Geometria Algebraica

José Luis Tábara

jltabara@gmail.com

Índice

1. Conjuntos algebraicos

La geometría algebraica clásica es el estudio de los lugares geométricos definidos por soluciones de un sistema de ecuaciones polinomiales. Si estudiamos el polinomio $x - y^2$ sobre el cuerpo $\mathbb{R}$, para calcular el lugar geométrico que define trabajamos con la ecuación $x - y^2 = 0$. El conjunto de soluciones de esta ecuación toma la forma de una parábola. Análogamente, si estudiamos la ecuación $x^2+y^2-1 = 0$ obtenemos una circunferencia. Para encontrar los puntos de corte de dichas figuras formamos un sistema de dos ecuaciones. Las soluciones del sistema son exactamente los puntos de corte. La geometría algebraica estudia ecuaciones (polinomiales) en varias variables y los posibles sistemas que se pueden formar con dichas ecuaciones.

Observación. En estas notas, y salvo mención explícita en contra, todos los cuerpos se suponen algebraicamente cerrados (y por lo tanto infinitos). Ello se hace para evitar ciertas situaciones patológicas que comentaremos oportunamente. $\square$

Definición 1.1 *Sea k un cuerpo. Llamamos* espacio afín *de dimensión n, y denotamos por $\mathbb{A}^n(k)$, al conjunto k^n. Si la referencia al cuerpo es clara lo denotaremos por $\mathbb{A}^n$.*

Si $n = 1$ el espacio afín se llama recta afín y en el caso bidimensional plano afín, por analogía con la geometría euclídea.

Dado un polinomio $f \in k[x_1, \dots, x_n]$ se induce una función $\overline{f} : \mathbb{A}^n \to k$. Para definir su valor sobre un punto $(a_1, \dots, a_n)$ sustituimos las variables x_i por los valores a_i en el polinomio y operamos. Como el cuerpo es infinito, a distintos polinomios le asociamos funciones distintas. Por ello, siempre que lo necesitemos, identificaremos a los polinomios con las funciones que inducen. Para no recargar la notación denotaremos exactamente igual al polinomio y a la función.

Definición 1.2 *Dado un polinomio $f \in k[x_1, \dots, x_n]$, decimos que se* anula en un punto $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ *si*

$$f(p) = f(a_1, \ldots, a_n) = 0$$

El conjunto de todos los puntos donde se anula f se denota $\mathcal{V}(f)$.

Si consideramos más de un polinomio (incluso un conjunto infinito) llegamos a la siguiente

Definición 1.3 *Sea $S \subset k[x_1, \ldots, x_n]$ una colección de polinomios. Denotamos por $\mathcal{V}(S)$ al conjunto*

$$\mathcal{V}(S) = \{p \in \mathbb{A}^n \text{ tales que } f(p) = 0 \text{ para todo } f \in S\}$$

Los conjuntos de la forma $\mathcal{V}(S)$ se llaman algebraicos.

Observación. Aunque la inclusión $S \subset S'$ sea estricta, la inclusión de los conjuntos algebraicos no tiene por qué serlo. Por ejemplo

$$\mathcal{V}(f) = \mathcal{V}(f, f^2, \ldots, f^n)$$

pues si se anula f se anulan todas sus potencias. □

Ejemplos.

- Una posible definición equivalente de $\mathcal{V}(S)$ es

  $$\mathcal{V}(S) = \bigcap_{f \in S} \mathcal{V}(f)$$

  y los conjuntos algebraicos se construyen con intersecciones de conjuntos de la forma $\mathcal{V}(f)$.

- Si tenemos dos conjuntos de polinomios S y S' tales que $S \subset S'$ entonces $\mathcal{V}(S') \subset \mathcal{V}(S)$, puesto que al tener "más" ecuaciones, el conjunto de puntos solución se reduce.

- En $\mathbb{A}^1$ los conjuntos $\mathcal{V}(f)$ son finitos. Todo conjunto algebraico de la recta afín es finito .

- Si $S = \{x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n\}$ entonces $\mathcal{V}(S)$ está formado por un único punto, precisamente $p = (a_1, \ldots, a_n)$. Todo punto es un conjunto algebraico. En general, cualquier conjunto finito de puntos es un conjunto algebraico (encontrar las ecuaciones o esperar a la proposición 1.7). En particular, si el cuerpo es finito todo subconjunto del espacio afín es algebraico. Debido a nuestro presupuesto inicial este problema no se nos presentará.

- Se verifican de modo inmediato las propiedades:

$$\mathcal{V}(1) = \varnothing \qquad \mathcal{V}(0) = \mathbb{A}^n \qquad \mathcal{V}(fg) = \mathcal{V}(f) \cup \mathcal{V}(g) \qquad \mathcal{V}(f^n) = \mathcal{V}(f)$$

- Si S tiene un único polinomio y este es de primer grado sin término independiente, el conjunto de sus soluciones es un hiperplano vectorial de k^n. Si el polinomio tiene término independiente, entonces el conjunto de soluciones es un hiperplano desplazado. Si todos los polinomios de S son de primer grado, el conjunto de soluciones se denomina subvariedad lineal afin. Si no es vacía, es un subespacio vectorial de k^n o bien un subespacio trasladado por un vector.

- Llamamos hipersuperficie a un conjunto algebraico definible por un solo polinomio (que no sea una constante). Todas las hipersuperficies son de la forma $\mathcal{V}(f)$ donde f es un polinomio. Puede ocurrir que distintos polinomios (por ejemplo f y f^n) definan la misma hipersuperficie.

- Si el conjunto de ecuaciones es finito, el conjunto algebraico es intersección de las hipersuperficies correspondientes a cada polinomio. El conjunto algebraico es intersección de un número finito de hipersuperficies. Si el conjunto de polinomios es infinito el resultado también es cierto, y su demostración es consecuencia directa del teorema de la base de Hilbert, como veremos posteriormente en este capítulo.

Proposición 1.1 *El complementario de una hipersuperficie (los puntos que no cumplen la ecuación) es infinito.*

Demostración.

En el caso unidimensional, los conjuntos algebraicos son finitos. Su complementario es entonces infinito.

Si $n > 1$ tomemos un polinomio f no constante. Supongamos que el grado de dicho polinomio en la variable x_n no es nulo. Damos valores arbitrarios a las $n-1$ primeras coordenadas, que denotamos $a_1, \ldots, a_{n-1}$. El polinomio, de una variable, $f(a_1, \ldots, a_{n-1}, x_n)$ solamente puede tener un número finito de soluciones. Por lo tanto, el conjunto de puntos que no son solución es infinito. $\square$

Observación. Ya hemos comentado que este resultado es falso si el cuerpo sobre el que trabajamos es finito. $\square$

Corolario 1.2 *El complementario de todo conjunto algebraico es infinito.*

Demostración.

Todo conjunto algebraico es intersección de hipersuperficies. $\square$

Las hipersuperficies también tendrán un número infinito de puntos, salvo en el caso de los polinomios en una variable, donde evidentemente es falso. Teniendo en cuenta este comentario formulamos la

Proposición 1.3 *Toda hipersuperficie tiene infinitos puntos.*

Demostración.

Sea $f \in k[x_1, \ldots, x_n]$ no constante. Supongamos que el grado en la última variable no es nulo. Fijamos las primeras $n-1$ coordenadas (que se pueden elegir de infinitas maneras) y consideramos el polinomio, de una variable, $f(a_1, \ldots, a_{n-1}, x_n)$. Como el cuerpo es algebraicamente cerrado, debe tener al menos una solución (que denotaremos a_n). El punto $(a_1, \ldots, a_{n-1}, a_n)$ pertenece a la hipersuperficie. $\square$

Observación. Este resultado es falso si el cuerpo no es algebraicamente cerrado. Por ejemplo, $f = x^2 + y^2 \in \mathbb{R}[x, y]$ tiene una única solución. Incluso la hipersuperficie puede ser vacía ($f = x^2 + y^2 + 1 \in \mathbb{R}[x, y]$). $\square$

Si un punto se anula para un conjunto de polinomios, necesariamente se anula para todo polinomio que se construya con sumas, restas y multiplicaciones de dichos polinomios. De esta forma entra en escena el ideal generado por un conjunto y podemos decir que un conjunto algebraico es el conjunto de puntos donde se anulan los polinomios pertenecientes a un ideal I del anillo de polinomios. Esta definición es más intrínseca que la anterior, pues depende únicamente del ideal I y no de los polinomios que lo generan. Hemos intuido la siguiente

Proposición 1.4 *Todo conjunto algebraico se puede definir como los ceros del ideal I generado por los polinomios que definen el sistema de ecuaciones.*

Otra manera de expresar la proposición anterior es decir que $\mathcal{V}(S) = \mathcal{V}(I)$, donde I es el ideal generado por el conjunto S en el anillo de polinomios. Podemos dar una nueva definición de conjunto algebraico, que será la que utilizaremos en lo que sigue.

Definición 1.4 *Dado un ideal I del anillo de polinomios, llamamos* conjunto algebraico *asociado al ideal I a*

$$\mathcal{V}(I) = \{p \in \mathbb{A}^n \text{ tales que } f(p) = 0 \text{ para todo } f \in I\}$$

Observación. Puede ocurrir que distintos ideales den lugar al mismo conjunto algebraico. El caso más claro se produce con los ideales I y $\mathrm{Rad}(I)$ (recordemos que $f \in \mathrm{Rad}(I)$ si existe un número natural n tal que $f^n \in I$). Ambos definen el mismo conjunto algebraico. Esta es la generalización del resultado $\mathcal{V}(f) = \mathcal{V}(f^n)$. $\square$

Corolario 1.5 *Todo conjunto algebraico es intersección de un conjunto finito de hipersuperficies.*

Demostración.

Si un conjunto $V \in \mathbb{A}^n$ es algebraico es de la forma $V = \mathcal{V}(I)$ para algún ideal. Por el teorema de la base de Hilbert, dicho ideal está generado por un conjunto finito. Entonces

$$V = \mathcal{V}(I) = \mathcal{V}(f_1, \dots, f_r) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r)$$

como se comprueba rápidamente. $\square$

Está claro que si I es el conjunto total, su conjunto algebraico asociado es vacío (puesto que la unidad pertenece al ideal). En los otros casos tenemos el siguiente resultado fundamental.

Proposición 1.6 *Si I no es el total, entonces $\mathcal{V}(I)$ no es vacío.*

Demostración.

Si I no es total, entonces está contenido en un ideal maximal $\mathfrak{m}$, lo que implica que $\mathcal{V}(\mathfrak{m}) \subset \mathcal{V}(I)$ y basta comprobar que el conjunto asociado a un maximal es no vacío. Por el teorema de los ceros de Hilbert, que probaremos posteriormente, se sabe que todo ideal maximal de $k[x_1, \dots, x_n]$ es de la forma

$$\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$$

para ciertos elementos $a_1, \dots, a_n$ del cuerpo. Pero entonces tenemos que $\mathcal{V}(\mathfrak{m}) = p = (a_1, \dots, a_n)$. $\square$

Observación. De nuevo este resultado es falso si el cuerpo no es algebraicamente cerrado. Para verlo considerese el ideal principal de $\mathbb{R}[x, y]$ generado por el polinomio $x^2 + y^2 + 1$. $\square$

Los conjuntos algebraicos se comportan bien bajo las operaciones de intersección y de unión.

Proposición 1.7 *La unión de un conjunto finito de conjuntos algebraicos es de nuevo un conjunto algebraico. La intersección de una colección arbitraria de conjuntos algebraicos es algebraico.*

Demostración.

La demostración se basa en las fórmulas

$$\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J) \qquad\qquad \mathcal{V}(\bigcup I_j) = \bigcap \mathcal{V}(I_j)$$

La segunda relación es de demostración muy sencilla. Probemos la primera.

Como $IJ \subset I$ deducimos que $\mathcal{V}(I) \subset \mathcal{V}(IJ)$ y análogamente con el otro ideal. Esto prueba la inclusión

$$\mathcal{V}(I) \cup \mathcal{V}(J) \subset \mathcal{V}(IJ)$$

Sea $x \in \mathcal{V}(IJ)$. Si $x \notin \mathcal{V}(I)$, entonces existe un polinomio $f \in I$ tal que $f(x) \neq 0$. Si g es un polinomio arbitrario de J entonces $fg \in IJ$ y por lo tanto $(fg)(x) = 0$. Como $f(x)$ no es nulo, necesariamente $g(x) = 0$ y por lo tanto $x \in V(J)$, que prueba la otra inclusión. $\square$

Observación. Una ligera modificación de esta demostración prueba también que

$$\mathcal{V}(IJ) = \mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$$

y por inducción lo mismo para una colección finita de ideales. $\square$

Como el conjunto vacío y el total son algebraicos, esta proposición nos permite definir una topología en el espacio afín.

Definición 1.5 *Llamamos* topología de Zariski *en $\mathbb{A}^n$ a la que tiene por cerrados a los conjuntos algebraicos.*

Cualquier subconjunto, en particular los conjuntos algebraicos, heredan la topología de Zariski definida en el espacio afín. Todo conjunto algebraico es de manera natural un espacio topológico.

Ejemplos.

- Si el cuerpo es finito, todo espacio afín es finito y la topología de Zariski es la discreta. En este caso la topología de Zariski no aporta nada nuevo.

- En la recta afín los cerrados son los conjuntos finitos. Los abiertos son aquellos conjuntos cuyo complemento es finito. En particular, todo abierto no nulo es denso. Hemos visto que todo abierto no nulo es "muy grande". Esto es típico de la topología de Zariski.
- En general la topología de Zariski no es Hausdorff. Algunas de las propiedades de esta topología pueden parecer extrañas a los que están acostumbrados a trabajar con topologías similares a las de los espacios euclídeos.

Definición 1.6 *Sea f un polinomio no constante. El conjunto*

$$D(f) = \mathcal{V}(f)^c = \mathbb{A}^n - \mathcal{V}(f)$$

se llama abierto estandar *asociado al polinomio f.*

Corolario 1.8 *Todo abierto de $\mathbb{A}^n$ es unión finita de abiertos estandard.*

Demostración.

Si U es abierto es de la forma $U = \mathcal{V}(I)^c$. Pero todo conjunto algebraico es intersección finita de hipersuperficies. Aplicando las leyes de De Morgan

$$U = \mathcal{V}(I)^c = (\mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_r))^c = D(f_1) \cup \cdots \cup D(f_r)$$

puesto que $D(f_i) = \mathcal{V}(f_i)^c$. $\square$

Corolario 1.9 *Los abiertos estandard forman una base de la topología de Zariski.*

2. Ideal de un subconjunto afín

A cada ideal del anillo de polinomios le hemos asociado un subconjunto de $\mathbb{A}^n$. Ahora le haremos corresponder un ideal a todo subconjunto de $\mathbb{A}^n$. Normalmente la geometría algebraica deduce resultados geométricos aplicables a los subconjuntos de $\mathbb{A}^n$ estudiando propiedades algebraicas de los ideales asociados.

Definición 2.1 *Sea $V \subset \mathbb{A}^n$ un conjunto no necesariamente algebraico. El* ideal asociado *a dicho conjunto es*

$$\mathfrak{I}(V) = \{f \in k[x_1, \dots, x_n] \text{ tales que } f(p) = 0 \text{ para todo } p \in V\}$$

Es claro que $\mathfrak{I}(V)$ es un ideal, pero no es un ideal arbitrario, sino que cumple la siguiente propiedad: Si $f^n \in \mathfrak{I}(V)$ entonces $f \in \mathfrak{I}(V)$. El ideal coincide con su radical.

Definición 2.2 *Un ideal I es* radical *si $I = \operatorname{rad}(I)$.*

Naturalmente dos conjuntos distintos de $\mathbb{A}^n$ pueden dar lugar al mismo ideal. Sin embargo si los dos conjuntos son cerrados, se tiene que sus ideales son iguales si y solamente son iguales los conjuntos. Esto se deduce del siguiente resultado.

Proposición 2.1 *Dado un conjunto V de $\mathbb{A}^n(k)$ se cumple la identidad*

$$\mathcal{V}(\mathfrak{I}(V)) = \overline{V},$$

donde denotamos por $\overline{V}$ el cierre (en la topología de Zariski) de V.

Demostración.

La inclusión $V \subset \mathcal{V}(\mathfrak{I}(V))$ se deduce directamente de la definición. Como la parte derecha es un cerrado, debe contener al cierre de V.

Sea W un cerrado que contiene a V. Dicho cerrado está asociado a un ideal J y se tiene la inclusión $V \subset \mathcal{V}(J)$. Tomando ideales obtenemos la inclusión contraria $\mathfrak{I}(\mathcal{V}(J)) \subset \mathfrak{I}(V)$. Pero es fácil comprobar que en general $J \subset \mathfrak{I}(\mathcal{V}(J))$. Tenemos la inclusión $J \subset \mathfrak{I}(V)$. Aplicamos la operación V, que cambia el orden de las inclusiones, para obtener $\mathcal{V}(\mathfrak{I}(V)) \subset \mathfrak{I}(J) = W$ y deducir la otra inclusión. $\square$

Corolario 2.2 *Si a cada cerrado V de $\mathbb{A}^n$ le asociamos el ideal $\mathfrak{I}(V)$, tenemos una aplicación inyectiva de los cerrados del espacio afín en los ideales radicales del anillo de polinomios. Los cerrados de $\mathbb{A}^n$ pueden considerarse ideales del anillo de polinomios.*

Pero de nuevo el teorema de los ceros de Hilbert nos permite deducir otro resultado transcendental: Si el cuerpo es algebraicamente cerrado todo ideal radical del anillo de polinomios es de la forma $\mathfrak{I}(V)$ para un cierto conjunto algebraico. Debemos reformular el corolario de la siguiente manera.

Corolario 2.3 *Si a cada cerrado V de $\mathbb{A}^n$ le asociamos el ideal $\mathfrak{I}(V)$, tenemos una aplicación biyectiva de los cerrados del espacio afín en los ideales radicales del anillo de polinomios. El conjunto algebraico asociado a un ideal radical I es precisamente $\mathcal{V}(I)$.*

Corolario 2.4 *Se cumplen las siguientes identidades*

$$\mathcal{V}(\mathfrak{I}(V) = V \qquad\qquad \mathfrak{I}(V(I)) = \mathrm{rad}(I)$$

Observación. El mismo ejemplo de siempre demuestra la falsedad de estos resultados si el cuerpo no es algebraicamente cerrado. $\square$

Ejemplos.

- Si tenemos dos conjuntos $V_1 \subset V_2$, sus ideales cumplen la relación de orden inversa, $\mathfrak{I}(V_2) \subset \mathfrak{I}(V_1)$. Cuanto "mayor" es el conjunto "menos" polinomios se anulan en él.

- Dado un punto $x \in \mathbb{A}^n$ el conjunto $\mathfrak{I}(x)$ lo denotamos por $\mathfrak{m}_x$. Veamos que este ideal es maximal. Consideremos el morfismo de anillos

$$\begin{array}{rccc} \varphi : & k[x_1, \ldots, x_n] & \to & k \\ & f & \to & f(x) \end{array}$$

  Es epiyectivo y su núcleo es precisamente $\mathfrak{m}_x$. Como al hacer cociente por el ideal obtenemos un cuerpo, necesariamente el ideal es maximal.

- El teorema de los ceros de Hilbert precisamente afirma que si el cuerpo es algebraicamente cerrado *todos* los ideales del anillo de polinomios son de esta forma. Se establece entonces una correspondencia biunívoca entre el conjunto de puntos de $\mathbb{A}^n$ y el conjunto de ideales maximales del anillo de polinomios.

- Si el cuerpo no es algebraicamente cerrado el resultado es falso. Basta recordar el isomorfismo

  $$\mathbb{R}[x]/(x^2+1) \sim \mathbb{C}$$

  El ideal es maximal, pues su cociente es un cuerpo, pero no es de la forma $\mathfrak{m}_x$ puesto que el cociente no es isomorfo al cuerpo sobre el que están definidos los polinomios.

A cada conjunto $V \subset \mathbb{A}^n$ le hemos asociado un ideal, que hemos denotado $\mathfrak{I}(V)$. Pero haciendo cociente por dicho ideal, a cada conjunto V le podemos asociar el anillo

$$\Gamma(V) = k[x_1, \dots, x_n]/\mathfrak{I}(V)$$

Este anillo que hemos construido no es arbitrario, sino que presenta tres características fundamentales:

- El anillo contiene a las constantes y se puede considerar en él una estructura de k-álgebra.

- La k-álgebra $\Gamma(V)$ es de generación finita. En efecto, las imagenes de los elementos $x_1, \dots, x_n$ forman un conjunto de generadores.

- El anillo $\Gamma(V)$ no tiene nilpotentes. Recordemos que los anillos sin nilpotentes se llamaban anillos reducidos. Esta propiedad es una consecuencia, casi inmediata, de que $\mathfrak{I}(V)$ sea siempre un ideal radical.

Definición 2.3 *Todo anillo que cumpla las tres propiedades anteriores se llama k-álgebra afín.*

A cada conjunto algebraico V le hemos asociado un álgebra afín, $\Gamma(V)$. Lo sorprendente es que a cada álgebra afín le podemos asociar un conjunto algebraico, que en principio no será único. Veamos el procedimiento.

Sea A un álgebra afín. Como es de generación finita debe existir un morfismo epiyectivo

$$\varphi : k[x_1, \ldots, x_n] \to A$$

para cierto anillo de polinomios (no necesariamente único). El núcleo de este morfismo es un ideal I. Como el cociente es reducido el ideal I debe ser un ideal radical. Pero por el teorema de Hilbert dicho ideal debe ser de la forma $\mathfrak{I}(V)$. Ya tenemos el conjunto algebraico asociado. Es claro ahora que $\Gamma(V)$ y A son isomorfos.

Observación. El conjunto algebraico V asociado al álgebra afín no es único. Depende del morfismo φ que hayamos elegido. Sin embargo, aunque ahora no lo haremos, se puede definir una noción de morfismo entre conjuntos algebraicos. Se puede demostrar que todos los conjuntos V que construyamos son isomorfos entre si. Por ello tiene sentido hablar "del" conjunto algebraico asociado, aunque la unicidad es solo salvo isomorfismos.

El lector ya debe ver claramente donde falla el procedimiento anterior en el caso de que el cuerpo no sea algebraicamente cerrado. $\square$

El anillo $\Gamma(V)$ asociado a un conjunto algebraico se ha construido aplicando únicamente procedimientos algebraicos. Sin embargo este anillo tiene una clara interpretación geométrica, que esbozamos a continuación.

Dado un polinomio f en n variables, lo podemos considerar como una función del espacio afin de dimensión n en el cuerpo k. Como tratamos con cuerpos que no son finitos, a distintos polinomios le corresponden distintas funciones. De esta manera podemos considerar el anillo de polinomios como un subanillo del anillo de todas las funciones de $\mathbb{A}^n$ en k. Esas funciones también las podemos considerar actuando sobre un conjunto algebraico $V \subset \mathbb{A}^n$. Pero aquí si puede ocurrir que dos polinomios distintos induzcan la misma función sobre el conjunto. En efecto, dos polinomios f y g dan la misma función al restringirlos a V si $f - g$ se anula en V. Esto es lo mismo que decir que $f-g \in \mathfrak{I}(V)$. Las funciones polinomiales sobre V se identifican entonces con el anillo cociente $k[x_1,\dots,x_n]/\mathfrak{I}(V) = \Gamma(V)$. Debido a esta discusión tomamos la siguiente

Definición 2.4 *Dado un conjunto algebraico V llamamos* anillo de funciones polinomiales *al conjunto*

$$\Gamma(V) = k[x_1,\dots,x_n]/\mathfrak{I}(V)$$

También se denomina a $\Gamma(V)$ el anillo coordenado *de V.*

Corolario 2.5 *El anillo coordenado asociado al espacio afín $\Gamma(\mathbb{A}^n)$ es justamente el anillo de polinomios en n variables.*

Observación. El anillo coordenado $\Gamma(V)$ asociado a un conjunto algebraico es en cierto sentido el mínimo anillo de funciones definidas en V. Consideramos el conjunto de todas las funciones de V en k. Con la suma y multiplicación punto a punto este conjunto es un anillo que contiene a k, entendiendo los elementos del cuerpo como funciones constantes. Además de las funciones constantes, en este anillo particular existe el concepto de función coordenada. La coordenada x_i es una función de V en k, que asocia a cada elemento $(a_1,\dots,a_n)$ su coordenada i-ésima. Si un anillo contiene a las constantes y a las coordenadas, contiene a cualquier expresión polinómica formada con las coordenadas. El mínimo anillo que contiene a las constantes y a las coordenadas es precisamente $\Gamma(V)$. $\square$

Anteriormente en este capítulo hemos demostrado que existía una biyección entre los puntos del espacio afín y los ideales maximales del anillo de polinomios. Siguiendo el mismo esquema se puede probar el siguiente resultado más general.

Proposición 2.6 *Sea V un conjunto algebraico. A cada punto $x \in V$ le asociamos el ideal $\mathfrak{m}_x \subset \Gamma(V)$ formado por las funciones polinomicas que se anulan en x. Esto establece una biyección entre el conjunto de puntos de V y el conjunto de ideales maximales de $\Gamma(V)$.*

Para formular de otra manera el resultado anterior introducimos un concepto nuevo.

Definición 2.5 *Dado un anillo A llamamos* espectro maximal *de A, y denotamos* $\mathrm{Spm}(A)$ *al conjunto de ideales maximales de A.*

La discusión anterior prueba que existe una biyección natural

$$V \sim \mathrm{Spm}(\Gamma(V))$$

Hemos visto que dado un conjunto algebraico V podemos construir de un modo natural el anillo de funciones $\Gamma(V)$. Pero ahora acabamos de ver que conociendo el anillo de funciones podemos recuperar el espacio donde dichas funciones están definidas. Esto nos permite un cambio de perspectiva que se ha demostrado muy útil. En principio para construir un conjunto algebraico V debíamos partir de un "espacio ambiente" $\mathbb{A}^n$ y nuestro conjunto V es un subconjunto de dicho espacio. Pero ahora podemos partir de un álgebra afín arbitraria A y construir un conjunto $\mathrm{Spm}(A)$, que tiene todas las propiedades deseables de los conjuntos algebraicos pero que tiene la ventaja no necesitar un "espacio ambiente" para su construcción. El lector avisado notará la tremenda analogía que produce con la geometría diferencial, donde el enfoque intrínseco, descubierto por Gauss, es el más geométrico.

3. Teorema de los ceros de Hilbert

El teorema de los ceros de Hilbert se utiliza en varios campos de las matemáticas. En cada campo, la formulación es distinta, aunque todos los teoremas son equivalentes. Así no es raro encontrar en la literatura expresiones como forma débil, forma fuerte... asociadas al teorema. También es habitual referirse a este teorema por su nombre en alemán, *Nullstellensatz*, dado que fue el nombre que le dió Hilbert.

La forma más simple de comprender el enunciado del teorema de los ceros es una especie de generalización del teorema fundamental del álgebra. Sobre un cuerpo algebraicamente cerrado, todo polinomio en una variable tiene una solución. ¿Qué ocurre cuando hay más variables? El teorema de Hilbert afirma que todo polinomio en n variables tiene una solución, siempre que el cuerpo sea algebraicamente cerrado.

Sin embargo para comprender otras formulaciones necesitamos recordar algunos conceptos de la teoría de anillos y cuerpos. Sea $k \subset K$ una extensión de cuerpos. Los subanillos de K que contienen al subcuerpo k los llamaremos k-álgebras (o simplemente álgebras). La intersección de k-álgebras es de nuevo una k-álgebra. Dado un elemento $\alpha \in K$, la intersección de todas las álgebras que contienen a α es el álgebra generada por el elemento α. Denotaremos a dicha k-álgebra por $k\langle\alpha\rangle$ (esta notación no es estandard). Si en vez de un elemento tenemos una colección, posiblemente infinita, $\{\alpha_i\}$, el álgebra generada se denota $k\langle\alpha_i\rangle$. Si la colección es finita utilizamos la notación $k\langle\alpha_1, \dots, \alpha_n\rangle$. Decimos que K es de generación finita como k-álgebra si puede ser generado por un número finito de elementos en este sentido. No debemos confundir este concepto con la generación como cuerpo, que es la intersección de los cuerpos que contienen a los elementos.

Proposición 3.1 *La k-álgebra $k\langle\alpha_1, \dots, \alpha_n\rangle$ es un cociente del anillo de polinomios $k[x_1, \dots, x_n]$.*

Demostración.

A la variable x_i le asignamos el elemento α_i. Por la propiedad universal del anillo de polinomios, existe un morfismo de anillos

$$\phi : k(x_1, \dots, x_n) \longrightarrow K$$

La imagen del anillo de polinomios es un subanillo de K que contiene a las constantes y está contenido en todo anillo que contenga a las constantes y a los elementos $\alpha_1, \dots, \alpha_n$. En definitiva, es la k-álgebra generada por dichos elementos. $\square$

Como la imagen de este morfismo es siempre íntegra, el núcleo es un ideal primo. En el caso de que la imagen sea un subcuerpo de K, el núcleo es maximal. Estamos especialmente interesados en los morfismos del anillo de polinomios en el cuerpo base k.

Lema 3.2 *Sea $\phi : k[x_1, \ldots, x_n] \to k$ un morfismo de anillos. El núcleo de ϕ es el ideal*

$$(x_1 - \phi(x_1), \ldots, x_n - \phi(x_n))$$

El conjunto asociado a dicho ideal es el punto $(\phi(x_1), \ldots, \phi(x_n))$.

Demostración.

El ideal $(x_1 - \phi(x_1), \ldots, x_n - \phi(x_n))$ es maximal (aplicar la división euclídea). Todos los generadores están contenidos en el núcleo de ϕ. De esta forma el ideal entero está contenido en el núcleo. Como el ideal es maximal debe coincidir con el núcleo.

Para hallar los ceros de todo polinomio de un ideal basta hallar los ceros de un conjunto de generadores. $\square$

Definición 3.1 *Decimos que una extensión $k \subset K$ es algebraica si todo elemento $\alpha \in K$ es solución de un polinomio con coeficientes en k.*

Dado $\alpha \in K$, definimos un morfismo del anillo de polinomios $k(x)$ en K. Un elemento es algebraico si y solo si dicho morfismo no es inyectivo. Si el morfismo es inyectivo, entonces el elemento es transcendente sobre k.

Para la demostración del teorema de Hilbert utilizaremos un lema debido a Zariski. La demostración utiliza conceptos referentes a extensiones enteras de anillos que nosotros estudiaremos en el tema 8. En dicho capítulo daremos una demostración de este resultado.

Lema 3.3 (Zariski) *Sea $k \subset K$ una extensión de cuerpos. Si K es finito generado como k-álgebra, entonces K es una extensión algebraica de k.*

Una extensión mediante un elemento algebraico es una extensión de dimensión finita. Si tenemos un número finito de elementos algebraicos, inductivamente se demuestra que la extensión es de dimensión finita (corolario 8.6).

Corolario 3.4 *Sea $\mathfrak{m}$ un ideal maximal de $k[x_1, \ldots, x_n]$. Entonces la extensión $k[x_1, \ldots, x_n]/\mathfrak{m}$ es de dimensión finita.*

Demostración.

La extensión es de generación finita por ser un cociente de un anillo de polinomios. Por el lema de Zariski es algebraica. Como está generada por un número finito de elementos algebraicos es de dimensión finita. $\square$

Observación. A partir de ahora consideraremos, salvo que se diga lo contrario, que todos los cuerpos son algebraicamente cerrados. $\square$

En realidad el lema de Zariski es más potente que el teorema de Hilbert, que es ahora un simple corolario.

Teorema 3.5 (Hilbert) *Sea k un cuerpo algebraicamente cerrado. Dado un ideal I que no sea el total, el conjunto asociado $\mathcal{V}(I)$ a dicho ideal es no nulo.*

Demostración.

Todo ideal I está contenido en un ideal maximal $\mathfrak{m}$. Si tenemos $I \subset \mathfrak{m}$, sus conjuntos cumplen

$$\mathcal{V}(\mathfrak{m}) \subset \mathcal{V}(I)$$

Si demostramos que el conjunto asociado a cualquier ideal maximal es no nulo habremos demostrado el teorema.

Dado un maximal, el cociente $k[x_1, \ldots, x_n]$ es un cuerpo que está generado como álgebra por un número finito de elementos. El lema de Zariski nos dice que dicho cuerpo es algebraico sobre k. Pero como k es algebraicamente cerrado, no puede tener extensiones algebraicas salvo la trivial. Estamos en el caso del lema anterior y tenemos un morfismo del anillo de polinomios en el cuerpo base. El núcleo de ese morfismo es justamente el ideal $\mathfrak{m}$. Su conjunto es un punto del espacio afín y es no vacío. $\square$

Corolario 3.6 *Sea k un cuerpo algebraicamente cerrado. Si $\mathcal{V}(I) = \varnothing$ entonces I es todo el anillo de polinomios.*

Corolario 3.7 *Todo polinomio f no constante en n variables tiene una solución.*

Corolario 3.8 *Sea f_i una colección de polinomios en n variables. Dicha colección de polinomios tiene una solución común si y solo si el ideal que generan no es total.*

Observación. Este corolario nos da condiciones necesarias y suficientes para la resolubilidad de un sistema de ecuaciones polinomiales, pero no nos facilita un método constructivo para obtenerlas. □

Corolario 3.9 *Todos los ideales maximales del anillo de polinomios son de la forma*

$$(x_1 - a_1, \dots, x_n - a_n)$$

donde $a_i \in k$. Existe una correspondencia biunívoca entre ideales maximales del anillo de polinomios y los puntos del espacio afín.

Este corolario es también cierto para todos los conjuntos algebraicos, debido a que los ideales maximales del anillo coordenado se identifican con los maximales del anillo de polinomios que contienen al ideal del conjunto. Formulado correctamente tenemos

Corolario 3.10 *Sea V un conjunto algebraico y $k(V)$ su anillo coordenado. Existe una biyección entre los puntos de V y los ideales maximales del anillo.*

Demostración.

Un punto, entendido como un ideal maximal, está en V si y solo si dicho ideal maximal contiene al ideal $\mathfrak{I}(V)$. Como los ideales del anillo cociente $k(V) = k[x_1, \dots, x_n]/\mathfrak{I}(V)$ están en correspondencia biunívoca con los ideales del anillo de polinomios que contienen a $\mathfrak{I}(V)$, concluimos. □

Este resultado y sus corolarios son lo que se denomina forma débil del teorema. A pesar de ser importantes, todavía son más importantes los resultados que daremos a continuación pues nos permitirán establecer una biyección entre los conjuntos algebraicos y ciertos ideales del anillo de polinomios. En realidad el teorema que demostraremos a continuación se debe a Rabinowitsch, pero se acostumbra a decir que es la forma fuerte del teorema de los ceros de Hilbert

Teorema 3.11 (Hilbert, Rabinowitsch) *Sea k algebraicamente cerrado. Para todo ideal I del anillo de polinomios se verifica*

$$\mathrm{Rad}(I) = \mathfrak{I}(\mathcal{V}(I))$$

Demostración.

Tenemos la inclusión $I \subset \mathfrak{I}(\mathcal{V}(I))$. Como los ideales de los conjuntos algebraicos son radicales, el radical de I está contenido también en $\mathfrak{I}(\mathcal{V}(I))$.

Tomemos un ideal $I \subset k[x_1, \ldots, x_n]$ y un elemento arbitrario g de dicho ideal. Como el anillo es noetheriano consideramos un conjunto finito $\{f_i\}$ de generadores de dicho ideal. Todo polinomio en n variables se puede entender como un polinomio en un número superior de variables. En el anillo de polinomios en una variable más, $k(x_1, \ldots, x_n, t)$, construimos el ideal I^* generado por los $\{f_i\}$ y por el polinomio $gt - 1$.

$$I^* = (f_1, \ldots, f_n, gt - 1)$$

Veamos que este ideal no tiene ningún cero. Supongamos que un elemento $(a_1, \ldots, a_n, b)$ es un cero de dicho ideal. Debe ser anulado por los generadores. Como está anulado por los $\{f_i\}$ las primeras n coordenadas $(a_1, \ldots, a_n)$ pertenecen al conjunto de I. Pero entonces el último generador sobre dichos puntos cumple

$$g(a_1, \ldots, a_n)b - 1 = 0 - 1 = -1$$

debido a que g se anula en el conjunto de I. Como el ideal I^* no tiene ningún cero es el total. Tenemos una expresión

$$1 = \sum_{i=1}^{m} r_i f_i + r_{m+1}(gt - 1)$$

donde los polinomios $\{r_i\}$ son polinomios en $n+1$ variables.

En la expresión anterior sustituimos la variable t por $1/g$ y obtenemos una expresión formal dada por un polinomio en las variables $(x_1, \ldots, x_n)$ dividido por una potencia de g. Multiplicando por una potencia N suficientemente elevada de g conseguimos quitar denominadores y obtenemos una expresión del tipo

$$g^N = \sum (\text{polinomios en } n \text{ variables}) \cdot f_i$$

que prueba que $g^N \in I$ y por lo tanto $\mathfrak{I}(\mathcal{V}(I))$ está contenido en el radical de I, probando la inclusión que nos faltaba. $\square$

En un cuerpo arbitrario tenemos una aplicación inyectiva de los conjuntos algebraicos en los ideales radicales del anillo de polinomios. En el caso de los cuerpos algebraicamente cerrados es una biyección pues dado un ideal radical I se cumple $I = \mathfrak{I}(V(I))$. Esta propiedad es lo que hace más sencillo el estudio de la geometría algebraica sobre los cuerpos algebraicamente cerrados, que sobre un cuerpo arbitrario.

Corolario 3.12 *Sobre un cuerpo algebraicamente cerrado existe una biyección que invierte el orden entre los conjuntos*

$$\{\textit{Conjuntos algebraicos de } \mathbb{A}^n\} \quad \longleftrightarrow \quad \{\textit{Ideales radicales de } k(x_1, \ldots, x_n)\}$$

En esta biyección los ideales maximales se identifican con los puntos del espacio afín y los ideales primos con los conjuntos irreducibles. Como vemos el conjunto $\mathbb{A}^n$ se puede reconstruir a partir del anillo. Resulta que el espacio afín es precisamente el conjunto de ideales maximales del anillo.

Corolario 3.13 *Dados dos ideales I_1 e I_2 sus conjuntos $\mathcal{V}(I_1)$ y $\mathcal{V}(I_2)$ son iguales si y solo si* $\mathrm{Rad}(I_1) = \mathrm{Rad}(I_2)$.

Exactamente las mismas conclusiones se pueden obtener para cualquier conjunto algebraico V, identificando los ideales del cociente con los ideales que contienen a $\mathfrak{I}(V)$.

Corolario 3.14 *Sea V una conjunto algebraico. Existe una biyección que invierte el orden*

$$\{\textit{Subconjuntos algebraicos de } V\} \longleftrightarrow \{\textit{Ideales radicales de } k(V)\}$$

Además los puntos del conjunto se identifican con el conjunto de ideales maximales del anillo.

Vistos estos ejemplos vemos que podemos tomar una k-álgebra y asociarle el conjunto formado por sus ideales maximales. Esta es una de las bases de la teoría espectral que pretende reconstruir espacios conociendo las funciones que actuan sobre ellos. La construcción el caso general conduce a la teoría de esquemas, pero si tomamos álgebras de generación finita y que no tengan elementos nilpotentes (reducidas) seguimos dentro de la teoría de los conjuntos algebraicos. La ventaja que tiene está manera de entender la geometría algebraica es que podemos considerar al conjunto algebraico por si mismo, sin suponer un espacio ambiente que la contenga. Esta relación es análoga a la relación existente entre la teoría de variedades diferenciables y las subvariedades de $\mathbb{R}^n$.

4. Localización

El propósito de esta sección es construir anillos de fracciones. Las fracciones se construirán con elementos de un anillo A.

Estudiaremos en primer lugar un caso particular e importante: el cuerpo de fracciones de un anillo íntegro. Como siempre A^* denota $A - \{0\}$.

Lema 4.1 *En el conjunto $A \times A^*$ la relación $(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$ es de equivalencia. La clase de equivalencia de (a, b) se denota por la fracción a/b.*

Demostración.

Claramente es reflexiva y simétrica debido a la conmutatividad del anillo.

Veamos la transitividad

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

$$(c, d) \sim (e, f) \Leftrightarrow cf = de$$

Tenemos que

$$adf = bcf = bde$$

Como A es íntegro y $d \neq 0$ obtenemos que $af = be$ que demuestra que $(a, b) \sim (e, f)$. $\square$

Definición 4.1 *El conjunto cociente $A \times A^*/\sim$ se designa Q_A y se llama* cuerpo de fracciones *del anillo A.*

Introducimos en Q_A las operaciones:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{db}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Se comprueba de modo rutinario que dichas operaciones no dependen de los representantes que tomemos y que Q_A es un cuerpo con dichas operaciones.

El elemento neutro para la suma es $0/1$, el neutro para el producto es $1/1$, el opuesto del elemento a/b es $(-a)/b$ y el inverso b/a. La mayor parte de las propiedades básicas del manejo de fracciones numéricas se trasladan sin cambio a este caso.

Proposición 4.2 *La función*

$$\begin{array}{rccc} \varphi: & A & \longrightarrow & Q_A \\ & a & \longrightarrow & a/1 \end{array}$$

es un morfismo de anillos inyectivo. Via este morfismo, podemos considerar a A como un subanillo del cuerpo Q_A.

Demostración.

Es claro que φ respeta la suma, el producto y el neutro gracias a la definición de las operaciones con fracciones. Es más, la definición de operaciones con fracciones es precisamente la única que hace que esta aplicación sea morfismo.

Si $\varphi(a) = 0$ entonces $a/1 = 0$, lo que implica que $a = 0$ y φ es inyectivo. □

Proposición 4.3 *Si A se puede inyectar en un cuerpo k, entonces Q_A también se puede inyectar en el cuerpo k. Q_A es el menor cuerpo que contiene a A.*

Demostración.

Sea $\varphi : A \to k$ un morfismo inyectivo. Si queremos prolongar este morfismo a todo el cuerpo de fracciones, la única definición posible es asociarle a la fracción a/b el elemento $\varphi(a)\varphi(b)^{-1}$. Así definimos $\varphi_* : Q_A \to k$ por la fórmula

$$\varphi_*(\frac{a}{b}) = \varphi(a) \cdot \varphi(b)^{-1} = \frac{\varphi(a)}{\varphi(b)}$$

Si $a/b = c/d$ tenemos que $ad = cb$ y aplicando que φ respeta la multiplicación $\varphi(a)\varphi(d) = \varphi(c)\varphi(b)$, lo que implica que la función φ_* no depende de los representantes que tomemos.

Es rutinaria la comprobación de que en efecto φ_* es morfismo de anillos, puesto que en el cuerpo k las operaciones con fracciones son las habituales.

Además φ_* es inyectivo pues si

$$\varphi_*(\frac{a}{b}) = 0 \Rightarrow \varphi(a)\varphi(b)^{-1} = 0$$

Como $\varphi(b)$ no es nulo, necesariamente $\varphi(a) = 0$ y como φ es inyectivo $a = 0$ y la fracción a/b es nula.

Por lo tanto cualquier cuerpo k que contenga a A, contiene también a Q_A, siendo éste entonces el mínimo cuerpo que contiene a A. □

Corolario 4.4 *Un anillo es íntegro si y solo si es un subanillo de un cuerpo.*

Ejemplos.

- El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$.
- Si $A = \mathbb{Z}(i)$, el cuerpo de fracciones es precisamente $\mathbb{Q}(i)$.
- Dado un anillo de polinomios, su cuerpo de fracciones está formado por todas las fracciones racionales.
- Si A es un cuerpo, su cuerpo de fracciones es isomorfo a A.
- Todo cuerpo k contiene un cuerpo isomorfo a $\mathbb{Z}_p$ o a $\mathbb{Q}$. En efecto, si k tiene característica positiva p, existe un morfismo inyectivo de $\mathbb{Z}_p$ en k. Si k tiene característica cero, $\mathbb{Z}$ es un subanillo de k y por lo tanto $\mathbb{Q}$ también es subanillo de k. Por lo tanto $\mathbb{Z}_p$ y $\mathbb{Q}$ son los únicos cuerpos que no poseen subcuerpos.

Definición 4.2 *Sea A un anillo. Un subconjunto $S \subset A$ es* multiplicativo[1] *si:*

- $1 \in S$
- $0 \notin S$
- *Si $a \in S$ y $b \in S$ entonces $ab \in S$*

Un subconjunto multiplicativo también se llama un sistema de denominadores de A.

Sea S un subconjunto multiplicativo. En $A \times S$ introducimos la relación

$$(a, s) \sim (a', s') \text{ si existe } s'' \in S \text{ tal que } s''(as' - a's) = 0$$

Lema 4.5 *La anterior relación es de equivalencia.*

[1] En algunas referencias bibliográficas no se exige la condición de que el 1 pertenezca al subconjunto. Añadir esta condición simplifica los cálculos y no se pierde generalidad, salvo que consideremos anillos sin unidad

Demostración.

Veamos la propiedad transitiva.

$$(a,s) \sim (b,t) \Leftrightarrow \text{ existe } s_1, \quad s_1(at - bs) = 0$$

$$(b,t) \sim (c,u) \Leftrightarrow \text{ existe } s_2, \quad s_2(bu - ct) = 0$$

Multiplicamos la primera igualdad por s_2u y la segunda por s_1s. Así conseguimos eliminar la b y nos queda

$$ats_1s_2u - cts_2s_1s = 0$$

Sacando factor común $ts_1s_2 \in S$ obtenemos que $(a,s) \sim (c,u)$. $\square$

El conjunto cociente de esta relación de equivalencia la denotamos A_S. La clase de equivalencia de (a,s) se suele denotar por a/s y debemos pensar en ella como en una fracción, donde los posibles denominadores son los elementos de S.

En A_S y con nuestra notación, introducimos las operaciones

$$\begin{aligned} \frac{a}{s} + \frac{a'}{s'} &= \frac{as' + a's}{ss'} \\ \frac{a}{s} \cdot \frac{a'}{s'} &= \frac{aa'}{ss'} \end{aligned}$$

Proposición 4.6 *El conjunto A_S junto con las operaciones inducidas es un anillo unitario. El neutro para la suma es $0/1$, el opuesto de a/s es $-a/s$, el neutro para el producto $1/1$. Si $a \in S$, entonces la fracción a/s es invertible y su inverso es s/a.*

Demostración.

La única dificultad es demostrar que las operaciones no dependen de los representantes. Todas las propiedades de esta estructura de anillo son entonces evidentes. $\square$

Observación.

Los elementos de S se transforman mediante el morfismo en unidades del anillo A_S.

Definición 4.3 *El anillo A_S se dice que es el* anillo de fracciones *de A con denominadores de S. También se dice que es el* localizado *en S del anillo A.*

Tenemos siempre una aplicación

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & A_S \\ & a & \longrightarrow & a/1 \end{array}$$

que es morfismo de anillos. Debemos observar que, a diferencia de lo que ocurría en el cuerpo de fracciones, esta aplicación puede no ser inyectiva si el anillo A no es íntegro.

Teorema 4.7 (Propiedad universal) *Sea $\varphi : A \longrightarrow B$ un morfismo de tal forma que $\varphi(s)$ sea invertible en B para todo elemento de S. Entonces existe un único morfismo*

$$\varphi_* : A_S \longrightarrow B$$

que cumple $\varphi_*(a/1) = \varphi(a)$.

Demostración.

Si φ_* debe ser morfismo, necesariamente se cumple

$$\varphi_*(a/s) = \varphi(as^{-1}) = \varphi(a)\varphi(s^{-1}) = \varphi(a)\varphi(s)^{-1}$$

Por lo tanto adoptaremos como definición de φ_* la fórmula

$$\varphi_*(a/s) = \varphi(a)\varphi(s)^{-1}$$

Tenemos que ver que φ_* no depende de los representantes.

Si $a/s = a'/s'$ entonces $s''(as' - a's) = 0$. Aplicando φ a esta expresión obtenemos

$$\varphi(s'')(\varphi(a)\varphi(s') - \varphi(a')\varphi(s)) = 0$$

y como $\varphi(s'')$ es unidad, es cancelable y obtenemos que

$$\varphi(a)\varphi(s') = \varphi(a')\varphi(s)$$

lo que demuestra que $\varphi_*(a/s) = \varphi(a'/s')$.

Que conserva la suma, el producto y la unidad es de fácil comprobación.
$\square$

Observación.

Se puede utilizar esta propiedad universal para caracterizar completamente al anillo A_S. En término categóricos, tenemos que A_S es el representante de un cierto functor y sabemos que los representantes de functores son únicos salvo isomorfismos.

Ejemplos.

- Sea $f \in A$ no nilpotente. $S = \{f^n\}_{n\geq 0}$ es un subconjunto multiplicativo. Las fracciones tienen como denominadores potencias de f. En este caso el anillo se suele denotar A_f en vez de A_S.

- Sea $\mathfrak{p}$ un ideal primo. $S = A - \mathfrak{p}$ es multiplicativo. En este caso A_S se denota $A_\mathfrak{p}$. Los denominadores en este caso no contienen elementos de $\mathfrak{p}$. El conjunto
$$\mathfrak{m} = \{a/s \text{ con } a \in \mathfrak{p}\}$$
es un ideal de $A_\mathfrak{p}$. Este ideal es maximal, pues todos los elementos que no están en $\mathfrak{m}$ son invertibles. Además este es único ideal maximal del anillo.

- El cuerpo de fracciones de un anillo íntegro.

- Sea S_0 el conjunto de todos los elementos de A que no son divisores de cero. S_0 es un subconjunto multiplicativo y A_{S_0} se denomina anillo total de fracciones de A. En este caso la aplicación canónica $\varphi : A \to A_{S_0}$ es inyectiva.

Definición 4.4 *Un anillo A es* local *si tiene un único ideal maximal.*

Todos los anillos $A_{\mathfrak{p}}$ son locales. Decimos que $A_{\mathfrak{p}}$ es el localizado de A en el "punto" $\mathfrak{p}$.

El proceso que nos transforma A en $A_{\mathfrak{p}}$ se denomina localización.

Proposición 4.8 *Sea $\varphi : A \to A_S$ el morfismo natural. Existe una correspondencia biunívoca entre los ideales primos de A_S e ideales primos que no cortan a S, dada por la fórmula $\mathfrak{p} \longleftrightarrow \varphi^{-1}(\mathfrak{p})$.*

Demostración.

Se basa en la siguiente observación. Si $\varphi^{-1}(\mathfrak{p}) \cap S$ no es vacío, existe un elemento s no nulo en dicha intersección. Por una parte $\varphi(s)$ está en el ideal $\mathfrak{p}$ y por otra parte $\varphi(s)$ es invertible. El ideal $\mathfrak{p}$ es entonces el total. $\square$

Corolario 4.9 *Los ideales de $A_{\mathfrak{p}}$ se identifican con los ideales de A que están contenidos en $\mathfrak{p}$.*

En particular, el ideal $\mathfrak{p}$, entendido en el localizado, es maximal pues no está contenido en ningún ideal superior. Además es el único maximal, pues todo ideal primo hemos visto que está contenido en él.

En geometría algebraica a cada subvariedad afín V le asociamos el anillo $k(V)$ de las funciones polinomiales sobre V. Si un elemento g de dicho anillo no se anula nunca, tiene sentido hablar de la función f/g. Estas son las funciones racionales, por ser división de polinomios.

Es claro que si un elemento no se anula en ningún punto, dicho elemento no puede ser un divisor de cero. Podemos entonces dar la siguiente

Definición 4.5 *Sea V una variedad afín. Llamamos* anillo de funciones racionales *en V y denotamos $R(V)$ al anillo total de fracciones del anillo $k(V)$.*

En particular, si la variedad es irreducible (capítulo 9) el ideal asociado a la variedad es primo. El anillo de funciones polinómicas es íntegro y por supuesto el anillo de funciones racionales es justamente el cuerpo de cocientes de dicho anillo.

Con ánimo de justificar algunas definiciones que se hacen en geometría algebraica estudiaremos un poco en profundidad la construcción de anillos de gérmenes. Tomaremos el ejemplo de la geometría diferencial.

Sea $\mathcal{V}$ una variedad diferenciable y x un punto de dicha variedad. Trabajaremos con el anillo $A = C^\infty(\mathcal{V})$ de las funciones infinitamente diferenciables en la variedad. En este anillo el conjunto de las funciones que se anulan en el punto x, lo denotamos $\mathfrak{m}_x$. Es un ideal maximal, pues es el núcleo del morfismo de anillos

$$\begin{array}{ccc} C^\infty(V) & \longrightarrow & \mathbb{R} \\ f & \longrightarrow & f(x) \end{array}$$

El localizado del anillo en $\mathfrak{m}_x$ se denomina **anillo de gérmenes** de funciones diferenciables en x. Veamos que coincide con la definición habitual de geometría diferencial.

Un elemento del localizado es de la forma f/g donde g no se anula en x. Por continuidad no se anula en un entorno de x. Sabemos entonces que f/g es una función diferenciable en dicho entorno.

Si f'/g' es otro representante del localizado, debe existir g'' no perteneciente a $\mathfrak{m}_x$ que cumpla $g''(f'g - fg') = 0$. Como g'' no se anula en x, no se anula en un entorno. La función $f'g - fg'$ es nula en dicho entorno y las fracciones f/g y f'/g' inducen la misma función en algún entorno abierto de x. Esto es equivalente a decir que ambos producen el mismo gérmen en el punto x. La misma construcción es válida para funciones continuas o para funciones holomorfas en superficies de Riemann.

Las funciones diferenciables cumplen una cierta propiedad local, que aunque es más simple enunciarla en términos de haces, viene a decir lo siguiente.

Una función $f : \mathcal{V} \to \mathbb{R}$ es diferenciable si y solo si su germen en todos los puntos es diferenciable. Decir que un germen es diferenciable, es afirmar que coincide con el germen de una función diferenciable definida en un entorno. Lo mismo en válido para la noción de continuidad: una función es continua si y solo si su gérmen es todos los puntos es continuo.

Sea V un variedad afín y $k(V)$ su anillo de funciones polinomiales. A cada punto x de V le asociamos el ideal maximal de las funciones polinomiales que se anulan en x. El localizado del anillo de V en dicho ideal maximal (que denotaremos $\mathfrak{m}_x$) es el anillo de gérmenes de funciones polinomiales en x. En general a cada cerrado irreducible le corresponde un ideal primo. Localizando en dicho ideal tenemos los gérmenes de funciones polinómicas en dicho conjunto algebraico.

Decimos que una función $f : V \to k$ es regular en un punto si su germen en dicho punto es equivalente a una división de polinomios. Llamamos regular a una función que sea regular en todo punto. El conjunto de todas las funciones regulares sobre la variedad se denota $\mathcal{O}(V)$.

La misma construcción se puede hacer con un abierto U de la variedad. Una función definida en U es regular si es regular en todo punto. El conjunto de funciones regulares en U lo denotamos por $\mathcal{O}(U)$. Utilizando el hecho de que el conjunto de gérmenes tiene una estructura de anillo, se prueba que todos estos conjuntos son anillos. Como además toda función constante es regular, resulta que los anillos $\mathcal{O}(U)$ contienen a las constantes. Esto los dota de modo natural de una estructura de k-álgebra. Con esta construcción hemos asociado una k-álgebra $\mathcal{O}(U)$ a cada abierto de una variedad algebraica afín. En realidad nos queda por definir el anillo asociado al conjunto vacío. Por definición lo tomaremos como el anillo que consta únicamente de la función cero.

Los anillos de funciones regulares de distintos abiertos están relacionados entre si. Veamos alguna de esas relaciones.

Corolario 4.10 *Si una función f es regular en un abierto U entonces su restricción a cualquier abierto $U' \subset U$ es también regular.*

La propiedad de regularidad es una propiedad local, en el sentido de que se cumple la siguiente

Proposición 4.11 *Sea f una función en U, de tal forma que cada punto $x \in U$ tenga un entorno abierto tal que la restricción de f a dicho abierto sea regular. Entonces la función es regular.*

Demostración.

Con la definición que nosotros hemos adoptado de función regular, es prácticamente tautológico, pues entonces en cada punto el germen de f coincide con un germen regular. $\square$

Por cumplir estas dos propiedades decimos que la variedad V es un espacio anillado, aunque no trataremos ahora este tópico.

En general la estructura de uno de los anillos $\mathcal{O}(U)$ puede ser complicada. Pero para algunos abiertos sencillos, la estructura es también sencilla. El conjunto algebraico más elemental con el que tratamos es la hipersuperficie. Su complementario será también un abierto bastante simple. Si tenemos una hipersuperficie $\mathcal{V}(g)$, denotaremos su complementario por $D(g)$. Trabajemos un poco más con estos abiertos. Se verifican de modo inmediato las siguientes propiedades.

Proposición 4.12 *Se cumple:*

- $D(fg) = D(f) \cap D(g)$
- $D(f^n) = D(f)$
- $D(f) = \varnothing$

La principal característica que tienen estos abiertos es que forman una base de la topología de Zariski. Todo abierto es unión de estos abiertos básicos. Pero como el anillo es noetheriano, esa unión es además finita (lema 7.10). Aplicando esta condición de finitud se prueba

Proposición 4.13 *El anillo $\mathcal{O}(D(g))$ es isomorfo a $\mathcal{O}(V)_g$ (anillo de fracciones con potencias de g en el denominador).*

De este modo conocemos el anillo de funciones regulares en los complementos de hipersuperficies. Conociendo los anillos asociados a abiertos de una base, se puede conocer el anillo asociado a todo abierto utilizando un procedimiento algebraico que consiste en tomar límites inversos de anillos. No nos detendremos en está construcción.

Tomando el caso en que g es una unidad, obtenemos.

Corolario 4.14 *El anillo $\mathcal{O}(V)$ de toda la variedad coincide con $k(V)$, el anillo de las funciones polinomiales.*

Si conocemos el anillo asociado a toda la variedad, podemos reconstruir la variedad V. En el caso de un cuerpo algebraicamente cerrado el teorema de los ceros de Hilbert afirma que V se corresponde de modo natural con el conjunto de ideales maximales del anillo de la variedad. Teniendo el anillo, podemos localizarlo en cualquier primo, en particular en cualquier maximal y obtener de este modo el anillo de gérmenes en todos los puntos. Con los anillos de gérmenes se le puede asociar a cada abierto el anillo de funciones regulares. Podemos reconstruir a partir del anillo todo lo interesante de la variedad. Es por ello que se le da tanta importancia al anillo. Al analizar los espectros se sigue el mismo esquema de trabajo, generalizando de este modo la geometría algebraica clásica y llegando al concepto de esquema.

Como en cualquier espacio topológico el conocer una función sobre un conjunto denso determina unívocamente la función. Si existe la prolongación continua al cierre del conjunto, esta es necesariamente única. Desafortunadamente en muchas variedades algebraicas las únicas funciones racionales definidas en toda la variedad son simplemente las constantes. Por ello tiene gran importancia el estudio de las funciones racionales definidas en conjuntos que no son el espacio total.

Definición 4.6 *Dada una variedad V y un abierto denso $U \subset V$, las funciones regulares que no pueden extender (manteniendo la regularidad) a ningún abierto U' que contenga a U se llaman* funciones racionales *en V. El conjunto denso U se dice que es el* dominio de definición *de la función y el cerrado $V - U$ es el conjunto de los* polos *de la función.*

Observación.

Estas mismas definiciones son las que se emplean en la teoría de superficies de Riemann. En el caso complejo las funciones racionales suelen llamarse meromorfas. Las funciones meromorfas que no tienen polos y por lo tanto están definidas en toda la variedad se denominan funciones holomorfas. Es conocido el hecho de que las funciones holomorfas definidas sobre superficies compactas son necesariamente constantes.

Las funciones racionales en V se pueden sumar y multiplicar teniendo en cuenta que probablemente cambien los conjuntos de definición. Con estas operaciones el conjunto de funciones racionales es de modo natural una k-álgebra, que denotaremos $R(V)$. Si la variedad es reducible, el anillo de funciones racionales es el producto de los anillos asociados a sus componentes irreducibles. De esta manera el estudio de las funciones racionales se reduce al estudio en variedades irreducibles. En este caso es importante el resultado.

Proposición 4.15 *Si V es irreducible, el anillo $R(V)$ es isomorfo al cuerpo de cocientes del anillo coordenado (e íntegro) $k(V)$.*

5. Localización de módulos

Sea ahora M un módulo y S un subconjunto multiplicativamente cerrado del anillo. En $M \times S$ se introduce la relación de equivalencia

$$(m, s) \sim (m', s') \text{ si } (ms' - m's)u = 0 \text{ para algún } u \in S$$

La clase de equivalencia se denota m/s. Se define la suma en este conjunto como

$$\frac{m}{s} + \frac{m'}{s'} = \frac{ms' + m's}{ss'}$$

El conjunto de las clases de equivalencia tiene estructura de grupo abeliano. Introducimos también la multiplicación por elementos de A_S.

$$\frac{a}{s} \cdot \frac{m'}{s'} = \frac{am}{ss'}$$

Todas las construcciones son independientes del representante y dotan al conjunto cociente, que de ahora en adelante dentoraremos M_S, de una estructura de A_S-módulo. En M_S también se puede considerar la estrutura de A-módulo definida por el morfismo φ:

$$x \cdot \frac{m}{s} = \frac{xm}{s} = \varphi(x) \cdot \frac{m}{s}$$

Como en M_S existe una estructura de módulo sobre dos anillos, siempre que exista una posible confusión se debe decir cual es el anillo considerado.

Cada morfismo de A-módulo $\phi : M \longrightarrow N$ induce un morfismo de A_S-módulos ϕ_S mediante la fórmula

$$\begin{array}{rccc} \phi_S : & M_S & \longrightarrow & N_S \\ & m/s & \longrightarrow & \phi(m)/s \end{array}$$

Si tenemos otro morfismo de módulos γ se cumple la relación $(\phi\gamma)_S = \phi_S\gamma_S$. Tenemos así construido un functor de la categoría de A-módulos en la de A_S-módulos.

Como en el caso de los anillos, cuando S sea $A - \mathfrak{p}$ con $\mathfrak{p}$ un ideal primo, se dirá que se localiza el módulo en el punto $\mathfrak{p}$.

Proposición 5.1 *Construir el módulo de fracciones es un functor exacto. Si* $M' \xrightarrow{\phi} M \xrightarrow{\gamma} M''$ *es exacta entonces* $M'_S \xrightarrow{\phi_S} M_S \xrightarrow{\gamma_S} M''_S$ *es también exacta.*

Demostración.

Como $\phi\gamma = 0 \Rightarrow (\phi\gamma)_S = 0 \Rightarrow \phi_S\gamma_S = 0$ lo que implica que

$$\mathrm{Im}(\phi_S) \subset \mathrm{Ker}(\gamma_S)$$

Reciprocamente, si $\gamma(m)/s = 0$ entonces existe $t \in S$ tal que

$$t(\gamma(m)) = 0 \Longrightarrow \gamma(tm) = 0$$

Entonces $tm \in \mathrm{Ker}(\gamma) = \mathrm{Im}(\phi)$. Así $tm = \phi(m')$ lo que conduce a que

$$m/s = \phi_S(m'/s)$$

lo que concluye la demostración. □

Proposición 5.2 *Si N y P son submódulos:*

$$(N + P)_S = N_S + P_S$$

$$(N \cap P)_S = N_S \cap P_S$$

$$(M/N)_S \sim M_S/N_S$$

Demostración.

Las dos primeras propiedades nos dicen que construir módulos de fracciones induce un morfismo de retículos. La última se deduce de la sucesión exacta

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

teniendo en cuenta que se conserva la exactitud. $\square$

El siguiente teorema nos da otro método de construcción del módulo de fracciones.

Teorema 5.3 *Sea M un A-módulo. Existe un único isomorfismo ϕ de A_S-módulos de $A_S \otimes_A M$ en M_S que manda al punto $a/s \otimes m$ hasta am/s.*

Demostración.

La aplicación

$$\begin{array}{ccc} A_S \times M & \longrightarrow & M_S \\ (a/s, m) & \longrightarrow & am/s \end{array}$$

es A-bilineal. Por la propiedad universal del producto tensorial existe una aplición $\phi : A_S \otimes M \longrightarrow M_S$ que satisface el enunciado. Siguiendo las ideas expuestas anteriormente, se comprueba que en efecto es un isomorfismo y que además es un morfismo de A_S-módulos. $\square$

Se dice que una propiedad de un A-módulo es una propiedad local, cuando se cumpla lo siguiente: El A-módulo tiene la propiedad P si y solo si para todo punto del espectro el $A_{\mathfrak{p}}$-módulo asociado tiene la propiedad P.

Esta definición algebraica de localidad coincide con la idea de localidad en el sentido topológico, tras introducir en el espectro la topología de Zariski.

La importancia de este concepto radica en que las propiedades locales basta estudiarlas sobre anillos locales.

Definición 5.1 *Un anillo conmutativo y con unidad es local si tiene un único ideal maximal* $\mathfrak{m}$*. El cuerpo* $k = A/\mathfrak{m}$ *se llama cuerpo residual.*

Lema 5.4 A *es local de ideal maximal* $\mathfrak{m}$ *si y solo si todos los elementos de* $A - \mathfrak{m}$ *son invertibles.*

Demostración.

$\Rightarrow$) Si $x \in A$ no es invertible, pertenece a algún ideal maximal.

$\Leftarrow$) Si el complementario de las unidades de A es un ideal, entonces es maximal y es el único ideal maximal. □

Teorema 5.5 $A_{\mathfrak{p}}$ *es local.*

Demostración.

Los elementos de la forma a/s con $a \in \mathfrak{p}$ forman un ideal. Si s/s' no pertenece a ese ideal, este elemento es invertible y su inverso es s'/s. □

Lema 5.6 (Nakayama) *Sea* A *local,* $\mathfrak{m}$ *su ideal maximal. Si* M *es de generación finita y* $\mathfrak{m}M = M$*, entonces* $M = 0$*.*

Demostración.

Sea $(m_1, \ldots, m_n)$ un conjunto mínimo de generadores. Como dicho conjunto genera M y además $\mathfrak{m}M = M$ tenemos que

$$m_n = a_1 m_1 + \cdots + a_n m_n \text{ con } a_i \in \mathfrak{m}$$

Entonces deducimos que

$$m_n(1 - a_n) = a_1 m_1 + \cdots + a_{n-1} m_{n-1}$$

Como $1 - a_n$ es invertible, tenemos que $(m_1, \dots m_{n-1})$ generan M. Esto solo es posible si $M = 0$. $\square$

Corolario 5.7 $M_{\mathfrak{m}} = 0 \Longleftrightarrow M = 0$.

Demostración.

$M_{\mathfrak{m}} = M/\mathfrak{m}M$. $\square$

Corolario 5.8 *La condición necesaria y suficiente para que una familia genere M es que sus imagenes generen $M_{\mathfrak{m}}$.*

Demostración.

$\Rightarrow$) $M_{\mathfrak{m}} = M \otimes k$. Si $\{m_i\}$ generan M como A-módulo $\Rightarrow$ $\{m_i \otimes 1\}$ generan $M_{\mathfrak{m}}$ como k-espacio.

$\Leftarrow$) Sea N es submódulo generado por los elementos $\{m_i\}$

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

Localizando esta sucesión tenemos

$$N_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \longrightarrow (N/M)_{\mathfrak{m}} \longrightarrow 0$$

$N = M$ si solo si $N_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}}$ es epiyectiva y lo es pues las imagenes de m_i generan $M_{\mathfrak{m}}$. $\square$

Veamos ahora algunas propiedades locales.

Proposición 5.9 *Sea M un A-módulo. Son equivalentes.*

I) $M = 0$.

II) $M_{\mathfrak{p}} = 0 \quad \forall\ \mathfrak{p}$ *primo.*

III) $M_{\mathfrak{m}} = 0 \quad \forall\ \mathfrak{m}$ *maximal.*

Demostración.

Solo tenemos que demostrar una implicación pues las otras son evidentes.

Sea I el anulador de M. Como $m/1 = 0$ en $M_{\mathfrak{m}}$, entonces existe un u que no pertenece a $\mathfrak{m}$ tal que $um = 0$. El anulador no está contenido en ningún ideal maximal. Por lo tanto el anulador es A. Entonces $1m = 0 \Longrightarrow m = 0$. $\square$

Proposición 5.10 *Sea $\phi : M \longrightarrow N$ A-lineal. Son equivalentes:*

1. *ϕ es inyectiva.*
2. *$\phi_{\mathfrak{p}}$ es inyectiva para todo ideal primo.*
3. *$\phi_{\mathfrak{m}}$ es inyectiva para todo ideal maximal.*

Demostración.

Localizamos la sucesión

$$0 \longrightarrow \mathrm{Ker}(\phi) \longrightarrow M \longrightarrow N$$

y aplicamos la proposición anterior. $\square$

Tenemos otra proposición si sustituimos inyectiva por epiyectiva.

Corolario 5.11 *$\phi : M \longrightarrow N$ es isomorfismo si y solo si lo es al localizar en cada ideal primo.*

Corolario 5.12 *Una sucesión $M \longrightarrow N \longrightarrow M'$ es exacta si y solo si lo es al localizarla en todos los ideales primos.*

6. Módulos y anillos noetherianos

Comenzaremos este capítulo con un teorema de teoría de conjuntos ordenados que establece la equivalencia de dos resultados.

Proposición 6.1 *Sea Σ un conjunto dotado de una relación de orden. Entonces son equivalentes las condiciones que siguen:*

i) *Cada sucesión creciente de elementos de Σ*

$$x_1 \leq x_2 \leq \cdots \leq x_n$$

es estacionaria, que quiere decir que existe un n tal que $x_n = x_{n+i}$ para todo $i > 0$.

ii) *Cada subconjunto no vacío de Σ admite un elemento maximal.*

Demostración.

$i) \Rightarrow ii)$ Si no existiera elemento maximal para el subconjunto Σ, entonces por inducción crearíamos una cadena que no estaciona.

$ii) \Rightarrow i)$ $\{x_n\}_{n\geq 1}$tiene elemento maximal. $\square$

La condición $i)$ se denomina condición de cadena ascendente y la condición $ii)$ la condición maximal. Estos conceptos los aplicaremos cuando Σ sea el retículo de submódulos de un módulo dado.

Definición 6.1 *Un módulo M es* noetheriano *si el conjunto Σ de sus submódulos satisface alguna de las condiciones equivalentes de la proposición anterior. El orden considerado en Σ es el de la inclusión.*

Si $A \subset B$ son anillos y M es un B-módulo, puede ocurrir que M sea noetheriano como B-módulo y no lo sea como A-módulo. Esto ocurre por ejemplo en el caso $A = k$, $B = k(x)$. Sin embargo si es noetheriano sobre el subanillo, necesariamente es noetheriano sobre todo anillo que lo contenga.

Ejemplos.

- Todo grupo finito abeliano es noetheriano como $\mathbb{Z}$-módulo.
- Todo módulo simple[2] es noetheriano.

[2] Un módulo es simple si sus únicos submodulos son el cero y el total

- Todo módulo M cuyo cardinal sea finito es noetheriano sobre cualquier anillo.
- Todo k-espacio de dimensión finita.
- Si A es un dominio de ideales principales, entonces es noetheriano como A-módulo.

La importancia de los módulos noetherianos radica en el siguiente teorema

Teorema 6.2 *M es un A-módulo noetheriano si y solo si todo submódulo de M es de generación finita.*

Demostración.

$\Rightarrow$) Sea N un submódulo de M y sea Σ' el conjunto de todos los submódulos menores que N y que además sean finito generados. Como Σ cumple la condición de cadena ascendente, lo mismo le ocurre a Σ'. Sea N' un elemento maximal de Σ'. Veamos que $N' = N$. Si esto no ocurriera, existiría un vector $m \in N - N'$. Entonces $N' + \langle m \rangle$ sería de generación finita y estaría contenido en N, contradiciendo la maximalidad de N'.

$\Leftarrow$) Sea $N_1 \subset \cdots \subset N_n \cdots$ una cadena ascendente de submódulos. Tenemos que $\cup_i N_i$ es un submódulo. Sea $\{m_i\}$ $(i = 1, \ldots, k)$ un conjunto generador del módulo unión. Sea N_n el primer submódulo que contenga a todos los m_i. La sucesión estaciona en N_n. $\square$

Teorema 6.3 *Si $0 \xrightarrow{i} M' \longrightarrow M \xrightarrow{\pi} M'' \longrightarrow 0$ es exacta, entonces M es noetheriano si y solo si M' y M'' son noetherianos.*

Demostración.

$\Rightarrow$) Los submódulos de M' son submódulos de M. Entonces M' es noetheriano. Por π^{-1} los submódulos de M'' se pueden considerar incluidos en los submódulos de M. M'' es noetheriano.

$\Leftarrow$) Si $\{N_i\}$ es una cadena es M, entonces $\{i^{-1}(N_i)\}$ y $\{\pi^{-1}(N_i)\}$ son cadenas que estacionan. Entonces la cadena $\{N_i\}$ estaciona y M es noetheriano. $\square$

Corolario 6.4 *La suma directa finita de módulos noetherianos es un módulo noetheriano.*

Demostración.

La sucesión

$$0 \longrightarrow M_n \longrightarrow \oplus_1^n Mi \longrightarrow \oplus_1^{n-1} M_i \longrightarrow 0$$

es exacta. Se deduce del teorema anterior por inducción. $\square$

Corolario 6.5 *Si A es noetheriano como A-módulo, entonces A^n es noetheriano. Si M es de generación finita es un cociente de A^n y por lo tanto es noetheriano.*

Definición 6.2 *Un anillo A se llama* noetheriano *cuando sea un módulo noetheriano con A como anillo de escalares.*

Las tres condiciones siguientes son equivalentes y definen un anillo noetheriano:

i) Cada ideal de A es de generación finita.

ii) Toda cadena ascendente de ideales estaciona.

iii) Todo conjunto no vacío de ideales posee al menos un elemento maximal.

Los anillos noetherianos son de gran importancia en álgebra y en geometría algebraica, pues incluyen a todos los anillos de polinomios en n variables sobre un cuerpo (Teorema de la base). Además los anillos noetherianos son cerrados bajo ciertas operaciones de interés.

Proposición 6.6 *Todo cociente de un anillo noetheriano es noetheriano.*

Demostración.

Sea A un anillo e I un ideal. $\pi : A \longrightarrow A/I$ la proyección canónica. Mediante π^{-1} el conjunto de ideales de A/I se puede suponer inyectado en el retículo de ideales de A. $\square$

Proposición 6.7 *Si A es noetheriano y S un conjunto multiplicativamente cerrado, A_S es noetheriano.*

Demostración.

De nuevo los ideales de A_S los podemos considerar incluidos en los ideales de A. Los ideales de A_S se identifican con los ideales de A que tienen intersección nula con S. $\square$

El siguiente teorema es de importancia clave en geometría algebraica clásica, pues nos dice que toda subvariedad de k^n definida por un conjunto de polinomios en n variables es la intersección de un número finito de hipersuperficies definidas por los ceros de un polinomio.

Teorema 6.8 (de la base de Hilbert) *Si A es noetheriano, entonces $A(x)$ es un anillo noetheriano.*

Demostración.

Existen muchas demostraciones del teorema de la base. La original de Hilbert y la que están más extendidas son demostraciones de existencia, pero no no son constructivas. Según algunos historiadores este es el primer teorema importante no constructivo. En su época muchos matemáticos no aceptaron este teorema en particular los seguidores de Kronecker y Brouwer que forman un grupo de matemáticos llamados intuicionistas.

No reproduciremos aquí la demostración. $\square$

Corolario 6.9 *Si A es noetheriano, entonces $A(x_1, \ldots, x_n)$ también.*

Demostración.

$A(x_1, \ldots, x_n) = A(x_1, \ldots, x_{n-1})(x_n)$ e inducción. $\square$

Tomemos un conjunto algebraico asociado a un ideal I. Sea $f_1, \ldots, f_n$ un conjunto de generadores del ideal I. Entonces

$$\mathcal{V}(I) = \bigcap_{i=1}^{n} \mathcal{V}(f_i)$$

y toda variedad algebraica afín es la intersección de un número finito de hipersuperficies.

Corolario 6.10 *Si $A \subset B$ noetheriano y B es de generación finita como álgebra sobre A, entonces B es un anillo noetheriano.*

Demostración.

B es un cociente del anillo de polinomios. $\square$

Definición 6.3 *Llamamos* álgebra afín *sobre el cuerpo k a toda k-álgebra que admita un número finito de generadores (como anillo).*

Si A es una k-álgebra afín, por la propiedad universal del anillo de polinomios existe un morfismo epiyectivo de un anillo de polinomios en un número finito de variables, en el anillo A. Un álgebra afín es un cociente de un anillo de polinomios sobre un cuerpo y es por lo tanto noetheriano.

En particular, dado un ideal I del anillo de polinomios, el anillo cociente es el álgebra de las funciones polinomiales sobre la variedad $\mathcal{V}(I)$. Es lo que hemos denotado $k(\mathcal{V}(I))$. Este es el ejemplo más evidente de álgebra afín.

7. Espectro

En álgebra conmutativa se introduce la noción de espectro para intentar conseguir que todos los anillos se puedan entender como anillos de funciones. Este objetivo no se consigue plenamente, puesto que no se puede definir en general el conjunto imagen adecuado. Ello se puede solucionar introduciendo la idea de haz de anillos. Todo anillo conmutativo tiene asociado de manera natural un haz de anillos locales, que denominaremos haz estructural. A pesar de ello, la interpretación geométrica que se añade a la teoría de anillos es suficientemente interesante para profundizar en su estudio.

En el estudio del espectro se pueden identificar varias fases. Primeramente construiremos el espectro de todo anillo. Posteriormente introduciremos, por analogía con el estudio de las variedades algebraicas, una topología, llamada también topología de Zariski. Por último dotaremos al espectro de un haz de anillos. Con esta última estructura los espectros de anillos también se llaman esquemas afines. La noción general de esquema se construye por agregación de esquemas afines.

Definición 7.1 *Sea A un anillo conmutativo. El* espectro *de A es el conjunto de los ideales primos de A. Lo denotaremos por* $\operatorname{Spec}(A)$. *El conjunto total no lo consideraremos ideal primo.*

Observación. En todo anillo no nulo, aplicando el lema de Zorn, se constata la existencia de ideales maximales. Como los ideales maximales son primos, el espectro de un anillo no nulo nunca es vacío. □

Para nosotros, de ahora en adelante, un ideal primo lo podemos entender como un subconjunto de A o como un punto del espacio $\operatorname{Spec}(A)$. Si pensamos en el ideal primo como un punto de $\operatorname{Spec}(A)$, lo denotaremos por una letra, por ejemplo x. Si lo entendemos como un subconjunto de A lo denotaremos $\mathfrak{p}_x$.

Ejemplos.

- Espectro de $\mathbb{Z}$. A cada número primo positivo p le corresponde un punto del espectro, el ideal (p). Como Z es íntegro, (0) es también un ideal primo.
$$\operatorname{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), \dots\}$$
- Espectro de k. Si k es un cuerpo, el único ideal primo es el (0).
- Espectro de $k[t]$. Sea k un cuerpo algebraicamente cerrado. Para cada elemento $a \in k$ el polinomio $(x - a)$ genera un ideal primo. El neutro también es un ideal primo. Con estas identificaciones podemos escribir
$$\operatorname{Spec}(k[t]) = k \cup \{0\}$$
- Espectro de $\mathbb{R}[t]$. Los polinomios irreducibles sobre $\mathbb{R}$ pueden ser de dos tipos. El primer tipo es $(t - a)$ donde $a \in \mathbb{R}$. Los otros polinomios

irreducibles son los de segundo grado con raices complejas conjugadas. Son de la forma $(t-z)(t-\bar{z})$ donde $z \in \mathbb{C}$. Para cada número real a el espectro tiene un punto, $(t-a)$. Para cada número complejo z situado en el semiplano superior, el espectro tiene un punto, $(t-z)(t-\bar{z})$. El neutro también es primo:

$$\operatorname{Spec}(\mathbb{R}[t]) = \{a + bi \in \mathbb{C} \text{ tales que } b \geq 0\} \cup \{(0)\}$$

- El espectro de todos los anillos íntegros tiene un punto correspondiente al ideal nulo. Dicho punto está contenido en todo ideal primo. Ese punto se denomina punto genérico.
- Si k es un cuerpo, el espectro de k^n tiene n puntos. El (0) no pertenece al espectro puesto que no es íntegro.
- Sea $X \subset \mathbb{C}^n$ una subvariedad afín irreducible y $\mathbb{C}[X]$ su anillo coordenado. Dado un ideal primo $\mathfrak{p} \subset k[X]$ no nulo, la subvariedad $\mathcal{V}(\mathfrak{p})$ es una subvariedad irreducible de X. Además de estos puntos tenemos el ideal (0) que es primo puesto que X es irreducible. Con estos convenios

  $$\operatorname{Spec}(\mathbb{C}[X]) = \{\text{Subvariedades irreducibles de } X\} \cup \{0\}$$

  Los ideales maximales de este espectro se corresponden con los puntos de X, según se desprende del teorema de los ceros de Hilbert. La variedad X puede considerarse inyectada en el espectro de su anillo de funciones. En particular $\mathbb{C}^n$ se puede considerar inyectado en el espectro del anillo de polinomios.

  Mismo esquema para cualquier cuerpo algebraicamente cerrado.

Lema 7.1 *Si $x \in \operatorname{Spec}(A)$, entonces $A/\mathfrak{p}_x$ es un anillo íntegro. El cuerpo de fracciones de este anillo se denota $k(x)$ y se dice que es el* cuerpo residual *del punto x.*

Demostración.

Sabemos que $\mathfrak{p}_x$ es un ideal primo que no es el total. Así $A/\mathfrak{p}_x$ es un anillo íntegro y no nulo. Su cuerpo de fracciones tampoco será nulo. $\square$

Dado un elemento $f \in A$ y un punto x del espectro, consideramos la clase de equivalencia de f módulo $\mathfrak{p}_x$.

$$\begin{array}{rccc} \pi : & A & \longrightarrow & A/\mathfrak{p}_x \\ & f & \longrightarrow & \pi(f) \end{array}$$

Dicha clase de equivalencia se denota $f(x)$ y se dice que es el valor que toma la "función" f en el punto x. Por lo tanto tenemos que $f(x) \in A/\mathfrak{p}_x \subset k(x)$. Con ello vemos que todo elemento de A se puede entender como una función con dominio $\mathrm{Spec}(A)$, pero con el problema de que el conjunto imagen cambia con el punto x.

Ejemplos.

- Dado el anillo de polinomios en una variable $k[t]$, sabemos que el ideal $(t - \alpha)$ es maximal. Entonces es un punto del espectro. El cociente es isomorfo a k de modo natural. Dado un polinomio arbitrario f, aplicando la división euclídea obtenemos

  $$f = c(t - \alpha) + f(\alpha)$$

  La "función" f sobre el primo $(t - \alpha)$ tiene como valor precisamente $f(\alpha)$.

- Sobre $\mathbb{R}[t]$ consideramos el ideal $(t^2 + 1)$. Es primo pues su cociente es el cuerpo complejo. El valor de f aplicado a este primo coincide con $f(i)$. (Hemos realizado la identificación canónica de $\mathbb{C}$ con el cociente $\mathbb{R}[t]/(t^2 + 1)$).

- En $k[t_1, \dots, t_n]$ tenemos el ideal primo $(t - \alpha_1, \dots, t - \alpha_n)$. Sobre este primo una función f tiene el valor $f(\alpha_1, \dots, \alpha_n)$.

Definición 7.2 *Llamamos* puntos *a los elementos de* $\mathrm{Spec}(A)$. *Llamamos* funciones *a los elementos de A. Una función $f \in A$ se anula en un punto x si $f(x) = 0$.*

Ejemplos.

- La función 0 se anula en todos los puntos. La función 1 no se anula en ningún punto. Las funciones invertibles son precisamente aquellas que no se anulan nunca, pues todo elemento no invertible está contenido en un ideal maximal y por lo tanto se anula en dicho maximal.

- Dado $x \in \operatorname{Spec}(A)$, el conjunto de funciones que se anulan en x es precisamente $\mathfrak{p}_x$. En efecto: decir que $f(x) = 0$ equivale a decir que $\pi(f) = 0$, que es otra forma de expresar que $f \in \mathfrak{p}_x$.

- Si dos funciones se anulan en x, su suma y su producto también se anulan en dicho punto. Esto es consecuencia de la estructura de ideal. Si un producto de dos funciones se anula en un punto, alguno de los factores se anula en el punto. Esta propiedad es consecuencia de la integridad de los anillos $A/\mathfrak{p}_x$, o también de la primalidad del ideal.

- Las funciones nilpotentes se anulan en todos los puntos: dado f, existe n tal que $f^n = 0$. Por lo tanto $f^n \in \mathfrak{p}$ para todo ideal primo. Necesariamente $f \in \mathfrak{p}$, debido al carácter primo del ideal.

Si una función se anula en todos los puntos, el elemento está en todos los ideales primos y en la intersección de ellos. Esta función está incluida en el radical del anillo, que es el conjunto de elementos nilpotentes.

Corolario 7.2 *Una función se anula en todos los puntos si y solo si es nilpotente.*

Si A es un anillo y $\mathfrak{r}$ su radical, los ideales primos de A y de $A/\mathfrak{r}$ están en correspondencia biunívoca, pues todo ideal primo de A contiene a $\mathfrak{r}$. Entonces los espectros de A y de $A/\mathfrak{r}$ son canónicamente isomorfos.

Definición 7.3 *Dado un anillo A se llama* anillo reducido *al cociente $A/\mathfrak{r}$.*

Un anillo y su anillo reducido tienen el mismo espectro, pero como el anillo reducido no tiene radical, no existen funciones no nulas que se anulen en todos los puntos.

El espectro de un anillo, además de ser un simple conjunto, puede ser dotado de una estructura de espacio topológico. Vamos a definir la topología dando los cerrados del espacio. La idea que nos guía es la siguiente: si intentamos que todas las funciones $f \in A$ sean continuas, la antiimagen de cualquier cerrado debe ser un cerrado. Como el espacio de llegada no tiene estructura topológica esto es imposible. Sin embargo tomamos una condición más débil que cumplen las funciones continuas valoradas en $\mathbb{R}$: la antiimagen del cero debe ser un cerrado. Como las intersecciones de cerrados deben ser cerradas podemos dar la siguiente

Definición 7.4 *Sea S un subconjunto de A. Los* ceros *de S son los puntos $x \in \operatorname{Spec}(A)$ donde se anulan todas las funciones de S. Se denota $\mathcal{V}(S)$. Tenemos entonces*

$$\mathcal{V}(S) = \{x \in \operatorname{Spec}(A) \text{ tales que } f(x) = 0 \text{ para todo } f \in S\}$$

En particular, cuando S tenga un único elemento lo denotaremos $\mathcal{V}(f)$.

Muchas veces es útil dar la definición con los ideales entendidos como conjuntos y no como puntos. En este caso

$$\mathcal{V}(S) = \{\mathfrak{p}_x \in \operatorname{Spec}(A) \text{ tales que } S \subset \mathfrak{p}_x\}$$

Lema 7.3 *Dado un conjunto S sea I el ideal que genera, $I = \langle S \rangle$. Entonces $\mathcal{V}(S) = \mathcal{V}(I)$.*

Demostración.

Como $S \subset I$ obtenemos que $\mathcal{V}(I) \subset \mathcal{V}(S)$. Todo elemento de I se puede escribir como una combinación lineal de elementos de S. Si $\sum a_i s_i$ es un elemento de I y $x \in \mathcal{V}(S)$ tenemos que $(\sum a_i s_i)(x) = \sum a_i(x) s_i(x)$, aplicando que la proyección canónica es morfismo de anillos. Pero este último resultado es nulo por lo que $x \in \mathcal{V}(I)$. Concluimos que $\mathcal{V}(S) \subset \mathcal{V}(I)$. $\square$

Gracias a este resultado podremos siempre suponer que el subconjuto S es un ideal, lo que nos ahorrará bastante trabajo en las demostraciones.

Corolario 7.4 *Para todo ideal I se tiene que $\mathcal{V}(I) = \mathcal{V}(\mathrm{rad}(I))$.*

Demostración.

La parte clave de la demostración se basa en la identificación del radical de I con la intersección de todos los ideales primos que contienen a I. $\square$

Para calcular los conjuntos $\mathcal{V}(I)$ basta considerar únicamente ideales radicales.

Proposición 7.5 *Se cumple:*

1.- *Si $I \subset J$ entonces $\mathcal{V}(J) \subset \mathcal{V}(I)$.*

2.- $\mathcal{V}(0) = \mathrm{Spec}(A)$ *donde* 0 *denota el ideal nulo.*

3.- $\mathcal{V}(A) = \emptyset$.

4.- $\mathcal{V}(\sum I_j) = \bigcap \mathcal{V}(I_j)$ *para toda familia de ideales.*

5.- $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$

Demostración.

1.- Es evidente.

2.- La función cero se anula en todos los puntos.

3.- La función 1 no se anula nunca.

4.- Si $x \in \bigcap \mathcal{V}(I_j)$ entonces $f_j(x) = 0$ para todo elemento $f_j \in I_j$. Por lo tanto $(\sum f_j)(x) = 0$ y como todo elemento de $\sum I_j$ es de esta forma, $x \in \mathcal{V}(\sum I_j)$.

Sea $I_j \subset \sum I_j$. Entonces $\mathcal{V}(\sum I_j) \subset \mathcal{V}(I_j)$ para todo j. Tenemos entonces que $\mathcal{V}(\sum I_j) \subset \bigcap \mathcal{V}(I_j)$ lo que prueba la inclusión que nos faltaba.

5.- Sabemos que si un ideal primo $\mathfrak{p}$ contiene a $I \cap J$, entonces contiene a uno de los dos ideales. $\square$

Estas propiedades nos permiten dar la siguiente definición:

Definición 7.5 *Llamamos cerrados de* $\operatorname{Spec}(A)$ *a los subconjuntos de la forma* $\mathcal{V}(I)$*, donde* I *es un ideal. Estos cerrados forman la* topología de Zariski*. Los complementarios de los conjuntos* $V(I)$ *se denotan* $D(I)$ *y sus elementos forman los abiertos de la topología.*

Siempre que nos refiramos a la topología del espectro, supondremos que es la de Zariski. Ello no implica que no se pueda dotar al espectro de otras topologías, algunas de ellas también muy útiles en álgebra conmutativa.

Corolario 7.6 *Se cumple la fórmula*

$$\mathcal{V}(I) = \bigcap_{f \in I} \mathcal{V}(f)$$

Este corolario prueba que los conjuntos $\mathcal{V}(f)$ forman una base de cerrados de la topología. Tomando complementarios en el corolario anterior obtenemos

$$D(I) = \bigcup_{f \in I} D(f)$$

Los conjuntos abiertos de la forma $D(f)$ forman una base de abiertos de la topología.

Definición 7.6 *Los abiertos de la forma* $D(f)$ *se llaman* abiertos afines*.*

Estos abiertos afines son muy usados debido a que forman una base de la topología y a que cumplen una serie de propiedades muy sencillas. En términos de ideales la definición de estos abiertos es:

$$D(f) = \{\mathfrak{p} \in \operatorname{Spec}(A) \text{ tales que } f \notin \mathfrak{p}\}$$

Ejemplos.

- Hemos visto que k^n se puede considerar incluido en $\mathrm{Spec}(k[x_1,\ldots,x_n])$. La topología inducida en k^n por la topología de Zariski, dota a k^n de una estructura natural de espacio topológico. Dicha topología coincide con la topología de Zariski que tiene k^n, considerando a k^n como variedad algebraica.

- Dado un conjunto S de polinomios en n variables, definen una variedad algebraica $X \subset k^n$

  $$X = \{x \in k^n \text{ tales que } f(x) = 0 \text{ para todo } f \in S\}$$

  Como vemos $X = \mathcal{V}(S) \cap k^n$, considerando la inyección natural de k^n en el espectro del anillo de polinomios. Toda variedad algebraica hereda entonces una topología.

- Consideremos el espectro de $\mathbb{Z}$. Dado un número primo p, el único primo que contiene a dicho número es el mismo. Tenemos que $\mathcal{V}(p) = p$. Luego cada punto del espectro de $\mathbb{Z}$ es un cerrado. Las uniones finitas de cerrados son cerrados. Veamos que esta construcción nos da todos los cerrados. Si I es un ideal de $\mathbb{Z}$ entonces $I = (n)$ para cierto entero:

  $$\mathcal{V}(I) = \mathcal{V}(n) = \{p \in \mathrm{Spec}(\mathbb{Z}) \text{ tales que } (n) \subset (p)\}$$

  Pero esto equivale a n sea un múltiplo de p. Dicho en otras palabras $p \in \mathcal{V}(n)$ si y solo si p "entra" en la descomposción en factores primos de n. Concluimos que si $n = p_1^{a_1} \cdots p_j^{a_j}$ entonces $\mathcal{V}(n) = \{p_1, \ldots, p_j\}$.

- Si k es un cuerpo algebraicamente cerrado, el estudio realizado para $\mathbb{Z}$ se traslada sin modificaciones para el estudio del espectro de $k[t]$.

Proposición 7.7 *El cierre de un punto $x \in \mathrm{Spec}(A)$ es precisamente $\mathcal{V}(\mathfrak{p}_x)$.*

Demostración.

Un cerrado $\mathcal{V}(I)$ contiene a x si $x \in \mathcal{V}(I)$. Esto es equivalente a que $I \subset \mathfrak{p}_x$. Tomando ceros en esta expresión obtenemos que $\mathcal{V}(\mathfrak{p}_x) \subset \mathcal{V}(I)$ y $\mathcal{V}(\mathfrak{p}_x)$ está contenido en todos los cerrados que contienen a x. Es el menor cerrado que contiene a x, que es el cierre de ese conjunto. $\square$

Corolario 7.8 *Un punto es cerrado si su ideal asociado es maximal.*

Demostración.

Si $\mathfrak{p}_x$ es maximal el conjunto $\mathcal{V}(\mathfrak{p}_x)$ tiene solo un punto, que es precisamente x. El cierre del punto x coincide con x. Es cerrado. $\square$

Ejemplos.

- En un anillo de ideales principales, todo ideal primo no nulo es maximal. Todos los puntos del espectro, salvo el correspondiente al punto cero, son puntos cerrados.
- En un anillo íntegro el cero es un ideal primo. Su cierre es entonces todo el espectro. Esto es otra forma de decir que el conjunto formado por el punto cero es denso. Los puntos densos también se denominan puntos genéricos, de ahí la notación empleada para los puntos genéricos en los anillos de polinomios.
- Si el radical $\mathfrak{r}$ es un ideal primo entonces $\mathcal{V}(\mathfrak{r})$ es el espacio total. Su cierre es todo el espacio. Es un punto genérico. Si el radical no es primo no puede tener punto genérico.
- La inclusión de k^n en el espectro del anillo de polinomios, hace corresponder a cada elemento de k^n un ideal maximal. Los puntos de k^n son puntos cerrados. El teorema de los ceros de Hilbert afirma que, si el cuerpo es algebraicamente cerrado, entonces todos puntos cerrados del espectro (maximales del anillo) son puntos de k^n. Un resultado similar se cumple para cualquier variedad afín: si X es una variedad afín y $A(X)$ es su anillo coordenado, los puntos cerrados de $\mathrm{Spec}(A(X))$ se identifican con los puntos de X. Ya hemos visto que los puntos puntos

no cerrados del espectro se identifican con las subvariedades irreducibles de X.

Teorema 7.9 *El espectro es un espacio topólogico compacto.*

Demostración.

Sea $\mathcal{V}(I_j)$ una familia de cerrados de intersección vacía. En virtud de la proposición 7.5

$$\bigcap \mathcal{V}(I_j) = \emptyset = \mathcal{V}(\sum I_j)$$

Entonces $\sum I_j = A$ puesto que A es el único ideal que no está contenido en ningún ideal primo.

Como $1 \in A$ y $A = \sum I_j$, existe un número finito de funciones tales que

$$f_1 + \cdots + f_n = 1$$

Si $f_i \in I_{j_i}$ la misma proposición nos asegura que

$$\mathcal{V}(I_{j_1}) \cap \cdots \cap \mathcal{V}(I_{j_n}) = \mathcal{V}(I_{j_1} + \cdots + I_{j_n}) = \emptyset$$

y una subfamilia finita de cerrados tiene intersección vacía. Esto demuestra que el espectro es compacto. $\square$

Observación. En muchas referencias esta propiedad que hemos demostrado se llama cuasicompacidad puesto que para la compacidad muchos autores exigen que el espacio en cuestión sea Haussdorf. $\square$

En la demostración de la compacidad del espectro hemos utilizado de modo esencial la existencia de la unidad. Para demostrar el mismo resultado para otros conjuntos debemos suponer que el anillo es noetheriano.

Lema 7.10 *Si $I = (f_1, \dots f_j)$ entonces $D(I) = D(f_1) \cup \cdots \cup D(f_j)$. En particular, si el anillo es noetheriano, todo abierto es unión finita de abiertos de la base.*

Demostración.

Si $I = (f_1, \dots, f_j)$ entonces sus variedades cumplen

$$\mathcal{V}(I) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_j)$$

Tomando complementarios se concluye. $\square$

Corolario 7.11 *Todo abierto del espectro de un anillo noetheriano es compacto.*

Demostración.

Podemos suponer que el recubrimiento se realiza con abiertos básicos. El lema anterior nos informa de la finitud de dicho recubrimiento. $\square$

Hemos asociado a cada ideal I de A un conjunto del espectro, $\mathcal{V}(I)$. De manera recíproca, se puede asociar a cada subconjunto del espectro un ideal. Es el ideal formado por todas las funciones que se anulan en dicho conjunto. Si $X \subset \operatorname{Spec}(A)$ denotaremos por $\mathfrak{I}(X)$ a dicho ideal:

$$\mathfrak{I}(X) = \{f \in A \text{ tales que } f(x) = 0 \text{ para todo } x \in X\}$$

Una manera equivalente de formular este concepto es decir que f pertenece a todos los primos del conjunto X. Tenemos entonces que

$$\mathfrak{I}(X) = \bigcap_{\mathfrak{p} \in X} \mathfrak{p}$$

que claramente es un ideal, por ser intersección de ideales. Este ideal no es arbitrario, pues por ser intersección de ideales primos, es un ideal radical y por lo tanto cumple siempre $\mathfrak{I}(X) = \operatorname{rad}(\mathfrak{I}(X))$. Podemos considerar que $\mathfrak{I}$ es una función que transforma subconjuntos del espectro en ideales radicales del anillo:

$$\mathfrak{I} : \text{Subconjuntos}(\operatorname{Spec}(A)) \longrightarrow \text{Ideales radicales de } A$$

Las propiedades más relevantes de esta aplicación se resumen en la

Proposición 7.12 *La aplicación $\mathfrak{I}$ cumple las propiedades:*

1. $\mathfrak{I}(\varnothing) = A$.

2. $\mathfrak{I}(\mathrm{Spec}(A)) = \mathrm{rad}(A)$.

3. *Si* $X \subset X'$ *entonces* $\mathfrak{I}(X') \subset \mathfrak{I}(X)$.

4. $\mathfrak{I}(\mathcal{V}(I)) = \mathrm{rad}(I)$. *En particular si el ideal* I *es radical* $\mathfrak{I}(\mathcal{V}(I)) = I$. *Este resultado es el análogo del teorema de los ceros de Hilbert.*

5. $\mathcal{V}(\mathfrak{I}(X)) =$ *cierre topológico del conjunto* X, *que denotamos* $\overline{X}$.

Demostración.

Las tres primeras propiedades se deducen directamente de la definición.

4.- Se prueba fácilmente que para todo ideal I se cumple

$$I \subset \mathfrak{I}(\mathcal{V}(I))$$

Como el segundo ideal es radical, el radical de I debe estar también contenido:

$$\mathrm{rad}(I) \subset \mathfrak{I}(\mathcal{V}(I))$$

Recíprocamente, si $f \in \mathfrak{I}(\mathcal{V}(I))$ tenemos que

$$f \in \bigcap_{x \in \mathcal{V}(I)} \mathfrak{p}_x$$

Pero la parte de la derecha es la intersección de todos los primos que contienen al ideal I. Es un resultado bien conocido que dicha intersección coincide con el radical de I, produciendose la inclusión contraria. El análogo del teorema de los ceros de Hilbert es casi evidente a nivel de espectros.

5.- Claramente $X \subset \mathcal{V}(\mathfrak{I}(X))$, que es un cerrado y contiene entonces al cierre de X. La inclusión $\overline{X} \subset \mathcal{V}(\mathfrak{I}(X))$ está probada.

Sea ahora $\mathcal{V}(I)$ un cerrado que contenga X. Tenemos que $I \subset \mathfrak{p}$ para todo primo del conjunto X. De esta forma I está contenido en la interseccción de todos los primos de X, que no es otra cosa que $\mathfrak{I}(X)$. Como $X \subset \mathfrak{I}(X)$, tomamos ceros en esta ecuación y obtenemos

$$\mathcal{V}(\mathfrak{I}(X)) \subset \mathcal{V}(I)$$

de tal forma que $\mathcal{V}(\mathfrak{I}(X))$ está contenido en todo cerrado que contiene a X. Esto demuestra que precisamente es el cierre del conjunto X. $\square$

Corolario 7.13 *La aplicación $\mathfrak{I}$ establece una correspondencia biunívoca, que invierte el orden, entre los subconjuntos cerrados de* $\operatorname{Spec}(A)$ *y los ideales radicales de A (su inversa es la aplicación $\mathcal{V}$). En particular, si A es noetheriano, el espacio topológico* $\operatorname{Spec}(A)$ *también lo es.*

Observación. El recíproco del corolario anterior no es cierto en general. El espectro puede ser un espacio topológico noetheriano sin ser noetheriano el anillo. $\square$

Si posee un espacio tiene un punto genérico, cualquier cerrado que contenga a dicho punto debe ser el total. El espacio es entonces irreducible. En el caso de los espectro la reducibilidad o irreducibilidad es una mera cuestión algebraica.

Proposición 7.14 *El espacio topológico* $\operatorname{Spec}(A)$ *es reducible si y solo si el nilradical no es un ideal primo, lo que equivale a decir que no tiene punto genérico.*

Demostración.

Si el radical no es primo, existen f y g tales que $fg \in \mathfrak{r}$ y ni f ni g son nilpotentes. En este caso

$$\operatorname{Spec}(A) = \mathcal{V}(f) \cup \mathcal{V}(g)$$

y los cerrados $\mathcal{V}(f)$ y $\mathcal{V}(g)$ son propios. $\square$

Dado un morfismo de anillos

$$\varphi : A \longrightarrow B$$

y un ideal primo $\mathfrak{p}$ de B, sabemos que $\varphi^{-1}(\mathfrak{p})$ es un ideal primo de A. Esto nos permite definir una aplicación

$$\begin{array}{rccc} \varphi^* : & \mathrm{Spec}(B) & \longrightarrow & \mathrm{Spec}(A) \\ & \mathfrak{p} & \longrightarrow & \varphi^{-1}(\mathfrak{p}) \end{array}$$

Si ϕ es otro morfismo, $(\varphi\phi)^* = \phi^*\varphi^*$ lo que pone de manifiesto que esta construcción es un functor contravariante.

Teorema 7.15 *φ^* es una aplicación continua.*

Demostración.

Sea $C = \mathcal{V}(I)$ un cerrado de $\mathrm{Spec}(A)$. Veamos que $(\varphi^*)^{-1}$ es cerrado

$$(\varphi^*)^{-1}(I) = \{x \in \mathrm{Spec}(B) \text{ tales que } I \subset \varphi^{-1}(\mathfrak{p}_x)\}$$

Aplicando el morfismo φ tenemos que este conjunto coincide con

$$\{x \in \mathrm{Spec}(B) \text{ tales que } \varphi(I) \subset \mathfrak{p}_x\} = \mathcal{V}(\varphi(I))$$

que es un cerrado de $\mathrm{Spec}(B)$. $\square$

Veamos ahora como se comporta el espectro al realizar cocientes y productos de anillos

Corolario 7.16 *Si I es un ideal de A y $\pi : A \longrightarrow A/I$ la proyección canónica*

$$\pi^* : \mathrm{Spec}(A/I) \longrightarrow \mathrm{Spec}(A)$$

establece un homeomorfismo de $\mathrm{Spec}(A/I)$ con el cerrado $\mathcal{V}(I)$. Cualquier cerrado de un espectro es a su vez el espectro de un anillo.

Demostración.

Aplicando el teorema de correspondencia, los ideales primos de A/I se identifican con los ideales primos de A que contienen a I. Pero este conjunto es precisamente $\mathcal{V}(I)$. La continuidad de la aplicación inversa es una simple comprobación. $\square$

Lema 7.17 *Dado un producto de anillos $A_1 \times A_2$, los ideales de este anillo son de la forma $I_1 \times I_2$ donde $I_i \subset A_i$ es un ideal.*

Demostración.

Sea $I \subset A_i \times A_2$. Denotemos por I_i la proyección de I en el i-ésimo factor. I_i es un ideal puesto que la proyección canónica es epiyectiva.

Dado un elemento (a_1, a_2), tenemos que tanto $(a_1, 0)$ como $(0, a_2)$ son múltiplos de dicho elemento. Por lo tanto $(a_1, a_2) \in I$ si y solo $a_1 \in I_1$ y $a_2 \in I_2$, lo que prueba que $I = I_1 \times I_2$. $\square$

Corolario 7.18 *Los ideales primos de $A_1 \times A_2$ son de la forma $\mathfrak{p}_1 \times A_2$ o de la forma $A_1 \times \mathfrak{p}_2$ donde $\mathfrak{p}_i \subset A_i$ es primo.*

Demostración.

Si hacemos el cociente de $A_1 \times A_2$ módulo el ideal $I_1 \times I_2$ obtenemos

$$(A_1 \times A_2)/(I_1 \times I_2) = A_1/I_1 \times A_2/I_2$$

Para que este producto sea íntegro debe ocurrir que un factor sea nulo y el otro factor sea íntegro. Pero esto equivale a decir que un ideal es el total y el otro un ideal primo. $\square$

Teorema 7.19 *El espectro del producto $A_1 \times A_2$ es la unión disjunta de los espectros de los anillos A_1 y A_2.*

Demostración.

Los resultados anteriores prueban que como conjuntos

$$\mathrm{Spec}(A_1 \times A_2) = \mathrm{Spec}(A_1) \oplus \mathrm{Spec}(A_2)$$

(La suma directa en la categoría de espacios topológicos es la unión disjunta)

Sea $\pi_i : A_1 \times A_2 \longrightarrow A_i$ la proyección canónica. Tenemos entonces que

$$\pi_1{}^* : \mathrm{Spec}(A_1) \longrightarrow \mathrm{Spec}(A_1 \times A_2)$$

es un homeomorfismo con su imagen, lo que prueba que la igualdad también es cierta como espacios topológicos. $\square$

Proposición 7.20 *El espectro de un localizado A_S se identifica con el conjunto de primos de A que tienen intersección vacía con S.*

Demostración.

Sea la aplicación $\varphi : A \to A_S$ de localización. Si la antiimagen de un primo del localizado tiene intersección con S, entonces su imagen contrendría un elemento inversible. El ideal primo es en este caso el total. La igualdad de las topologías es una simple comprobación. $\square$

El espectro de A_f se identifica con los ideales primos de A que no contienen al elemento f. Pero este último conjunto es justamente $D(f)$. Se tiene la siguiente identificación canónica

$$\mathrm{Spec}(A_f) = D(f)$$

Los abiertos básicos del espectro son a su vez espectros de anillos localizados.

8. Extensiones enteras

Definición 8.1 *Sea B un anillo y $A \subset B$ un subanillo con unidad. Un elemento $b \in B$ es* entero *sobre A si existe un polinomio unitario*[3]*, con coeficientes en A, que anula a dicho elemento.*

Si el polinomio es

$$p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

entonces b cumple la ecuación polinomial

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

El elemento b es entonces una raiz de un polinomio cuyo término de mayor grado es uno.

Observación.

En general en teoría de anillos se denomina extensión de un anillo A a todo morfismo de anillos con unidad $\varphi : A \to B$. La imagen de A mediante φ es un subanillo de B. En esta situación diremos que un elemento de B es entero sobre A, si entero sobre el subanillo imagen $\varphi(A)$.

Proposición 8.1 *Sea B una extensión entera de un anillo A. El subanillo $A(b) \subset B$, generado por el anillo A y el elemento b, es un módulo de generación finita sobre el anillo A.*

Demostración.

Tenemos que

$$b^n = -(a_0 + a_1 b + \cdots + a_{n-1}b^{n-1})$$

y en general

$$b^{n+r} = -(a_0 b^r + a_1 b^{r+1} + \cdots + a_{n-1}b^{n+r-1})$$

[3]Decimos que un polinomio es unitario si el coeficiente de mayor grado es 1. También se dice que el polinomio es mónico.

por lo que los elementos $1, b, \ldots, b^{n-1}$ generan dicho módulo. $\square$

Proposición 8.2 *Sea $A \subset B$ un subanillo. Si $b \in B$ es entero sobre A, entonces el morfismo $\varphi : A(x) \to B$ que transforma x en b no es inyectivo.*

Demostración.

Si b es entero sobre A, existe un polinomio $p \in A(x)$ que anula al elemento b. Pero como $\varphi(p) = p(b)$ dicho elemento está en el núcleo de φ, que no puede entonces ser inyectivo. $\square$

Ejemplos.

- Todo elemento de A es entero sobre A puesto que $x - a$ anula a dicho elemento.

- El número real $\sqrt[3]{2}$ es entero sobre $\mathbb{Z}$. Un polinomio que lo anula es precisamente $x^3 - 2$.

- El número complejo i es entero sobre $\mathbb{Z}$. Es fácil encontrar un polinomio que lo anule. En general, todo elemento de la forma $a + bi$ con a y b enteros, es entero sobre $\mathbb{Z}$.

- Consideramos el número real $1/\sqrt{2}$. Un polinomio que anula a dicho elemento es $2x^2 - 1$. Sin embargo dicho elemento no es entero sobre $\mathbb{Z}$, pues no existe ningún polinomio unitario que lo anule.

- Si un número racional es entero sobre $\mathbb{Z}$ entonces necesariamente es un elemento de $\mathbb{Z}$. Demostremos este hecho.

  Sea r/s la fracción irreducible del número racional. Entonces dicho número cumple una ecuación del tipo

  $$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

  Multiplicamos por s^n para quitar denominadores

  $$r^n + a_{n-1}sr^{n-1} + \cdots + a_1rs^{n-1} + a_0s^n = 0$$

Sacando factor común s deducimos

$$r^n = s(-a_{n-1}r^{n-1} - \cdots - a_1 r s^{n-2} - a_0 s^{n-1})$$

Entonces s divide a r^n y por lo tanto divide a r. Como la fracción es irreducible, necesariamente $s = \pm 1$ y el número es entero.

- En el caso de los cuerpos, el estudio de la dependencia entera se simplifica utilizando conceptos elementales de la teoría de espacios vectoriales. Veamos un ejemplo.

  Sea k un cuerpo, $k \subset B$ y B un anillo que como espacio vectorial sea de dimensión finita n sobre el cuerpo k. Los elementos $1, b, \dots, b^n$ no pueden ser linealmente independientes. Luego existe una combinación lineal no nula

  $$a_0 1 + a_1 b + \cdots + a_n b^n = 0$$

  Construimos de este modo un polinomio, de grado menor o igual a n que anula al elemento b. Pero en principio este polinomio no es unitario. Si i es el grado del polinomio, entonces podemos dividir entre a_i y obtenemos un polinomio cuyo término de mayor grado es uno. Como conclusión, tenemos que si B es de dimensión finita sobre k, entonces todo elemento de B es entero sobre k.

Llamamos extensión de un anillo A a cualquier anillo B que lo contenga. Estamos especialmente interesados en aquellos anillos B tales que todos sus elementos sean enteros sobre A.

Definición 8.2 *Una extensión $A \subset B$ es* entera *si todo elemento de B es entero sobre A. En el caso de que A sea un cuerpo, las extensiones enteras se denominan extensiones* algebraicas.

Ejemplos.

- El cuerpo $\mathbb{C}$ es una extensión entera de $\mathbb{R}$. En general toda extensión $k \subset B$ de un cuerpo, que sea de dimensión finita, es una extensión entera. El recíproco sin embargo no es cierto. Existen extensiones de dimensión infinita que son enteras.

- $\mathbb{Z} \subset \mathbb{Z}(i)$ es una extensión entera.
- $\mathbb{Z} \subset \mathbb{Q}$ no es entera, puesto que existen elementos en Q que no son enteros sobre $\mathbb{Z}$.
- $\mathbb{R}$ tampoco es entero sobre $\mathbb{Q}$. En general, los números reales (o complejos) que son enteros sobre $\mathbb{Q}$ se denominan **números algebraicos** . Aquellos que no son enteros se denominan **transcendentes**.

  Es un ejercicio fácil demostrar que el conjunto de números algebraicos es numerable. Esto implica la existencia de números transcendentes. Sin embargo encontrar ejemplos explícitos de números transcendentes no es tarea fácil. Se sabe, no obstante, que e y π son números transcendentes.

Hemos dado una definición de elemento entero sobre A. Daremos ahora un criterio, o definición equivalente, que nos será útil en multitud de cálculos.

Proposición 8.3 *Sea $A \subset B$ una extensión. Son equivalentes las siguientes condiciones:*

i) *El elemento b es entero sobre A.*

ii) *El módulo $A(b)$ es de generación finita sobre el anillo A.*

iii) *El elemento b está incluido en un anillo C que es un A-módulo de generación finita.*

Demostración.

La implicación $i) \Rightarrow ii)$ es justamente la proposición 8.1. Para la implicación $ii) \Rightarrow iii)$ basta tomar $C = A(b)$. Veamos entonces la implicación $iii) \Rightarrow i)$.

Sea C un módulo de generación finita que contenga al elemento b. Denotaremos por $(m_1, m_2 \dots, m_n)$ un conjunto de generadores de C como A-módulo. Tenemos que bm_i es un elemento de C y por lo tanto se puede escribir, en principio de forma no única, como una combinación lineal de elementos del conjunto generador.

$$bm_i = a_{i1}m_1 + \cdots + a_{in}m_n$$

Esto nos da un sistema de n ecuaciones con n incognitas. Los elementos a_{ij} forman una matriz cuadrada, donde los coeficientes pertenecen al anillo A.

Pasamos los elementos bm_i al otro miembro y obtenemos un sistema equivalente y homogéneo. La matriz de este sistema es precisamente $(a_{ij} - b\delta_{ij})$. Calculamos el determinante de esta matriz. Dicho determinante es un elemento de B que tiene la forma de un polinomio unitario[4] en B. Si denotamos por Δ a dicho determinante, tenemos que $\Delta m_i = 0$ para todo generador del módulo. Como el anillo tiene unidad, en particular el 1 es combinación de elementos m_i y obtenemos que $\Delta 1 = 0$. Necesariamente $\Delta = 0$ y hemos obtenido un polinomio unitario que anula a b. $\square$

Corolario 8.4 *Sea $A \subset B$ una extensión. Si B es de generación finita como A-módulo, entonces B es una extensión entera de A.*

Observación.

Si $A = k$ es un cuerpo, los anillos finito generados son precisamente aquellos que tienen dimensión finita y este resultado ya nos era conocido.

Lema 8.5 *Sea $A \subset B \subset C$ una cadena de anillos. Si B es de generación finita como A-módulo y C es de generación finita como B-módulo, entonces C es también de generación finita como A módulo.*

Demostración.

Sea $(c_1, \ldots, c_n)$ un conjunto generador de C como B módulo. Denotamos por $(b_1, \ldots, b_m)$ un conjunto generador de B como A-módulo.

Dado un elemento arbitrario $c \in C$, tenemos que

$$c = \beta_1 c_1 + \cdots + \beta_n c_n \text{ donde los } \beta_i \in B$$

[4] El término de mayor grado puede ser $\pm b^n$ dependiendo de si n es par o impar

Cada β_i se puede expresar como una combinación lineal finita de los elementos b_i

$$\beta_i = a_{i1}b_1 + \cdots + a_{im}b_m \text{ con } a_{ij} \in A$$

Sustituyendo esto en la anterior expresión de c, obtenemos que los elementos $b_ic_j, i = 1, \ldots, m, j = 1, \ldots, n$ generan C como A-módulo. □

Corolario 8.6 *Sea $A \subset B$ una extensión. Si los elementos $b_1, \ldots, b_n$ son enteros sobre A, entonces el anillo $A(b_1, \ldots, b_n)$ es de generación finita.*

Demostración.

Consideramos la cadena de anillos

$$A \subset A(b_1) \subset A(b_1, b_2) \subset \cdots \subset A(b_1, \ldots, b_n)$$

Cada extensión es de generación finita, pues si un elemento b_i es entero sobre A, también es entero sobre $A(b_1, \ldots, b_{i-1})$. Aplicando inducción y el lema anterior concluimos. □

Corolario 8.7 *Sea $A \subset B$ una extensión. Si b_1 y b_2 son enteros sobre A, entonces $b_1 + b_2$ y b_1b_2 son enteros sobre A.*

Demostración.

Si b_1 y b_2 son enteros, entonces $A(b_1, b_2)$ es de generación finita y todos sus elementos son enteros sobre A. En particular $b_1 + b_2$ y b_1b_2 , que son elementos de dicho anillo, son enteros sobre A. □

Del corolario anterior se deduce que el conjunto de todos los elementos enteros de una extensión es un subanillo de B.

Definición 8.3 *Sea $A \subset B$ una extensión. Denotamos por $\widetilde{A}$ al conjunto de los elementos de B que son enteros sobre A. El conjunto $\widetilde{A}$ se denomina* clausura íntegra *del anillo A en B.*

Como ya hemos anunciado, $\widetilde{A}$ es un subanilo de B. Si en una extensión tenemos que $\widetilde{A} = A$, decimos que A es integramente cerrado en B. Como ya sabemos, si $\widetilde{A} = B$ decimos que B es entero sobre A.

En el caso de un dominio de integridad, si decimos que es íntegramente cerrado estaremos suponiendo que dicho anillo es íntegramente cerrado en la extensión dada por su cuerpo de fracciones.

En el caso de los cuerpos la cosa queda más o menos así. En un cuerpo no se diferencian los polinomios unitarios y no unitarios, pues si nos dan un polinomio no unitario, simplemente lo dividimos entre el coeficiente de mayor grado y obtenemos un polinomio unitario. Los elementos algebraicos sobre un cuerpo k son los elementos de un cuerpo K que son raices de los polinomios con coeficientes en k. Si todos los polinomios en k tienen al menos una raiz en el cuerpo base, por inducción vemos que tienen tantas como su grado también en el cuerpo raiz. De este modo, si todo polinomio tiene una raiz en el cuerpo base, no pueden existir extensiones algebraicas (enteras) del cuerpo. Los cuerpos que no admiten extensiones algebraicas se denominan algebraicamente cerrados.

Corolario 8.8 *Sea $A \subset B \subset C$. Si B es entero sobre A y C es entero sobre B, entonces C es entero sobre A.*

Demostración.

Sea $c \in C$. Entonces c cumple una ecuación polinomial

$$c^n + b_{n-1}c_{n-1} + \cdots + b_1 c + b_0 = 0 \text{ con } b_i \in B$$

El anillo $A(b_0, b_1, , \ldots, b_{n-1}, c)$ es de generación finita sobre A, puesto que c es entero sobre el anillo $A(b_0, b_1, \ldots, b_{n-1})$ y este último anillo es de generación finita pues todos los elementos de B son enteros. De este modo concluimos que c es entero sobre A. $\square$

Corolario 8.9 *Sea $A \subset B$ una extensión y $\widetilde{A}$ la clausura entera de A en B. Entonces $\widetilde{A}$ es integramente cerrado en B.*

Demostración.

Consideramos la cadena $A \subset \widetilde{A} \subset B$. Si $b \in B$ es entero sobre $\widetilde{A}$, entonces también es entero sobre A. De este modo $b \in \widetilde{A}$ y $\widetilde{A}$ es integramente cerrado en B. $\square$

Ejemplos.

- $\mathbb{Z}$ es íntegramente cerrado en $\mathbb{Q}$. Sin embargo este mismo anillo no es íntegramente cerrado cuando consideramos a $\mathbb{Z}$ incluido en $\mathbb{R}$ o en $\mathbb{C}$. Por lo tanto al hablar de íntegramente cerrado debemos conocer con precisión la extensión a la que nos referimos.

- Dada la extensión $\mathbb{Z} \subset \mathbb{Q}(i)$, su clausura íntegra coincide con los enteros de Gauss.

- Hemos visto que $\mathbb{Q}$ no es íntegramente cerrado en $\mathbb{C}$, pues existen números transcendentes. De este modo existe un anillo $\widetilde{\mathbb{Q}}$ que contiene estrictamente a $\mathbb{Q}$ y contenido en $\mathbb{C}$. Este anillo (que posteriormente veremos que es un cuerpo) no puede ser de dimensión finita sobre $\mathbb{Q}$, puesto que en los racionales existen polinomios irreducibles de grado arbitrariamente grande (considerensen los polinomios de la forma $x^n - 2$). Sea a un elemento de la clausura algebraica y tal que el polinomio irreducible que lo anula sea de grado n. Entonces el anillo $\mathbb{Q}(a)$ es de dimensión n y debe estar contenido en $\widetilde{\mathbb{Q}}$.

- La demostración dada para $\mathbb{Z}$ de su integridad es válida para todo anillo factorial, donde todo elemento se puede escribir de modo único, salvo unidades, como producto de irreducibles.

Veamos ahora el comportamiento de las extensiones enteras bajo la operaciones de localización y toma de cocientes.

Proposición 8.10 *Sea $A \subset B$ una extensión entera de anillos. Dado un ideal I de B, seguimos denotando por I al ideal $I \cap A$ del anillo A. En estas condiciones tenemos una extensión $A/I \hookrightarrow B/I$ que es entera.*

Demostración.

Consideramos el morfismo natural de A en B/I resultado de la composición de la inclusión canónica y del paso al cociente. Resulta que el ideal I de A está contenido en el núcleo de dicho morfismo y por el teorema de factorización canónica se induce una aplicación i_* que hace conmutativo el siguiente diagrama.

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[d, "\pi"'] & B \arrow[d, "\pi"] \\ A/I \arrow[r, "i_*"] & B/I \end{tikzcd}$$

La aplicación i_* es inyectiva y consideraremos a A/I incluido en B/I via esta aplicación. Hemos visto entonces que es una extensión.

Sea $\pi(b)$ un elemento del cociente B/I. El elemento b es entero sobre A. Entonces cumple una ecuación polinomial con coeficientes de A

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

Tomando clases módulo I en esta ecuación obtenemos una ecuación polinomial unitaria para el elemento $\pi(b)$

$$\pi(b)^n + \pi(a_{n-1})\pi(b)^{n-1} + \cdots + \pi(a_1)\pi(b) + \pi(a_0) = 0$$

Luego el elemento $\pi(b)$ es entero sobre A/I. $\square$

Proposición 8.11 *Sea $A \subset B$ una extensión entera y $S \subset A$ un subconjunto multiplicativo. Entonces $A_S \subset B_S$ es una extensión entera.*

Demostración.

Podemos inyectar A_S en B_S haciendo corresponder al elemento a/s de A_S el mismo elemento de B_S. Esta correspondencia es claramente inyectiva.

Sea b/s un elemento de B_S. Como b es entero sobre A. Se cumple

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

Multiplicando esta expresión por el inverso de s^n obtenemos

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_1}{s^{n-1}}\right) + \frac{a_n}{s^n} = 0$$

Todo elemento de B_S es solución de una ecuación polinomial unitaria con coeficientes en A_S. $\square$

Proposición 8.12 *Sea $A \subset B$ una extensión y $S \subset A$ un conjunto multiplicativo. La clausura algebraica de A_S en B_S es precisamente $(\widetilde{A})_S$ (anillo de fracciones de la clausura algebraica).*

Demostración.

Debemos demostrar que $(\widetilde{A})_S = \widetilde{A_S}$. Para ello probaremos que cada conjunto es subconjunto del otro.

Como $\widetilde{A}$ es entero sobre A, tenemos que $(\widetilde{A})_S$ es entero sobre A_S. Esto demuestra que $(\widetilde{A})_S \subset \widetilde{A_S}$

Tomamos ahora un elemento b/s de B_S que sea entero sobre A_S. Entonces dicho elemento cumple una ecuación polinomial

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s_1}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_1}{s_{n-1}}\right) + \frac{a_n}{s_n} = 0$$

Denotemos por t al producto de todos los denominadores. Multiplicamos esta ecuación por $(st)^n$ y conseguimos quitar denominadores. Nos queda una ecuación polinomial para el elemento bt donde los coeficientes pertenecen al anillo A. De este modo bt está en $\widetilde{A}$. Pero $b/s = bt/st$ que está contenido en la clausura algebraica. Hemos probado la otra inclusión $\square$

Corolario 8.13 *Si A es integramente cerrado en B, entonces A_S es integramente cerrado en B_S.*

Haremos ahora un estudio de la correspondencia que existe entre el retículo de ideales de una extensión entera B y el retículo de ideales del anillo A.

Principalmente estudiaremos ideales primos, por lo que será interesante recordar los siguientes hechos, que utilizaremos continuamente.

- El espectro de A/I se identifica con los puntos del espectro de A que contienen al ideal I.
- El espectro del localizado A_S lo podemos entender como el conjunto de ideales primos de A que tienen intersección vacía con el conjunto S.

Definición 8.4 *Sea $A \subset B$ una extensión. Decimos que un ideal $J \subset B$ está situado sobre un ideal $I \subset A$ si $J \cap A = I$*

En particular estaremos interesados en este concepto cuando ambos ideales sean primos. Resulta que un ideal primo $\mathfrak{q} \subset B$ está sobre un ideal primo $\mathfrak{p} \subset A$ si $i^*(\mathfrak{q}) = \mathfrak{p}$, donde i denota la inyección canónica de A en B.

Visualicemos este hecho. Consideramos la inclusión

$$\begin{tikzcd} B \\ A \arrow[u, "i"] \end{tikzcd}$$

Pasando a los espectros obtenemos una aplicación

$$\begin{tikzcd} \operatorname{Spec}(B) \arrow[d, "i^*"] \\ \operatorname{Spec}(A) \end{tikzcd}$$

entre los espectros. Un ideal $\mathfrak{q}$ está sobre $\mathfrak{p}$ si al proyectarlo mediante i^* obtenemos el ideal $\mathfrak{p}$.

Este concepto se puede entonces generalizar a cualquier morfismo de anillos $\varphi : A \to B$, no necesariamente inyectivo.

Un problema fundamental de la teoría es conocer cuando la aplicación entre los espectros es epiyectiva. Naturalmente en multitud de casos la aplicación no puede ser epiyectiva.

Ejemplos.

- Consideramos la extensión $\mathbb{Z} \subset \mathbb{R}$. El espectro de $\mathbb{R}$ consta de un solo punto y el de $\mathbb{Z}$ de infinitos. Es imposible que la aplicación sea epiyectiva.

- $\mathbb{R}(x) \subset \mathbb{C}(x)$. El espectro de $\mathbb{C}(x)$ es el conjunto de los polinomios de la forma $(x-a)$ con $a \in \mathbb{C}$. Los primos de $\mathbb{R}(x)$ son de dos tipos: $(x-a)$ con $a \in \mathbb{R}$ y $(x-a)(x-\overline{a})$ con $a \in \mathbb{C}$. La aplicación entre espectros en este caso es epiyectiva.

- Sea $\varphi : A \to A_S$ el morfismo canónico en el localizado. Sabemos que el espectro de A_S está formado por los ideales primos de A que no cortan a S. Dado un conjunto S arbitrario, la aplicación entre espectros no será epiyectiva.

- Sea $\pi : A \to A/I$ la proyección canónica. El espectro de A/I se identifica con los puntos del espectro de A que contienen al ideal I. Al hacer cociente perdemos puntos del espectro, por lo que en general, la aplicación no será epiyectiva.

En el caso caso de las extensiones enteras la aplicación si es epiyectiva. Esto es lo que afirma el teorema de Cohen-Seidenberg, llamado también teorema del ascenso.

Proposición 8.14 *Sea $A \subset B$ una extensión entera, donde B es un dominio de integridad. Entonces A es cuerpo si y solo si lo es B.*

Demostración.

Supongamos que A es cuerpo. Tenemos que ver que todo elemento de B es invertible.

Sea $b \in B$ no nulo. Como b es entero, cumple una ecuación polinomial unitaria

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

Podemos suponer que a_0 es no nulo, pues en caso de que no lo fuera podemos sacar factor común a b y obtener un polinomio unitario con el término independiente no nulo. Como B es íntegro, este nuevo polinomio tiene que anular al elemento b.

Ahora que tenemos el término independiente no nulo, sacamos factor común a b en la expresión anterior.

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0$$

Multiplicando por $-a_0^{-1}$ vemos que b es invertible y que su inverso es precisamente

$$-a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)$$

Supongamos ahora que B es cuerpo y sea $\alpha \in A$ un elemento no nulo. Naturalmente existe α^{-1}, pero está contenido en B. Debemos demostrar que también está en A.

Como $\alpha^{-1} \in B$, es íntegro y satisface una ecuación polinomial.

$$(\alpha^{-1})^n + a_{n-1}(\alpha^{-1})^{n-1} + \cdots + a_1(\alpha^{-1}) + a_0 = 0$$

Multiplicamos esta ecuación por α^{n-1} y obtenemos

$$\alpha^{-1} = -(a_{n-1} + \cdots + a_1\alpha^{n-1} + a_0\alpha^n)$$

Como la parte derecha está en A, pues es un subanillo, entonces α^{-1} también pertenece al anillo A. $\square$

Corolario 8.15 *Sea $A \subset B$ una extensión entera. Un punto $\mathfrak{q} \in \operatorname{Spec}(B)$ es maximal si y solo si $\mathfrak{p} = \mathfrak{q} \cap A = i^*(\mathfrak{q} \in \operatorname{Spec}(A)$ es maximal.*

Demostración.

Tenemos que la extensión $A_\mathfrak{p} \subset B_\mathfrak{q}$ es también entera. Uno es cuerpo si y solo si lo es el otro. De este modo $\mathfrak{q}$ es maximal si y solo si lo es $\mathfrak{p}$. $\square$

En otras palabras, esto significa que la aplicación $i^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ manda el espectro maximal dentro del espectro maximal.

Naturalmente la aplicación no será en general inyectiva. Pero si podemos afirmar que los primos $\mathfrak{q}$ que se proyectan en $\mathfrak{p}$ no pueden estar contenidos unos en otros.

Corolario 8.16 *Sea $\mathfrak{q}_1$ y $\mathfrak{q}_2$ dos primos de B que se proyectan en un primo $\mathfrak{p}$. Si $\mathfrak{q}_1 \subset \mathfrak{q}_2$ entonces necesariamente $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Demostración.

Localizaremos en el conjunto $S = A - \mathfrak{p}$. Abusando de la notación utilizaremos $B_\mathfrak{p}$ para designar el localizado de B en S.

La extensión $A_\mathfrak{p} \to B_\mathfrak{p}$ es entera en virtud de la proposición 8.11. El ideal maximal de $A_\mathfrak{p}$, que es un anillo local, se identifica con el ideal $\mathfrak{p}$. Los ideales $\mathfrak{q}_1$ y $\mathfrak{q}_2$, considerandolos dentro del localizado, se proyectan en $\mathfrak{p}$. Como la antiimagen es maximal, los dos ideales $\mathfrak{q}_1$ y $\mathfrak{q}_2$ deben ser maximales. Como uno está contenido dentro del otro, necesariamente coinciden.

Teorema 8.17 *Sea $A \subset B$ una extensión entera. Dado un ideal primo $\mathfrak{p}$ existe un ideal primo $\mathfrak{q}$ en B que cumple $\mathfrak{q} \cap A = \mathfrak{p}$.*

Demostración.

Consideramos el conjunto multiplicativo $S = A - \mathfrak{p}$. Utilizando la notación del corolario anterior tenemos que la extensión $A_\mathfrak{p} \to B_\mathfrak{p}$ es entera. Tomamos un ideal maximal $\mathfrak{q}$ del anillo $B_\mathfrak{p}$. Su antiimagen debe ser un ideal maximal del anillo local $A_\mathfrak{p}$. Pero el ideal maximal del localizado es precisamente $\mathfrak{p}$ por lo que ideal $\mathfrak{q}$ está situado sobre $\mathfrak{p}$. $\square$

Corolario 8.18 (Teorema del ascenso) *Sea $A \subset B$ una extensión entera. Dados dos ideales primos $\mathfrak{p}_1 \subset \mathfrak{p}_2$, existen dos ideales primos $\mathfrak{q}_1 \subset \mathfrak{q}_2$ tales que $\mathfrak{q}_i$ está situado sobre $\mathfrak{p}_i$.*

Demostración.

Tenemos que $A/\mathfrak{p}_1 \to B/\mathfrak{q}_1$ es entera. Le aplicamos el teorema anterior a esta extensión y obtenemos un ideal $\mathfrak{q}_2$ situado sobre $\mathfrak{p}_2$. Como siempre, debemos identificar los primos del cociente con los primos que contienen al ideal por el que se hace cociente. $\square$

Este teorema se puede generalizar a cadenas de primos formadas por más de dos eslabones, sin más que aplicar inducción.

9. Espacios topológicos noetherianos

En geometría algebraica se dota a las variedades algebraicas de una estructura topológica. En el caso de los espectros de anillos, o en general en el estudio de los esquemas, también tenemos una topología natural en los conjuntos considerados. Bajo hipótesis bastante generales todos los espacios topológicos son de un tipo especial, llamados espacios noetherianos. Sobre estos espacios se pueden estudiar de modo abstracto los conceptos de irreducibilidad y de dimensión de un modo satisfactorio.

Definición 9.1 *Un espacio topológico es* noetheriano *si toda cadena decreciente de cerrados estaciona. Si tenemos una cadena de cerrados*

$$V_0 \supset V_1 \supset \cdots \supset V_n \supset \dots$$

necesariamente existe un índice j que cumple $V_j = V_{j+1} = \dots$

Tomando complementos podemos ver que la definición equivale a que toda cadena creciente de abiertos estaciona. Sin embargo se suele trabajar con cerrados pues estos conjuntos son los que aparecen en geometría algebraica de modo natural. Como vimos en el tema 6, la condición de cadena ascendente es equivalente a la condición maximal. La condición de cadena descendente es entonces equivalente a la condición minimal. Resumiendo:

Proposición 9.1 *Un espacio topológico es noetheriano si y solo si toda colección Σ de cerrados tiene un elemento minimal, si y solo si toda cadena ascendente de abiertos es estacionaria, si y solo si toda colección Σ de abiertos tiene un elemento maximal.*

Ejemplos.

- Consideremos el espacio afin $\mathbb{A}^n$ con su topología de Zariski. Los cerrados de esta topología son los conjuntos algebraicos. A cada subconjunto algebraico V se le puede asociar el ideal $\mathfrak{I}(V)$, formado por los polinomios que se anulan en V. Esta correspondencia es inyectiva. Si tenemos una sucesión decreciente de cerrados, considerando sus ideales, obtenemos una cadena creciente de ideales. Como el anillo de polinomios es noetheriano, la cadena de ideales estaciona y también la cadena de cerrados. El espacio $\mathbb{A}^n$ es noetheriano.

- Trabajemos en el espacio $\mathrm{Spec}(A)$. Sabemos que a cada cerrado del espectro le asociamos un ideal del anillo. Una cadena decreciente de cerrados se transforma, tomando ideales, en una cadena creciente de ideales. Si el anillo es noetheriano, las cadenas decrecientes de cerrados estacionan. $\mathrm{Spec}(A)$ es noetheriano como espacio topológico si y solo A es noetheriano como anillo.

- Cualquier espacio topológico que solamente tenga un número finito de cerrados es noetheriano. Esto incluye el caso de los espacios topológicos con un número finito de elementos.

- Sea V un subconjunto de un espacio topológico noetheriano X. Los cerrados del subespacio son cerrados también del espacio total y cumplen por tanto la condición de cadena. Todo cerrado de un noetheriano es también noetheriano. En particular, todo conjunto algebraico es noetheriano.

- Sea U un abierto de un espacio euclídeo. Fijado un punto, existe una bola (abierta) de radio r contenida en U. Consideramos las bolas cerradas de radio estrictamente menor que r. Esta sucesión de cerrados no estaciona y el espacio no es noetheriano. En general cualquier variedad topológica no puede ser noetheriana.

Definición 9.2 *Un espacio topológico X es* reducible *si existen dos cerrados* *propios X_1 y X_2 que cumplen:*

$$X = X_1 \cup X_2$$

Los espacios irreducibles son aquellos en los que siempre que se tenga una descomposición del tipo anterior es debido a que X_1 o X_2 son iguales a X. Si consideramos un subespacio de X diremos que es reducible o irreducible si tiene dichas características con la topología inducida por el espacio total.

Tomando complementos en la definición anterior se pueden obtener otras caracterizaciones de los espacios irreducibles.

Proposición 9.2 *Un espacio X es irreducible si y solo si todo par de abiertos distintos tiene intersección no nula, si y solo si todo abierto de X es un conjunto denso, si y solo si todo abierto de X es conexo.*

Ejemplos.

- Sea $Y \subset X$ un subconjunto. Un recubrimiento (finito) de Y por cerrados es una inclusión

$$Y \subset X_1 \cup X_2 \cup \cdots \cup X_n$$

  donde X_i son cerrados del espacio total. Si Y es irreducible, necesariamente existe un índice que cumple $Y \subset X_i$. El recubrimiento se puede reducir a un único conjunto.

- $\mathbb{A}^1$ es irreducible si el cuerpo es infinito, puesto que es imposible que $\mathbb{A}^1 = X_1 \cup X_2$, puesto que los cerrados son conjuntos finitos.

- Todo conjunto formado por un solo punto es irreducible, puesto que la única topología posible que se puede introducir en dicho subconjunto da un espacio irreducible.

- En un espacio topológico Haussdorf cualquier conjunto que contenga más de un punto es reducible. Si tomamos dos puntos distintos, existen abiertos de intersección vacía.

- Veremos posteriormente que las hipersuperficies definidas por un polinomio primo (también llamado irreducible) son subconjuntos irreducibles.

- Prácticamente de la misma definición de irreducibilidad se deduce que el cierre de todo conjunto irreducible es también irreducible. En particular el cierre de cualquier punto es un conjunto irreducible. Si un punto x tiene como cierre el espacio total, decimos que x es un punto genérico. En los espectros de anillos íntegros el punto correspondiente al ideal nulo es un punto genérico.

- Un conjunto $Y \subset X$ es irreducible si y solo si es irreducible su cierre. En particular, si $U \subset X$ es un abierto y X es irreducible, necesariamente U es irreducible, puesto que el abierto es denso y su cierre es el espacio total.

- Si $f : X \to Y$ es continua y X es irreducible, necesariamente su imagen es irreducible.

Definición 9.3 *Una* componente irreducible *de un espacio topológico X es un subconjunto irreducible maximal, lo que significa que no está contenido en ningún conjunto irreducible mayor.*

Aplicando los resultados anteriores, tenemos que las componentes irreducibles son entonces conjuntos cerrados (pues el cierre de un irreducible es irreducible).

Lema 9.3 *Sea $\{V_i\}$ una cadena creciente de subconjuntos irreducibles. La unión de esa cadena es un conjunto irreducible.*

Demostración.

Supongamos que la unión no fuese irreducible. Sería entonces reducible y existirían dos abiertos con intersección nula. Llamemos a los abiertos U_1 y U_2. Necesariamente existen dos conjuntos V_{j_1} y V_{j_2} que tienen intersección no nula respectivamente con U_1 y U_2. Tomamos un cerrado mayor y tiene intersección no vacía con los dos abiertos. Dicho cerrado es entonces reducible, produciendose la contradicción. □

Tomemos ahora un punto $x \in X$. Consideremos la clase de todos los conjuntos irreducibles que contienen a x. Esta clase no es vacía pues hemos visto que contiene al conjunto $\{x\}$. El lema anterior nos permite usar el lema de Zorn, que nos asegura la existencia de un elemento maximal, que naturalmente tiene que ser una componente irreducible. Como conclusión tenemos la

Proposición 9.4 *Todo punto está contenido en una componente irreducible. En general, todo conjunto irreducible está contenido en una componente irreducible.*

Corolario 9.5 *Todo espacio topológico es unión de componentes irreducibles.*

En principio el corolario anterior afirma la existencia de una descomposición en componentes irreducibles, pero no sabemos si dicha descomposición es finita. El caso noetheriano nos asegura esta condición de finitud.

Proposición 9.6 *En un espacio noetheriano existe un número finito de componentes irreducibles. Dicha descomposción es única.*

Demostración.

Sea Σ el conjunto de todos los cerrados que no se pueden expresar como unión de un número finito de conjuntos irreducibles (no necesariamente maximales). Como estamos en un espacio noetheriano, existe un elemento minimal para Σ. Lo llamaremos V. Este conjunto V no puede ser irreducible pues entonces si es unión de un número finito (en este caso 1) de conjuntos irreducibles. Necesariamente es reducible. Sea $V = V_1 \cup V_2$. Los cerrados V_i son estrictamente menores que V. No pueden ser elementos de Σ. Cada uno de ellos es unión de un número finito de irreducibles. De este modo V es también unión de un número finito de irreducibles, produciendose una contradicción. Como conclusión tenemos que todos los cerrados del espacio topológico son unión de un número finito de conjuntos irreducibles. Pero cada conjunto irreducible está contenido en una componente y hemos demostrado el teorema.

Para demostrar la unicidad supongamos dos descomposiciones en componentes irreducibles

$$X = X_1 \cup \cdots \cup X_n \qquad\qquad X = Y_1 \cup \cdots \cup Y_m$$

Tomemos X_1. Como es irreducible, debe estar contenido en una componente maximal. Según la segunda descomposición las componentes irreducibles de X son $Y_1 \ldots Y_m$. X_1 debe de estar contenido en algún Y_i. Por la maximalidad se produce la igualdad. El resto de la demostración son detalles. □

Observación. La descomposición en irreducibles del espacio no tiene por qué ser única. Pero si consideramos las componentes (maximales) irreducibles si es única. Siempre que digamos que descomponemos un espacio topológico noetheriano, supondremos implícitamente que lo hacemos en sus componentes maximales. □

Corolario 9.7 *Toda variedad algebraica afín es unión finita de sus componentes irreducibles. La descomposición es única. Lo mismo es cierto para espectros de anillos noetherianos.*

Una vez construida la teoría, debemos dar criterios que nos aseguren la irreducibilidad de un espacio. Como estamos estudiando geometría algebraica lo normal es dar criterios de tipo algebraico.

Proposición 9.8 *Un conjunto algebraico V es irreducible si y solo si su ideal asociado $\mathfrak{I}(V)$ es primo.*

Demostración.

Supongamos que $fg \in \mathfrak{I}(V)$. Como el producto de los dos polinomios es cero en todo punto del conjunto, entonces, en cada punto, uno de los dos debe ser nulo. Esto nos indica que

$$V \subset \mathcal{V}(f) \cup \mathcal{V}(g)$$

Tenemos entonces la descomposición

$$V = (V \cap \mathcal{V}(f)) \cup (V \cap \mathcal{V}(g))$$

Como el subespacio es irreducible, alguna de las componentes es el espacio total. Supongamos que sea la primera. Entonces $V = V \cap \mathcal{V}(f)$, lo que implica que $V \subset \mathcal{V}(f)$ que es otra forma de decir que $f \in \mathfrak{I}(V)$. Resulta entonces que el ideal es primo.

Sea $\mathfrak{I}(V)$ un ideal primo. Supongamos que descomponemos la variedad $V = V_1 \cup V_2$. "Tomando" ideales en esta expresión obtenemos

$$\mathfrak{I}(V) = \mathfrak{I}(V_1) \cap \mathfrak{I}(V_2)$$

Existen elementos $f_i \in \mathfrak{I}(V_i)$ y $f_i \notin \mathfrak{I}(V)$. Tenemos entonces que $f_1 f_2$ está en el ideal de V lo que implica una contradicción. $\square$

Ejemplos.

- A^n es irreducible, pues su ideal asociado es primo, por ser íntegro el anillo de polinomios.
- Una hipersuperficie es irreducible si y solo si puede ser generada por un polinomio irreducible.
- Para descomponer en irreducibles una hipersuperficie debemos descomponer en irreducibles el polinomio que la define. Aplicando la factorización única, todo polinomio se puede expresar en la forma

$$f = f_1^{r_1} \cdots f_n^{r_n}$$

Pasando a los ideales

$$\mathcal{V}(f) = \mathcal{V}(f_1^{r_1}) \cup \cdots \cup \mathcal{V}(f_n^{r_n}) = \mathcal{V}(f_1) \cup \cdots \cup \mathcal{V}(f_n)$$

produciendose la descomposición en irreducibles.

En definitiva, para descomponer en componentes una hipersuperficie, debemos tomar un polinomio que la defina, descomponer dicho polinomio en producto de factores y eliminar los repetidos. Las componentes son las asociadas a los factores primos que "entran" en la descomposición del polinomio.

10. Dimensión

En álgebra lineal se define el concepto de dimensión de un espacio vectorial como el cardinal de una base. Existen sin embargo definiciones equivalentes. La más útil para nuestros propositos es la que emplea series de composición. La dimensión de un espacio vectorial es la longitud de la más larga de las cadenas que se pueden formar con subespacios, siendo las inclusiones estrictas en todos los eslabones. Los subespacios, y en general las subvariedades afines, son los ceros de los polinomios de primer grado, que son los que se usan en álgebra lineal. Una posible definición de dimensión de una variedad algebraica afín se puede realizar con el siguiente procedimiento. Tomamos cadenas (estrictas) formadas por conjuntos algebraicos irreducibles. La mayor longitud que encontremos será la dimensión de la variedad. Si asociamos a cada cadena sus ideales, las cadenas de cerrados se transforman en cadenas de ideales primos. Toda esta discusión sirve como base para la siguiente

Definición 10.1 *La* dimensión[5] *de un espacio topológico X es el supremo de las longitudes de las cadenas estrictas*

$$X_0 \subset X_1 \subset \cdots \subset X_n$$

[5]El concepto de dimensión que introducimos se conoce como dimensión de Krull. Como no utilizaremos otros conceptos de dimensión omitimos este hecho

formadas con cerrados irreducibles.

El vacío tiene dimensión igual a -1 por convenio. Si existen cadenas infinitas formados con elementos irreducibles, la dimensión no puede ser finita.

Definición 10.2 *Llamamos* dimensión *de una variedad afín o de un espectro a la dimensión del espacio topólogico.*

Sea $Y \subset X$ un cerrado irreducible de X. Para calcular la dimensión de Y debemos utilizar cerrados irreducibles contenidos en Y. Si lo que nos interesa es la codimensión de Y en X debemos adoptar una definición análoga a la de dimensión, pero donde las cadenas comiencen en Y.

Definición 10.3 *Sea $Y \subset X$ un cerrado irreducible. La codimensión de Y en X es el supremo de las longitudes de cadenas*

$$X_0 \subset X_1 \subset \cdots \subset X_n$$

donde X_0 es precisamente el cerrado Y.

Para calcular codimensiones de cerrados que no son irreducibles, descomponemos en irreducibles dicho cerrado. La codimensión del cerrado es el ínfimo de las codimensiones de sus componentes. En otras palabras, es la codimensión de la "mayor" componente irreducible, donde "mayor" significa que tenga la dimensión más alta.

Proposición 10.1 *Si descomponemos X en componentes irreducibles, la dimensión de X es el supremo de las dimensiones de sus componentes.*

Demostración.

El término de orden más alto X_n de una cadena es irreducible y está contenido en una componente irreducible del espacio. Esa cadena mide entonces menos que la dimensión de esa componente. Esto es cierto para todas las cadenas y el supremo de las cadenas es menor que el supremo de las dimensiones de las componentes. $\square$

En general si un espacio está descompuesto como unión de cerrados

$$X = A_1 \cup \cdots \cup A_n$$

la dimensión de X es el supremo de las dimensiones de sus "componentes" cerradas.

En general sabemos de geometría diferencial que las subvariedades cerradas de una variedad diferenciable tienen dimensión menor que la dimensión de la variedad. En variedades algebraicas no todo es tan sencillo. Sea $Y \subset X$ dos espacios irreducibles. Si $\dim(Y) < \dim(X)$ necesariamente $Y \neq X$ puesto que al ser X irreducible, le podemos añadir un término más a cada cadena de Y. Si tienen la misma dimensión necesariamente $Y = X$.

Si X no es irreducible no se puede afirmar nada, pues existe al menos una componente con la misma dimensión que X, que claramente no coincide con X. En general tenemos el siguiente resultado

Proposición 10.2 *Sea X un espacio irreducible. Sea Y un cerrado (no necesariamente irreducible) Entones $Y \subset X$ estrictamente si y solo si* $\dim(Y) < \dim(X)$.

En general una variedad puede tener componentes de distinta dimensión. Si todas las componentes tienen la misma dimensión d decimos que la variedad tiene dimensión d pura.

Pasamos ahora al tema de los anillos. A cada cadena de cerrados irreducibles le corresponde una cadena de ideales primos. Las dos tienen el mismo número de eslabones. La manera más evidente de definir la dimensión de un anillo es decir que tiene la misma que su espectro. Sin embargo se puede utilizar la siguiente definición equivalente que solamente emplea términos algebraicos.

Definición 10.4 *Llamamos* dimensión *de un anillo A al supremo de las longitudes de todas las cadenas estrictas*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$$

formadas por ideales primos.

Corolario 10.3 *La dimensión de un anillo y de su espectro coinciden.*

Si tenemos un ideal I de A, le asignamos una dimensión. Será la dimensión del anillo cociente A/I. En particular esto se aplica a los ideales primos. Teniendo en cuenta que el anillo de funciones polinomicas sobre una variedad V es precisamente el cociente del anillo de polinomios módulo el ideal asociado a V obtenemos.

Corolario 10.4 *Sea $\mathfrak{p} \subset A$ un ideal primo. La dimensión del espacio topológico $\mathcal{V}(\mathfrak{p})$ es igual a la dimensión de $\mathfrak{p}$.*

Proposición 10.5 *La dimensión de una variedad afín coincide con la dimensión de su anillo de funciones polinomiales.*

Demostración.

Existe una correspondencia entre los cerrados irreducibles de la variedad y los primos del anillo coordenado. $\square$

El mismo resultado es válido sin cambio alguno en el caso de los espectros.

Ejemplos.

- Si A tiene dimensión cero, las únicas cadenas que se pueden formar con ideales primos deben tener un único elemento. Si el anillo es íntegro, el cero es primo y no pueden existir más ideales primos. Todo elemento que no es cero debe ser invertible. A es un cuerpo. Si A no es íntegro, el cero no es primo. Para que las cadenas tengan una sola componente, todo primo (recordemos que el cero no es primo) es maximal.
- Sea A un dominio de ideales principales. Cada ideal primo no nulo es maximal. El cero es primo por ser íntegro. Toda cadena tiene dos componentes. La dimensión de cualquier dominio de ideales principales es 1. Como consecuencia $\mathbb{Z}$ y $k(x)$ tienen dimensión 1.

- Sea A un dominio de ideales principales. El espectro de A consta de puntos cerrados y de un punto denso. La dimensión del espacio topológico es 1.

- En $k(x_1, \dots, x_n)$ tenemos la siguiente cadena de primos

$$0 \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \dots, x_n)$$

  La dimensión de $k(x_1, \dots, x_n)$ (y de su espectro) es entonces igual o superior a n. Se puede demostrar que es precisamente n.

- Los anillos de dimensión cero tienen sus puntos cerrados. Si un anillo es noetheriano tienen un número finito de puntos. La descomposición del espectro induce una descomposición en producto de anillos. Se puede demostrar que si A no tiene nilpotentes cada uno de los factores es un cuerpo.

- El teorema del ascenso (8.18) prueba que toda extensión entera de una anillo A tiene la misma dimensión que A.

Sea $k \subset A$ una extensión de un cuerpo por un anillo (k-algebra). Dado una familia finita de n elementos $\{a_i\}$ de A se puede construir un morfismo de anillos de $k[x_1, \dots, x_n]$ en A, asociando a cada variable x_i el elemento a_i. Decimos que los elementos son algebraicamente independientes si dicho morfismo es inyectivo. En dicho caso la imagen, que es la k-álgebra generada por los elementos a_i, es isomorfa al anillo de polinomios en n variables.

El siguiente teorema demuestra que todo anillo asociado a una variedad es la extensión entera de un anillo de polinomios. Como la dimensión se conserva por extensiones enteras, la dimensión del anillo de la variedad es la dimensión del anillo de polinomios sobre el que dicha extensión es entera.

Teorema 10.6 (Lema de normalización de Noether) *Sea A una k-álgebra de generación finita. Existen elementos $y_1, \dots, y_d$ que cumplen:*

a) Los elementos $y_1, \dots, y_n$ son algebraicamente independientes sobre k.

b) A es módulo de generación finita sobre el anillo $k\langle y_1, \ldots, y_d\rangle$.

Demostración.

Haremos la demostración en el caso en que k tiene cardinal infinito. En el caso de los cuerpos finitos también es cierto el resultado, pero la demostración que esbozamos no es válida en ese caso.

Como A es de generación finita, existen elementos a_i que generan el álgebra. Asociando a x_i el elemento α_i tenemos un morfismo de anillos epiyectivo

$$\phi : k(x_1, \ldots, x_n) \longrightarrow k\langle a_1, \ldots, a_n\rangle$$

Si ϕ es inyectivo, entonces el teorema está demostrado. Supongamos que no es inyectivo. Debe existir un elemento f no nulo que pertenezca al núcleo. En este caso se cumple

$$f(a_1, \ldots, a_n) = 0$$

Nuestra intención es ver que en este caso bastan $n-1$ elementos para generar el álgebra y que elemento restante es entero sobre el álgebra generada por los $n-1$ elementos. Encontremos dichos elementos. Sea

$$\begin{array}{rcl} a'_1 & = & a_1 - \alpha_1 a_n \\ \ldots & = & \ldots \\ a'_{n-1} & = & a_{n-1} - \alpha_{n-1} a_n \end{array}$$

Como f se anula sobre los elementos a_i tenemos que

$$f(a'_1 + \alpha_1 a_n, \ldots, a'_{n-1} + \alpha_{n-1} a_n, a_n) = 0$$

Si f es de grado d podemos encontrar ciertos valores de las α_i que hagan que la ecuación anterior sea un polinomio unitario de grado d en a_n. Aquí se utiliza la infinitud del cuerpo para asegurar que existen valores para los que los polinomios en varias variables no son nulos.

Demostrado este hecho, vemos que los elementos $a'_1, \ldots, a'_{n-1}$ generan también el álgebra pues a_n se puede expresar en función de ellos y entonces cada a_i con $i < n$ también. Como el elementos a_n es entero sobre el anillo $A\langle a'_1, \ldots, a_{n-1}\rangle$ tenemos que $A = k\langle a'_1, \ldots, a_{n-1}\rangle(a_n)$ es finito sobre el anillo $k\langle a'_1, \ldots, a_{n-1}\rangle$. Inductivamente podemos seguir eliminando variables mientras no tengamos una colección algebraicamente independiente. $\square$

Definición 10.5 *Dada una k-álgebra de generación finita toda subálgebra $k\langle y_1, \ldots y_d\rangle$ que cumpla las condiciones del lema anterior se denomina una* normalización de Noether *del álgebra A.*

Observación.

Existe un refinamiento del lema de Noether que también es útil. En las condiciones del lema, dado un ideal I de A se pueden elegir los elementos $y_1, \ldots, y_d$ de la normalización de tal forma que se cumpla

$$I \cap k\langle y_1, \ldots, y_d\rangle = (y_1, \ldots, y_\delta) \text{ con } \delta \leq d$$

de este modo todo ideal I al intersecarlo con la normalización nos da un anillo de polinomios en δ variables.

Como A es generación finita sobre el anillo de polinomios, también es entera sobre dicho anillo. El teorema del ascenso nos dice que la dimensión de A coincide con la dimensión de una de sus normalizaciones de Noether. Como claramente la dimensión de A no puede depender de la normalización tomada, todas las normalizaciónes producen la misma dimensión.

Debemos hallar ahora la dimensión de los anillos de polinomios. Utilizando la observación realizada en el lema de Noether se puede demostrar que la dimensión de un anillo de polinomios sobre un cuerpo coincide con el número de variables.

Proposición 10.7 *La dimensión del anillo $k[x_1, \ldots, x_n]$ es precisamente n.*

Demostración.

Hemos visto en los ejemplos anteriores que

$$0 \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n)$$

luego la dimensión es mayor o igual al número de variables.

Tomamos ahora una cadena estricta de primos

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m$$

Debemos demostrar que m es menor que n. Tomamos el ideal no nulo $\mathfrak{p}_1$. Aplicando el lema de normalización de Noether tenemos una normalización

$$k(y_1, \ldots, y_n) \subset k(x_1, \ldots x_n)$$

que cumple que $\mathfrak{p}_1 = (x_1, \ldots, x_\delta)$. En este caso tenemos otra normalización de Noether

$$k(y_{\delta+1}, \ldots, y_n) \subset k[x_1, \ldots, x_n]/\mathfrak{p}_1$$

y se concluye por inducción. □

11. Anillos y módulos graduados

La intención de este capítulo es introducir unos conceptos que nos serán de gran utilidad en el estudio de las variedades proyectivas. También es útil este tema para el estudio de los tensores y de la cohomología y homología. Empezamos con definiciones generales que serán válidas tanto para anillos como para módulos.

Definición 11.1 *Dado un grupo conmutativo G, se llama* graduación *a una colección de subgrupos $\{G_i\}$ $i \in \mathbb{Z}$ tales que G es la suma directa de esos subgrupos.*

$$G = \bigoplus_{i \in \mathbb{Z}} G_i$$

La proyección canónica de G en el sumando G_i se denota por π_i y es un morfismo de grupos. La inclusión canónica de cada sumando G_i en G es también morfismos de grupos.

Definición 11.2 *Se dice que un elemento x de G es* homogéneo *de grado i si $x \in G_i$.*

Esto equivale a decir que $\pi_i(x) = x$. En este caso necesariamente $\pi_j(x) = 0$ si $i \neq j$. El cero del grupo es un elemento homogéneo de todos los grados. Los otros elementos solo pueden tener un grado, debido a que al ser la suma directa, tenemos que $G_i \cap G_j = 0$ si $i \neq j$. Debido también a la descomposición en suma directa, todo elemento $x \in G$ se puede escribir de modo único en la forma (la suma es siempre finita)

$$x = \sum \pi_i(x) = \sum x_i$$

donde cada x_i es homogéneo de grado i. El elemento $x_i = \pi_i(x)$ se llama componente homogénea de grado i de x.

Ejemplos.

- Los polinomios en una variable sobre un cuerpo k, con la graduación habitual. Los elementos homogéneos de grado n son los monomios ax^n. El conjunto de elementos de grado cero son justamente las constantes. Todos los grupos asociados a grados negativos son nulos. El mismo razonamiento es válido para el anillo de polinomios sobre un anillo A.

- Los tensores de un k-espacio vectorial. Los tensores homogéneos de grado n son las sumas de elementos formados por multiplicación tensorial de n elementos del espacio vectorial. También las formas exteriores o las simétricas forman estructuras graduadas. En todos los casos, los elementos de grado negativo son identicamente nulos. En las formas exteriores, si la dimensión del espacio es n, a partir del grado $n+1$ también son nulos, debido a la anticonmutatividad del producto exterior.

- Los polinomios sobre k en n variables. El subgrupo de grado i es

$$k(x_1, \ldots, x_n)_i = \{\text{Polinomios homogéneos de grado i}\}$$

  Es un ejercicio de combinatoria encontrar la dimensión de estos espacios vectoriales.

- Sea A un anillo e I un ideal. A partir de I podemos formar todas las potencias positivas I^n de dicho ideal. Por definición, el grupo de grado cero coinicide con el anillo A. Abusando de la notación lo denotaremos I^0. Las potencias negativas serán, también por definición, nulas. Con estas condiciones podemos construir el grupo graduado

$$G = \bigoplus_{n \geq 0} I^n$$

- Nos hemos encontrado con muchos ejemplos donde los elementos homogéneos de grado negativo son nulos. Decimos que un grupo esta graduado positivamente si $G_n = 0$ para los n negativos.

Si sobre el anillo A se ha dado una graduación, se dice que esta estructura es compatible con la estructura anular si

$$A_i \cdot A_j \subset A_{i+j}$$

Definición 11.3 *Un anillo con una estructura graduada compatible se llama* anillo graduado.

Si denotamos por $grad(x)$ al grado del elemento homogéneo x, entonces las definiciones se reducen a la conocida fórmula

$$grad(x \cdot y) = grad(x) + grad(y)$$

Ejemplos.

- El álgebra de polinomios $A(x)$ con el concepto de grado habitual es un anillo graduado.
- Los polinomios en n variables sobre un anillo A con la noción de grado total.

- El algebra exterior de un espacio vectorial es un anillo graduado. En este caso la multiplicación no es conmutativa. Lo mismo es válido para el álgebra tensorial y para el álgebra simétrica. En el caso del álgebra simétrica, si que estamos ante un anillo conmutativo.
- En el grupo $G = \oplus I^n$, definimos una multiplicación. Un elemento de I^i es en particular un elemento del anillo. Definimos la multiplicación de un elemento de I^i por otro de I^j como la multiplicación de dichos elementos en el anillo A. Por definición se cumple $I^i \cdot I^j \subset I^{i+j}$. Con esta multiplicación tenemos un anillo graduado.

Proposición 11.1 *El conjunto de elementos de grado cero, A_0, es un subanillo con unidad.*

Demostración.

Naturalmente se cumple $A_0 + A_0 \subset A_0$ por ser subgrupo. Análogamente se cumple $A_0 \cdot A_0 \subset A_0$ debido a la condición de compatibilidad de la estructrua de anillo y la estructura graduada. Veamos que la unidad está en A_0. Descomponemos en componentes homogéneas la unidad

$$1 = \sum e_i$$

Dado un elemento homogéneo y arbitrario a del anillo tenemos

$$a = 1 \cdot a = \sum e_k \cdot a$$

y esta es la descomposión homogénea de g (que recordemos es única). Necesariamente $e_0 \cdot a = a$ comparando grados. Como es cierto para los homogéneos se cumple que $e_0 \cdot a = a$ para todo elemento y e_0 es la unidad. □

Corolario 11.2 *La componente homogénea A_n es un módulo sobre el anillo A_0.*

Proposición 11.3 *Sea A un anillo graduado positivamente. Denotamos por A^+ a la suma directa de homogéneos, pero a partir del uno*

$$A^+ = \bigoplus_{i \geq 1} A_i$$

En estas condiciones A^+ es un ideal de A.

Demostración.

Tomemos un elemento homogéneo arbitrario a del anillo. Tomamos ahora otro elemento homogéneo a' de A^+. Como no tiene componentes negativas $a \cdot a'$ tiene grado igual o superior al grado de a'. Está entonces contenido en A^+. Para la demostración general se descompone cada elemento es sus componentes homogéneas. □

Corolario 11.4 *A/A^+ es isomorfo a A_0.*

Como en el caso de todas las estructuras algebraicas es interesante considerar los subconjuntos que heredan la estructura. Aquí deben heredar la estructura de anillo y la estructura graduada. Dado un conjunto S de un anillo graduado, denotaremos por S_i a la imagen de S por el morfismo π_i. Son los elementos de S que son homogéneos de grado i.

Definición 11.4 *Sea A un anillo graduado. Un* subanillo graduado *es un conjunto S que cumple:*

- *Es un subanillo de A.*
- *S es canónicamente isomorfo a $\oplus S_i$.*

Todo subanillo graduado es en si mismo un anillo graduado. La definición de ideal graduado es similar. Normalmente en la literatura, los ideales y subanillos graduados no reciben dicho nombre, sino que se llaman subanillos e ideales homogéneos. La siguiente proposición justifica dicho nombre. Nosotros seguiremos el convenio habitual y los denominaremos homogéneos.

Proposición 11.5 *Dado un ideal I de un anillo graduado son equivalentes:*

1) *I es un ideal graduado (homogéneo).*

2) *Si I contiene a un elemento x entonces contiene a cada componente homogénea x_i de dicho elemento.*

3) *El ideal se puede generar con elementos homogéneos.*

Demostración.

1) $\Rightarrow$ 2). Sea $x \in I$. Como I es la suma directa de sus componentes homogéneas $I = \oplus I_i$, entonces las componentes homogéneas de x pertenecen a la componente homogénea del ideal, que está contenido en I.

2) $\Rightarrow$ 3). Sea a_λ una familia, posiblemente infinita, de generadores del ideal. Denotamos por $a_{\lambda,i}$ a las componentes homogéneas de dichos elementos. Tenemos que cada elemento $a_{\lambda,i}$ está en el ideal I. Estos elementos generan el ideal y son homogéneos.

3) $\Rightarrow$ 1). Tomamos una familia de generadores homogéneos a_λ. Cada elemento del ideal generado se puede expresar como suma de múltiplos de dichos elementos. Un elemento arbitrario del ideal se expresa como $\sum h_\lambda a_\lambda$. Descomponemos en partes homogéneas los coeficientes y los denotamos $h_{\lambda.i}$. El producto es ahora suma de elementos homogéneos y cada elemento homogéneo está en el ideal pues se obtiene multiplicando los generadores por ciertos elementos. Es ahora claro que I es la suma directa de sus componentes homogéneas y el ideal es graduado. $\square$

Ejemplos.

- A^+ es un ideal homogéneo en cualquier anilllo graduado positivamente.
- En el álgebra tensorial de un espacio vectorial (que no es conmutativa) el ideal generado por los elementos de la forma $x \otimes x'$ es un ideal graduado. Al hacer cociente se obtiene el álgebra exterior. Razonamientos similares sirven para construir las álgebras simétricas, las álgebras envolventes de álgebras de Lie, ...

- El ejemplo más importante es geometría algebraica es el siguiente. Sea $\mathbb{P}^n(k)$ el espacio proyectivo n dimensional. Decimos que un polinomio f (en $n+1$ variables) se anula en un punto $x \in \mathbb{P}^n(k)$ si $f(x) = 0$ para cualquier representante del punto x. Si el cuerpo es infinito, para que se anule un polinomio sobre todos los representantes, deben anularse sus componentes homogéneas. Veamoslo. Todos los representantes de x son de la forma λx con λ no nulo. Descomponemos f en sus componentes homogéneas y se lo aplicamos a todos los representantes de x

  $$f_0(\lambda x) + f_1(\lambda x) + \ldots f_n(\lambda) = f_0(x) + \lambda f_1(x) + \cdots + \lambda^n f_n(x)$$

  Nos queda un polinomio en "λ" que si es nulo sobre cualquier punto debe tener todos los elementos nulos.

  Sea V un subconjunto del espacio proyectivo de dimensión n. Definimos $\mathfrak{I}(V)$ como el conjunto de polinomios de $k(x_0, \ldots, x_n)$ (una variable más) que se anulan sobre todos los puntos de V. Es un ideal homogéneo por la discusión anterior. Toda la geometría algebraica proyectiva (clásica) se basa en esta correspondencia entre conjuntos del espacio proyectivo e ideales homogéneos.

Utilizando los ideales homogéneos podemos hacer cocientes y los anillos resultantes son también graduados. Es más se cumple

$$A/I \sim \bigoplus_{i \in \mathbb{Z}} (A_i/I_i)$$

Corolario 11.6 *La suma, el producto y la intersección de ideales homogéneos es homogéneo. La imagen de un ideal homogéneo es un ideal homogéneos del cociente (pues la aplicación es epiyectiva). La antiimagen de un ideal homogéneo es homogénea.*

Con estos resultados podemos considerar el ideal homogéneo generado por un subconjunto. Es simplemente la intersección de todos los ideales homogéneos que lo contienen. Si tomamos un ideal arbitrario I del anillo A, denotaremos por I^* al ideal homogéneo que genera. Si ya de por si el ideal es homogéneo tenemos que $I = I^*$, pero en general se cumple $I \subset I^*$. Otra forma de construir los ideales I^* es considerar las componentes homogéneas de los elementos de I, que generalmente no son elementos de I. Dichos elementos homogéneos generan un ideal, que es homogéneo. Dicho ideal coincide con I^*. Utilizando la descomposición en partes homogéneas se puede probar la siguiente

Proposición 11.7 *Sea $\mathfrak{p}$ un ideal primo. El ideal homogéneo asociado $\mathfrak{p}^*$ es también primo.*

Corolario 11.8 *El radical de un ideal homogéneo es la intersección de los primos homogéneos que contienen al ideal.*

Si consideramos morfismos adaptados a las estructuras graduadas, muchos resultados se pueden generalizar.

Definición 11.5 *Sea A y A' dos anillos graduados. Un morfismo de anillos graduados es una aplicación*

$$\varphi : A \longrightarrow A'$$

que cumple

- *Es morfismo de anillos.*
- *Conserva el grado. $\varphi(A_i) \subset A'_i$*

La aplicación canónica de paso al cociente es un morfismo graduado, siempre que el cociente se haya realizado con un idea homogéneo. Del mismo modo las inclusiones canónicas de los subanillos e ideales homogéneos son morfismos graduados.

Consideremos ahora módulos graduados. Si M es un A-módulo y tanto M como A están graduados, la compatibilidad de estructuras se refleja en la propiedad

$$A_i \cdot M_i \subset M_{i+j}$$

Decimos en este caso que M es un módulo graduado. Tenemos resultados similares al caso de los anillos. Las demostraciones también son similares. Normalmente se procede del siguiente modo: se descomponen los elementos en suma de homogéneos, se prueban resultados para los elementos homogéneos y se extiende el resultado a todo el conjunto.

Lema 11.9 *Si M es un módulo graduado y N es un submódulo de M, son equivalentes las afirmaciones siguientes:*

a) *N es suma directa de $(N \cap M_i)$ $i \in \mathbb{Z}$.*

b) *Las componentes homogéneas de todo elemento de N, pertenecen también a N.*

c) *N está engendrado linealmente por elementos homogéneos.*

Definición 11.6 *Un* submódulo graduado *es aquel que cumple alguna de las condiciones del anterior lema.*

Definición 11.7 *Sean M y M' dos módulos graduados. Se dice que un morfismo de módulos*

$$\varphi : M \longrightarrow M'$$

es de grado *j si $\varphi(M_i) \subset M'_{i+j}$.*

Fácilmente se comprueba que la composición de dos morfismos de grado definido nos da otro morfismo cuyo grado se obtiene sumando los grados de los dos morfismos.

Ejemplos.

- La contracción interior con un vector es un morfismo del álgebra tensorial de un k-espacio. Su grado es -1.
- La diferencial exterior que se estudia en geometria diferencial es un morfismo entre las álgebras exteriores de las variedades y tiene grado $+1$. Se cumple que su cuadrado es nulo. Estas son las condiciones

preliminares que nos van a servir para estudiar una teoría de cohomología. En este caso la cohomología resultante se denomina cohomología de De Rham.

- Multiplicar en un algebra por un elemento homogéneo de grado i, es un morfismo de grado i.

Proposición 11.10 *Sea M, M' módulos graduados. $\varphi : M \longrightarrow M'$ un morfismo de grado r. Entonces $\mathrm{Ker}(\varphi)$ e $\mathrm{Im}(\varphi)$ son submódulos graduados.*

Demostración.

Sea $e' \in \mathrm{Im}(\varphi)$. Existe $e \in M$ tal que $\varphi(e) = e'$. Descomponemos e en sus componentes homogéneas $e = \sum e_i$. Por lo tanto $e' = \sum \varphi(e_i)$ que es la descomposición en componentes homogéneas de e'. Así las componentes homogéneas están en la imagen y el submódulo es graduado.

La otra parte de la demostración utiliza argumentos análogos. $\square$

En anillo graduado tiene sentido considerarlos ideales que son a la vez primos y homogéneos. De esta manera se prodría definir una especie de "espectro homogéneo" para cualquier anillo gruduado. Sin embargo, estamos interesados en relacionar esta estructura con la teoría de esquemas. Para ello debemos considerar solamente algunos primos homogéneos de los ideales. Estudiaremos solamente el caso de los anillos graduados positivamente.

Definición 11.8 *Sea A un anillo graduado positivamente yA^+ el ideal de elementos estrictamente positivos. Decimos que un ideal homogéneo I es relevante si $A^+ \not\subset I$.*

Definición 11.9 *Dado un anillo graduado llamamos $\mathrm{Proj}(A)$ al conjunto de primos relevantes de A. Es lo que llamamos* espectro homogéneo *de A.*

Como el espectro homogéneo es un subconjunto del espectro total del anillo, hereda la topología de Zariski de dicho espacio. No es dificil demostrar que dicha topología se puede definir utilizando variedades (en el espectro homogéneo) definidas como ceros de ideales homogéneos.

Vistas las propiedades más importantes hagamos una excursión por las variedades proyectivas. Todos los resultados son ahora fácilmente deducibles tomando los análogos del caso afín.

Una variedad proyectiva es un subconjunto de $\mathbb{P}^n$ dado por los ceros de cierto ideal homogeneo I del anillo de polinomios en $n+1$ variables. El conjunto de variedades proyectivas se comporta del mismo modo que los cerrados de una topología, pues la intersección arbitraria de variedades proyectivas es de nuevo una variedad y unión finita también. Esto permite introducir la topología de Zariski en el espacio proyectivo. Como los anillos de polinomios son noetherianos, la topología de Zariski inducida en el espacio proyectivo es también noetheriana y podemos descomponer en irreducibles toda variedad proyectiva. Para que una variedad sea irreducible basta que el ideal homogeneo asociado sea primo. Esto es equivalente a que el anillo coordenado asociado a la variedad sea íntegro.

El teorema de los ceros de Hilbert admite versiones proyectivas. En su forma fuerte nos permite afirmar que existe una biyección que invierte el orden entre subvariedades proyectivas e ideales homogeneos y radicales de anillo de polinomios o en general del anillo coordenado de la variedad. El único problema que se presenta es que al conjunto vacío le debemos hacer corresponder el ideal $(x_0, x_1, \ldots, x_n)$.

El espacio afín se puede inyectar de manera natural en el proyectivo, asociando a cada elemento $(x_1, \ldots, x_n)$ la clase del elemento $(1, x_1, \ldots, x_n)$. Toda variedad afín es de este modo un subconjunto del espacio proyectivo. La intersección de todas las variedades afines que contienen a este conjunto es la mínima variedad proyectiva que lo contiene. Coincide con el cierre topológico del conjunto en el espacio proyectivo. La descomposición en irreducibles de la variedad afín se traduce en una descomposición análoga de su cierre proyectivo. El proceso de añadir a una variedad unos ciertos "puntos del infinito" es una argucia empleada desde hace mucho tiempo. Muchas veces es más útil considerar variedades proyectivas debido a que los teoremas sobre intersecciones de variedades son mucho más simples en el caso proyectivo que en el afín. En cierta forma el paso de afín a proyectivo se puede entender como una compactificación del espacio. En general sabemos que las "cosas" compactas son siempre mucho más simples que las no compactas.

A. El espacio proyectivo

Un conocimiento básico de las principales nociones proyectivas es imprescindible para la comprensión de la geometría algebraica. En particular la geometría proyectiva tiene como base a los espacios proyectivos.

Definición de espacio proyectivo

Sea E un espacio vectorial sobre un cuerpo k. Cuando sea preciso supondremos que su dimensión es finita. En $E - \{0\}$ se define la siguiente relación de equivalencia: $e \sim e'$ cuando exista un λ distinto de cero tal que $e = \lambda e'$.

Definición A.1 *Al conjunto cociente lo llamaremos* espacio proyectivo *asociado a E y lo denotaremos por* $\mathbb{P}(E)$.

La aplicación de paso al cociente se denotará

$$\begin{array}{rccc} \pi & : E - \{0\} & \longrightarrow & \mathbb{P}(E) \\ & e & \longrightarrow & \pi(e) \end{array}$$

aunque muchas veces cometeremos el abuso de notación de escribir

$$\begin{array}{rccc} \pi & : E & \longrightarrow & \mathbb{P}(E) \\ & e & \longrightarrow & \pi(e) \end{array}$$

a pesar de que la función no está definida en el cero.

Dos vectores son equivalentes si y solo si generan el mismo subespacio vectorial. Las clases de equivalencia son las rectas vectoriales a las que se le ha quitado el origen. Por ello el espacio proyectivo se identifica con el conjunto de rectas de E. Si $p = \pi(e)$ diremos que el punto p es la proyectivización de e, o bien que e es un representante de p. Esta observación nos permite dar una nueva definición de espacio proyectivo.

Definición A.2 *El* espacio proyectivo *asociado a* E *es el conjunto de todas las rectas vectoriales de* E.

En el caso en que $E = k^{n+1}$ denotaremos el espacio proyectivo por $\mathbb{P}^n$ o por $\mathbb{P}^n(k)$ si es necesario hacer referencia al cuerpo.

Subvariedades lineales

Diremos que un subconjunto de $\mathbb{P}(E)$ es una subvariedad lineal cuando sea la imagen por la proyección canónica π de algún subespacio de E.

Si V es un subespacio vectorial de E y $X = \pi(V)$, diremos que X es la proyectivización de V, y se verifica que los puntos de X se corresponden de modo canónico con los del espacio proyectivo asociado a V. Por ello cada subvariedad lineal se puede entender como un espacio proyectivo.

El conjunto vacío también se considerará, por convenio, una subvariedad lineal del espacio proyectivo. Será la proyectivización del subespacio $\{0\}$.

El subespacio que le corresponde a una subvariedad lineal es único pues un subespacio es la unión de todas las rectas que contiene. Si $X = \pi(V)$ entonces $V = \pi^{-1}(X) \cup \{0\}$.

La relación de inclusión entre subconjuntos de $\mathbb{P}(E)$ define una relación de orden entre las subvariedades lineales que llamaremos incidencia. Si X,Y son dos subvariedades lineales tales que $X \subseteq Y$ diremos que X e Y son incidentes. Si $X = Y$ diremos que son coincidentes.

Este conjunto tiene una estructura de retículo, dado de la siguiente manera: si $X = \pi(V)$, $Y = \pi(W)$ entonces

$$\sup(X, Y) = X + Y = \pi(V + W)$$

$$\text{ínf}(X, Y) = X \cap Y = \pi(V \cap W)$$

La comprobación de estas propiedades es inmediata. Las subvariedades lineales forman un retículo, cuyo primer elemento es el conjunto vacío y el último elemento es el espacio total. Hemos probado el

Teorema A.1 *Consideremos el retículo de subespacios y el de subvariedades lineales. La aplicación que manda a cada subespacio V a su proyectivizado $\pi(V)$, es un isomorfismo de retículos.*

La aplicación considerada es también un morfismo de conjuntos ordenados:

$$\text{si } V \subseteq W \text{ entonces } \pi(V) \subseteq \pi(W)$$

Sea S un subconjunto de $\mathbb{P}(E)$. La intersección de todas las subvariedades de $\mathbb{P}(E)$ que contienen a S es una subvariedad lineal que denotamos por $\langle S \rangle$. Por construcción $\langle S \rangle$ es la mínima subvariedad que contiene a S.

Definición A.3 *Diremos que $\langle S \rangle$ es la* subvariedad lineal generada *por S.*

Dado el subconjunto S consideramos su imagen inversa por π. Como $\pi^{-1}(S)$ es un subconjunto de un espacio vectorial, existe un mínimo subespacio vectorial que lo contiene. Sea V dicho subespacio. En estas condiciones tenemos

$$\pi(V) = \langle S \rangle$$

por lo que la subvariedad generada es la proyectivización del subespacio generado por las rectas del conjunto.

Definición A.4 *Si $X = \pi(V)$ es una subvariedad lineal, llamaremos* dimensión *de X al número $dim(X) = dim(V) - 1$.*

A la subvariedad $\varnothing$ se le asigna por convenio dimensión igual a -1. Si el espacio proyectivo tiene dimensión uno se dice que es una recta proyectiva. Si tiene dimensión dos es un plano proyectivo. En el caso real la dimensión de X coincide con la dimensión como variedad topológica.

Definición A.5 *Si $X = \pi(V)$, llamaremos* codimensión *de X al número*

$$codim(X) = dim(\mathbb{P}(E)) - dim(X) = dim(E) - dim(V)$$

Las subvariedades lineales de dimensión cero son los puntos. Las de dimensión uno las llamaremos rectas, las de dimensión dos planos y las de codimensión uno hiperplanos.

De las propiedades conocidas de los espacios vectoriales se deduce que dadas dos subvariedades X, Y incidentes y de la misma dimensión, necesariamente coinciden. Del mismo modo si $X \subseteq Y$ entonces $\dim(X) \leq \dim(Y)$ y el menor es estricto cuando la inclusión también lo es.

La fórmula de las dimensiones es válida para subvariedades:

$$\dim(X+Y) = \dim(X) + \dim(Y) - \dim(X \cap Y)$$

Esto es consecuencia directa de las definiciones y de la fórmula análoga para subespacios vectoriales.

De ello se pueden deducir consecuencias acerca de la intersección y la suma de subvariedades.

Ejemplos.

- Si A y B son dos puntos distintos, entonces $A+B$ es una subvariedad que pasa por A y por B. Veamos cual es su dimensión aplicando la fórmula anterior

  $$\dim(A+B) = \dim(A) + \dim(B) - \dim(\varnothing)$$

  $$\dim(A+B) = 0 + 0 - (-1) = 1$$

  Por lo tanto $A+B$ es una recta y además es única. Por lo tanto por dos puntos distintos pasa una única recta.

- Dos rectas de un plano proyectivo se cortan en un punto, siempre que ambas rectas no sean coincidentes. Por lo tanto en el plano proyectivo no hay rectas paralelas.

- Si el espacio proyectivo tiene dimensión 3, un plano y una recta no contenida en dicho plano se cortan en un punto.

- En general una recta y un hiperplano que no contiene a la recta se cortan en un punto.

Una de las contrucciones típicas en el álgebra lineal es la construcción de espacios cociente. Damos el análogo en el caso proyectivo.

Definición A.6 *Si X es una subvariedad lineal de dimensión d, llamaremos* radiación *de base X al conjunto de las subvariedades de dimensión $d+1$ que pasan por X. Se denotará por $\mathbb{P}(E)/X$*

La radiación de base X se puede entender como un espacio proyectivo gracias al siguiente teorema.

Teorema A.2 *Si $X = \pi(V)$ es una subvariedad de $\mathbb{P}(E)$, entonces la radiación de base X se corresponde canónicamente con el espacio proyectivo $\mathbb{P}(E/V)$.*

Demostración.

La proyección canónica $\pi : E \to E/V$ establece una biyección entre los subespacios de E/V y los de E que contienen a V, dada por $V' \to \pi^{-1}(V')$.

A los subespacios de dimensión $d + 1$ le corresponden los subespacios unidimensionales de E/V. Como el conjunto de subespacios de dimensión $d+1$ está en correspondencia biunívoca con la radiación de base X se concluye el teorema.

Ejemplos

- Las rectas de $\mathbb{P}^2$ que pasan por un punto dado forman una recta proyectiva.
- Las rectas de $\mathbb{P}^3$ que pasan por un punto dado forman un plano proyectivo.
- Los planos de $\mathbb{P}^3$ que pasan por una recta forman una recta proyectiva.

Homografías. Grupo proyectivo

Si $\varphi : E \to E'$ es una aplicación lineal biunívoca, la imagen por φ de cada recta de E es una recta de E'. Ello nos permite construir una aplicación de $\mathbb{P}(E)$ en $\mathbb{P}(E')$ que denotaremos $\pi(\varphi)$. Vendrá definida por la fórmula

$$\pi(\varphi)(\pi(e)) = \pi(\varphi(e))$$

La función no depende del representante tomado en cada clase de equivalencia por ser φ una aplicación lineal. Esta aplicación se llama proyectivización de φ.

Definición A.7 *Una* proyectividad *u* homografía *es una función de* $\mathbb{P}(E)$ *en* $\mathbb{P}(E')$ *dada por algún isomorfismo* φ.

La proyectivización de φ hace que el diagrama siguiente sea conmutativo

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \downarrow & & \downarrow \\ \mathbb{P}(E) & \xrightarrow{\pi(\varphi)} & \mathbb{P}(E') \end{array}$$

Si las aplicaciones lineales se pueden componer, sus homografías asociadas también y cumplen en este caso las siguientes propiedades:

- $\pi(\varphi \circ \phi) = \pi(\varphi) \circ \pi(\phi)$
- $(\pi(\varphi))^{-1} = \pi(\varphi^{-1})$
- $\pi(\mathrm{Id}) = \mathrm{Id}$

De las propiedades enunciadas anteriormente se deduce que el conjunto de homografías de un espacio proyectivo forma un grupo, que denotaremos $PGL(E)$ y llamaremos grupo proyectivo. La asociación $\varphi \to \pi(\varphi)$ es un morfismo de grupos de $GL(E)$ en $PGL(E)$.

Esta aplicación es por definición epiyectiva y su núcleo está formado por todas las homotecias, pues si todos los vectores de E son propios de una aplicación lineal φ, necesariamente esta aplicación es una homotecia. Este grupo así construido es el grupo de la geometría proyectiva.

Definición A.8 *Dos figuras (conjunto de puntos) son* proyectivamente equivalentes *si existe una homografía que transforma una en la otra. Una propiedad es* proyectiva *si es invariante por homografías*

Dada una homografía $\pi(\varphi)$, un punto invariante de la homografía cumple $\pi(\varphi)e = e$. Por lo tanto $\pi(\varphi(e)) = e \quad \Rightarrow \quad \varphi(e) = \lambda e$. De este modo el estudio de los puntos invariantes de las homografías es equivalente al estudio de los valores propios de las aplicaciones lineales.

Aplicaciones proyectivas

En el caso de las aplicaciones biyectivas no hay ningún problema para construir la aplicación proyectivizada, debido a que solamente el vector nulo tiene como imagen el vector nulo. Sin embargo si una aplicación lineal tiene núcleo, la imagen de esos vectores no genera ninguna recta y no se puede definir la aplicación proyectivizada en dicho subconjunto.

Definición A.9 *Dada una aplicación lineal $\varphi : E \to E'$, se llama centro de dicha aplicación lineal al proyectivizado de su núcleo $\pi(\mathrm{Ker}(\varphi))$. La* aplicación proyectiva *$\pi(\varphi)$ está definida en el complementario del centro y responde a la fórmula*

$$\pi(\varphi)(\pi(e) = \pi(\varphi(e))$$

A pesar de que en realidad la aplicación π está definida en el conjunto $\mathbb{P}(E) - \pi(\mathrm{Ker}(\varphi))$ cometeremos el abuso de notación de escribir

$$\pi(\varphi) : \mathbb{P}(E) \longrightarrow \mathbb{P}(E')$$

teniendo claro que dicha aplicación no está definida en todo el espacio.

Como vemos las homografías no son sino las aplicaciones proyectivas asociadas a aplicaciones biyectivas.

El espacio dual

Sea E^* el espacio dual de E. Diremos que $\mathbb{P}(E^*)$ es el espacio proyectivo dual de $\mathbb{P}(E)$. Como las rectas de E^* se corresponden por incidencia con los hiperplanos de E, podemos considerar a $\mathbb{P}(E^*)$ como el conjunto de hiperplanos de $\mathbb{P}(E)$.

Si $X = \pi(V)$ es una subvariedad, diremos que $X^o = \pi(V^o)$ es la subvariedad dual o subvariedad incidente de X.

Entendiendo $\mathbb{P}(E^*)$ como el conjunto de hiperplanos del espacio proyectivo, X^o estaría formada por los hiperplanos que contienen a X. La dimensión de X^o es igual a $\mathrm{codim}(X) - 1$, fórmula que no es análoga a la de los espacios vectoriales.

Teorema A.3 (Principio de dualidad) *El paso al incidente es un anti-isomorfismo de retículos. Por lo tanto tomar incidente manda el supremo al ínfimo, el ínfimo al supremo e invierte el orden de las inclusiones.*

Demostración.

Es consecuencia directa del teorema A.1 y del principio de dualidad para espacios vectoriales.

Si por π denotamos los pasos al incidente y las flechas verticales indican las identificaciones del teorema A.1 tenemos el siguiente cuadro conmutativo.

$$\begin{array}{ccc} \text{Subvariedades de } \mathbb{P}(E) & \xrightarrow{\pi} & \text{Subvariedades de } \mathbb{P}(E^*) \\ \downarrow & & \downarrow \\ \text{Subespacios de } E & \xrightarrow{\pi} & \text{Subespacios de } E^* \end{array}$$

Cambio de base

Si E es un espacio vectorial sobre k, para cada extensión $k \hookrightarrow K$ del cuerpo base el morfismo inyectivo $E \hookrightarrow E \otimes_k K$ define una inyección de $\mathbb{P}(E)$ en $\mathbb{P}(E \times_k K)$. El último espacio proyectivo se construye considerándolo como K-espacio y no como k-espacio. La inyección manda a cada punto $\pi(e)$ al punto $\pi(e \otimes 1)$.

Diremos que $\mathbb{P}(E \otimes_k K)$ se obtiene del espacio primitivo por un cambio de cuerpo base. También diremos que los puntos de $\mathbb{P}(E \otimes_k K)$ son los puntos de $\mathbb{P}(E)$ con valores en la extensión K.

Del mismo modo que para subvariedades de dimensión cero, a cada subvariedad X se le asigna una subvariedad del espacio obtenido por cambio de base, $X_K = \pi(V \otimes_k K)$ si $X = \pi(V)$. Esto inyecta el retículo de $\mathbb{P}(E)$ en el del espacio extendido. La dimensión y la incidencia son estables por cambio de base. Es decir se cumple:

- $\dim(X_K)=\dim(X)$
- $(X_K)^o = (X^o)_K$ mediante el isomorfismo $(E \otimes_k K)^* = E^* \otimes_k K$.

Por supuesto la dimensión de X_K se calcula entendiendo el espacio extendido como un K-espacio.

Como las propiedades geométricas son estables por cambio de cuerpo base, es suficiente demostrarlas después de hacer una extensión, con lo que puede suponerse que el cuerpo base es algebraicamente cerrado, (recordemos que todo cuerpo admite una extensión algebraicamente cerrada).

Del mismo modo que a las subvariedades, a cada proyectividad $\varphi = \pi(\varphi)$ le podemos asociar una proyectividad del espacio extendido mediante la fórmula $\varphi_K = \pi(\varphi \otimes 1)$. De esta manera se inyecta el grupo lineal proyectivo del espacio E en el grupo lineal proyectivo de $E \otimes_k K$ (como K-espacio).

Coordenadas homogeneas

Se introducirá ahora un concepto análogo al de base de un espacio vectorial en los espacios proyectivos asociados a espacios vectoriales de dimensión finita.

Si $\mathbb{P}(E)$ es un espacio proyectivo de dimensión n, diremos que un conjuntos de $n+1$ puntos $(P_0, P_1, \ldots, P_n)$ es un símplice cuando $(P_0 + P_1 + \cdots + P_n)$ es el espacio total. Los hiperplanos resultantes de quitar un punto al símplice se denominan caras del símplice.

Tomando un representante de cada punto del símplice se obtiene una base del espacio vectorial, puesto que los puntos engendrarán el espacio proyectivo total.

Definición A.10 *Diremos que una sucesión ordenada de $n+2$ puntos*

$$\mathbf{R} = (P_0, P_1, \cdots, P_n, U)$$

es un sistema de referencia*, cuando al quitar un punto cualquiera nos quede un símplice. Diremos que los primeros $n+1$ puntos forman el* símplice de referencia *y que U es el* punto unidad*.*

Teorema A.4 *Sea $\mathbf{R} = (P_0, P_1, \cdots, P_n, U)$ un sistema de referencia. Existe una base, única salvo un factor de proporcionalidad, $\{e_i\}$ de tal que $P_i = \pi(e_i)$ y $U = \pi(e_1 + e_2 + \cdots + e_n)$. La proporcionalidad significa que si $\{e'_i\}$ es otra base que cumpla el teorema entonces se cumple: $e'_i = \lambda e_i$, donde λ es un escalar no nulo.*

Demostración.

Elijamos vectores v_i tales que representen a cada punto P_i. Entonces estos vectores forman un base del espacio vectorial. Luego si u es un representante de U

$$u = \lambda_0 v_0 + \cdots + \lambda_n v_n$$

para ciertos escalares λ_i ninguno de los cuales puede ser nulo. Si λ_i fuera nulo al quitar el punto P_i a la sucesión formada por el sistema de referencia no nos quedaría un símplice, pues no generaría el espacio total.

La base $\{\lambda_i v_i\}$ verifica el enunciado. Si $\{e_i\}$ y $\{e'_i\}$ cumplen el enunciado entonces $e'_i = \mu_i e_i$ y $\sum e_i = \sum \mu e'_i$. Entonces $\mu = \mu_i$ y $e'_i = \mu e_i$.

Corolario A.5 *Dados dos sistemas de referencia en sendos espacios proyectivos de la misma dimensión, existe una única proyectividad que transforma el primer sistema en el segundo.*

Demostración.

Sean $\{e_i\}$ y $\{e'_i\}$ dos bases asociadas a los sistemas de referencia. La aplicación lineal φ que transforma una base en la otra da al proyectivizarla una aplicación que cumple el enunciado. Como las bases son únicas, salvo un factor de proporcionalidad la aplicación lineal construida puede diferir también en un factor de proporcionalidad que no tiene importancia al proyectivizar la aplicación lineal.

Definición A.11 *Las bases a las que se refiere el teorema anterior reciben el apelativo de* bases normalizadas *asociadas al sistema de referencia en cuestión.*

Sea P un punto del espacio proyectivo y $\mathbf{R}$ una referencia en dicho espacio. Si e es un representante de P y $\{e_i\}$ una base normalizada asociada a $\mathbf{R}$, podemos expresar $e = \sum x_i e_i$. Los números (indeterminados en una constante no nula) x_i son por definición las coordenadas homogéneas del punto P en la referencia R.

Ejemplos.

- En una recta proyectiva, dar una referencia es dar tres puntos distintos y ordenados.
- En un plano proyectivo una referencia está formada por cuatro puntos. Los tres primeros formarán un triángulo y el último no podrá estar sobre los lados del triángulo.

B. El haz estructural

En el capítulo anterior hemos estudiado el espectro de un anillo como un simple espacio topológico. Si embargo sobre dicho espacio topológico se puede definir una estructura de **espacio anillado**. Un espacio anillado es un caso particular de lo que comunmente se denomina **haz**. La definición y el concepto general de haz es en primera estancia bastante difícil, debido a su alto grado de abstracción. Por ello, antes de dar la teoría general, damos un ejemplo, destacando las partes relacionadas con la teoría de haces.

Consideremos el conjunto $\mathbb{R}^n$ con su estructura habitual de espacio topológico. A cada abierto $U \subset \mathbb{R}^n$ le asociamos el conjunto de las funciones continuas de U en $\mathbb{R}$, que denotamos $\mathcal{C}(U)$

$$\mathcal{C}(U) = \{f : U \to \mathbb{R} \text{ continuas}\}$$

Este conjunto tiene estructura de anillo. Si tenemos dos abiertos $V \subset U$ a cada función continua $f : U \to \mathbb{R}$ le podemos asociar su restricción $f_{|V} : V \to \mathbb{R}$ que es una aplicación continua. Tenemos de este modo una aplicación de $\mathcal{C}(U)$ en $\mathcal{C}(V)$

$$\begin{array}{rccc} \rho_{UV}: & \mathcal{C}(U) & \to & \mathcal{C}(V) \\ & f & \to & f_{|V} \end{array}$$

Dicha aplicación es siempre un morfismo de anillos y ρ_{UU} es el morfismo identidad. Si tenemos un tercer abierto $W \subset V \subset U$ se comprueba sin dificultad que $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$. Los morfismos que acabamos de construir se denominan, por razones obvias, morfismos **restricción**.

Fijemos un punto $x \in \mathbb{R}^n$ y dos entornos abiertos, U y V del punto.

Decimos que dos funciones $f \in \mathcal{C}(U)$ y $g \in \mathcal{C}(V)$ tiene el mismo germen en el punto x si existe un tercer entorno $W \subset U \cap V$ de x que cumple $f_{|W} = g_{|W}$. Esta definición establece una relación de equivalencia en el conjunto

$$\{\bigcup \mathcal{C}(U) \text{ donde } U \text{ es abierto y contiene a } x\}$$

El conjunto cociente lo denotamos $\mathcal{C}_x$ y decimos que el anillo de gérmenes en el punto x (comprobar que se puede dotar de estructura de anillo). Existe un morfismo natural de $\mathcal{C}(U)$ en $\mathcal{C}_x$ que asocia a cada función su germen en el punto (y es morfismo de anillos). En este caso la aplicación es siempre epiyectiva, como se deduce de los teoremas de extensión de funciones continuas. Esta propiedad es propia de este ejemplo y no es cierta en general. Es más, en los ejemplos más importantes de geometría algebraica será falso.

Para denotar uno de los elementos de la clase empleamos la notación (f, U), donde f denota la función y U el abierto donde está definida. Llamamos valor del germen (f, U) en el punto x a $f(x)$. Esta definición no depende del representante tomado. Consideramos ahora los gérmenes que se anulan en el punto x

$$\mathfrak{m}_x = \{f \in \mathcal{C}_x \text{ tales que } f(x) = 0\}$$

Este conjunto es un ideal maximal del anillo. Además es el único ideal maximal que posee, puesto que si un germen no se anula en el punto entonces es invertible (si $f(x) \neq 0$ la función $1/f$ es continua en un entorno del punto).

La teoría de haces y prehaces se puede estudiar sobre cualquier categoría, sin embargo nosotros daremos la definición para haces de grupos abelianos. Las generalizaciones y particularizaciones no son difíciles.

Definición B.1 *Sea X un espacio topológico. Un* prehaz *$\mathcal{F}$ de grupos abelianos sobre X consta de los siguientes ingredientes:*

- *A cada abierto $U \subset X$ se le asocia un grupo abeliano $\mathcal{F}(U)$.*
- *Para cada inclusión de abiertos $V \subset U$ se define un morfismo de grupos*

$$\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$$

Los grupos y los morfismos asociados deben verificar las siguientes condiciones:

- $\mathcal{F}(\varnothing) = \{0\}$ *(grupo abeliano trivial).*
- ρ_{UU} *es la identidad del grupo* $\mathcal{F}(U)$.
- *Para cada inclusión de abiertos* $W \subset V \subset U$ *se cumple que* $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.

Si en la definición cambiamos grupos abelianos por anillos obtenemos un prehaz de anillos y lo mismo con cualquier otra estructura.

Ejemplos

- Sea X un espacio topológico arbitrario. Sea $\mathcal{F}(U)$ el conjunto de funciones continuas de U en $\mathbb{R}$. Los morfismos restricción son la restricción de funciones. Hemos contruido un prehaz de anillos sobre X.
- Sea $X = \mathbb{R}^n$ o en general una variedad diferenciable. Al abierto U le asignamos el anillo de las funciones infinitamente diferenciables $\mathcal{C}^\infty(U)$. Los morfismos restricción son los habituales. Hemos construido otro prehaz de anillos.
- Sea X una superficie de Riemann. A cada abierto U de X le asociamos el anillo de las funciones holomorfas, que denotamos $\mathcal{O}(U)$. Dado un germen (f, V), por el principio de prolongación analítica se puede extender de modo único dicha función a abiertos cada vez mayores. Sin embargo muchas veces dichas prolongaciones presentaran polos y no será posible encontrar una función definida en toda la superficie, que siga siendo holomorfa y que extienda al germen. Es más, si la superficie es compacta las únicas funciones holomorfas definidas en toda la variedad son las constantes. Esta situación es la más habitual en geometría algebraica.

- En los dos ejemplos anteriores $\mathcal{F}(U)$ es un subconjunto del anillo de funciones de dominio U y que tienen como imagen el conjunto $\mathbb{R}$. Eligiendo otra característica de las funciones que se conserve por restricción obtenemos nuevos prehaces. Pero todos estos tiene una característica común: $\mathcal{F}(U)$ está formado por funciones cuyo espacio de llegada es siempre el mismo.

- Sea $\pi : Y \to X$ una aplicación continua y epiyectiva. Una **sección** sobre un abierto $U \subset X$ es una aplicación continua $s : U \to Y$ que cumple $\pi \circ s = \mathrm{Id}_U$. El conjunto de todas las secciones sobre U lo denotamos $\Gamma(U, Y)$. Asociando a cada abierto U el conjunto $\Gamma(U, Y)$ tenemos un prehaz de conjuntos sobre el espacio X, con los morfismos restricción evidentes. En todos los casos se cumple que $s(x) \in \pi^{-1}(x)$.

- Dada una aplicación $\pi : Y \to X$ continua y epiyectiva los subconjuntos de la forma $\pi^{-1}(x)$ se llaman **fibras** de la proyección. En principio fibras de puntos distintos pueden ser también distintas. Dar el conjunto Y es equivalente a dar el conjunto de todas las fibras. Obsérvese que una sección s sobre U se puede entender como una función con dominio U pero cuyo espacio de llegada "varía" con el punto. Notemos la analogía con las "funciones" que nos aparecen en el estudio del espectro. Esto parece inducirnos a pensar que en realidad los elementos del anillo son más bien secciones que funciones.

- Si cada fibra tiene una estructura de grupo, podemos sumar secciones, sumando punto a punto. Lo mismo es cierto con otras operaciones. En principio nada nos asegura que partiendo de secciones continuas, la suma sea también una sección continua, pero en muchos casos interesantes esto será cierto y el conjunto $\Gamma(U, Y)$ tendrá una estructura algebraica.

- Sea X arbitrario y A un anillo también arbitrario. Asociamos a cada abierto el anillo A (salvo al vacío que le asociamos el anillo nulo) y $\rho_{UV} = \mathrm{Id}_A$.

- Sea A un anillo arbitrario. Lo dotamos de la topología discreta. Denotamos por $\mathcal{C}(U, A)$ al conjunto de funciones continuas de U en A. Esta construcción es un prehaz de anillos. No es difícil demostrar que si U es conexo entonces $\mathcal{C}(U, A)$ es isomorfo a A.

- Sea $V \subset \mathbb{A}^n$ una variedad algebraica irreducible y $k(V)$ su anillo de funciones. Dado un abierto U decimos que una función $f : U \to k$ es regular en el punto x si existen elementos $g, h \in k(V)$ y un entorno abierto V de x tal que $f(y) = g(y)/h(y)$ para todo elemento $y \in V$ (en particular estamos exigiendo que $h(y) \neq 0$ en todo punto de V). Decimos que la función es regular en U si es regular en todos sus puntos. No es difícil comprobar que el conjunto de funciones regulares en U es un anillo. Por construcción si una función es regular en un abierto, necesariamente su restricción es también regular. Esto dota a toda variedad algebraica de un prehaz.

- $\mathrm{Spec}(A) = \{\mathfrak{p} \subset A$ tales que $\mathfrak{p}$ es un ideal primo$\}$.
- Si I es ideal $\mathcal{V}(I) = \{\mathfrak{p}$ tales que $I^{o} subset \mathfrak{p}\}$.
- $\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$.
- $\mathcal{V}(\sum I_i) = \bigcap \mathcal{V}(I_i)$.
- $\mathcal{V}(I) \subset \mathcal{V}(J)$ si y solo si $\mathrm{rad}(J) \subset \mathrm{rad}(I)$.
- Topología de Zariski: Cerrados de la forma $\mathcal{V}(I)$ con I ideal de A.
- $\mathcal{O}(U) =$ secciones sobre U que localmente son cocientes de elementos de A.
- $\mathcal{O}$ es un haz, por estar definido localmente.
- Llamamos epectro al conjunto $\mathrm{Spec}(A)$ junto con el haz de anillos.
- $D(f) = \mathcal{V}(f)^c$. Forman base de abiertos.
- $\mathcal{O}_{\mathfrak{p}} = A_{\mathfrak{p}}$
- $\mathcal{O}(D(f)) = A_f$.
- En particular $\mathcal{O}(X) = A$.
- Espacio anillado. Espacio topológico y haz de anillos.
- Morfismo de espacios anillados. $f : X \to Y$ y $f^{\#} : \mathcal{O}_Y \to f_*(\mathcal{O}_X)$.
- Si la fibra es un anillo local, espacio localmente anillado.
- Morfismo de espacios localmente anillados. $f^{\#}$ es un morfismo local

$$f^{\#}_{\mathfrak{p}} : \mathcal{O}_{Y,f(p)} \to \mathcal{O}_{X,p}$$

- $\varphi : A \to B$ es local si $\varphi^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$.
- Isomorfismo. Si f es un homeomorfismo y $f^{\#}$ es isomorfismo de haces.

- $\mathrm{Spec}(A), \mathcal{O}$ es un espacio localmente anillado.
- Si $\varphi : A \to B$ es de anillos se induce $\varphi^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ de espacios anillodos localmente.
- Cada morfismo de espacios anillados locales deriva de un único morfismo de anillos.
- Esquema afín.
- Esquema. Haz estructural.
- Morfismo de esquemas. Morfismo de espacios localmente anillados.
- Línea afín.
- Plano afín.
- Pegado de esquemas.