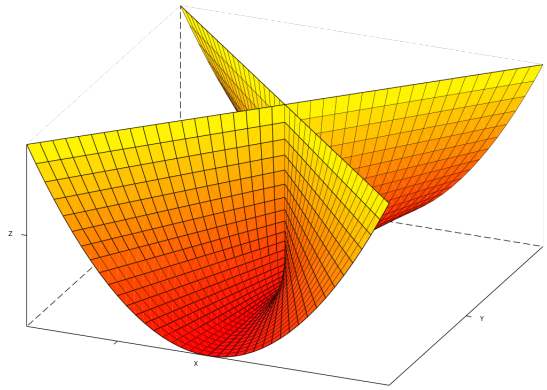
tenemos, obtenemos $t^2 - y$ ya que en la fórmula suponemos $t_0 := 1$. Por otro lado para calcular el resto de los generadores del ideal debemos calcular primero los generadores de la sizigia $syz(u_0, u_1)$ es decir, encontrar f, g tal que $fu_0 + gu_1 = 0 \in A$. El resultado será $x \cdot x - y \cdot y^2 = 0$ de donde sale $x - yt$ y también $y^2 \cdot y - x \cdot y^2 = 0$ de donde sale $y^2 - xt$. Por tanto usando ahora por el punto 3 del lema 7.2.9, tenemos el isomorfismo de A-álgebras

$$A[t]/\langle t^2 - y, xt - y^2, yt - x\rangle \to^{\cong} Hom_A(J, J).$$

Observemos que $A[t]/\langle t^2 - y, xt - y^2, yt - x\rangle \cong K[t]$ puesto que de la primera ecuación que generan el ideal I obtenemos $y = t^2$ y sustituyendo en la ultima tendremos que $x = t^3$, es decir podemos reducirlo a $K[t]$ que es normal y por tanto nos sirve con hacer una iteración. También veamos que $x \to t^3$ y $y \to t^2$ nos da una parametrización de $x^2 - y^3$.

7.4.2. Paraguas de Whitney

Ahora veremos la normalización del Paraguas de Whitney. El paraguas de Whitney se llama así debido al matemático estadounidense Hasseler Whitnet. Es una superficie específica auto-intersecada del espacio tridimensional. Es la unión de todas las lineas rectas que pasan a través de los puntos de una parábola fija y son perpendiculares a una linea recta fija, paralela al eje de la parábola u que se encuentran en su plano de bisección perpendicular. Observemos mejor la figura para que quede más claro.



El paraguas de Whitney se puede definir mediante las ecuaciones paramétricas en coordenadas cartesianas

$$\begin{cases} x(u,v) = u \\ y(u,v) = uv \\ z(u,v) = v^2 \end{cases}$$

donde los parámetros u y v varían sobre los números reales. También viene dada por la ecuación implícita

$$x^2 - y^2 z = 0.$$

Esta fórmula también incluye el eje z negativo (que se llama el mango del paraguas).
Aquí estamos hablando del dibujo en $\mathbb{R}$ del paraguas. En $\mathbb{C}$ la situación es más homogenea, $\forall z = \alpha \in \mathbb{C}$ tenemos que $x^2 - \alpha y^2$ es el producto de un par de rectas complejas de las que solo vemos en $\mathbb{R}$ el origen.
Ahora escribiremos el algoritmo de normalización del paraguas de Whitney, implementado con el programa SINGULAR.

```
ring A = 0,(x,y,z),dp;
ideal I = y2-zx2;
LIB ‘‘surf.lib";
plot(I,‘‘rot_x=1.45;rot_y=1.36;rot_z=4.5;");

list nor = normal(I);
def R = nor[1][1]; setring R;
norid;
//-> norid[1]= T(1)* x-y
norid[2]= -T(1)* y+x * z
norid[3]= T(1)^2-z
norid[4]= x^2 * z-y^2
normap;
//->  normap[1]=T(1)  normap[2]=T(1)*T(2)  normap[3]=T(2)^2
```

Luego la normalización de A/I es $K[T_1, T_2]$ con aplicación de normalización $x \mapsto T_1$, $y \mapsto T_1 T_2$ y $z \mapsto T_2^2$. Es fácil observar que coincide con la parametrización dada al inicio.

Vamos ahora a explicar que hace cada comando del programa.
Al definir el anillo A, el `0` corresponde a que el cuerpo base tiene característica 0 que se identifica con los número racionales, `(x,y,z)` representaran las variables y `dp` se corresponde con el orden inverso del orden lexicográfico.
Ahora definimos el ideal `I`, observemos que para singular y^2 se correspondería con `y2`. A continuación carga la librería para poder dibujar el paraguas de Whitney.
Sea crea una lista que la almacenaremos en `nor` al hacer la normalización del ideal `I`. `nor[1]` es una lista de r anillo, donde r es el número de primos asociados P_i, como es primo entonces solo aparecerá un elemento en la

lista. Dentro de `nor[1][1]` tendremos 2 ideales: `norid` y `normap`. Tenemos `nor[1][1]/norid` es la normalización, es decir, la clausura integral de A/P_i en su cuerpo de fracciones. `normap` dará la aplicación de normalización de $A/I \to$ A/`norid`. En el caso de que hubiera más anillos al realizar `nor[1]`, la suma directa de `nor[1][i]/norid`, cada uno con su respectivo `norid` sería la normalización de A/I. En este caso solo hay un anillo y por tanto es todo más sencillo.

Ahora lo veremos en términos matemáticos.
Consideramos $A := K[x,y,z]/\langle y^2 - x^2 z\rangle$. Igual que para el ejemplo de la cúspide debemos calcular J.
Realizamos las derivadas parciales

$$\frac{\partial y^2 - x^2 z}{\partial x} = -2xy, \frac{\partial y^2 - x^2 z}{\partial y} = 2y, \frac{\partial y^2 - x^2 z}{\partial z} = -x^2$$

y hacemos el radical. Obtenemos $J = \langle x, y\rangle$. Elegimos $x \in J$ que no es divisor de cero en A.
Tenemos que $\langle xJ : J\rangle = x\langle x,y\rangle : \langle x,y\rangle = \langle x^2, xy\rangle : \langle x,y\rangle = \langle x,y\rangle$. Luego $\frac{1}{x}\langle xJ : J\rangle = \frac{1}{x}(x,y) = A\cdot 1 + A\cdot \frac{y}{x} = A[y/x]$.

Si identifico $t = \frac{y}{x}$ tengo que $A[y/x] = A[t]/\langle tx - y\rangle = K[x,y,z,t]/\langle y^2 - x^2 z, tx - y\rangle \cong K[x,t]$ que será la normalización de A, es decir, $\overline{A}$. De la ecuación $y = tx$ podemos obtener $y^2 = t^2x^2$ que a su vez es $y^2 = zx^2$, luego $x^2(t^2 - z) \in \langle y^2 - x^2 z, tx - y\rangle$ y por tanto $x = x, y = tx, z = t^2, t = t$, que se corresponde con la parametrización que habíamos dado al inicio. Si ahora renombramos $x = t_1$ y $t = t_2$ tenemos que la normalización $K[x,y,z]/\langle y^2 - x^2 z\rangle \to K[t_1,t_2]$ envía $x \mapsto t_1, y \mapsto t_1 t_2, z \mapsto t_2^2$.
La aplicación que SINGULAR daría como `normap` el isomorfismo

$$K[x,y,z]/\langle y^2 - x^2 z\rangle \hookrightarrow K[x,y,z,t]/\langle y^2 - x^2 z, y - xt, xz - yt, z - t^2\rangle \cong K[x,t].$$

Bibliografía

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802].

[2] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[3] Wolfram Decker, Gert-Martin Greuel, and Gerhard Pfister. Primary decomposition: Algorithms and comparisons. In *Algorithmic algebra and number theory. Selected papers from a conference, Heidelberg, Germany, October 1997*, pages 187–220. Berlin: Springer, 1999.

[4] Gert-Martin Greuel and Gerhard Pfister. *A Singular introduction to commutative algebra. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.* Berlin: Springer, 2nd extended ed. edition, 2007.

[5] Miles Reid. *Undergraduate commutative algebra*, volume 29 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1995.