# Apuntes Álgebra Conmutativa

4 de marzo de 2021

# Capítulo 1

# Repaso estructuras

**Definición 1.1.** Un *anillo* conmutativo unitario es una terna $(A, +, \cdot)$ de un conjunto con dos operaciones internas, suma $+$ y producto $\cdot$, donde $(A, +)$ es un grupo conmutativo, el producto es asociativo y conmutativo, se cumple la propiedad distributiva, y existe $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$.

Todos los anillos con los que trabajaremos serán conmutativos y unitarios. Un subconjunto $S \subset A$ de un anillo es un *subanillo* de $A$ si es un anillo con la suma y el producto de $A$.

**Definición 1.2.** Un *ideal* de un anillo $A$ es un subconjunto $\mathfrak{a} \subset A$ que cumple:

1. Para todo $a, b \in \mathfrak{a}$ se tiene $a + b \in \mathfrak{a}$.
2. Para todo $a \in \mathfrak{a}$ y $x \in A$ se tiene $ax \in \mathfrak{a}$.

Obviamente, si un ideal de un anillo $A$ contiene el $1 \in A$, entonces es el total.

Dado un subconjunto $S$ de un anillo $A$, se puede considerar $\langle S \rangle$ el menor ideal que lo contiene, que resulta ser

$$\langle S \rangle = \left\{ \sum_{i=1}^{m} s_i a_i \Big| \; s_i \in S, a_i \in A, m \in \mathbb{N} \right\}$$

Dado un ideal $\mathfrak{a}$ se puede definir una relación de equivalencia $x \sim y \iff x - y \in \mathfrak{a}$ y el conjunto cociente resultante ${}^{A}\!/\!_{\mathfrak{a}}$ se dota de estructura de anillo con las operaciones $(a + \mathfrak{a}) + (b + \mathfrak{a}) := (a + b) + \mathfrak{a}$ y $(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) := ab + \mathfrak{a}$. Es necesario que sea un ideal para que el producto esté bien definido.

**Definición 1.3.** Un anillo $A$ es un dominio de integridad (DI) si para cualesquiera $a, b \in A$ tales que $ab = 0$ se tiene $a = 0$ o bien $b = 0$.

**Definición 1.4.** Sean $A, B$ anillos, un *homomorfismo de anillos* entre $A$ y $B$ es una aplicación $\varphi : A \to B$ que tal que para todo $x, y \in A$ respeta la suma $\varphi(x +_A y) = \varphi x +_B \varphi y$, respeta el producto $\varphi(x \cdot_A y) = \varphi(x) \cdot_B \varphi(y)$, y además $\varphi(1_A) = 1_B$.

Dado un homomorfismo de anillos $\varphi : A \to B$ el núcleo $\ker\varphi$ es un ideal de $A$ y la imagen $\mathrm{Im}\varphi$ es un subanillo de $B$. Además, para todo $\mathfrak{b}$ ideal de $B$, la preimagen $\varphi^{-1}(\mathfrak{b})$ es un ideal de $A$.

**Teorema 1.5. (de isomorfía)** *Dado un homomorfismo de anillos $\varphi : A \to B$, se cumple $A/_{\ker\varphi} \cong Im\varphi$. En particular, si $\varphi$ es sobreyectivo, entonces $A/_{\ker\varphi} \cong B$.*

**Teorema 1.6. (de la correspondencia)** *Sea $A$ una anillo y $\mathfrak{a}$ un ideal de $A$. Existe una biyección entre los ideales de $A$ que contienen a $\mathfrak{a}$ y los ideales del cociente $A/_{\mathfrak{a}}$. En particular, todos los ideales de $A/_{\mathfrak{a}}$ son de la forma $\mathfrak{b}/_{\mathfrak{a}} = \{x + \mathfrak{a} : x \in \mathfrak{b}\}$ donde $\mathfrak{b}$ es un ideal que contiene a $\mathfrak{a}$.*

**Definición 1.7.** Un ideal $\mathfrak{p}$ de un anillo $A$ se dice *primo* si es propio y para cualesquiera $a, b \in A$ tales que $ab \in \mathfrak{p}$ se tiene que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Un ideal $\mathfrak{m}$ de $A$ se dice maximal si es propio y no está contenido en ningún otro ideal propio de $A$.

Comprobar que un ideal $\mathfrak{m}$ de una anillo $A$ es maximal consiste en ver que si $\mathfrak{a} \supset \mathfrak{m}$ para otro $\mathfrak{a}$ ideal propio, entonces $\mathfrak{a} = \mathfrak{m}$.

Tanto la maximalidad como la primalidad se conservan por el teorema de la correspondencia, es decir, $\mathfrak{b}$ es primo / maximal en $A$ si y solo si $\mathfrak{b}/_{\mathfrak{a}}$ es primo / maximal en $A/_{\mathfrak{a}}$.

**Proposición 1.8.** *Un ideal $\mathfrak{p}$ de un anillo $A$ es primo si y solo si $\mathfrak{A}/_{\mathfrak{p}}$ es DI. Un ideal $\mathfrak{m}$ de $A$ es maximal si y solo si $\mathfrak{A}/_{\mathfrak{m}}$ es un cuerpo.*

Como todo cuerpo es dominio de integridad tenemos probado automáticamente que

**Corolario 1.9.** *Todo ideal maximal es primo.*

## 1.1 Operaciones con ideales

Sea $A$ un anillo y sean dos ideales $\mathfrak{a}_1, \mathfrak{a}_2 \subset A$. Se define la *suma* de los ideales como

$$\mathfrak{a}_1 + \mathfrak{a}_2 = \left\{x + y \middle|\, x \in \mathfrak{a}_1, y \in \mathfrak{a}_2\right\}$$

y resulta ser el menor ideal que contiene a ambos. La *intersección* de los ideales es la intersección conjuntista con las operaciones heredadas, y es el mayor ideal que está contenido en ambos ideales. El *producto* de los ideales

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \left\{\sum_{i=1}^{m} x_i y_i \middle|\, x_i \in \mathfrak{a}_1, y_i \in \mathfrak{a}_2, m \in \mathbb{N}\right\}$$

y también es un ideal.

**Observación 1.10.** Se cumple $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2$ (trivial), y se tiene la igualdad si $\mathfrak{a}_1 + \mathfrak{a}_2 = A$. Efectivamente, en tal caso, $1 = a_1 + a_2$ para ciertos $a_i \in \mathfrak{a}_i$, y entonces para todo $t \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, $t = ta_1 + ta_2 \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$.

Cuando $\mathfrak{a}_1 + \mathfrak{a}_2 = A$ se dice que los ideales son *comaximales*.

# Capítulo 2

**Definición 2.1.** Sea $\varphi : A \to B$ homomorfismo de anillos (conmutativos unitarios). Se dice que $B$ es una $A$-álgebra.

**Ejemplo 2.2.**
1. Si $A$ es un subanillo de $B$, entonces $B$ tiene estructura de $A$-álgebra via la inclusión $i : A \to B$.

2. En concreto, si $\mathbb{K}$ es un cuerpo, tenemos el ejemplo anterior para $B = \mathcal{M}_n(\mathbb{K})$ y $A = \{D \in B : \ D \text{ es diagonal con } \operatorname{diag}(D) = (\lambda, \ldots, \lambda)\}$.

3. Si consideramos un cociente de un anillo $A$ por un ideal suyo $\mathfrak{a}$, entonces la proyección canónica $p : A \to {}^{A}\!/_{\mathfrak{a}}$ dota al cociente de estructura de $A$-álgebra.

4. Si $K$ es un cuerpo, entonces una extensión suya $L|K$ es una $K$-álgebra.

**Observación 2.3.** En estos ejemplos se ve que el homomorfismo de anillos que da la estructura de álgebra no debe cumplir nada en particular: puede o no ser inyectivo, sobreyectivo, etc.

**Definición 2.4.** Sean $A$ un anillo y $B, C$ dos $A$-álgebras. Se dice que $f : B \to C$ es un hhomomorfismo de $A$-álgebras si hace conmutativo el diagrama siguiente:

$$\begin{tikzcd}
A \arrow[r, "\varphi_B"] \arrow[dr, "\varphi_C"'] & B \arrow[d, "f"] \\
 & C
\end{tikzcd}$$

**Definición 2.5.** Sea $A$ un anillo, se llama $A$-módulo a cualquier grupo abeliano $(M, +)$ de $(A, +)$ junto con una operación externa $A \times M \to M$ que cumpla que para todo $m, n \in M, a, b \in A$:

1. $a(m + n) = am + an$

2. $(a + b)m = am + bm$

3. $(ab)m = a(bm)$

4. $1_A m = m$.

**Ejemplo 2.6.**
1. Si $\mathbb{K}$ es un cuerpo, todo $\mathbb{K}$-espacio vectorial es un $\mathbb{K}$-módulo..

2. Si $V$ es un $\mathbb{K}$-espacio vectorial de dimensión finita y $f : V \to V$ un endomorfismo, entonces $V$ es un $\mathbb{K}[x]$-módulo via la aplicación

$$\begin{aligned} \mathbb{K}[x] \times V &\to V \\ (p(x), v) &\mapsto p(f) = a_n f^{(n)} + \cdots + a_1 f + a_0 \end{aligned}$$

siendo $p(x) = a_n x^n + \cdots + a_1 x + a_0$ y $f^(k) = f \circ \overset{k)}{\ldots} \circ f$.

3. Toda $A$-álgebra $B$ de un anillo $A$ es un $A$-módulo. $B$ es un anillo luego $(B, +)$ es un grupo abeliano. Por ser $A$-álgebra, existe un homomorfismo $\varphi : A \to B$, y entonces podemos definir la operación externa de la definición 2.5 como $A \times B \to B$ que hace corresponder $(a, b) \mapsto \varphi(a)b$.

**Observación 2.7.** Atendiendo al último ejemplo resulta que dados dos anillos $A, B$, dar a $B$ estructura de $A$-álgebra es equivalente a darle estructura de $A$-módulo junto con la propiedad adicional de que

$$\forall b, b' \in B,\ \forall a \in A \quad a \cdot_{\text{ext}} (bb') = (a \cdot_{\text{ext}} b)b'$$

**Definición 2.8.** Sea $B$ una $A$-álgebra mediante $f : A \to B$. Se dice que $B$ está finitamente generada si existen $b_1, \ldots, b_r \in B$ tales que para todo $x \in B$ se cumpla

$$x = \sum_{i_1,\ldots,i_r} f(a_{i_1,\ldots,i_r}) b_1^{i_1} \ldots b_r^{i_r}$$

**Observación 2.9.** Sea $B$ una $A$-álgebra, si utilizamos la caracterización de la observación 2.7, entonces $B$ es finitamente generada si y solo si existen $b_1, \ldots, b_r \in B$ tales que para todo $x \in B$ se escribe $x = \sum_{i_1,\ldots,i_r} a_{i_1,\ldots,i_r} b_1^{i_1} \ldots b_r^{i_r}$.

En el caso particular en que $A \subset B$, entonces $B$ es una $A$-álgebra finitamente generada si y solo si $B = A[b_1, \ldots, b_r]$ para ciertos $b_1, \ldots, b_r \in B$, es decir, el menor anillo que contiene a $A$ y a los $b_i$.

**Ejemplo 2.10.** 1. Si $A$ es un anillo, entonces $A \subset A[X_1, \ldots, X_n]$ y el anillo de polinomios es una $A$-álgebra finitamente generada.

2. Sean $A$ subanillo de $B$, con $B$ una $A$-álgebra finitamente generada por $\{b_1, \ldots, b_r\}$. Se puede tomar el anillo de polinomios $A[X_1, \ldots, X_r]$ y el homomorfismo evaluación en los $b_i$:

$$\begin{aligned} \text{eval}_{b_1,\ldots,b_r} : A[X_1, \ldots, X_r] &\to B \\ X_i &\mapsto b_i \\ A \ni a &\mapsto a \end{aligned}$$

El homomorfismo $\text{eval}_{b_1,\ldots,b_r}$ es suprayectivo porque los elementos de $B$ son expresiones polinomiales en $b_1, \ldots, b_r$. Aplicando el primer teorema de isomorfía tenemos

$$A[X_1, \ldots, X_r \big/ \ker \text{eval}_{b_1,\ldots,b_r} \cong B$$

3. Más generalmente, si $B$ es una $A$-álgebra finitamente generada, también es una $f(A)$-álgebra finitamente generada y se puede repetir el ejemplo anterior con $f(A)$, que es subanillo de $B$.

## 2.1 Uso del lema de Zorn en álgebra conmutativa

**Definición 2.11.** Sea un conjunto parcialmente ordenado $(S, \leq)$. Una cadena $T \subset S$ es un subconjunto tal que para cualesquiera $x, y \in T$ se cumple $x \leq y$ o $y \leq x$.

**Lema 2.12. (de Zorn)** *Sea un conjunto parcialmente ordenado $(S, \leq)$. Si toda cadena $T \subset S$ tiene una cota superior, entonces existe un elemento maximal en $S$.*

**Proposición 2.13.** *Todo anillo $A \neq 0$ tiene un ideal maximal*

*Prueba.* Consideramos el conjunto $\Sigma$ de los ideales propios de $A$, que no es vacío porque $0 \in \Sigma$, y lo ordenamos con la inclusión. Sea $(\mathfrak{a}_i)_{i\in I}$ una cadena en $\Sigma$. Veamos que tiene una cota superior. Consideramos $\mathfrak{a}^* = \bigcup_{i\in I} \mathfrak{a}_i$, que es un ideal:

1. Para todos $x, y \in \mathfrak{a}^*$ existen $i, j \in I$ tales que $x \in \mathfrak{a}_i$ e $y \in \mathfrak{a}_j$. Como pertenecen a una cadena, podemos suponer que $\mathfrak{a}_i \subset \mathfrak{a}_j$ y por tanto $x, y \in \mathfrak{a}_j$, que es un ideal, luego $x - y \in \mathfrak{a}_j \subset a^*$.
2. Para todo $x \in \mathfrak{a}^*$ y todo $a \in A$, existe $i \in I$ tal que $x \in \mathfrak{a}_i$ y por tanto $xa \in \mathfrak{a}_i \subset \mathfrak{a}^*$.

Además, es un ideal propio porque $1 \notin \mathfrak{a}_i$ para todo $i \in I$ luego no pertenece a la unión. Entonces $\mathfrak{a}^* \in \Sigma$ y está claro que es una cota superior de la cadena, que es arbitraria. Podemos aplicar el lema de Zorn y concluimos que $\Sigma$ tiene un elemento maximal, y por tanto $A$ tiene un ideal maximal. □

**Corolario 2.14.** *Para todo ideal $\mathfrak{a}$ de un anillo $A$ existe un ideal maximal que lo contiene*

*Prueba.* Se aplica la proposición anteior al anillo ${}^{A}\!/_{\mathfrak{a}}$ teniendo en cuenta que en el teorema de la correspondencia se conservar los ideales maximales. □

**Proposición 2.15.** *Sea $A$ anillo, existe un ideal primo minimal*[1] $\mathfrak{p}$.

*Prueba.* Sabemos que existe un ideal maximal $\mathfrak{p} \subset A$, y este es primo por ser maximal. Consideramos $\Sigma$ el conjunto de los ideales primos de $A$, que es no vacío porque $\mathfrak{p} \in \Sigma$, y lo ordenamos parcialmente con la inclusión tal que $\mathfrak{p} \leq \mathfrak{p}' \iff \mathfrak{p} \supset \mathfrak{p}'$ . Sea $\{\mathfrak{q}_i\}_{i\in I} \subset \Sigma$ una cadena y consideramos $\mathfrak{q}^* := \bigcap_{i\in I} q_i$. Este es un ideal (la intersección siempre lo es) y $\mathfrak{q}^* \subset \mathfrak{q}_i$ para todo $i \in I$, por tanto es cota superior (para nuestro orden) de la cadena.

Veamos que $\mathfrak{q}^*$ es primo. Sean $ab \in \mathfrak{q}^*$, por ser así, $ab \in \mathfrak{q}_i$ para toda $i \in I$. Si $a \in \mathfrak{q}_i \forall i \in I$, entonces $a \in \mathfrak{q}^*$. Por otra parte, si existe $i_0 \in I$ tal que $a \notin \mathfrak{q}_{i_0}$

$$\begin{aligned} &\text{entonces } b \in \mathfrak{q}_j \forall j \in I: \\ &\quad \text{si } \mathfrak{q}_{i_0} \subseteq \mathfrak{q}_j,\ \text{como } b \in \mathfrak{q}_{i_0},\ \text{se tiene que } b \in \mathfrak{q}_j \text{y}, \end{aligned}$$

Así se tiene $\mathfrak{q}^* \in \Sigma$ y aplicando el lema de Zorn, existe un elemento maximal para el orden dado, equivalemente, minimal en sentido de la inclusión. □

**Corolario 2.16.** *Sea $A$ anillo y $\mathfrak{a}$ ideal de $A$, existe un ideal primo minimal entre los que contienen a $\mathfrak{a}$.*

[1] Un ideal primo que no contiene a ningún otro ideal primo.

**Definición 2.17.** Sea $A$ un anillo. Un elemento $x \in A$ se dice *nilpotente* si existe un $n \in \mathbb{N} \setminus \{0\}$ tal que $x^n = 0$.

**Definición 2.18.** Sea $A$ un anillo. El *radical* de un ideal $\mathfrak{a}$ de $A$ se define como

$$\sqrt{\mathfrak{a}} = \{x \in A : \exists n > 0 \text{ tal que } x^n \in \mathfrak{a}\}$$

**Proposición 2.19.** *Sea $A$ un anillo, entonces el conjunto $\mathfrak{N}_A$ de todos los elementos nilpotentes de $A$ es un ideal. Se le llama* nilradical *de $A$.*

*Prueba.*

1. Si $x \in \mathfrak{N}_A$ y $a \in A$, existe $n > 0$ tal que $x^n = 0$ y por tanto $(xa)^n = x^n a^n = 0$.
2. Si $x, y \in \mathfrak{N}_A$, existen $m, n > 0$ tales que $x^n = y^m = 0$. Utilizando el binomio de Newton se tiene que $(x+y)^{n+m-1}$ es una suma de multiplos de productos de la forma $x^r y^s$ con $r + s = m + n - 1$, y por tanto no se puede tener a la vez $r < n$ y $s < m$, de manera que cada uno de los sumandos es 0 y $(x+y)^{n+m-1} = 0$.

□

**Proposición 2.20.** *El nilradical de un anillo $A$ verifica $\mathfrak{N}_A = \bigcap_{\mathfrak{p}\ primo} \mathfrak{p}$.*

*Prueba.* Denotamos por $\mathfrak{N}$ a la intersección. Si $x \in \mathfrak{N}_A$ entonces existe $n > 0$ con $x^n = 0$. El cero pertenece a todo ideal, en particular para todo $\mathfrak{p}$ primo $0 = x^n = xx^{n-1} \in \mathfrak{p}$, lo que implica que $x \in \mathfrak{p}$ (porque o bien $x \in \mathfrak{p}$ o bien $x^{n-1} \in \mathfrak{p}$ y repetimos). Por tanto $x \in \mathfrak{N}$ y $\mathfrak{N}_A \subset \mathfrak{N}$.

Para ver el otro contenido, comprobamos que si $x_0 \notin \mathfrak{N}_A$ entonces existe $\mathfrak{p}$ primo tal que $x \notin \mathfrak{p}$. Sea $\Sigma = \{\mathfrak{a} :\ \text{ideal propio tal que } x_0^n \notin \mathfrak{a} \text{ para todo } n > 0\}$, que es un conjunto no vació porque pertenece el 0, ya que si $x_0$ no es nilpotente, ninguna de sus potencias es 0, así que $x_0^n \notin \{0\}$ para todo $n$. Argumentamos igual que en la proposición 2.13 y obtenemos un elemento maximal de $\mathfrak{p}^* \in \Sigma$.

Veamos que $\mathfrak{p}^*$ es primo, equivalentemente, que si $x, y \notin \mathfrak{p}^*$, entonces $xy \notin \mathfrak{p}^*$. Sean entonces $x, y \notin \mathfrak{p}^*$, y consideramos $\mathfrak{p}^* + (x)$ y $\mathfrak{p}^* + (y)$ ideales que contienen a $\mathfrak{p}^*$ estrictamente. Como $\mathfrak{p}^*$ es un elemento maximal de $\Sigma$, esos dos ideales no pueden pertenecer a $\Sigma$, así que por definición existen $m, n > 0$ tales que $x_0^n \in \mathfrak{p}^* + (x)$ y $x_0^m \in \mathfrak{p}^* + (y)$. Entonces existen $p, q \in \mathfrak{p}^*$ tales que

$$x_0^{m+n} = x_0^n x_0^m = (p+x)(q+y) = \underset{\in\mathfrak{p}}{pq} + \underset{\in(xy)}{py} + \overset{\in(xy)}{qx} + \overset{\in(xy)}{xy} \in \mathfrak{p}^* + (xy)$$

Por tanto $\mathfrak{p}^* + (xy) \notin \Sigma$, y como $\mathfrak{p}^* \in \Sigma$, entonces $xy \notin \mathfrak{p}^*$. □

## 2.2 Extensión y contracción de ideales

**Definición 2.21.** Sea $\phi : A \to B$ un homomorfismo de anillos y sea $\mathcal{I}(A), \mathcal{I}(B)$ los conjuntos de ideales de $A$ y $B$. Se define la *extensión de ideales* como la aplicación

$$\begin{aligned} e : \mathcal{I}(A) &\to \mathcal{I}(B) \\ \mathfrak{a} &\mapsto \mathfrak{a}^e = \left\{ \sum_{i=1}^{m} \phi(a_i) b_i \,\middle|\, a_i \in \mathfrak{a}, b_i \in B, m \in \mathbb{N} \right\} \end{aligned}$$

y la *contracción de ideales* como

$$\begin{aligned} c : \mathcal{I}(B) &\to \mathcal{I}(A) \\ \mathfrak{b} &\mapsto \phi^{-1}(\mathfrak{b}) \end{aligned}$$

**Observación 2.22. Propiedades de la extensión y la contracción**

1. La contracción conserva ideales primos.
2. $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$.
3. $(\mathfrak{b}_1 \cap \mathfrak{a}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.

## 2.3 Lenguaje geométrico en álgebra conmutativa

**Definición 2.23.** Sea $K$ un cuerpo, se dice que es *algebraicamente cerrado* si se cumple cualquiera de las condiciones equivalentes:

1. Para todo $f \in K[x] \setminus \{0\}$ existe $a \in K$ tal que $f(a) = 0$.
2. Todo $f \in K[x] \setminus \{0\}$ se descompone en factores de primer grado, es decir, si $\deg f = n$, $f(x) = \lambda \prod_{i=1}^n (x - a_i)$ para ciertos $\lambda, a_1, \ldots, a_n$.
3. Toda extensión algebraica $L|K$ es trivial: $L = K$.

**Proposición 2.24.** *Para todo cuerpo $K$ existe una extensión $L|K$ algebraicamente cerrada.*

*Prueba.* Ver teorema II.2.4 en [FG17]. □

**Definición 2.25.** Si $K$ es un cuerpo y $S \subset K[X_1, \ldots, X_n]$, entonces se dice que

$$Z_{\mathbb{A}^n_K} = \{a \in \mathbb{A}^n_K \,\big|\, f(a) = 0 \text{ para cada } f \in S\}$$

es un *conjunto algebraico* en $\mathbb{A}^n_K$.

El estudio de los conjuntos de ceros de polinomios está íntimamente relacionado con el estudio de ideales porque $\mathcal{Z}(S) = \mathcal{Z}(\langle S \rangle)$. Efectivamente, si $a \in \mathcal{Z}(\langle S \rangle)$, como $S \subset \langle S \rangle$, entonces en particular $a$ anula a todo polinomio de $S$, luego $\mathcal{Z}(S) \supset \mathcal{Z}(\langle S \rangle)$. Recíprocamente, sea $a' \in \mathcal{Z}(S)$ y $g \in \langle S \rangle$ entonces existen $f_i \in S, g_i \in K[X_1, \ldots, X_n]$ para $i = 1, \ldots, m$ tales que $g(a') = \sum_{i=1}^m f_i(a') g_i(a') = 0$, así que $\mathcal{Z}(S) \subset \mathcal{Z}(\langle S \rangle)$.

**Ejemplo 2.26.** Sea un cuerpo $K$ algebraicamente cerrado y estudiemos los conjuntos algebraicos de $K[X]$ en $\mathbb{A}^n_K$. Solo hay tres tipos:

1. $\mathcal{Z}(0) = \mathbb{A}^n_K$ porque el 0 se anula en todas partes.
2. $\mathcal{Z}(K[X]) = \varnothing$ porque hay polinomios constantes no nulos.
3. Si $g(x) = \langle \prod_{i=1}^n (x - a_i) \rangle$, entonces $\mathcal{Z}(g) = a_1, \ldots, a_n$ porque un $f$ se anula en todos los $a_i$ si y solo si es múltiplo de $\prod_{i=1}^n (x - a_i)$.

Si $K$ es un cuerpo, para todo $f \in K[x]$ se pueden encontrar $f_1, \ldots, f_r$ sin factores irreducibles en $K[x]$ múltiples tales que $f = f_1 f_2^2 \ldots f_r^r$. En particular, $f_{\text{red}} = f_1 f_2 \ldots f_r$ es un polinomio con mismos ceros que $f$ pero de multiplicidad 1 [2]. Esto es útil, porque como $K[X]$ es un DIP, todo ideal es de la forma $\mathfrak{a} = fK[x]$. Dicho $f$ puede ser en principio más complejo de lo que es necesario, por ejemplo, para definir el conjunto algebraico $\{x \in \mathbb{R} |\ x^2 = 0\}$ podemos usar, en vez de $x^2$, el polinomio $x$.

**Lema 2.27.** *Sea $K$ un cuerpo, si $\mathfrak{a} \subset \mathfrak{b}$ son ideales de $K[X_1, \ldots, X_n]$, entonces $\mathcal{Z}(\mathfrak{a}) \supset \mathcal{Z}(\mathfrak{b})$.*

**Proposición 2.28.** *Sea $K$ un cuerpo y $A = K[X_1, \ldots, X_n]$*

1. *Si $\{\mathfrak{a}_i\}_{i \in I}$ una familia arbitraria de ideales de $A$, entonces $\mathcal{Z}(\sum_i \mathfrak{a}_i) \subset \bigcap_i \mathcal{Z}(\mathfrak{a}_i)$.*
2. *Si $\{\mathfrak{b}_j\}_{j=1}^m$ una familia finita de ideales de $K[X_1, \ldots, X_n]$, entonces $\bigcup_{j=1}^m \mathcal{Z}(\mathfrak{b}_j) = \mathcal{Z}(\mathfrak{b}_1 \ldots \mathfrak{b}_m)$.*

*Prueba.* Por orden

1. Sea $a \in \mathcal{Z}(\sum_i \mathfrak{a}_i)$. Cualquier $f_i \in \mathfrak{a}_i$ es en particular un elemento de $\sum_i \mathfrak{a}_i$ así que $f_i(a) = 0$. Como $i$ es arbitrario y $f_i$ también, entonces $a \in \bigcap_i \mathcal{Z}(\mathfrak{a}_i)$.

2. Comprobamos el doble contenido. Primero, como $\mathfrak{a} \cdot \mathfrak{b} \subset (\mathfrak{a} \cap \mathfrak{b})$ y este está contenido en ambos $\mathfrak{a}$ y $\mathfrak{b}$, entonces por el lema 2.27 $\mathcal{Z}(\mathfrak{a}), \mathcal{Z}(\mathfrak{b}) \subset \mathcal{Z}(\mathfrak{a} \cdot \mathfrak{b})$, y así su unión también está contenida.

El otro contenido lo hacemos por contrarrecíproco. Si $a \notin \mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b})$, entonce es que $a \notin \mathcal{Z}(\mathfrak{a})$ y $a \notin \mathcal{Z}(\mathfrak{b})$. Existen $f \in \mathfrak{a}$ y $g \in \mathfrak{b}$ tales que $f(a) \neq 0$ y $g(a) \neq 0$, por tanto $fg(a) = f(a)g(a) \neq 0$, y entonces $a \notin \mathcal{Z}(\mathfrak{a} \cdot \mathfrak{b})$.

□

De acuerdo a lo que hemos visto, los conjuntos algebraicos en $\mathbb{A}_K^n$ son una colección $\mathcal{A}$ de subconjuntos que cumplen:

1. $\varnothing, \mathbb{A}_K^n \in \mathcal{A}$,
2. la intersección arbitraria de conjuntos de $\mathcal{A}$ pertenece a $\mathcal{A}$,
3. la unión finita de conjuntos de $\mathcal{A}$ pertenece a $\mathcal{A}$.

Estos son los tres axiomas que debe cumplir una familia de conjuntos para ser los cerrados de una *topología*.

**Teorema 2.29. (de la base de Hilbert)** *Si $A$ es un anillo tal que todo ideal de $A$ está finitamente generado, entonces $A[X]$ también cumple esa propiedad.*

*Prueba.* Sea $\mathfrak{I} \subset A[x]$ un ideal, y formamos el conjunto de los coeficientes principales de polinomios en $\mathfrak{I}$.

$$\mathfrak{a} = \{c \in A \setminus \{0\} |\ \exists r \in \mathbb{N} \text{ con } cx^r + \text{tmg} \in \mathfrak{i}\} \cup \{0\}^3$$

Comprobamos que $\mathfrak{a}$ es un ideal.

[2] Ver apéndice.

[3] Aquí tmg significa términos de menor grado. Expresamos así el polinomio porque no será necesario prestar atención al resto.

1. Sean $c, d \in \mathfrak{a}$. Si $c = d$ entonces $c - d = 0 \in \mathfrak{a}$. Si $c \neq d$, entonces existen $r, s$ tales que $f = cx^r + \text{tmg}, g = dx^s + \text{tmg} \in \mathfrak{I}$. Entonces por ser $\mathfrak{I}$ un ideal tenemos que

$$\mathfrak{I} \ni f - x^{r-s}g = (c-d)x^r + \text{tmg}$$

con lo que $c - d \in \mathfrak{a}$ también.

2. Sean $c \in \mathfrak{a}$ y $\lambda \in A$. Si $\lambda = 0$ es trivial. Si no, existe $f \in \mathfrak{I}$ con $c$ de coeficiente principal, y $\lambda f \in \mathfrak{I}$ tiene a $\lambda c$ de coeficiente principal, luego $\lambda c \in \mathfrak{a}$.

Por hipótesis, $\mathfrak{a}$ está finitamente generado $\mathfrak{a} = \langle c_1, \ldots, c_s \rangle$. Para cada $i = 1, \ldots, s$ existe un $f_i \in \mathfrak{I}$ con $c_i$ como coeficiente principal. Sea $\delta = \max_{1 \leq i \leq s} \deg f_i$, y para cada $\gamma \leq \delta$ definimos

$$\mathfrak{a}_\gamma = \{d \in A \setminus \{0\} | \ \exists f \in \mathfrak{I} \text{ con } \deg f = \gamma y c o n d \text{ como coeficiente principal}\} \cup \{0\}$$

que también es un ideal de $A$:

1. Sean $c, d \in \mathfrak{a}_\gamma$. Si $c = d$ entonces $c - d = 0 \in \mathfrak{a}$. Si $c \neq d$, entonces existen $f, g \in \mathfrak{I}$ de grado $\gamma$ con coeficientes principales $c, d$ respectivamente, entonces $f - g \in \mathfrak{I}$ es de grado $\gamma$ y tiene a $c - d$ por coeficiente principal.

2. Si $c \in \mathfrak{a}$ y $\lambda \in A$. Si $\lambda = 0$ es trivial. Si no, existe $f \in \mathfrak{I}$ de grado $\gamma$ con $c$ de coeficiente principal, y $\lambda f \in \mathfrak{I}$ es de grado $\gamma$ y tiene a $\lambda c$ de coeficiente principal.

De nuevo, por hipótesis, $\mathfrak{a}_\gamma$ es finitamente generado, así que $\mathfrak{a}_\gamma = \langle d_{\gamma_1}, \ldots, d_{\gamma_m} \rangle$, y para cada $j = 1, \ldots, m_\gamma$ existe un polinomio $g_{\gamma_j} \in \mathfrak{I}$ que tiene a $d_{\gamma_j}$ por coeficiente principal.

Vamos a comprobar que $\mathfrak{I} = \mathfrak{H}$ donde

$$\mathfrak{H} = \langle \{f_1, \ldots, f_s\} \cup \{g_{\gamma_j}\}_{\substack{1 \leq \gamma \leq \delta \\ 1 \leq j \leq m_\gamma}} \rangle \subset \mathfrak{I}$$

El contenido $\supset$ se tiene por construcción. Para el otro, sea $F \in \mathfrak{I} \setminus \{0\}$ (si $\mathfrak{I} = \{0\}$, es trivial) y sea $\mu = \deg F$. Distinguimos dos casos.

**Caso 1** Supongamos $\mu \geq \delta$, en caso contrario pasamos al caso 2. Sea $b \in \mathfrak{a}$ el coeficiente principal de $F$, entonces $b = \sum_{i=1}^{s} \lambda_i c_i$ para ciertos $\lambda_i \in A$. Resulta entonces que

$$F_1 = F - \underbrace{\sum_{i=1}^{s} \lambda_i x^{\mu - r_i} f_i}_{\in \mathfrak{H}} \in \mathfrak{I}, \qquad r_i = \deg f_i$$

es un polinomio de grado $< \mu$ por construcción. Además basta demostrar que $F_1 \in \mathfrak{H}$ para que $F \in \mathfrak{H} \subset \mathfrak{I}$.

Si $\mu_1 = \deg F_1 \geq \delta$, repetimos lo anterior para $F_1$ y obtenemos otro polinomio $F_2 \in \mathfrak{I}$ de grado estrictamente menor que $\mu_1$. Se cumple entonces que $F =$ (polinomio en $\mathfrak{H} + F_2$. Continuamos repitiendo hasta que obtenemos $F^* \in \mathfrak{I}$ de grado $\nu$ estrictamente menor que $\delta$. Entonces

$$F = (\text{polinomio en } \mathfrak{H}) + F^* \tag{2.1}$$

y basta ver que $F^*$ está en $\mathfrak{H}$ para que $F \in \mathfrak{H} \subset \mathfrak{I}$. Pasamos al caso 2.

**Caso 2** Como $\nu < \delta$, el coeficiente principal de $F^*$, $u$, está en $\mathfrak{a}_\nu$, o bien $F^* = 0$ en cuyo caso hemos terminado por (2.1). Como ese ideal está finitamente generado, tenemos $u = \sum_{j=1}^{m_\nu} t_j d_{\nu_j}$ para ciertos $t_j \in A$. Por definición de $\mathfrak{a}_\nu$, existen $g_{\nu_j}(x) \in \mathfrak{H}$ con $d_{\nu_j}$ como coeficiente principal para cada $j = 1, \ldots, m_\nu$. Podemos imitar el caso 1 y formar

$$F_1^* = F^* - \underbrace{\sum_{j=1}^{m_\nu} t_j g_{\nu_j}}_{\in \mathfrak{H}}$$

que por construcción es un polinomio de grado menor que $\nu$. Basta ver que $F_1^* \in \mathfrak{H}$ para que $F^* \in \mathfrak{H}$. Podemos repetir este paso para $F_1^*$ y obtendremos otro polinomio $F_2^* \in \mathfrak{I}$, de manera que $F_1^* \in \mathfrak{H}$ si $F_2^* \in \mathfrak{H}$. Como los grados de cada uno de los polinomios que obtenemos son cada vez menores, necesariamente en algún momento obtendremos un polinomio $F^{**} = 0 \in \mathfrak{H}$ y hemos terminado.

$\square$

**Corolario 2.30.** *Si $A$ es tal que todo ideal está finitamente generado, entonces $A[X_1, \ldots, X_n]$ también cumple es propiedad.*

**Teorema 2.31. (Nullstellensatz)** *Sea $K$ un cuerpo algebraicamente cerrado y $\mathfrak{a}$ un ideal de $K[X_1, \ldots, X_n]$, entonces*

$$\mathfrak{I}(\mathcal{Z}(\mathfrak{a})) = \{f \,\big|\, f(a) = 0 \text{ para todo } a \in \mathcal{Z}(\mathfrak{a})\} = \sqrt{\mathfrak{a}}$$

# Apéndice A

# Factorización de polinomios

Factorizamos el siguiente polinomio $f$ como $F_1(F_2)^2 \dots (F_r)^r$ para ciertos polinomios $F_i$ que tienen todos sus factores irreducibles de multiplicidad 1.

$$f(x) = (x-3)^4(x-2)^2(x+7)^2(x^2+1)$$

Calculamos su derivada formal, que comparte con $f$ los factores irreducibles múltiples de $f$. El máximo común divisor $f_1$ entre $f$ y $f'$ tiene como factores irreducibles exactamente a los factores irreducibles con multiplicidad mayor o igual a 2 de $f$, pero ahora con multiplicidad 1 menos que en $f$.

$$f_1 = \gcd(f, f') = (x-3)^3(x-2)(x+7)$$

Por lo tanto, al dividir $f$ entre $f_1$ nos queda un polinomio con todos los factores irreducibles de $f$ pero ahora con multiplicidad 1.

$$g_1 = \frac{f}{f_1} = (x-3)(x-2)(x+7)(x^2+1)$$

Ahora tomamos $f_1$ y repetimos el proceso. Este comparte con su derivada sus factores irreducibles múltiples, que son los factores irreducibles de multiplicidad mayor o igual a 3 de $f$. Esos son exactamente los factores irreducibles del máximo común divisor $f_2$ entre ambos, en el cual aparecen con multiplicidad 1 menos que en $f_1$, es decir, con multiplicidad 2 menos que en $f$.

$$f_2 = \gcd(f_1, f_1') = (x-3)^2$$

Ahora al calcular el cociente $\frac{f_1}{f_2}$ obtenemos un polinomio que tiene por factores irreducibles exactamente los de $f$ de multiplicidad mayor o igual a 2, pero ahora son simples.

$$g_2 = \frac{f_1}{f_2} = (x-3)(x-2)(x+7)$$

Finalmente, podemos sacar $F_1$, el primero de los polinomios que necesitamos para la factorización, sin más que dividir $g_1$ entre $g_2$. Efectivamente, $g_1$ tiene por factores irreducibles todos los de $f$ pero con multiplicidad 1, y $g_2$ todos los múltiples de $f$ pero con multiplicidad 1. Así al dividir solo quedarán los factores irreducibles simples.

$$F_1 = \frac{g_1}{g_2} = x^2 + 1$$

Ahora repetimos el proceso para $f_1$, es decir, en lo anterior hacer $f = f_1$. De esta forma obtendremos un polinomio que tiene por factores irreducibles exactamente a los factores irreducibles simples de $f_1$, que son los factores irreducibles dobles de $f$. Observamos que ya tenemos calculados el primer paso $\gcd(f_1, f_1') = f_2$, y el segundo $\frac{f_1}{f_2} = g_2$, así que sacamos

$$\begin{aligned} f_3 &= \gcd(f_2, f_2') = x - 3 \\ g_3 &= \frac{f_2}{f_3} = x - 3 \\ F_2 &= \frac{g_2}{g_3} = (x-2)(x+7) \end{aligned}$$

Repetimos dos veces más

$$\begin{aligned} f_4 &= \gcd(f_3, f_3') = 1 \\ g_4 &= \frac{f_3}{f_4} = x - 3 \\ F_3 &= \frac{g_3}{g_4} = 1 \end{aligned}$$

$$\begin{aligned} f_5 &= \gcd(f_3, f_3') = 1 \\ g_5 &= \frac{f_3}{f_4} = 1 \\ F_4 &= \frac{g_3}{g_4} = x - 3 \end{aligned}$$

¿Cómo sabemos cuando parar? Precisamente si intentamos repetir una vez más, obtenemos $f_6 = g_6 = F_5 = 1$, y como las siguientes etapas las construimos a partir de estos polinomios, quiere decir que todo lo que obtendremos a partir de ahora serán 1, así que debemos concluir el proceso con $F_4$. Esto nosotros lo sabíamos de antemano porque hemos escrito el polinomio factorizado en sus factores irreducibles y 4 era la mayor multiplicidad que teníamos, pero el criterio anterior es un criterio de parada general.

De esta forma tenemos$f$ factorizado como

$$f = F_1(F_2)^2(F_3)^3(F_4)^4$$

Además, el producto $f_{\text{red}} = F_1F_2F_3F_4$ es un polinomio que tiene mismos ceros que $f$ pero todos ellos simples.