Variedades afines

Benjamín Macías Quezada

2024
Santiago, Chile

Índice

1. Variedades algebraicas afines

La Geometría Algebraica, en su forma más clásica, estudia lugar de ceros en común de alguna familia de polinomios con coeficientes en algún cuerpo, a través de métodos algebraicos. Esta teoría es fundamentalmente distinta a la revisada, por ejemplo, en Cálculo (Real o Complejo), donde se trabaja con topologías euclidianas y funciones diferenciables u holomorfas. En Geometría Algebraica, eso es precisamente lo que *debemos* evitar, porque los espacios con los que nos toparemos simplemente no están dotados de una noción evidente de Cálculo, como por ejemplo es el caso de una clausura algebraica de un cuerpo finito.

Así, nuestro estudio será guiado por el querer asignar a cada objeto geométrico (que estamos prontos a definir), un objeto algebraico, y obviamente determinar cómo se traducen las propiedades entre estos dos mundos. También, vamos a poder definir una topología que captura la cualidad algebraica de nuestros objetos, que resultará radicalmente distinta a la euclideana.

1.1. Conjuntos algebraicos

Dado k un cuerpo y $n \in \mathbb{N}$, el *n-espacio afín* sobre k es el conjunto $\mathbb{A}^n_k := k^n$. Dado $S \subseteq k[x_1, \ldots, x_n]$, definimos su *lugar de ceros en* $\mathbb{A}^n_k$ como

$$\mathbb{V}(S) := \{a \in \mathbb{A}^n_k \colon f(a) = 0 \text{ para cada } f \in S\} \subseteq \mathbb{A}^n_k.$$

Los subconjuntos de $\mathbb{A}^n_k$ que son lugares de ceros de alguna familia de polinomios en $k[x_1, \ldots, x_n]$ se llaman *conjuntos algebraicos* de $\mathbb{A}^n_k$.

Ejemplo 1.1.

(1) Un punto $a := (a_1, \ldots, a_n) \in \mathbb{A}^n_k$ es un conjunto algebraico de $\mathbb{A}^n_k$, pues se tiene que $a = \mathbb{V}(x_1 - a_1, \ldots, x_n - a_n)$.

(2) En $\mathbb{A}^2_{\mathbb{R}}$, tenemos que $\mathbb{V}(y - x^2)$ (pictóricamente una parábola), y $\mathbb{V}(xy)$ (pictóricamente la unión de los ejes de coordenadas) son conjuntos algebraicos.

(3) Un hecho general es que los polinomios en una variable tienen siempre finitos ceros, por lo que en $\mathbb{A}^1_k$ los conjuntos algebraicos son precisamente los conjuntos finitos.

(4) En $\mathbb{A}^2_{\mathbb{R}}$, los conjuntos algebraicos de la forma $\mathbb{V}(x^3 - y^2 + ax + b)$, se llaman *curvas elípticas*, y son objetos importantes en Teoría de Números.

(5) En $\mathbb{A}^2_{\mathbb{Q}}$, podemos definir los conjuntos algebraicos $X_m := \mathbb{V}(x^m + y^m - z^m)$ para cada $m \in \mathbb{N}$. La afirmación que para $m \geq 3$ cada X_m solo tiene a los puntos triviales es el famoso *Último Teorema de Fermat*.

La notación $\mathbb{V}(-)$ es de hecho la de un funtor

$$\left\{\begin{array}{c}\text{subconjuntos de}\\ k[x_1,\ldots,x_n]\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{conjuntos}\\ \text{algebraicos de } \mathbb{A}^n_k\end{array}\right\},$$

con inclusión de conjuntos como morfismos. El funtor es contravariante, lo que se traduce a que invierte inclusiones:

Proposición 1.2. *Si* $T_1 \subseteq T_2 \subseteq k[x_1,\ldots,x_n]$*, entonces* $\mathbb{V}(T_2) \subseteq \mathbb{V}(T_1)$*.*

Demostración. Intuitivamente, mientras más polinomios consideremos, son menos los puntos de $\mathbb{A}^n_k$ que anulan a todos estos polinomios. Formalmente, un $a \in \mathbb{V}(T_2)$ anula a cada polinomio de T_2, en particular a todos aquellos que pertenezcan a T_1, es decir, $a \in \mathbb{V}(T_1)$. $\square$

Como anunciamos al principio del capítulo, podemos definir una topología en $\mathbb{A}^n_k$, que incluso cuando $k = \mathbb{R}$ o $\mathbb{C}$, es muy distinta a sus variantes euclidianas. Resulta que en $\mathbb{A}^n_k$, los conjuntos algebraicos son los cerrados de una topología, llamada *de Zariski*:

Proposición 1.3. *Los conjuntos algebraicos de* $\mathbb{A}^n_k$ *son los cerrados de una topología en* $\mathbb{A}^n_k$*, es decir:*

(1) *Tanto* $\emptyset$ *como* $\mathbb{A}^n_k$ *son conjuntos algebraicos.*

(2) *Toda unión arbitraria de conjuntos algebraicos de* $\mathbb{A}^n_k$ *es un conjunto algebraico de* $\mathbb{A}^n_k$*.*

(3) *Toda intersección arbitraria de conjuntos algebraicos de* $\mathbb{A}^n_k$ *es un conjuntos algebraicos de* $\mathbb{A}^n_k$*.*

Demostración.

(1) Esto es porque $\mathbb{A}^n_k = \mathbb{V}(\{0\})$ y $\emptyset = \mathbb{V}(\{1\})$.

(2) De hecho, podemos escribir cómo se ve tal unión explícitamente: probemos que para $T_1, T_2 \subseteq k[x_1,\ldots,x_n]$, se tiene que $\mathbb{V}(T_1) \cup \mathbb{V}(T_2) = \mathbb{V}(T_1T_2)$:

   $\subseteq$: Si $a \in \mathbb{V}(T_1) \cup \mathbb{V}(T_2)$, por definición es un cero de cada $f \in T_1$ o de cada $g \in T_2$. En cualquier caso, será un cero de fg, es decir, $a \in \mathbb{V}(T_1T_2)$.

   $\supseteq$: Probamos la afirmación contrarecíproca. Si $a \notin \mathbb{V}(T_1) \cup \mathbb{V}(T_2)$, entonces no es cero de ningún $f \in T_1$ ni de ningún $g \in T_2$. En cualquier caso, no puede ser cero de fg, es decir, $a \notin \mathbb{V}(T_1T_2)$.

(3) Si $(T_j)_{j\in\Lambda}$ son subconjuntos de $k[x_1,\dots,x_n]$, se tiene que

$$\begin{aligned}\textstyle\bigcap_{j\in\Lambda}\mathbb{V}(T_j) &= \{a\in\mathbb{A}^n_k\colon \forall j\in\Lambda, a\in\mathbb{V}(T_j)\}\\ &= \Big\{a\in\mathbb{A}^n_k\colon a\in\textstyle\bigcup_{j\in\Lambda}\mathbb{V}(T_j)\Big\}\\ &= \Big\{a\in\mathbb{A}^n_k\colon \forall f\in\textstyle\bigcup_{j\in\Lambda}T_j, f(a)=0\Big\}\\ &= \mathbb{V}\Big(\textstyle\bigcup_{j\in\Lambda}T_j\Big).\end{aligned}$$

□

Ejemplo 1.4. Veamos algunos ejemplos de esta topología.

(1) En $\mathbb{A}^1_{\mathbb{C}}$, el disco unitario $\mathbb{D}$ es sabemos que los Zariski-cerrados de $\mathbb{A}^1_{\mathbb{C}}$ son los conjuntos finitos, y $\mathbb{D}$ es infinito.

(2) Es más, en $\mathbb{A}^n_{\mathbb{C}}$ todo Zariski-cerrado también es cerrado en la topología euclidiana: sea $X\subseteq\mathbb{A}^n_{\mathbb{C}}$ un conjunto algebraico, y $f_1,\dots,f_r$ funciones polinomiales que lo definen. Así, podemos escribir $X=\bigcap_{i=1}^r f_i^{-1}(\{0\})$, y como $\{0\}$ es un cerrado en la topología euclidiana, y cada f_i es continua en la topología euclidiana (sabemos de cálculo diferencial que toda función polinomial lo es), concluimos que X es intersección de cerrados euclidianos, y por tanto un cerrado euclidiano en sí.

(3) Los dos puntos anteriores verifican que la topología de Zariski en $\mathbb{A}^n_{\mathbb{C}}$ está estrictamente contenida en la topología euclidiana de $\mathbb{A}^n_{\mathbb{C}}$.

(4) Toda función inyectiva $f\colon\mathbb{A}^1_k\to\mathbb{A}^1_k$ es continua en la topología de Zariski: basta recordar que la preimagen de un singleton bajo una función inyectiva sigue siendo un singleton. Dado $X:=\{a_1,\dots,a_r\}=\bigcup_{i=1}^r\{a_i\}\subseteq\mathbb{A}^1_k$ un conjunto algebraico, se tiene que

$$\begin{aligned}f^{-1}(X) &= f^{-1}(\textstyle\bigcup_{i=1}^r\{a_i\})\\ &= \bigcup_{i=1}^r f^{-1}(\{a_i\})\\ &= \bigcup_{i=1}^r\{b_i\},\end{aligned}$$

para algunos $b_i\in\mathbb{A}^1_k$. Esto verifica que $f^{-1}(X)$ es finito, y por tanto un conjunto algebraico de $\mathbb{A}^1_k$.

(5) Como conjuntos, se tiene que $\mathbb{A}^2_k=\mathbb{A}^1_k\times\mathbb{A}^1_k$, por lo que es natural preguntarnos cómo se relacionan la topología de Zariski de $\mathbb{A}^2_k$ con la topología producto de $\mathbb{A}^1_k\times\mathbb{A}^1_k$. Resulta que estas topologías no coinciden: por ejemplo, $X:=\mathbb{V}(x-y)=\{(a,a)\colon a\in k\}$ es por definición un Zariski-cerrado de $\mathbb{A}^2_k$, pero en $\mathbb{A}^1_k\times\mathbb{A}^1_k$ no puede ser cerrado porque en ese caso tendría que poder escribirse como producto de conjuntos finitos, el que va a tener cardinalidad finita, lo que choca con el hecho de que X es claramente infinito.

1.2. El ideal asociado a un conjunto algebraico

Familias de polinomios distintas pueden definir el mismo conjunto algebraico. Por ejemplo, el origen $(0,0) \in \mathbb{A}^2$ aparece como $\mathbb{V}(x,y)$ y como $\mathbb{V}(2x,\ x+y)$, pero los polinomios de cada familia son evidentemente distintos. ¿Podemos evitar tal ambigüedad?

Dado un conjunto algebraico $V := \mathbb{V}(f_1,\dots,f_r)$, es claro que cada f_i se anula en puntos de V—es su lugar de ceros después de todo. También, debería ser claro que para todos $g_1,\dots,g_r \in k[x_1,\dots,x_r]$ se tiene que

$$g_1 f_1 + \cdots + g_r f_r \in V,$$

es decir, todo polinomio en el ideal $(f_1,\dots,f_r) \subseteq k[x_1,\dots,x_n]$ también se anula en V, o equivalentemente,

$$\mathbb{V}(\langle f_1,\dots,f_r\rangle) \subseteq V.$$

Resulta que esta contención es de hecho una igualdad:

Proposición 1.5. *El lugar de ceros de una familia de polinomios es el mismo lugar de ceros del ideal que genera esta familia. Es decir, si $T \subseteq k[x_1,\dots,x_n]$, entonces $\mathbb{V}(T) = \mathbb{V}((T))$.*

Demostración. De acuerdo a la discusión anterior, queda por probar solo la inclusión $\subseteq$. Consideremos $a \in \mathbb{V}(T)$, es decir, a anula a todo polinomio de T. Debemos probar que a también anula a todo polinomio en (T).

Consideremos $f \in (T)$ arbitrario. Por definición, f se escribe como una combinación $k[x_1,\dots,x_n]$-lineal de elementos de T, es decir, $f = \sum_{i=1}^r g_j s_j$ para algún $r \in \mathbb{N}$, con cada $g_j \in k[x_1,\dots,x_n]$ y $s_j \in T$. Por tanto,

$$\begin{aligned} f(a) &= \textstyle\sum_{j=1}^r g_j(a) s_j(a) \\ &= \textstyle\sum_{j=1}^r g_j(a)\cdot 0 \\ &= 0. \end{aligned}$$

Por tanto, $f \in \mathbb{V}((T))$. $\square$

Esta Proposición permite especializar nuestro estudio no a cualquier familia de polinomios, sino a ideales de un anillo de polinomios. En particular, no perdemos generalidad al reescribir la asignación funtorial $\mathbb{V}(-)$ como

$$\mathbb{V}\colon \left\{ \begin{array}{c} \text{ideales de} \\ k[x_1,\dots,x_n] \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{conjuntos} \\ \text{algebraicos de } \mathbb{A}^n_k \end{array} \right\}.$$

Es natural preguntar si existe una construcción inversa a $\mathbb{V}(-)$, que a cada conjunto algebraico de $\mathbb{A}^n_k$ asigne un ideal. Dado $X \subseteq \mathbb{A}^n_k$ escribamos como $\mathbb{I}(X)$ al conjunto de todos los polinomios que se anulan en X, es decir,

$$\mathbb{I}(X) := \{f \in k[x_1,\dots,x_n]\colon f(a) = 0 \text{ para todo } a \in X\}.$$

Se verifica rápidamente que $\mathbb{I}(X)$ es un ideal de $k[x_1, \ldots, x_n]$, y que de hecho es un funtor contravariante

$$\mathbb{I}\colon \left\{ \begin{array}{c} \text{subconjuntos de} \\ \mathbb{A}_k^n \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{ideales de} \\ k[x_1, \ldots, x_n] \end{array} \right\},$$

pues dados $X_1 \subseteq X_2 \subseteq \mathbb{A}_k^n$, se tiene que un $f \in \mathbb{I}(X_2)$ se anula en todo elemento de X_2, en particular los de X_1, por lo que $f \in \mathbb{I}(X_1)$.

Así, nuestra misión es determinar cómo se relaciones las construcciones $\mathbb{V}$ e $\mathbb{I}$. En particular, querremos determinar si es que son inversas una de la otra, y si no lo son, qué condiciones podemos imponer sobre nuestros objetos de interés para que sí lo sea.

El caso de la composición $\mathbb{V}(\mathbb{I}(X))$ para $X \subseteq \mathbb{A}_k^n$ es particularmente esperanzador:

Proposición 1.6. *Dado $X \subseteq \mathbb{A}_k^n$, se tiene que $X \subseteq \mathbb{V}(\mathbb{I}(X))$, con igualdad si y solo si X es un conjunto algebraico.*

Demostración. En orden, probamos que la primera contención siempre se tiene, y que la segunda ocurre si y solo si X es algebraico.

$\subseteq$: Todo punto de X anula a todo polinomio que se anula en los puntos de X.

Ahora, supongamos que X es un conjunto algebraico.

$\Longrightarrow$: Si $X = \mathbb{V}(\mathbb{I}(X))$, entonces es un conjunto algebraico por definición.

$\Longleftarrow$: Basta probar que la otra contención es cierta en este caso.

- $\supseteq$: Probemos la afirmación contrarecíproca. Escribimos $X = \mathbb{V}(J)$ para algún ideal $J \subseteq k[x_1, \ldots, k_n]$. Por tanto, dado $a \notin X$, podemos encontrar algún polinomio $f \in J$ que no se anule en a. Ahora, como $J \subseteq \mathbb{I}(X)$, en particular hemos encontrado un polinomio $f \in \mathbb{I}(X)$ que no se anula en a, es decir, que $a \notin \mathbb{V}(\mathbb{I}(X))$. □

Por lo tanto, si restringimos los objetos de la correspondencia a

$$\left\{ \begin{array}{c} \text{conjuntos} \\ \text{algebraicos de } \mathbb{A}_k^n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{ideales de} \\ k[x_1, \ldots, x_n] \end{array} \right\},$$

de hecho $\mathbb{V}$ es la inversa de $\mathbb{I}$.

Vemos qué ocurre con la otra composición. Por definición, es claro que si $J \subseteq k[x_1, \ldots, x_n]$ es un ideal, entonces

$$J \subseteq \mathbb{I}(\mathbb{V}(J)),$$

pues todo polinomio en J es uno de los polinomios que se anulan en los ceros de los polinomios de J—valga la redundancia. ¿Será esta contención una igualdad? En general, no:

Ejemplo 1.7. En $k[x]$, tanto (x) como (x^2) definen el mismo lugar de ceros en $\mathbb{A}^1_k$: el conjunto $\{0\}$. Sin embargo, $\mathbb{I}(\{0\}) = (x) \neq (x^2)$, pues en (x^2) no hay elementos de grado 1.

Esto basta para ver que la correspondencia $\mathbb{I}(-)$ no es inyectiva. Por tanto, nos interesaría poder distinguir alguna familia de ideales de modo que la asignación sí sea biyectiva. El ejemplo anterior es síntoma de algo más profundo: la construcción $\mathbb{I}(-)$ no registra las multiplicidades de un cero. Esto nos indica que de haber una correspondencia biyectiva, no es con todos los ideales de $k[x_1, \ldots, x_n]$, sino que solo con aquellos formados polinomios cuyos ceros no tienen multiplicidad mayor a 1, es decir, con *ideales radicales*. Esto es insinuado por el hecho de que $\mathbb{I}(X)$ siempre es radical:

Proposición 1.8. *Dado cualquier conjunto $X \subseteq \mathbb{A}^n_k$, se tiene que $\mathbb{I}(X)$ es un ideal radical de $k[x_1, \ldots, x_n]$.*

Demostración. Hay que probar que $\mathbb{I}(X) = \sqrt{\mathbb{I}(X)}$, lo que hacemos vía doble contención:

$\subseteq$: Es un hecho general que un ideal está contenido en su radical.

$\supseteq$: Por definición, los $f \in \sqrt{\mathbb{I}(X)}$ son aquellos polinomios que tienen alguna potencia que se anula en todo X. Como $k[x_1, \ldots, x_n]$ es un dominio entero, si $f^j(a) = 0$ para algún $j \in \mathbb{N}$, $a \in X$, entonces $f(a) = 0$, por lo que $f \in \mathbb{I}(X)$. □

Un intento noble de solucionar esta situación ciertamente es solo considerar ideales radicales de $k[x_1, \ldots, x_n]$. Lamentablemente, esto no suficiente, pues por mucho que estemos considerando solo ideales radicales, un ideal puede tener lugar de ceros vacío. Este es el caso de $(x^2 + 1) \in \mathbb{R}[x]$, que es primo y por tanto radical, pero cuyo lugar de ceros en $\mathbb{A}^1_{\mathbb{R}}$ es $\emptyset$. Así, todo polinomio que no tenga soluciones en su cuerpo de base tiene lugar de ceros vacío, por lo que en este caso no podemos tener inyectividad.

Por tanto, si queremos determinar una correspondencia biyectiva, lo mínimo que debemos hacer es considerar solo los ideales radicales de $k[x_1, \ldots, x_n]$, y trabajar con k algebraicamente cerrado. El hecho de que estas hipótesis sean todo lo que hay que pedir para que se arregle nuestra vida es crucial para la geometría algebraica, y la literatura suele rendirle honores conservando el nombre del Teorema en su idioma alemán original: *Nullstellensatz* (lit. "Teorema del lugar de ceros"):

Teorema 1.9 (Nullstellensatz de Hilbert, 1893). *Sea k un cuerpo algebraicamente cerrado. Dado un ideal $J \subseteq k[x_1, \ldots, x_n]$, se tiene que*

$$\mathbb{I}(\mathbb{V}(J)) = \sqrt{J},$$

es decir, $\mathbb{V}$ *y* $\mathbb{I}$ *definen una correspondencia biyectiva*

$$\left\{\begin{array}{c}\text{conjuntos}\\ \text{algebraicos de } \mathbb{A}_k^n\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ideales radicales de}\\ k[x_1,\dots,x_n]\end{array}\right\}.$$

La demostración de este resultado es técnica, y la dejamos en el Apéndice A para quién desee leerla. De momento, nos quedamos con una lista de aplicaciones relevantes. Unas palabras de advertencia: cada vez que querramos aplicar el Nullstellensatz (o alguna de sus consecuencias) debemos asegurarnos de estar trabajando sobre un cuerpo algebraicamente cerrado.

Ejemplo 1.10.

(1) Podemos probar de forma más elegante que si $Z \subseteq \mathbb{A}_k^n$ es un conjunto algebraico, entonces $\mathbb{V}(\mathbb{I}(Z)) = Z$. En efecto, sea $J \subseteq k[x_1,\dots,x_n]$ un ideal tal que $\mathbb{V}(J) = Z$. Directamente,

$$\begin{aligned}\mathbb{V}(\mathbb{I}(Z)) &= \mathbb{V}(\mathbb{I}(\mathbb{V}(J)))\\ &= \mathbb{V}(\sqrt{J})\\ &= \mathbb{V}(J)\\ &= Z,\end{aligned}$$

donde en la segunda igualdad ocupamos el Nullstellensatz, y en la tercera el que J es un ideal radical.

(2) Como $k[x]$ es un dominio de ideales principales, todo ideal $J \subseteq k[x]$ se escribe como $J = (f)$ para algún $f = (x-a_1)^{k_1}\dots(x-a_r)^{k_r} \in k[x]$. Así, su lugar de ceros es $\mathbb{V}(f) = \{a_1,\dots,a_r\}$. Por tanto,

$$\begin{aligned}\mathbb{I}(\mathbb{V}(J)) &= \sqrt{J}\\ &= (x-a_1,\dots,x-a_r),\end{aligned}$$

donde la primera igualdad ocupa el Nullstellensatz.

(3) Se puede probar de forma sencilla que el ideal de todo el espacio es (0). En efecto, se tiene que

$$\begin{aligned}\mathbb{I}(\mathbb{A}_k^n) &= \mathbb{I}(\mathbb{V}(0))\\ &= \sqrt{0}\\ &= 0,\end{aligned}$$

donde la segunda igualdad utiliza el Nullstellensatz.

(4) El ideal de la intersección de dos conjuntos algebraicos es el radical de su

suma. En efecto, dados $X_1, X_2 \in \mathbb{A}_k^n$ conjuntos algebraicos, se tiene que

$$
\begin{aligned}
\mathbb{I}(X_1 \cap X_2) &= \mathbb{I}\Big(\mathbb{V}(\mathbb{I}(X_1)) \cap \mathbb{V}(\mathbb{I}(X_2))\Big) \\
&= \mathbb{I}\Big(\mathbb{V}\big(\mathbb{I}(X_1) + \mathbb{I}(X_2)\big)\Big) \\
&= \sqrt{\mathbb{I}(X_1) + \mathbb{I}(X_2)},
\end{aligned}
$$

donde la última igualdad es por Nullstellensatz.

1.3. El anillo asociado a un conjunto algebraico

Sea k un cuerpo. La propiedad universal de las álgebras de polinomios indica que dado $a \in \mathbb{A}_k^n$, hay un único morfismo $\mathrm{ev}_a : k[x_1, \ldots, x_n] \to k$, llamado *morfismo de evaluación en a* que envía $x_j \mapsto a_j$. El considerar todas estas evaluaciones al mismo tiempo es el hecho natural de que podemos evaluar cualquier polinomio en cualquier punto. Formalmente, estamos observando que todo polinomio induce una función

$$
\begin{aligned}
\tilde{f} : \mathbb{A}_k^n &\longrightarrow k \\
a &\longmapsto \mathrm{ev}_a(f),
\end{aligned}
$$

llamada una *función polinomial en $\mathbb{A}_k^n$*. El conjunto de todas estas funciones polinomiales se denota como $k[\mathbb{A}_k^n]$, y se llama el *anillo de coordenadas de $\mathbb{A}_k^n$*, aunque también es una k-álgebra, y solemos utilizar principalmente esta estructura en vez de solo la de anillo:

Lema 1.11. *Dado un cuerpo k, el conjunto $k[\mathbb{A}_k^n]$ es una k-álgebra de tipo finita. La estructura de anillo son la suma y producto punto a punto, y la acción de k es escalar.*

En nuestro día a día, tenemos la costumbre de no distinguir entre un polinomio y la función polinomial que define, principalmente porque solemos trabajar en contextos en los que de partida no hay ambigüedad. Pero sí pueden haber problemas, y aparecen cuando consideramos cuerpos finitos:

Ejemplo 1.12. En $\mathbb{F}_2[x]$, los polinomios 0 y $x^2 + x$ son elementos distintos, pero inducen la misma función polinomial en $k[\mathbb{A}_{\mathbb{F}_2}^1]$, a saber, la constante 0.

Para solucionar este problema de ambigüedad basta considerar cuerpos infinitos. Este hecho general no es directo, y una demostración se puede encontrar en [CLO18, Proposition 5, Corollary 6]. En nuestro caso, nos interesan los cuerpos algebraicamente cerrados, que siempre son infinitos. Una ventaja de trabajar en el caso algebraicamente cerrado es que podemos dar una prueba simple de la no-ambigüedad usando el Nullstellensatz:

Proposición 1.13. *Si k es un cuerpo algebraicamente cerrado, entonces dos polinomios $f, g \in k[x_1, \ldots, x_n]$ definen las mismas funciones polinomiales en $k[\mathbb{A}_k^n]$ si y solo si son iguales.*

Demostración. Veamos ambas implicancias.

$\Longleftarrow$: Si $f = g$, es claro que $\tilde{f} = \tilde{g}$.

$\Longrightarrow$: El que $\tilde{f}(x) = \tilde{g}(x)$ para todo $x \in \mathbb{A}_k^n$, es equivalente a que $(\tilde{f} - \tilde{g})(x) = 0$ para todo $\mathbb{A}_k^n$, es decir, a que $f - g \in \mathbb{I}(\mathbb{A}_k^n)$. El Ejemplo 1.10(4) indica que $\mathbb{I}(\mathbb{A}_k^n) = (0)$, de lo que $f - g = 0$, que es equivalente a lo afirmado. □

Esto, de pasada, verifica que los anillos $k[\mathbb{A}_k^n]$ y $k[x_1, \ldots, x_n]$ son canónicamente isomorfos, por lo que a partir de ahora omitimos el símbolo $\sim$ sobre f, a menos que sea necesario.

Restringiendo las funciones polinomiales de $\mathbb{A}_k^n$ a sus conjuntos algebraicos $X \subseteq \mathbb{A}_k^n$, obtenemos *funciones polinomiales definidas en X*. El conjunto de todas estas funciones polinomiales se denota $k[X]$, lo que nos permitirá hablar de “subconjuntos algebraicos”(contenidos en un conjunto algebraico, como una curva dentro de una superficie).

Al igual que antes, $k[X]$ es una k-álgebra con las mismas operaciones, y se llama el *anillo de coordenadas de X*. Una pregunta natural es si en este caso hay ambigüedad entre funciones polinomiales y polinomios. Sigamos la misma idea que antes: dados $f, g \in k[x_1, \ldots, x_n]$, se tiene que

$$\begin{aligned} \tilde{f}|_X = \tilde{g}|_X &\iff \tilde{f}(x) = \tilde{g}(x), \ \forall x \in X \\ &\iff (\tilde{f} - \tilde{g})(x) = 0, \ \forall x \in X \\ &\iff f - g \in \mathbb{I}(X) \\ &\iff f = g \pmod{\mathbb{I}(X)} \end{aligned}$$

Por tanto, no hay ambigüedad siempre que estemos considerando la correspondencia de $k[X]$ con el cociente $k[x_1, \ldots, x_n]/\mathbb{I}(X)$ X, en vez de con todo $k[x_1, \ldots, x_n]$. El siguiente lema describe la correspondencia de forma explícita:

Proposición 1.14. *Dado un conjunto algebraico $X \subseteq \mathbb{A}_k^n$, se tiene que las k-álgebras $k[X]$ y $k[x_1, \ldots, x_n]/\mathbb{I}(X)$ son canónicamente isomorfas.*

Demostración. Consideremos el morfismo de k-álgebras de restricción,

$$\begin{aligned} \mathrm{res}_X \colon k[x_1, \ldots, x_n] &\longrightarrow k[X] \\ f &\longmapsto \tilde{f}|_X, \end{aligned}$$

que es claramente sobreyectivo (basta considerar el polinomio sin restringir correspondiente). Calculando su kernel directamente, obtenemos que

$$\begin{aligned}\ker(\mathrm{res}_X) &= \left\{f \in k[x_1, \ldots, x_n] \colon \tilde{f}|_X = 0\right\} \\ &= \{f \in k[x_1, \ldots, x_n] \colon f(a) = 0, \forall a \in X\} \\ &= \mathbb{I}(X).\end{aligned}$$

Por tanto, el Teorema del kernel nos indica que $\frac{k[x_1,\ldots,x_n]}{\mathbb{I}(X)} \cong k[X]$. □

Veamos algunos ejemplos concretos de anillos de coordenadas:

Ejemplo 1.15. Los ejemplos (2) y (3) fueron recuperados de [Har10, Problema 1.1(a,b)].

(1) Pictóricamente, el conjunto algebraico $X := \mathbb{V}(x) \subseteq \mathbb{A}^2_k$ corresponde al eje y. Pensando en su anillo de coordenadas, es intuitivo que el restringir una función polinomial de $k[\mathbb{A}^2_k] \cong k[x, y]$ al eje y, resulta en una función polinomial sin variable x. Esta idea se formaliza haciendo el cálculo: basta notar que $\mathbb{I}(X) = \mathbb{I}(\mathbb{V}(x)) = (x)$, donde la tercera igualdad usa el Nullstellensatz y que (x) es radical. Así,

$$k[X] \cong \frac{k[x, y]}{\mathbb{I}(x)} = \frac{k[x, y]}{(x)} \cong k[y].$$

(2) En $\mathbb{A}^2_k$, sean $X_1 := \mathbb{V}(x)$, $X_2 := \mathbb{V}(y)$ y $X_3 := \mathbb{V}(y - x^2)$. En el punto anterior probamos que $k[X_1] \cong k[y]$. Un cálculo similar muestra que $k[X_2] \cong k[x]$, y es sabido que $k[x] \cong k[y]$ de forma canónica. El ideal $(y - x^2)$ también es primo y por tanto radical, por lo que el mismo argumento de antes muestra que

$$k[X_3] \cong \frac{k[x, y]}{(y - x^2)} \cong k[x],$$

donde el último isomorfismo es debido que en ese cociente cada instancia de y en un polinomio se reemplaza con x^2, por lo que solo quedan polinomios en x.

Así, hemos encontrado tres conjuntos algebraicos distintos con anillos de coordenadas isomorfos. Esto no es coincidencia, pero lo explicaremos posteriormente.

(3) Sea $X := \mathbb{V}(xy - 1) \subseteq \mathbb{A}^2_k$. Como $(xy - 1)$ es primo (es generado por un irreducible), es radical, por lo que el argumento estándar verifica que

$$k[X] \cong \frac{k[x, y]}{(xy - 1)} \cong k[x, x^{-1}],$$

donde el último isomorfismo viene de que en el cociente cada producto xy es igual a 1, es decir, x (o y) es invertible. Esto verifica que un anillo de coordenadas no es necesariamente un anillo de polinomios, pues en este caso resultó en una localización de uno (estamos localizando por las potencias de x).

Como anunciamos antes, los anillos de coordenadas de una variedad permiten formalizar el concepto de que una familia de polinomios se anule en puntos de un conjunto algebraico dado. En primera instancia, veamos que lo que planteamos sigue funcionando para todo el espacio afín

Gracias al isomorfismo canónico, toda familia de polinomios $S \subseteq k[x_1, \ldots, x_n]$ corresponde biyectivamente con una familia de funciones polinomiales $S' \subseteq k[\mathbb{A}_k^n]$. Así, escribimos

$$\mathbb{V}(S') := \{a \in \mathbb{A}_k^n \colon f(a) = 0, \forall f \in S'\},$$

y gracias al isomorfismo canónico, se tiene que $\mathbb{V}(S') = \mathbb{V}(S)$. Análogamente, dado un conjunto $X \subseteq \mathbb{A}_k^n$, escribimos

$$\mathbb{I}'(X) := \{f \in k[\mathbb{A}_k^n] \colon f(x) = 0, \forall \in X\},$$

y gracias al isomorfismo canónico, se tiene $\mathbb{I}'(X) = \mathbb{I}(X)$.

La generalización a conjuntos algebraicos contenidos en un conjunto algebraico fijo $X \subseteq \mathbb{A}_k^n$ es la natural. Dada una familia de funciones polinomiales $S \subseteq k[X]$, definimos su *lugar de ceros relativo a* X como el conjunto

$$\mathbb{V}_X(S) := \{a \in X \colon f(a) = 0, \forall a \in X\}.$$

Los subconjuntos de X que son el lugar de ceros relativo de alguna familia de unciones polinomiales se llama un *subconjunto algebraico de* X. También, dado un subconjunto $Y \subseteq X$, definimos su *ideal relativo a* X como el conjunto

$$\mathbb{I}_X(Y) := \{f \in k[X] \colon f(a) = 0, \forall a \in Y\}.$$

Haciendo las modificaciones necesarias (que la verdad son mínimas), se puede demostrar que estas construcciones relativas satisfacen las mismas propiedades funtoriales que sus contrapartes generales. Entramos solo en los detalles de la versión relativa del Nullstellensatz:

Teorema 1.16 (Nullstellensatz relativo). *Sea $X \subseteq \mathbb{A}_k^n$ un conjunto algebraico. Las construcciones $\mathbb{V}_X(-)$ y $\mathbb{I}_X(-)$ dan biyecciones*

$$\left\{\begin{array}{c}\text{subconjuntos}\\ \text{algebraicos de } X\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ideales radicales de}\\ k[X]\end{array}\right\}.$$

Demostración. El Lema 1.14 (más Teorema de Correspondencia) implica que todo ideal radical $J \subseteq k[X]$ es isomorfo canónicamente a un ideal radical $I \subseteq k[x_1, \ldots, x_n]$ que contenga a $\mathbb{I}(X)$. Luego, como $\mathbb{I}(X) \subseteq I$, se tiene que $\mathbb{V}(I) \subseteq$

$\mathbb{V}(\mathbb{I}(X)) = X$, donde la igualdad es por Nullstellensatz. Esto prueba que a I le corresponde biyectivamente (nuevamente por Nullstellensatz) un subconjunto algebraico de X. En particular, la biyección buscada es dada por componer la proyección al cociente con la construcción $\mathbb{V}(-)$. $\square$

1.4. Irreducibilidad

En $\mathbb{A}^2_k$, el conjunto $X := (xy)$, que corresponde pictóricamente a la unión de los ejes x e y, se puede escribir $X = \mathbb{V}(x) \cup \mathbb{V}(y)$, es decir, como la unión de dos cerrados más pequeños. También, su anillo de coordenadas es

$$k[X] = k[x, y]/(xy),$$

que claramente no es un dominio entero, pues las funciones $x, y \in k[X]$ son no-nulas, pero su producto por definición es nulo. Esto no es coincidencia.

Un conjunto algebraico $X \subseteq \mathbb{A}^n_k$ se dice *irreducible* si no se puede escribir como unión de subconjuntos algebraicos de X, por lo que el párrafo anterior verifica que $\mathbb{V}(xy)$ es reducible en $\mathbb{A}^2_k$. De hecho lo que ocurre en este caso es una instancia de un hecho general.

La idea es que si tenemos una reducción de un conjunto algebraico $X = X_1 \cup \cdots \cup X_r$, los anillos de coordenadas de cada X_j nos permitirán encontrar elementos no-nulas de las coordenadas cuyo producto sí es nulo, y viceversa:

Teorema 1.17. *Un conjunto algebraico $X \subseteq \mathbb{A}^n_k$ es irreducible si y solo si $k[X]$ es un dominio entero.*

Demostración. Veamos ambas implicancias.

$\Longrightarrow$: Probemos la afirmación contrarecíproca. Supongamos que $k[X]$ no es un dominio entero, es decir, que hay funciones no-nulas $f_1, f_2 \in k[X]$ tales que $f_1 f_2 = 0$. Como son no-nulas, se tiene que tanto $X_1 := \mathbb{V}_X(f_1)$ como $X_2 := \mathbb{V}_X(f_2)$ son cerrados propios de X. Finalmente,

$$X_1 \cup X_2 = \mathbb{V}_X(f_1) \cup \mathbb{V}_X(f_2) = \mathbb{V}_X(f_1 f_2) = \mathbb{V}_X(0) = X.$$

Esto exhibe a X como reducible.

$\Longleftarrow$: Probemos la afirmación contrarecíproca. Supongamos que X es reducible, es decir, que podemos escribir $X = X_1 \cup X_2$ para algunos $X_1, X_2 \subseteq X$ cerrados propios. Gracias al Nullstellensatz (relativo), el que sean propios asegura que $\mathbb{I}_X(X_1), \mathbb{I}_X(X_2) \neq (0)$, por lo que podemos elegir $f_1 \in \mathbb{I}_X(X_1)$ y $f_2 \in \mathbb{I}_X(X_2)$ no-nulos, y podemos concluir que $f_1 f_2$ se anula en $X_1 \cup X_2 = X$. Así, $f_1 f_2 \in k[X]$ es un producto nulo de funciones no-nulas, lo que prueba que efectivamente $k[X]$ no es un dominio entero. $\square$

Como $k[X] = k[x_1, \ldots, x_n]/\mathbb{I}(X)$, se tiene que $k[X]$ es dominio entero si y solo si $\mathbb{I}(X)$ es ideal primo de $k[x_1, \ldots, x_n]$. Por el Teorema anterior, esto quiere decir que $X \subseteq \mathbb{A}^n_k$ es irreducible si y solo si su ideal $\mathbb{I}(X)$ es primo en el anillo $k[x_1, \ldots, x_n]$.

A partir de ahora, un conjunto algebraico irreducible $V \subseteq \mathbb{A}^n_k$ se dirá una *variedad afín*. También, dado un conjunto algebraico $X \subseteq \mathbb{A}^n_k$ (no necesariamente irreducible), sus subconjuntos algebraicos irreducibles se llaman *subvariedades afines de* X. Con esta terminología, podemos enunciar un teorema tipo Nullstellensatz para variedades afines:

Teorema 1.18 (Nullstellensatz en variedades). *Sea $X \subseteq \mathbb{A}^n_k$ un conjunto algebraico. Hay una correspondencia biyectiva dada por $\mathbb{I}_X$(-) y $\mathbb{V}_X(-)$,*

$$\left\{ \begin{array}{c} \text{subvariedades} \\ \text{afines de } X \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{ideales primos de} \\ k[X] \end{array} \right\}.$$

Ejemplo 1.19.

(1) El anillo de coordenadas de $\mathbb{A}^n_k$ es $k[x_1, \ldots, x_n]$, que es un dominio entero, lo que indica que $\mathbb{A}^n_k$ es irreducible, y por tanto una variedad afín. La correspondencia del Nullstellensatz se lee

$$\left\{ \begin{array}{c} \text{variedades afines} \\ \text{en } \mathbb{A}^n_k \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{ideales primos de} \\ k[x_1, \ldots, x_n] \end{array} \right\}.$$

(2) En la topología euclidiana, $\mathbb{A}^1_{\mathbb{C}}$ es reducible porque se puede escribir como

$$\mathbb{A}^1_{\mathbb{C}} = \mathbb{D} \cup \overline{(\mathbb{C} - \mathbb{D})} = \{z \in \mathbb{C} \colon |z| \leq 1\} \cup \{z \in \mathbb{C} \colon |z| \geq 1\},$$

claramente cerrados. Sin embargo, en la topología de Zariski es irreducible, porque de lo contrario se escribiría como unión de dos conjuntos finitos, lo que no tiene sentido.

Intuitivamente, podemos "descomponer" un conjunto algebraico $X \subseteq \mathbb{A}^n_k$ en sus partes irreducibles: si X fuese reducible, lo podemos escribir como $X_1 \cup X_2$ para algunos cerrados propios. Si alguno de estos fuese reducible, digamos X_1, lo escribimos como unión de cerrados propios $X_{11} \cup X_{12}$ y así sucesivamente. Lo que no es evidente de este procedimiento es que termina en finitos pasos:

Teorema 1.20. *Todo conjunto algebraico $X \subseteq \mathbb{A}^n_k$ se descompone como una unión finita de cerrados irreducibles $X = X_1 \cup \cdots \cup X_r$.*

Demostración. Basta probar que la cantidad de componentes irreducibles es finita. Si no lo fuese, de acuerdo a la discusión anterior, tendríamos una cadena descendente de cerrados distintos $X \supset Y_1 \supset Y_2 \supset \ldots$ (que de hecho son los X_1, X_{11} del párrafo anterior). Por Nullstellensatz, esto correspondería a una cadena ascendente de ideales distintos de $k[x_1, \ldots, x_n]$, $\mathbb{I}(X) \subset \mathbb{I}(Y_1) \subset \mathbb{I}(Y_2) \subset \ldots$, lo que no puede ser, pues el Teorema de la Base de Hilbert asegura que el anillo $k[x_1, \ldots, x_n]$ es noetheriano, y por tanto la última cadena es eventualmente constante. $\square$

1.5. Funciones regulares (o morfismos)

Hemos cumplido con definir objetos geométricos (las variedades afines), y sus contrapartes algebraicas (anillos de coordenadas y sus ideales). Más aún, hemos visto cómo es el diccionario entre estos dos mundos (los avatares del Nullstellensatz).

Ahora nos interesa estudiar funciones entre variedades (o más generalmente, conjuntos algebraicos), obviamente que tengan aluga contraparte algebraica. Intuitivamente, $\mathbb{V}(x)$ y $\mathbb{V}(y)$ en $\mathbb{A}_k^2$ deberían ser "lo mismo"que $\mathbb{A}_k^1$. Así, la noción de morfismo a la que apuntamos resulta ser una especia de "cambio de coordenadas", como en Álgebra Lineal, pero en vez de ser lineales necesariamente, admitimos grados superiores.

Una función $F\colon \mathbb{A}_k^n \to \mathbb{A}_k^m$ se dirá *regular* si sus coordenadas coinciden con funciones polinomiales $\mathbb{A}_k^n \to \mathbb{A}_k^m$, es decir, si existen $f_1, \dots, f_m \in k[\mathbb{A}_k^n]$ tal que para todo $x \in \mathbb{A}_k^n$ se tenga

$$F(x) = (f_1(x), \dots, f_m(x)) \in \mathbb{A}_k^m.$$

Análogamente, una función entre variedades $F\colon V \subseteq \mathbb{A}_k^n \to \mathbb{A}_k^m$ se dirá *regular* si sus coordenadas son dadas por funciones en $k[V]$.

Se verifica directamente que estas funciones regulares son de hecho morfismos para las variedades afines:

Proposición 1.21. *La identidad es una función regular en cualquier variedad, y la composición de funciones regulares, de estar bien definida, es regular. Así, las variedades afines con las funciones regulares son una categoría.*

Demostración. La primera afirmación es clara: dada una variedad afín $V \subseteq \mathbb{A}_k^n$, se tiene que

$$\mathrm{id}_V((x_1, \dots, x_n)) = (x_1, \dots, x_n),$$

y se tiene que cada $x_j \in k[V]$. Por otro lado, consideremos tres variedades afines $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$, $X \subseteq \mathbb{A}^r$, y funciones regulares

$$V \xrightarrow{F} W \xrightarrow{G} X,$$

tales que $F(x) = (f_1(x), \dots, f_m(x)) \in W$ y $G(y) = (g_1(y), \dots, g_r(y)) \in X$ para algunos $f_i \in k[V]$ y $g_j \in k[W]$. De acá, se tiene

$$\begin{aligned}(G \circ F)(x) &= G((f_1(x), \dots, f_m(x))) \\ &= (g_1((f_1(x), \dots, f_m(x))), \dots, g_r((f_1(x), \dots, f_m(x)))),\end{aligned}$$

donde cada coordenada es polinomio en $k[X]$. $\square$

1.6. Funciones racionales

Ahora, queremos extender la familia de funciones que admitimos en variedades, particularmente, a abiertos de ellas.

Dada una variedad afín $X \subseteq \mathbb{A}_k^n$, se tiene que su anillo de coordenadas $k[X]$ es un dominio entero, por lo que tiene un cuerpo de fracciones bien definido, que llamamos su *cuerpo de cocientes polinomiales*, y lo denotamos como $k(X)$. Este objeto es meramente formal, y está formado por todos los cocientes de la forma

$$\frac{f}{g}, \text{ con } f, g \in k[X].$$

En contraste al anillo de coordenadas, $k(X)$ no se identifica con funciones $X \to k$: por ejemplo, dado $a \in \mathbb{A}_k^1$, se tiene que $\frac{1}{x-a} \in k(\mathbb{A}_k^1)$ es un cociente polinomial. Sin embargo, no define una función $\mathbb{A}_k^1 \to k$, pues no tiene sentido evalaurla en el punto $x = a$.

Por tanto, el problema al que nos enfrentamos es determinar cuándo estos cocientes polinomiales efectivamente definen funciones. Para lograr dar una respuesta satisfactoria, vamos a ir cubriendo distintos niveles de abstracción, cada uno con su propia importancia. En orden, revisaremos los casos de funciones definidas en: un punto de $\mathbb{A}_k^n$, en un abierto de $\mathbb{A}_k^n$, en un abierto de una variedad afín (y entre dos de estos), y finalmente en una variedad afín y entre dos de estas.

Funciones racionales en un punto de $\mathbb{A}_k^n$

Tiene sentido agrupar todas las funciones racionales que sí estén definidas en un punto particular $P \in \mathbb{A}_k^n$. Claramente el único estorbo es que el denominador se anule, por lo que una función racional estará bien definida en un punto si y solo si su denominador no tiene a dicho punto como un cero. El conjunto de las *funciones racionales de* $\mathbb{A}_k^n$ *definidas en* P es

$$\mathscr{O}_{\mathbb{A}_k^n, P} := \left\{ \frac{f}{g} \in k(\mathbb{A}_k^n) \colon g(P) \neq 0 \right\}, \tag{1.1}$$

pero ahora sí las podemos identificar con funciones $\mathbb{A}_k^n \to k$.

El anillo $\mathscr{O}_{\mathbb{A}_k^n, P}$ se suele llamar directamente el *anillo local de* $\mathbb{A}_k^n$ *en* P, aunque también es una k-álgebra, y solemos considerar principalmente esta estructura:

Lema 1.22. *Dado punto $P \in \mathbb{A}_k^n$, se tiene que $\mathscr{O}_{\mathbb{A}_k^n, P}$ es una k-álgebra. La estructura de anillo es dada por la suma y producto punto a punto, y la acción de k es escalar.*

El apellido "local" no es de gratis, sino que es porque el anillo es local en el sentido de álgebra conmutativa (es decir, tiene solamente un ideal maximal):

Proposición 1.23. *Dado $P \in \mathbb{A}^n_k$, el anillo $\mathscr{O}_{\mathbb{A}^n_k,P}$ es local, con ideal maximal $\mathfrak{m}_{\mathbb{A}^n_k,P} := \{f \in k[\mathbb{A}^n_k] \colon f(P) = 0\}$.*

Demostración. Basta probar que todo elemento en $\mathscr{O}_{\mathbb{A}^n_k,P} - \mathfrak{m}_{\mathbb{A}^n_k,P}$ es invertible (según [AM18, Proposition 1.6i]). El que $\mathfrak{m}_{\mathbb{A}^n_k,P}$ sea un ideal de $\mathscr{O}_{\mathbb{A}^n_k,P}$ es una cuenta directa, y por tanto lo omitimos.

Para la localidad, notamos que

$$\mathscr{O}_{\mathbb{A}^n_k,P} - \mathfrak{m}_{\mathbb{A}^n_k,P} = \left\{ \frac{f}{g} \in k(\mathbb{A}^n_k) \colon f(P) \neq 0 \right\}.$$

En particular, todo elemento de este conjunto es invertible, con inversa $\frac{g}{f}$, que está bien definida precisamente porque f no se anula en P. □

Funciones racionales en un abierto de $\mathbb{A}^n_k$

Notemos que la condición de la Ecuación 1.1 se puede reescribir como

$$\begin{aligned} g(P) \neq 0 &\iff P \notin \mathbb{V}(g) \\ &\iff P \in \mathbb{A}^n_k - \mathbb{V}(g), \end{aligned}$$

es decir, la función racional está definida en P si y solo dicho punto está en el abierto $\mathbb{A}^n_k - \mathbb{V}(g)$. Estos abiertos son importantes, pues forman una base para la topología de Zariski de $\mathbb{A}^n_k$:

Proposición 1.24. *Los conjuntos de la forma $\mathcal{D}_{\mathbb{A}^n_k}(f) := \mathbb{A}^n_k - \mathbb{V}(f)$ para $f \in k[\mathbb{A}^n_k]$, forman una base para la topología de $\mathbb{A}^n_k$.*

Demostración. Esto es una cuenta directa, pues cada abierto $U \subseteq \mathbb{A}^n_k$ es el complemento en $\mathbb{A}^n_k$ del lugar de ceros de finitas funciones polinomiales $f_1, \dots, f_r \in k[\mathbb{A}^n_k]$. Así, efectivamente

$$\begin{aligned} U = \mathbb{A}^n_k - \mathbb{V}(f_1, \dots, f_r) &= \mathbb{A}^n_k - \bigcap_{j=1}^r \mathbb{V}(f_j) \\ &= \bigcup_{j=1}^r [\mathbb{A}^n_k - \mathbb{V}(f_j)]. \end{aligned}$$

□

Por tanto, es natural darle atención a los abiertos de una variedad afín. Las funciones racionales en $k(\mathbb{A}^n_k)$ bien definidas en un abierto $U \subseteq \mathbb{A}^n_k$ son aquellas definidas en todo punto del abierto simultáneamente, o equivalentemente, aquellas cuyo denominador se anula exclusivamente en los puntos que el abierto evita. Así, las *funciones racionales de $\mathbb{A}^n_k$ en el abierto $U \subseteq \mathbb{A}^n_k$* es el conjunto

$$\mathscr{O}_{\mathbb{A}^n_k}(U) := \bigcup_{P \in U} [k(\mathbb{A}^n_k) - \mathscr{O}_{\mathbb{A}^n_k,P}] = \bigcap_{P \in U} \mathscr{O}_{\mathbb{A}^n_k,P}.$$

Muevamente es una k-álgebra con las operaciones de antes, y usaremos principalmente esa estructura.

Ejemplo 1.25.

(1) En $\mathscr{O}_{\mathbb{A}_k^n}(\mathbb{A}_k^n)$, los posibles denominadores son solo aquellas funciones en $k[\mathbb{A}_k^n]$ que no tienen ningún cero en $\mathbb{A}_k^n$. Pero estas son solo las constantes, por lo que las funciones racionales globales son solo polinomios, es decir, que $\mathscr{O}_{\mathbb{A}_k^n}(\mathbb{A}_k^n) = k[\mathbb{A}_k^n] = k[x_1, \dots, x_n]$.

(2) Un abierto $U \subseteq \mathbb{A}_k^1$ es el complemento de finitos puntos $\{p_1, \dots, p_r\}$, por lo que las funciones racionales en U corresponden precisamente a aquellas cuyos denominadores se anulan en estos puntos,

$$\mathscr{O}_{\mathbb{A}_k^n}(U) = \left\{ \frac{f(x)}{(x-p_1)^{k_1} \dots (x-p_r)^{k_r}} : f \in k[x],\ k_i \in \mathbb{N} \right\}.$$

Funciones racionales en una variedad cuasi-afín

Genéricamente, a un abierto de una variedad afín $U \subseteq X \subseteq \mathbb{A}_k^n$ se llama una *variedad cuasi-afín* de $\mathbb{A}_k^n$. Si bien X es un cerrado de $\mathbb{A}_k^n$, es abierto en su propia topología, por lo que cae dentro de las variedades cuasi-afines.

Definir funciones racionales en el caso de una cuasi-afín $U \subseteq X$ es sutil. De partida, U no es necesariamente un abierto de $\mathbb{A}_k^n$, por lo que en verdad no tiene sentido considerar $\mathscr{O}_{\mathbb{A}_k^n}(U)$. Otro candidato natural sería considerar las funciones racionales de $\mathbb{A}_k^n$ restringidas a U, pero, quizás sorpendentemente, esto no resulta en algo satisfactorio:

Ejemplo 1.26. Consideremos la variedad afín

$$V := \mathbb{V}(xy - zw) \subseteq \mathbb{A}_k^4,$$

que claramente contiene al plano $W := \mathbb{V}(z, y)$, por lo que $U := V - W$ es una variedad cuasi-afín. Por definición,

$$\frac{x}{z},\ \frac{w}{y} \in k(\mathbb{A}_k^4)$$

(i.e., son cocientes polinomiales de $\mathbb{A}_k^4$). La primera solo define una función en $U_1 := U - \mathbb{V}(z)$, mientras que la segunda solo en $U_2 := U - \mathbb{V}(y)$, y es claro que ni U_1 ni U_2 son todo U.

Lo interesante es que en la intersección $U_1 \cap U_2$, sí podemos definir una función racional a partir de estas sin problemas, pues coinciden: este conjunto es *precisamente* donde z y y no se anulan, y se satisface que

$$\frac{x}{z} = \frac{w}{y},$$

pues acá $xy = zw$. Como U_1 y U_2 cubren todo U, la función

$$\begin{aligned} F\colon U &\longrightarrow k \\ p := (x,y,z,w) &\longmapsto \begin{cases} x/z \text{ si } p \in U_1 \\ w/y \text{ si } p \in U_2 \end{cases} \end{aligned}$$

está bien definida en todo U. $\square$

Por lo tanto, las funciones racionales en una variedad cuasi-afín deben ser definidas de modo que admitan a funciones como las del ejemplo anterior, es decir, definidas parcialmente. Así, dada una variedad cuasi-afín $U \subseteq \mathbb{A}_k^n$, las funciones racionales $F\colon U \to k$ serán aquellas que

1.7. Dimensión

Nos interesa definir una noción de dimensión para un conjunto algebraico afín. El candidato más razonable es su dimensión noetheriana:

Definición 1.27. Sea X un espacio topológico.

1. Su *dimensión noetheriana* es el mayor entero $d \geq 0$ tal que haya una cadena estrictamente ascendente $\emptyset \neq Y_0 \subsetneq \cdots \subsetneq Y_d \subseteq X$ de cerrados irreducibles de X de largo d. Se denota $\dim(X)$.
2. Dado un cerrado irreducible $Y \subseteq X$, su *codimensión noetheriana en* X es el mayor entero $d \geq 0$ tal que haya una cadena estrictamente ascendente $Y \subseteq Y_0 \subsetneq Y_1 \cdots \subsetneq Y_d \subseteq X$ de largo d de cerrados irreducibles de X que contengan a Y. Se denota $\operatorname{codim}_X(Y)$.
3. Así, definimos la *dimensión* de un conjunto algebraico de $X \subseteq \mathbb{A}_k^n$ como su dimensión noetheriana, y dado una variedad afín $Y \subseteq X$, definimos su *codimensión en* X como su codimensión noetheriana en X.

Observación. En el último punto de la definición anterior, es importante notar que Y, aparte de tener su codimensión en X asociada, también tiene una dimensión noetheriana como espacio topológico independiente de X, y en general no están obligadas a coincidir.

Ejemplo 1.28. Las únicas cadenas estrictamente ascendentes de variedades afines en $\mathbb{A}_k^1$, son las de la forma $\{a\} \subseteq \mathbb{A}_k^1$ para algún $a \in \mathbb{A}_k^1$, por lo que $\dim \mathbb{A}_k^1 = 1$. Por otro lado, la misma cadena verifica que $\operatorname{codim}_{\mathbb{A}_k^1}(\{a\}) = 1$.

A priori, no es claro que la dimensión de un conjunto algebraico sea finita, y mucho menos cómo calcularla de ser finita, por lo que hay que ir a buscar respuestas a otro lugar. Recordemos del Corolario **??**, que cualquier conjunto algebraico tiene una descomposición en componentes irreducibles, por lo que sería deseable, de algún modo, calcular su dimensión utilizando estas componentes. Esto se unifica con la siguiente intuición: un conjunto algebraico $X \subseteq \mathbb{A}_k^n$ puede tener varias componentes, todas de distintas dimensión, pero la dimensión de X debe ser lo suficientemente "grande" de modo que registre a la componente más "grande" que tenga. La pregunta natural es ¿necesitamos efectivamente más dimensión que la de la componente más "grande"? La respuesta, satisfactoriamente, es que no, y de hecho esto no aplica solo a conjuntos algebraicos, sino que a espacios topológicos noetherianos en general (cf. [Gat21, Observación 2.31(a)]):

Lema 1.29. *Sea X un espacio topológico noetheriano. Dada su descomposición en componentes irreducibles $X = X_1 \cup \dots X_r$, se tiene que*

$$\dim(X) = \max\{\dim(X_1), \dots, \dim(X_r)\}.$$

Una de las desventajas de esta caracterización de la dimensión es que no coopera mucho a la hora de sacar cuentas. Para solucionar esto, es conveniente aplicar nuevamente la filosofía de usar herramientas algebraicas para obtener información geométrica. El Corolario 1.18 da una correspondencia biyectiva entre variedades afines e ideales primos de sus anillos de coordenadas, y por tanto, también entrega una correspondencia biyectiva entre cadenas ascendentes de subvariedades afines con cadenas ascendentes de ideales primos en sus anillos de coordenadas. Así, si tuviésemos una buena noción de dimensión de un anillo, en el sentido que sea referente a cadenas ascendentes de ideales primos, podríamos deducir información sobre la dimensión de una variedad afín.

Interludio: teoría de dimensión en álgebra conmutativa

El área del álgebra conmutativa que lidia con el problema de definir (y posteriormente estudiar) una noción de dimensión en anillos y sus ideales se llama—muy originalmente—teoría de dimensión. Una referencia estándar es [AM18, §11], y una menos estándar es [Gat14, §11].

Definición 1.30. Sea R un anillo.

1. La *dimensión de Krull de R* es el mayor entero $d \geq 0$ tal que haya una cadena estrictamente ascendente $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d$ de largo d de ideales primos en R. Se denota $\operatorname{Kdim}(R)$.
2. La *altura* de un ideal primo $\mathfrak{p} \subseteq R$ es el mayor entero $d \geq 0$ tal que haya una cadena estrictamente ascendente $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d$ de largo d de ideales primos en R contenidos en $\mathfrak{p}$. Se denota $\operatorname{ht}_R(\mathfrak{p})$, y omitimos el subíndice si el anillo ambiente es claro del contexto.

Ejemplo 1.31. Veamos algunos ejemplos de dimensión de anillos.

(1) El único ideal primo de un cuerpo k es el (0), por lo que solo hay una única cadena de ideales primos posible: la trivial. Esto verifica que $\operatorname{Kdim}(k) = 0$.

(2) En un dominio de ideales principales R que no es cuerpo, es sabido que las nociones de ideal primo y la de ideal maximal coinciden. Por tanto, toda cadena estrictamente ascendiente de ideales primos en R es $(0) \subsetneq \mathfrak{m}$, con $\mathfrak{m}$ un ideal maximal de R. Esto verifica que, en este caso, $\mathrm{Kdim}(R) = 1$.

(3) En particular, $\mathbb{Z}$ y $k[x]$ son dominios de ideales principales y no son cuerpos, por lo que el punto anterior asegura que tienen dimensión de Krull igual a 1.

(4) En $k[x, y]$, los únicos ideales primos son (0), los generados por un elemento irreducible (f), y los maximales $(x - a, y - b)$ para algunos $a, b \in k$. Por tanto, las cadenas estrictamente ascendentes de ideales primos de $k[x, y]$ más largas son precisamente las del tipo

$$(0) \subsetneq (f) \subsetneq (x - a, y - b),$$

por lo que $\mathrm{Kdim}(k[x, y]) = 2$.

(5) Más generalmente, se puede probar utilizando el Teorema de normalización de Noether, que $\mathrm{Kdim}(k[x_1, \ldots, x_n]) = n$. De momento, esto es omitido, pero si alguien quiere ver una demostración, puede ir a [Gat14, Proposición 11.9(a)].

Ahora, presentamos unos cuantos resultados relevantes sobre esta noción de dimensión. No probamos nada, pero todos los resultados serán debidamente referenciados.

Lema 1.32.

(1) *El cocientar un anillo R de dimensión de Krull finita en el que todas las cadenas ascendentes de ideales primos de R de largo maximal son del mismo largo, por un ideal primo $\mathfrak{p} \subseteq R$, mantiene estas propiedades, y*

$$\mathrm{Kdim}(R) = \mathrm{Kdim}(R/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p}).$$

(2) **(Hauptidealsatz de Krull).** *Sea R un anillo noetheriano. Dado un ideal principal $(x) \subsetneq R$, se tiene que todo ideal primo $\mathfrak{p}$ minimal entre los que contienen a (x) tiene altura $\mathrm{ht}(\mathfrak{p}) \leq 1$, y hay igualdad si x no es divisor de cero ni invertible.*

(3) *Sea R un dominio entero noetheriano. Se tiene que R es un dominio de factorización única si y solo si todos sus ideales primos de altura 1 son principales.*

Referencias. (1) está en [Gat14, Lema 11.6(a,b)]; (2) en [Gat14, Proposición 11.15] o en [AM18, Corolario 11.17]; y (3) en [Gat21, Proposición 2.37] □

Prontamente estudiaremos ejemplos, todos de naturaleza geométrica, particularmente las interpretaciones e implicancias geométricas de los resultados vistos. De momento, vamos a revisar otra noción algebraica de dimensión de un anillo, una que toma inspiración del álgebra lineal. Acá, la dimensión es el número máximo de vectores independientes que satisfacen un polinomio de grado 1 con coeficientes en el cuerpo base. Por tanto, la generalización natural sería considerar ya no polinomios lineales, sino de cualquier grado, y no sobre un cuerpo, sino sobre un anillo. En este instancia nos centramos solo en el caso de extensiones de cuerpos, porque son mejor portadas y es el caso que nos interesa para hacer geometría. El primer desafío es fijar una idea decente de "independencia":

Definición 1.33. Sea L/k una extensión de cuerpos. Decimos que un conjunto $B \subseteq L$ es *k-algebraicamente dependiente* si existe algún $f \in k[x_1, \dots, x_n]$ no nulo tal que $f(b_1, \dots, b_n) = 0$, con $b_j \in B$. En el caso contrario, decimos que B es *k-algebraicamente independiente*. Si además B es maximal (en el sentido que agregarle cualquier elemento $a \in L - B$ hace que $B \cup \{a\}$ sea k-algebraicamente dependiente), decimos que B es una *k-base de transcendencia para L*.

Una diferencia importante con álgebra lineal es que en ninguna parte de la definición de base de trascendencia solicitamos que estas generen de ningún modo a la extensión en cuestión. Lo que sí ocurre es que L es algebraica sobre el subcuerpo generado por B y el k:

Lema 1.34. *Sea L/k una extensión de cuerpos. Un subconjunto $B \subseteq L$ es k-base de trascendencia si y solo si la extensión $L/k(B)$ es algebraica.*

Demostración. Esta demostración está adaptada de [Wri06, p. 2]. Probemos ambas implicancias.

$\Longleftarrow$: Sea $\alpha \in L$ algebraico sobre $k(B)$, es decir, que satisface una ecuación polinomial con coeficientes en $k(B)$, digamos

$$\sum_{i=0}^{m} \frac{p_i(b_1, \dots, b_n)}{q_i(b_1, \dots, b_n)} \alpha^i = 0,$$

con $p_i, q_i \in k[x_1, \dots, x_n]$ y $b_j \in B$. Eliminando los denominadores (basta multiplicar por $q_0 \dots q_m$ a ambos lados de la igualdad), se obtiene un polinomio en $k[x_1, \dots, x_n]$ que se anula en α, lo que verifica que $B \cup \{\alpha\}$ es k-linealmente dependiente. Por tanto, B es efectivamente maximal.

$\Longrightarrow$: Si B es maximal, dado $\alpha \in L - B$ se tendrá que $S \cup \{\alpha\}$ es k-algebraicamente dependiente, por lo que podemos encontrar $f \in k[x_1, \dots, x_n]$ de modo que $f(b_1, \dots, b_{n-1}, \alpha) = 0$, para algunos $b_i \in B$. Agrupar las potencias de α que aparezcan en el desarrollo, resulta en una expresión polinomial a coeficientes en $k(B)$ que se anula en α, y como α era arbitrario, esto verifica que $L/k(B)$ es algebraica. $\square$

Ejemplo 1.35. Veamos algunos ejemplos de dependencia algebraica.

(1) Sea L/k una extensión de cuerpos. Por definición, el que $a \in L$ sea algebraico sobre k es precisamente que el conjunto $\{a\}$ sea k-algebraicamente dependiente.

(2) Por tanto, el que una extensión L/k sea algebraica es precisamente que todos los elementos de L son k-algebraicamente dependientes, por lo que en la única k-base de trascendencia para L es $\emptyset$.

(3) Dado un cuerpo k, el cuerpo de fracciones de sus polinomios

$$L := \mathrm{Frac}(k[x_1, \ldots, x_n]) = \left\{ \frac{f}{g} : f, g \in k[x_1, \ldots, x_n], g \neq 0 \right\}$$

es una extensión de k, y el conjunto $B := \{x_1, \ldots, x_n\} \subseteq L$ es una k-base de trascendencia para L. En efecto, si un polinomio con coeficientes en k se anula en B, eso por definición está indicando que tal polinomio es el polinomio nulo, es decir, B es k-algebraicamente independiente. Por otro lado, es sabido que el subcuerpo de L más pequeño que contiene a k y a las variables es el mismo L, es decir $L/k(B)$ es trivial, y por tanto algebraica.

Ahora, presentamos el Teorema principal sobre bases de trascendencia. Debería recordar a álgebra lineal, pues una de las primeras cosas que se demuestra es que todo espacio vectorial tiene una base, y que todas las bases tienen la misma cantidad de elementos. Nuevamente, no lo probamos, pero la referencia es [Gat14, Lema 11.28, Proposición 11.29]:

Teorema 1.36. *Toda extensión de cuerpos L/k tiene alguna k-base de trascendencia B. De ser finita, cualquier otra k-base de trascendencia tiene la misma cantidad de elementos que B.*

Por tanto, la siguiente definición está hecha sin ambigüedad:

Definición 1.37. Sea L/k una extensión de cuerpos. De ser finita, la cantidad de elementos de una k-base de trascendencia de L se llama el *grado de trascendencia de L sobre k*, y se denota $\mathrm{trdeg}_k(L)$.

Ejemplo 1.38. Veamos un par de ejemplos de grado de trascendencia.

(1) El Ejemplo 1.35(2) prueba que toda extensión algebraica L/k tiene grado de trascendencia $\mathrm{trdeg}_k(L) = 0$. Esto es cierto particularmente para $\mathrm{trdeg}_k(k)$.

(2) El Ejemplo 1.35(3) verifica que $\mathrm{trdeg}_k(\mathrm{Frac}(k[x_1, \ldots, x_n])) = n$.

Podemos notar una similitud entre la dimensión de Krull y el grado de trascendencia: si k es un cuerpo, entonces

$$\mathrm{Kdim}(k) = \mathrm{trdeg}_k(k) = \mathrm{trdeg}_k(\mathrm{Frac}(k)) = 0, \text{ y también}$$
$$\mathrm{Kdim}(k[x_1, \ldots, x_n]) = \mathrm{trdeg}_k(\mathrm{Frac}(k[x_1, \ldots, x_n])) = n.$$

Esto no es en absoluto una coincidencia. Usando el Teorema de normalización de Noether, se puede probar lo siguiente:

Teorema 1.39. *Sea k un cuerpo. Dada R una k-álgebra de tipo finita que es dominio entero, se tiene que*

$$\mathrm{Kdim}(R) = \mathrm{trdeg}_k(\mathrm{Frac}(R)).$$

Referencia. En [Gat14, Proposición 11.31]. □

De vuelta a la geometría

La correspondencia entre cadenas ascendentes de variedades y cadenas ascendentes de ideales primos, más el Teorema 1.39, prueba más de lo que deseábamos, vale decir, no una, sino dos formas algebraicas de computar la dimensión de una variedad:

Teorema 1.40. *Dada una variedad afín $X \subseteq \mathbb{A}_k^n$ se tiene que*

$$\dim(X) = \mathrm{Kdim}(k[X]) = \mathrm{trdeg}_k(\mathrm{Frac}(k[X])),$$

y dada una subvariedad afín $Y \subseteq X$, se tiene que

$$\mathrm{codim}_X(Y) = \mathrm{ht}_{k[X]}(\mathbb{I}(Y)).$$

Ejemplo 1.41. Podemos calcular $\dim(\mathbb{A}_k^n)$ de dos maneras equivalentes: por el Ejemplo 1.31(5), se tiene que $\dim(\mathbb{A}_k^n) = \mathrm{Kdim}(k[x_1, \ldots, x_n]) = n$; también, usando el Ejemplo 1.38(2), se tiene $\dim(\mathbb{A}_k^n) = \mathrm{trdeg}_k(\mathrm{Frac}(k[x_1, \ldots, x_n])) = n$.

Con este resultado, podemos dar interpretación geométrica a los resultados que vimos anteriormente. El lema 1.32(1,2) se traduce como sigue (después nos encargaremos del tercer punto):

Lema 1.42. *Sea $X \subseteq \mathbb{A}_k^n$ una variedad afín.*

(1) *Dada una subvariedad afín $Y \subseteq X$, se tiene que*

$$\dim X = \dim Y + \mathrm{codim}_X(Y).$$

(2) *Si $f \in k[X]$ es no-nula, entonces cada componente irreducible de la subvariedad $\mathbb{V}(f) \subseteq X$ tiene codimensión 1 en X, y por el punto anterior, tiene dimensión $\dim X - 1$.*

Ejemplo 1.43.

(1) Sea $X := \mathbb{V}(y-x^2) \subseteq \mathbb{A}^2_{\mathbb{C}}$. Es una variedad afín (en particular, irreducible) porque su anillo de coordenadas es $k[X] \cong \mathbb{C}[x,y]/(y-x^2) \cong \mathbb{C}[x]$, que es dominio entero. Así, su única componente irreducible es el mismo X. Por tanto, la parte (2) del lema anterior indica que $\dim(X) = \dim(\mathbb{A}^2_{\mathbb{C}})-1 = 1$.

(2) El conjunto algebraico $X := \mathbb{V}(xz, yz) \subseteq \mathbb{A}^3_k$ corresponde pictóricamente a la unión del plano de ecuación $z = 0$ (es decir, a $X_1 := \mathbb{V}(z)$), con la recta $X_2 := \mathbb{V}(x, y)$, ambas partes irreducibles. Como z es irreducible, el punto (2) del lema anterior indica que X_1 tiene dimensión $\dim(\mathbb{A}^3_k) - 1 = 2$, y el punto (1) que por tanto X_2 tiene dimensión 1. Por tanto, $\dim(X) = \max\{1, 2\} = 2$. También, dado $a \in X_1$ se puede calcular

$$\operatorname{codim}_{X_1}(\{a\}) = \dim(X_1) - \dim(\{a\}) = 2 - 0 = 2,$$

y similarmente, dado $b \in X_2$, se tiene que $\operatorname{codim}_{X_2}(\{b\}) = 1$.

La pregunta natural es si hay alguna manera sencilla de calcular la dimensión de un conjunto algebraico. El ejemplo anterior es evidencia a favor de que la dimensión de una componente se puede calcular como la codimensión de un punto en la componente que habita (cf. [Gat21, Observación 2.31(b)]):

Lema 1.44. *Sea $X \subseteq \mathbb{A}^n_k$ un conjunto algebraico y $X = X_1 \cup \cdots X_r$ su descomposición en variedades afines. Se tiene que $\dim(X_j) = \operatorname{codim}_{X_j}(\{a\})$ para $a \in X_j$. En particular, podemos calcular*

$$\dim(X) = \max\{\operatorname{codim}_X(\{a\}) : a \in X\}.$$

En general, nos van a interesar los conjuntos algebraicos cuyas componentes irreducibles son todas de la misma dimensión:

Definición 1.45. Un conjunto algebraico $X \subseteq \mathbb{A}^n_k$ se dirá de *dimensión pura* si todas sus componentes irreducibles son de la misma dimensión. En particular, un conjunto algebraico se llama una *curva* si tiene dimensión pura 1, *superficie* si tiene dimensión pura 2, y si $Y \subseteq X$ es de dimensión pura $\dim(X) - 1$ (equivalentemente, si todas sus componentes irreducibles tienen codimensión 1), se dirá una *hipersuperficie en X*.

Con esta notación, podemos interpretar geométricamente el lema 1.32(3):

Lema 1.46. *El ideal de cualquier hipersuperficie $X \subseteq \mathbb{A}^n_k$ es principal, y el generador es único salvo multiplicar por unidades de $k[x_1, \dots, x_n]$.*

Demostración. Sea $X = X_1 \cup \cdots \cup X_r$ su descomposición en componentes irreducibles. Como X es hipersuperficie, se tiene que $\operatorname{codim}_X(X_j) = 1$, y por tanto $\mathbb{I}(X_j)$ es un ideal primo de $k[x_1, \dots, x_n]$ con altura $\operatorname{ht}(\mathbb{I}(X_j)) = 1$. Como

$k[x_1,\ldots,x_n]$ es un dominio de factorización única, el lema 1.32(3) indica que cada $\mathbb{I}(X_j)$ es principal, digamos con generador $f_j \in k[x_1,\ldots,x_n]$. Finalmente, basta notar que $\mathbb{I}(X) = (f_1 \cdots f_r)$, que es principal. $\square$

Por lo tanto, la siguiente definición no es ambigua:

Definición 1.47. Sea $X \subseteq \mathbb{A}^n_k$ una hipersuperficie de ideal $\mathbb{I}(X) = (f)$. El *grado de* X, denotado $\deg(X)$ es el grado de f. Si el grado es 1, 2, o 3, diremos que la hipersuperficie es *lineal, cuadrática* o *cúbica*, respectivamente.

A. Demostración del Nullstellensatz

Un camino estándar para demostrar este resultado, es probar primero alguna de las "versiones débiles", y luego usar un truco algebraico para deducir la versión que nos interesa. Ahora, en la literatura hay varios Teoremas equivalentes que son referidos como el "Nullstellensatz débil". Nosotros elegimos uno de estos de forma (no tan) arbitraria:

Teorema A.1 (Nullstellensatz débil, versión punto–ideal maximal). *Sea k un cuerpo algebraicamente cerrado no-numerable. Hay una correspondencia biyectiva entre puntos de $\mathbb{A}^n_k$ e ideales maximales de $k[x_1, \ldots, x_n]$, dadas por*

$$\begin{aligned} \{\text{puntos de } \mathbb{A}^n_k\} &\longleftrightarrow \left\{ \begin{matrix} \text{ideales maximales} \\ \text{de } k[x_1, \ldots, x_n] \end{matrix} \right\} \\ a &\longmapsto \ker(\mathrm{ev}_a) \\ (\phi_{\mathfrak{m}}(x_1), \ldots, \phi_{\mathfrak{m}}(x_n)) &\longleftarrow\!\shortmid\ \mathfrak{m} \end{aligned}$$

donde $\phi_{\mathfrak{m}}$ es el único morfismo de k-álgebras $k[x_1, \ldots, x_n] \to k$ de kernel $\mathfrak{m}$.

Hay bastante que desempacar de este Teorema, por lo que desmenuzaremos su demostración en dos partes. Es importante notar que hay una hipótesis adicional en el enunciado—que el cuerpo base sea no-numerable—que parece algo gratuita. El motivo de hacer esto es porque la demostración se vuelve más sencilla, y porque siempre podemos reducir el caso no-numerable al caso general. No entraremos en detalle de como hacer eso, pero hay una respuesta satisfactoria, más una discusión interesante, en [MO1].

Lema A.2. *Sea k un cuerpo algebraicamente cerrado no-numerable. Se tiene que*

$$\begin{aligned} \ker\colon \mathrm{Hom}_{k-\mathsf{alg}}(k[x_1, \ldots, x_n], k) &\longrightarrow \mathrm{Specm}(k[x_1, \ldots, x_n]) \\ \phi &\longmapsto \ker(\phi) \end{aligned}$$

es una asignación biyectiva.

Demostración. Probamos la inyectividad y sobreyectividad por separado.

(1) Para la inyectividad, sean $\phi_1, \phi_2 \in \mathrm{Hom}_{k-\mathsf{alg}}(k[x_1, \ldots, x_n], k)$ tales que $\ker(\phi_1) = \ker(\phi_2)$. Dada una variable $x_j \in k[x_1, \ldots, x_n]$, se tiene que

$$\begin{aligned} \phi_1(x_j) = b &\iff \phi_1(x_j - b) = 0 \\ &\iff x_j - b \in \ker(\phi_1) \\ &\iff x_j - b \in \ker(\phi_2) \\ &\iff \phi_2(x_j - b) = 0 \\ &\iff \phi_1(x_j) = b, \end{aligned}$$

de lo que cada variable toma un solo valor. Por otro lado, dado $a \in k[x_1, \ldots, x_n]$ polinomio idénticamente igual a $a \in k$, se tiene que

$$\phi_1(a) = a\phi_1(1) = a\phi_2(1) = \phi_2(a).$$

(2) Para la sobreyectividad, notamos que a cada $\mathfrak{m} \in \operatorname{Specm}(k[x_1, \ldots, x_n])$, le corresponde un cuerpo $F_{\mathfrak{m}} := k[x_1, \ldots, x_n]/\mathfrak{m}$, el cual es extensión de k. Si la extensión es trivial, es decir, $F_{\mathfrak{m}} = k$, entonces la proyección canónica

$$\pi \colon k[x_1, \ldots, x_n] \longrightarrow \frac{k[x_1, \ldots, x_n]}{\mathfrak{m}}$$

tiene $\ker(\pi) = \mathfrak{m}$, y como $\frac{k[x_1, \ldots, x_n]}{\mathfrak{m}} = k$, de hecho hemos probado la sobreyectividad en este caso.

Probemos que el caso en que la extensión es no-trivial no puede ser. Para ello, calcularemos el grado de la extensión de dos formas distintas, que resultarán ser incompatibles.

En efecto, supongamos que $F_{\mathfrak{m}}$ es una extensión no-trivial de k, y veamos que esto fuerza que el grado de la extensión sea no-numerable. Dado un $T \in F_{\mathfrak{m}} - k$, como estamos suponiendo que k es algebraicamente cerrado, se tiene que T es trascendente sobre k, y por tanto el subcuerpo de $F_{\mathfrak{m}}$ generado por k y T es isomorfo a $k(T)$, el cuerpo de las fracciones en la variable T. Consideremos el conjunto no-numerable

$$\left\{ \frac{1}{T - \lambda} \colon \lambda \in k \right\} \subseteq k(T) \subseteq F_{\mathfrak{m}},$$

y probemos que sus elementos son k-linealmente independientes entre sí: considerando una combinación k-lineal nula de ellos, se tiene

$$\begin{aligned} \sum_{\lambda \in k} a_\lambda \frac{1}{T - \lambda} = 0 &\iff \sum_{\lambda \in k} a_\lambda \frac{\prod_{\alpha \in k}(T - \alpha)}{T - \lambda} = 0 \\ &\iff \sum_{\lambda \in k} a_\lambda \left(\prod_{\alpha \neq \lambda} (T - \alpha) \right) = 0, \end{aligned}$$

donde en la primera equivalencia multiplicamos a ambos lados de la igualdad por el producto que aparece, y en la segunda simplificamos la fracción.

Ahora, para cada $\lambda_0 \in k$, evaluamos la última igualdad en $T = \lambda_0$, obteniendo que

$$\begin{aligned} \sum_{\lambda \in k} a_\lambda \left(\prod_{\alpha \neq \lambda} (\lambda_0 - \alpha) \right) = 0 &\iff a_{\lambda_0} \prod_{\alpha \neq \lambda_0} (\lambda_0 - \alpha) = 0 \\ &\iff a_{\lambda_0} = 0, \end{aligned}$$

donde la primera equivalencia es porque el factor $\lambda_0 - \alpha$ en la izquierda no es cero si y solo si $\alpha \neq \lambda_0$, lo que ocurre solo cuando $\lambda = \lambda_0$; y la segunda porque la productoria de la derecha no se anula y estamos trabajando en un dominio entero. Esto prueba la independencia k-lineal entre todos los $\frac{1}{T-\lambda}$.

En particular, todo esto prueba que en $F_{\mathfrak{m}}$ hay al menos tantos elementos k-linealmente independientes entre sí como elementos de k, el que es no-numerable. Por tanto $[F_{\mathfrak{m}} : k] = \dim_k(F_{\mathfrak{m}})$ es no-numerable. Por otro lado, $\dim_k(k[x_1, \ldots, x_n])$ es numerable, de lo que $\dim_k(\frac{k[x_1,\ldots,x_n]}{\mathfrak{m}}) = [F_{\mathfrak{m}} : k]$ también debe ser numerable. Esto es claramente contradictorio, por lo que concluimos que la extensión $F_{\mathfrak{m}}/k$ es siempre trivial. □

Si alguien sabe el suficiente álgebra conmutativa puede haber notado que el lema anterior es una instancia particular del *lema de Zariski*, que indica que si una k-álgebra de tipo finita A es un cuerpo, entonces es una extensión finita (y por tanto algebraica) de k. Esto simplifica la demostración de que $F_{\mathfrak{m}}$ es extensión trivial de k: basta notar que $F_{\mathfrak{m}}$ cumple las hipótesis del lema de Zariski para concluir que la extensión es algebraica, y por tanto trivial, pues estamos suponiendo que k es algebraicamente cerrado. De momento no entraremos en más detalles sobre esto, pero si a alguien le urge, puede revisar [AM18, Proposition 7.9].

Lema A.3. *Dado k un cuerpo, se tiene que*

$$\begin{aligned} \mathrm{ev}\colon \mathbb{A}_k^n &\longrightarrow \mathrm{Hom}_{k\text{-}\mathsf{alg}}(k[x_1,\ldots,x_n],k) \\ a &\longmapsto \mathrm{ev}_a \end{aligned}$$

define una correspondencia biyectiva, con inversa $\mathrm{pt} := \phi \mapsto (\phi(x_1), \ldots, \phi(x_n))$.

Demostración. Lo probamos directamente. Dado $a := (a_1, \ldots, a_n) \in \mathbb{A}_k^n$, se tiene que

$$\begin{aligned} \mathrm{pt} \circ \mathrm{ev}(a) &= \mathrm{pt}(\mathrm{ev}_a) \\ &= (\mathrm{ev}_a(x_1), \ldots, \mathrm{ev}_a(x_n)) \\ &= (a_1, \ldots, a_n), \end{aligned}$$

de lo que $\mathrm{pt} \circ \mathrm{ev} = \mathrm{id}_{\mathbb{A}_k^n}$. Por otro lado, dado $\phi \in \mathrm{Hom}_{k-\mathsf{alg}}(k[x_1, \ldots, x_n], k)$, tenemos que

$$\begin{aligned} \mathrm{ev} \circ \mathrm{pt}(\phi) &= \mathrm{ev}((\phi(x_1), \ldots, \phi(x_n))) \\ &= \mathrm{ev}_{(\phi(x_1),\ldots,\phi(x_n))} \\ &= \phi, \end{aligned}$$

Concluimos que $\mathrm{ev} \circ \mathrm{pt} = \mathrm{id}_{\mathrm{Hom}_{k-\mathsf{alg}}(k[x_1,\ldots,x_n],k)}$. Por lo tanto, ev es efectivamente una biyección. □

Con esto tenemos los ingredientes para concluir la versión débil:

Demostración del Teorema A.1 (Nullstellensatz débil). Basta notar que los dos lemas anteriores prueban que la correspondencia $a \mapsto \ker(\mathrm{ev}_a)$ es una composición de biyecciones, y por tanto una biyección en sí. $\square$

A estas alturas—sin haber probado el Nullstellensatz más general— podemos hacer observaciones geométricas importantes. Por nombrar algo, recordemos que sin restringir el cuerpo de base, hay ideales propios cuyo lugar de ceros es vacío. Bajo las hipótesis del Nullstellensatz (débil), más un poco de álgebra conmutativa, esto no es problema. Necesitamos invocar un resultado estándar de álgebra conmutativa que indica que todo ideal propio está contenido en algún ideal maximal, ver [AM18, Theorem 1.3, Corollary 1.4]. Con esto:

Corolario A.4. *Un ideal $J \subseteq k[x_1, \dots, x_n]$, con k un cuerpo algebraicamente cerrado, tiene lugar de ceros vacío si y solo si $J = k[x_1, \dots, x_n]$.*

Demostración. Veamos ambas implicancias:

$\Longleftarrow$: No hay ningún punto en k que anule a absolutamente todos los polinomios de $k[x_1, \dots, x_n]$ al mismo tiempo.

$\Longrightarrow$: Sea $J \subseteq k[x_1, \dots, x_n]$ un ideal con lugar de ceros vacío. Buscando una contradicción, supongamos que $J \neq k[x_1, \dots, x_n]$, es decir, que es un ideal propio. Así, el Teorema de Krull nos indica que existe un ideal maximal $\mathfrak{m}$ de $k[x_1, \dots, x_n]$ que contiene a J. Como $J \subseteq \mathfrak{m}$, se tiene que $\mathbb{V}(\mathfrak{m}) \subseteq \mathbb{V}(J)$, y por el Nullstellensatz débil, $\mathbb{V}(\mathfrak{m})$ es un punto de $\mathbb{A}_k^n$ (lo importante es que es no-vacío), por lo que $\mathbb{V}(J)$ es en sí no-vacío. $\square$

Finalmente, estamos en condiciones de probar el resultado más general. Para esto, usamos una técnica estándar, conocida como el "truco de Rabinowitsch":

Demostración del Teorema 1.9 (Nullstellensatz de Hilbert). Recordar que debemos probar que $\mathbb{I}(\mathbb{V}(J)) = \sqrt{J}$ bajo las hipótesis adecuadas. Para esto, probamos la doble contención.

$\supseteq$: Si $f \in \sqrt{J}$, entonces existe $n \in \mathbb{N}$ tal que $f^n \in J$. Si $a \in \mathbb{V}(J)$, se tiene que $f^n(a) = 0$, y como estamos en un dominio integral, se sigue que $f(a) = 0$, es decir, $f \in \mathbb{I}(\mathbb{V}(J))$.

$\subseteq$: En esta contención vamos usar la notación $\overline{x} := (x_1, \dots, x_n)$ únicamente por motivos cosméticos. Por ejemplo, en vez de anotar $k[x_1, \dots, x_n]$, vamos a escribir $k[\overline{x}]$. Terminada la prueba, esto será abandonado.

Sea $f \in \mathbb{I}(\mathbb{V}(J))$ no-nulo, y $f_1, \dots, f_r \in J$ generadores de J. Consideremos el anillo resultante de agregar una variable, $k[\overline{x}, x_{n+1}]$, y definamos el nuevo polinomio $f_{r+1} := 1 - x_{n+1} f$. Notemos que los f_j no se anulan todos al mismo tiempo, pues si tuviesen a un $a \in \mathbb{A}_k^{n+1}$ como un cero en común, entonces se tendría que $f_{r+1}(a) = 1 - af(0) = 1$, lo que contradice el que a sea un cero de f_{r+1}.

Así, tenemos que $\mathbb{V}(f_1, \dots, f_{r+1}) = \emptyset$, y el Corolario A.4 indica que $(f_1, \dots, f_{r+1}) = k[\overline{x}, x_{n+1}]$, por lo que existen $h_1, \dots, h_{r+1} \in k[\overline{x}, x_{n+1}]$ tales que $\Sigma := \sum_{j=1}^{r+1} h_j f_j = 1$. En tanto $k[\overline{x}, x_{n+1}]$ es una $k[\overline{x}]$-álgebra, la propiedad universal de las álgebras de polinomios indica que podemos evaluar Σ en $x_{n+1} = \frac{1}{f}$, que está bien definido porque f es no-nulo, obteniendo

$$\left[\sum_{j=1}^{r} h_j\left(\overline{x}, \frac{1}{f}\right) \cdot f_j(\overline{x})\right] + h_{r+1}\left(\overline{x}, \frac{1}{f}\right) \cdot \left(1 - \frac{1}{f} \cdot f\right) = 1$$
$$\Longrightarrow \sum_{j=1}^{r} h_j\left(\overline{x}, \frac{1}{f}\right) \cdot f_j(\overline{x}) = 1.$$

Multiplicando la última igualdad por una potencia de f suficientemente grande, digamos f^N de modo que no hayan denominadores, se tendrá que

$$f^N \cdot \left[\sum_{j=1}^{r} h_j\left(\overline{x}, \frac{1}{f}\right) \cdot f_j(\overline{x})\right] = f^N \in (f_1, \dots, f_r)$$

es un polinomio en $k[\overline{x}]$, es decir, hemos encontrado una potencia de f que cae en J, lo que es por definición que $f \in \sqrt{J}$. $\square$

Referencias

[AM18] Michael Atiyah and Ian Macdonald, *Introduction to commutative algebra*, Addison-Wesley Series in Mathematics, CRC Press, Taylor & Francis Group, Boca Raton London New York, 2018.

[CLO18] David A. Cox, John B. Little, and Donal O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, fourth edition, corrected publication ed., Undergraduate texts in mathematics, Springer, Cham Heidelberg New York Dordrecht London, 2018.

[Gat14] Andreas Gathmann, *Commutative algebra*, Technische Universität Kaiserslautern, 2014.

[Gat21] ______, *Algebraic geometry*, Technische Universität Kaiserslautern, 2021.

[Har10] Robin Hartshorne, *Algebraic geometry*, rpt. ed., Graduate Texts in Mathematics, vol. 52, Springer, New York, N.Y, 2010.

[MO1] *To prove the Nullstellensatz, how can the general case of an arbitrary algebraically closed field be reduced to the easily-proved case of an uncountable algebraically closed field?*, https://mathoverflow.net/questions/15611/to-prove-the-nullstellensatz-how-can-the-general-case-of-an-arbitrary-algebraic, Accedido el 09-02-2023.

[Wri06] Alex Wright, *Transcendence degree*, University of Michigan, 2006.