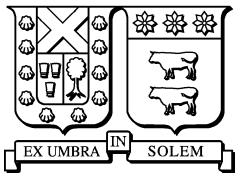
Universidad Técnica Federico Santa María
Departamento de Matemática
Valparaíso - Chile



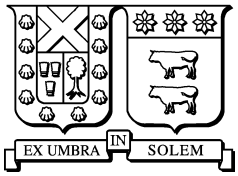
Introducción a la teoría de los esquemas afines

Tesis presentada por
Felipe Andrés Valladares Cornejo
como requisito parcial para optar al grado de
Magíster en Ciencias Mención Matemática

Director de tesis
Gabriele Ranieri
Codirector de tesis
Pedro Montero

enero, 2020

Universidad Técnica Federico Santa María
Departamento de Matemática
Valparaíso - Chile



Introducción a la teoría de los esquemas afines

Tesis presentada por
Felipe Andrés Valladares Cornejo
como requisito parcial para optar al grado de
Magíster en Ciencias Mención Matemática

Director de tesis
Gabriele Ranieri
Codirector de tesis
Pedro Montero

Examinadores
Sebastián Herrero
Pontificia Universidad Católica de Valparaíso
Leonelo Iturriaga
Universidad Técnica Federico Santa María

enero, 2020

Agradecimientos

Este trabajo no habría sido posible sin la enorme ayuda del profesor Gabriele Ranieri, quien sin tener ninguna obligación de recibir alumnos provenientes de alguna universidad ajena a la suya, tuvo la gentileza de acogerme y asumir el rol de mi profesor tutor.

Esta tesis fue financiada por el Proyecto Fondecyt Regular número 1140946.

A mi familia.

Resumen

En la primera parte de esta tesis se presentan y discuten algunos resultados importantes de la teoría de los esquemas afines. Se define el espectro primo de un anillo conmutativo con identidad y se analizan sus características como espacio topológico. Por otro lado, se presenta una breve introducción a la teoría de los haces, la cual servirá para luego construir el haz estructural de anillos conmutativos sobre el espacio topológico Spec(R). De esta manera, se entrega la noción de esquema afín como un espacio topológico vinculado a un haz de anillos conmutativos.

La segunda parte de este trabajo se basa en algunas aplicaciones de la teoría de los esquemas a las áreas de la geometría algebraica y la teoría de números. Se examinan ejemplos relacionados con curvas algebraicas, puntos regulares y singulares. Por último, se utilizan las herramientas de la teoría de los esquemas para realizar un estudio detallado acerca de las características del anillo $\mathbb{Z}[\sqrt{3}]$.

Abstract

In the first part of this thesis, some important results on affine scheme theory are presented and discussed. The prime spectrum of a commutative ring with identity is defined and its properties as a topological space are analyzed. On the other hand, a brief introduction to sheaf theory is presented, which will be useful for building the structural sheaf of commutative rings on the topological space Spec(R). In this sense, the notion of an affine scheme as a topological space linked to a sheaf of commutative rings is given.

The second part of this work is based on some applications of the scheme theory on algebraic geometry and number theory. Examples related to algebraic curves, regular and singular points are examined. Finally, the tools given by scheme theory are used to make a full research about the properties of the ring $\mathbb{Z}[\sqrt{3}]$.

Índice general

Capítulo 1

Introducción

El propósito de esta tesis es entregar las nociones básicas de la teoría de los esquemas afines. Para ello, expondremos y explicaremos varios resultados importantes en este ámbito. Hacia el final de esta tesis aplicaremos estas nuevas herramientas en ejemplos específicos relacionados con geometría algebraica y teoría de números. Las primeras definiciones y algunas aplicaciones importantes se pueden encontrar en varios textos clásicos, como aquellos escritos por Hartshorne [1], Eisenbud [2] y Ueno [3]. Sin embargo, estos libros (y muchos otros más) son extremadamente densos de leer, su enfoque es sumamente abstracto y muchos de los conceptos clave no son decantados en ejemplos concretos. Por estas razones es que esta tesis también tiene como objetivo dar una lectura más amigable a estas nuevas ideas. Nos detendremos a profundizar algunas definiciones cruciales, e ilustraremos con ejemplos cercanos cuando sea necesario.

Las bases de esta teoría fueron establecidas por el matemático Alexander Grothendieck en la década de 1960 y sus resultados significaron un gran avance en el desarrollo de la geometría algebraica moderna. La gran mayoría de los algebristas contemporáneos a Grothendieck, tales como David Mumford, David Eisenbud y Michael Artin (entre muchos otros), adoptaron este nuevo lenguaje a pesar de su profunda abstracción y difícil absorción. Actualmente, muchos artículos científicos que tratan temas de geometría algebraica y teoría de números ocupan estas técnicas innovadoras.

En términos muy generales, la geometría algebraica clásica es el estudio de las soluciones de los sistemas de ecuaciones polinómicas sobre algún espacio afín o proyectivo, es decir, es el estudio

de las variedades algebraicas. Muchos de los problemas que surgen en este campo son aquellos denominados "problemas de clasificación" y cuyo objetivo consiste en clasificar todas las posibles variedades algebraicas, salvo isomorfismo, que satisfagan alguna condición específica. No obstante, es muy común que este tipo de problemas sean tan difíciles de resolver que quizás nadie esperaría poder resolverlos cabalmente. La teoría de los esquemas es una primera aproximación para poder clasificar nuestros objetos geométricos. La idea básica es reemplazar el espacio geométrico clásico por el álgebra de funciones sobre este espacio, o incluso, de manera más general, por algún conjunto de funciones de este espacio hacia otro. Una de las ventajas de esta generalización es la posibilidad de extender las mismas técnicas de la geometría algebraica clásica hacia objetos más generales que, desde un punto de vista tradicional, podrían no ser considerados como variedades propiamente tales.

Geométricamente, existen varias razones por las cuales es necesario trabajar con objetos más generales que las variedades algebraicas. Una de ellas hace referencia a la ventaja que nos otorga contar con una definición de variedad algebraica que sea independiente de cualquier incrustación de ella en algún espacio proyectivo. En este punto podemos hacer una comparación con la teoría de grupos. Originalmente, los matemáticos del siglo XIX concebían el concepto de grupo como algún subconconjuto del conjunto de permutaciones de un conjunto, el cual debe ser cerrado bajo composiciones e inversiones. Claramente es mucho más conveniente contar con una definición abstracta de grupo, y luego de ello estudiar todas las posibles maneras que incrustarlo en algún grupo de permutaciones. Desde este punto de vista podremos analizar, por ejemplo, si dos grupos son o no isomorfos, sin necesidad de preocuparnos por alguna incrustación en particular.

Otro ejemplo elemental que ilustra la utilidad de los esquemas tiene relación con la clasificación de las cónicas (curvas planas cuadráticas) en $\mathbb{R}^2$. Desde una mirada muy rudimentaria, las cónicas se pueden agrupar en tres grandes categorías: están las "agradables" (parábolas, elipses e hipérbolas), las "razonablemente degeneradas" (dos rectas distintas que se intersectan o dos rectas distintas y paralelas) y las "extrañamente degeneradas" (una recta doble, un punto o el conjunto vacío). Cualquier persona sensata podría incluso llegar a pensar que los objetos pertenecientes esta última categoría no deberían ser considerados como cónicas propiamente tales. Ahora bien, si observamos esta categorización desde una mirada esquemática, será completamente claro y revelador que todas las cónicas se ajustan al mismo molde. La teoría de los esquemas nos permitirá concluir que aquellas cónicas "extrañamente degeneradas" son esencialmente las mismas que las "agradables" o incluso que las "razonablemente degeneradas". De todas las cónicas "extrañamente degeneradas", las rectas

dobles son especialmente difíciles de explicar sin el uso de la teoría de los esquemas, mientras que las otras dos cónicas de esta misma categoría son una consecuencia de que $\mathbb{R}$ no es un cuerpo algebraicamente cerrado.

De manera resumida, un esquema afín X es el conjunto $X = \mathrm{Spec}(R)$ de ideales primos de un anillo conmutativo con identidad R al cual dotamos de la llamada *topología de Zariski* y de un *haz estructural* $\mathcal{O}_X$. Por ejemplo, si R es una $\mathbb{C}-$álgebra finitamente generada, entonces $R \cong \mathbb{C}[x_1, \ldots, x_n]/I$ donde el ideal $I = (f_1, \ldots, f_r)$ está generado por finitos polinomios (teorema de la base de Hilbert). En este caso, gracias al teorema de los ceros de Hilbert, tenemos que el conjunto $Y = \mathrm{Specm}(R)$ de ideales maximales de R está en biyección con el conjunto de soluciones

$$V(I) = \{a \in \mathbb{C}^n \mid f_1(a) = \ldots = f_r(a) = 0\},$$

el cual es llamado una *variedad algebraica afín*. En la literatura clásica, la topología de Zariski se construye al declarar que los conjuntos cerrados corresponden a ceros de polinomios. Además, cada abierto de Zariski U en $V(I)$ puede ser asociado con su correspondiente $\mathbb{C}-$álgebra $\mathcal{O}_X(U)$ de *funciones regulares*, es decir, funciones que lucen localmente como cociente de funciones polinomiales. La asignación (functorial) $U \mapsto \mathcal{O}_X(U)$ es un ejemplo de lo que conocemos como un *haz*. Del mismo modo que una variedad diferenciable está determinada por sus abiertos y sus correspondientes coordenadas locales (o, equivalentemente, su haz de funciones diferenciables), es natural esperar que una variedad algebraica afín esté determinada por sus abiertos de Zariski y su haz de funciones regulares.

La generalización del ejemplo anterior a anillos conmutativos con identidad arbitrarios, así como su aplicación a situaciones concretas en teoría de números mediante diversos y novedosos ejemplos, es el principal problema de esta tesis. En particular, al considerar $X = \mathrm{Spec}(R)$ en lugar de $Y = \mathrm{Specm}(R)$ obtenemos un espacio topológico más grande cuya estructura debe ser comprendida. Del mismo modo, por el hecho de que R no sea necesariamente una álgebra finitamente generada sobre un cuerpo, resulta más delicado definir lo que deber ser el haz de funciones regulares.

Por último, existe una razón muy potente para generalizar nuestro concepto de variedad algebraica. Con el fin de aclararla, supongamos que queremos entender las soluciones enteras de la ecuación $x^n + y^n = z^n$. Es ampliamente sabido que determinar una solución general de esta ecuación es

sumamente difícil. Además, es natural atacar este tipo de problemas mediante dos mecanismos: en primer lugar, considerar qué sucede con esta ecuación sobre $\mathbb{C}$, y en segundo lugar, estudiar sus soluciones al reducirla módulo algún primo p. Estos procedimientos nos facilitan el análisis de este tipo de ecuaciones y asimismo nos clarifican el comportamiento de sus soluciones enteras. No obstante, también podemos enfrentar este tipo de problemas desde un punto de vista esquemático (¡y con muy buenos resultados!). Sin ir muy lejos, la demostración del último teorema de Fermat fue publicada por Andrew Wiles en 1995 y en gran parte de su trabajo se utilizan herramientas relacionadas con la teoría de los esquemas. Esta nueva noción ha servido de amalgama entre la geometría algebraica y la teoría de números, ya que nos permite generalizar el concepto de variedad algebraica a cualquier anillo conmutativo, sin la necesidad de remitirnos exclusivamente a un cuerpo algebraicamente cerrado.

Capítulo 2

Esquemas

2.1. Espectro primo

A lo largo de este capítulo, R denotará un anillo conmutativo con identidad.

Definición 2.1.1. El *espectro primo* de R corresponde a

$$\mathrm{Spec}(R) = \{P \subset R \mid P \text{ es un ideal primo de } R\}.$$

Un elemento $P \in \mathrm{Spec}(R)$ se llamará un *punto* de $\mathrm{Spec}(R)$.

Ejemplo 2.1.2. Los ideales primos de $\mathbb{Z}$ son $\{0\}$ o $p\mathbb{Z}$, donde $p \in \mathbb{Z}$ es primo. Luego,

$$\mathrm{Spec}(\mathbb{Z}) = \{\{0\}, 2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}, \ldots\}.$$

Ejemplo 2.1.3. Sea k un cuerpo algebraicamente cerrado. Los ideales primos de $k[x]$ son $\{0\}$, o bien $(x-a)k[x]$ con $a \in k$. Por lo tanto,

$$\mathrm{Spec}(k[x]) = \{\{0\}\} \cup \{(x-a)k[x] \mid a \in k\}.$$

A continuación, analizaremos algunos resultados de álgebra conmutativa, los cuales tendrán por objetivo final la caracterización del conjunto $\mathrm{Spec}\,(\mathbb{Z}[x])$.

Proposición 2.1.4. *Sea $f : R \to S$ un homomorfismo de anillos conmutativos con identidad. Si P es un ideal primo de S, entonces $f^{-1}(P)$ también es un ideal primo de R.*

Demostración. Recordemos que

$$f^{-1}(P) = \{r \in R \mid f(r) \in P\}.$$

Sean $r, s \in f^{-1}(P)$, es decir, $f(r), f(s) \in P$. Además, elijamos arbitrariamente $a \in R$. Dado que P es un ideal de S, podemos notar que $f(r-s) = f(r) - f(s) \in P$ y $f(ar) = f(a)f(r) \in P$, por lo que $r - s \in f^{-1}(P)$, $ar \in f^{-1}(P)$ y $f^{-1}(P)$ es ciertamente un ideal de R.

Para probar que este ideal es primo, notemos en primer lugar que $f^{-1}(P) \neq R$, ya que el caso contrario implicaría que $f(1) = 1 \in P$, una contradicción. En segundo lugar, supongamos que $a, b \in R$ son tales que $ab \in f^{-1}(P)$. Luego, $f(ab) = f(a)f(b) \in P$. Dado que P es un ideal primo de S, necesariamente tenemos que $f(a) \in P$ o $f(b) \in P$, o escrito de manera equivalente, $a \in f^{-1}(P)$ o $b \in f^{-1}(P)$. ♦

Proposición 2.1.5. *Sea $f : R \to S$ un homomorfismo sobreyectivo de anillos conmutativos con identidad. Si P es un ideal primo de R tal que $\ker(f) \subset P$, entonces $f(P)$ es un ideal primo de S.*

Demostración. Recordemos que

$$f(P) = \{f(r) \in S \mid r \in P\}.$$

Sean $r, s \in f(P)$, es decir, existirán $a, b \in P$ tales que $r = f(a)$ y $s = f(b)$. Por otro lado, elijamos cualquier $t \in S$. Dado que f es un homomorfismo sobreyectivo, existirá $c \in R$ tal que $t = f(c)$. Como P es un ideal de R, podemos notar que $r - s = f(a) - f(b) = f(a-b) \in f(P)$ y $rt = f(a)f(c) = f(ac) \in f(P)$. Por lo tanto, $f(P)$ es efectivamente un ideal de S.

Para probar que $f(P)$ es un ideal primo de S, en primer lugar notemos que $f(P) \neq S$, ya que el caso contrario nos dice que existiría $r \in P$ tal que $f(r) = 1$. Además, dado que $f(1) = 1$, tendríamos que $f(r-1) = f(r) - f(1) = 1 - 1 = 0$, por lo que $r - 1 \in \ker(f) \subset P$. En vista de que $r \in P$ y $r - 1 \in P$, concluiríamos que $1 \in P$, una contradicción. En segundo lugar, tomemos $u, v \in S$ tales que $uv \in f(P)$, esto es, existirá $z \in P$ tal que $uv = f(z)$. Nuevamente, como f es sobreyectivo, existirán $x, y \in R$ tales que $u = f(x)$ y $v = f(y)$. Así, $f(z - xy) = f(z) - f(x)f(y) = f(z) - uv = 0$, por lo que $z - xy \in \ker(f) \subset P$. Dado que $z \in P$, necesariamente $xy \in P$. Como P es primo,

tenemos que $x \in P$ o $y \in P$. Finalmente, $u = f(x) \in f(P)$ o $v = f(y) \in f(P)$. ♦

Corolario 2.1.6. *Sea R un anillo conmutativo con identidad e I un ideal de R. Los ideales primos de R/I están en biyección con aquellos ideales primos P de R tales que $I \subset P$ bajo la aplicación $P \leftrightarrow P/I$.*

Demostración. Por el cuarto teorema del isomorfismo de anillos (ver [4], página 246), la aplicación $P \leftrightarrow P/I$ es efectivamente una biyección entre los ideales P de R que contienen a I y los ideales de R/I.

Sea $\pi : R \to R/I$ el homomorfismo de proyección natural. Notemos que π es un homomorfismo sobreyectivo y además $\ker(\pi) = I \subset P$. Por las proposiciones 2.1.4 y 2.1.5, P es un ideal primo de R si y solamente si $\pi(P) = P/I$ también lo es. ♦

Definición 2.1.7. Sea S algún subconjunto de R tal que $0 \notin S$. Diremos que S es un conjunto *multiplicativamente cerrado* si cada vez que $a, b \in S$, entonces $ab \in S$.

Proposición 2.1.8. *Si R es un dominio de integridad, entonces el conjunto $S = R - \{0\}$ es un conjunto multiplicativamente cerrado.*

Demostración. El resultado se obtiene directamente de la definición de dominio de integridad. Si $a, b \in R$ son tales que $a \neq 0$ y $b \neq 0$, entonces $ab \neq 0$. ♦

Definición 2.1.9. Sea S un subconjunto multiplicativamente cerrado de R. Sobre el conjunto $R \times S$ definimos la siguiente relación de equivalencia.

$$(r_1, s_1) \sim (r_2, s_2) \;\Leftrightarrow\; \text{existe } s' \in S \text{ tal que } s'(r_1 s_2 - r_2 s_1) = 0.$$

Cuando S no contenga a ningún divisor de cero en R, la última relación se simplifica como $r_1 s_2 = r_2 s_1$, pues $s' \neq 0$. Si denotamos por $\dfrac{r}{s}$ a la clase de equivalencia de $(r, s) \in R \times S$, podemos definir las siguientes operaciones sobre el conjunto cociente $(R \times S)/\sim$.

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \quad \text{y} \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

Estas operaciones no dependen del representante de cada clase de equivalencia y quedan bien definidas. Además, si $s \in S$, la clase $\dfrac{0}{s}$ es neutro para la suma y la clase $\dfrac{s}{s}$ es neutro para la multiplicación. Con esta construcción, $(R \times S)/\sim$ puede ser dotado con estructura de anillo

conmutativo con identidad y por simplicidad lo denotaremos como

$$S^{-1}R = \left\{ \frac{r}{s} \;\middle|\; r \in R \text{ y } s \in S \right\} \cong (R \times S)/\sim .$$

Este anillo se conoce comúnmente como *anillo de fracciones* de R con respecto a S. En particular, si R es un dominio de integridad y $S = R - \{0\}$, entonces $S^{-1}R$ se conoce como *cuerpo de fracciones* de R.

Si fijamos algún elemento $s \in S$, obtenemos un homomorfismo natural

$$\begin{array}{rccc} \varphi: & R & \to & S^{-1}R \\ & r & \mapsto & \dfrac{rs}{s}. \end{array}$$

Dado que para todos $s_1, s_2 \in S$ se cumple $\dfrac{rs_1}{s_1} = \dfrac{rs_2}{s_2}$, el homomorfismo anterior no depende de la elección de $s \in S$.

Proposición 2.1.10. *Sea R un anillo conmutativo con identidad y $S \subset R$ un conjunto multiplicativamente cerrado que no contenga divisores de cero. Si P es un ideal primo de R tal que $P \cap S = \emptyset$, entonces $S^{-1}P$ es un ideal primo de $S^{-1}R$.*

Demostración. Sea P un ideal primo de R tal que $P \cap S = \emptyset$. Es necesario verificar que

(i) $S^{-1}P$ es un ideal de $S^{-1}R$;

(ii) $S^{-1}P$ está propiamente contenido en $S^{-1}R$;

(iii) $S^{-1}P$ es un ideal primo de $S^{-1}R$.

Demostraremos estas afirmaciones.

(i) Sean $p_1, p_2 \in P$ y $s_1, s_2 \in S$ tales que $\dfrac{p_1}{s_1}, \dfrac{p_2}{s_2} \in S^{-1}P$. Si elegimos cualquier elemento de la forma $\dfrac{r}{s} \in S^{-1}R$, podemos observar que

$$\frac{p_1}{s_1} - \frac{p_2}{s_2} = \frac{p_1 s_2 - p_2 s_1}{s_1 s_2} \in S^{-1}P \quad \text{y} \quad \frac{r}{s} \cdot \frac{p_1}{s_1} = \frac{r p_1}{s s_1} \in S^{-1}P.$$

Por consiguiente, $S^{-1}P$ es un ideal de $S^{-1}R$.

(ii) Supongamos que $S^{-1}P = S^{-1}R$ y elijamos $s \in S$. Luego, $\frac{s}{s} \in S^{-1}R = S^{-1}P$, por lo que existirán $p \in P$ y $s' \in S$ tales que

$$\frac{s}{s} = \frac{p}{s'} \Leftrightarrow ss' = sp \Leftrightarrow s(s'-p) = 0.$$

Dado que $s \neq 0$ y éste no tiene divisores de cero en R, necesariamente concluimos que $p = s' \in P \cap S$, una contradicción. Por lo tanto, $S^{-1}P \neq S^{-1}R$.

(iii) Sean $r_1, r_2 \in R$, $s_1, s_2 \in S$ tales que $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} \in S^{-1}P$. Luego, existirán $p \in P$ y $s \in S$ tales que

$$\frac{r_1 r_2}{s_1 s_2} = \frac{p}{s} \Leftrightarrow r_1 r_2 s = s_1 s_2 p \in P.$$

Como $r_1 r_2 s \in P$ y P es un ideal primo de R, tenemos tres opciones.

$$r_1 \in P \quad \text{o} \quad r_2 \in P \quad \text{o} \quad s \in P.$$

La última opción es imposible, ya que $P \cap S = \emptyset$. Luego, concluimos que $\frac{r_1}{s_1} \in S^{-1}P$ o $\frac{r_2}{s_2} \in S^{-1}P$, y por ende, $S^{-1}P$ es un ideal primo de $S^{-1}R$. ♦

Proposición 2.1.11. *Sea R un anillo conmutativo con identidad y $S \subset R$ un conjunto multiplicativamente cerrado que no contenga divisores de cero. Luego, aquellos ideales primos $P \subset R$ tales que $P \cap S = \emptyset$ están en biyección con los ideales primos de $S^{-1}R$ mediante la aplicación $P \leftrightarrow S^{-1}P$.*

Demostración. En la proposición 2.1.10 hemos demostrado que la aplicación

$$\begin{aligned} \{\text{Ideales primos } P \subset R \text{ tales que } P \cap S = \emptyset\} &\to \{\text{Ideales primos de } S^{-1}R\} \\ P &\mapsto S^{-1}P \end{aligned}$$

está bien definida. Solo resta probar que ella es una biyección.

(i) Sean I y J ideales primos de R tales que $I \cap S = J \cap S = \emptyset$ y $S^{-1}I = S^{-1}J$. Si elegimos cualesquier elementos $a \in I$ y $s \in S$, tendremos que $\frac{a}{s} \in S^{-1}I = S^{-1}J$, por lo que existirán $b \in J$ y $s' \in S$ tales que

$$\frac{a}{s} = \frac{b}{s'} \Leftrightarrow as' = bs \in J.$$

Como $as' \in J$ y J es un ideal primo de R, necesariamente sucederá que $a \in J$ o $s' \in J$. Esta

última opción es imposible, ya que $J \cap S = \emptyset$. De esta manera, concluimos que $I \subset J$.

De manera análoga podremos probar que $J \subset I$, por lo que $I = J$ y la aplicación en cuestión es inyectiva.

(ii) Sea J un ideal primo de $S^{-1}R$. Si fijamos $s \in S$, podemos constuir el siguiente homomorfismo de anillos conmutativos con identidad.

$$\begin{array}{rccc} \varphi: & R & \to & S^{-1}R \\ & r & \mapsto & \dfrac{rs}{s}. \end{array}$$

Gracias a la proposición 2.1.4, sabemos que $I = \varphi^{-1}(J)$ es un ideal primo de R.

Supongamos que existe $s' \in I \cap S$. Luego, $\varphi(s') = \dfrac{s's}{s} \in J$, lo cual es una contradicción, ya que esta última fracción es un elemento invertible en $S^{-1}R$ y no puede formar parte de J. En consecuencia, tenemos que $I \cap S = \emptyset$.

A continuación, probaremos que $S^{-1}I = J$. Sean $r \in I$ y $s' \in S$ tales que $\dfrac{r}{s'} \in S^{-1}I$. Observemos que $\varphi(r) = \dfrac{rs}{s} \in J$, por lo que

$$\frac{rs}{s} = \frac{r}{s'} \cdot \frac{s's}{s} \in J.$$

Como J es un ideal primo de $S^{-1}R$, necesariamente sucederá que $\dfrac{r}{s'} \in J$ o $\dfrac{s's}{s} \in J$. Esta última opción es imposible, ya que la fracción $\dfrac{s's}{s}$ es un elemento invertible en $S^{-1}R$. Es por esta razón que $S^{-1}I \subset J$.

Por otro lado, sean $r \in R$ y $s' \in S$ tales que $\dfrac{r}{s'} \in J$. En este caso, necesariamente tendremos que $r \in I$, ya que J es un ideal de $S^{-1}R$ y

$$\varphi(r) = \frac{rs}{s} = \frac{r}{s'} \cdot \frac{s's}{s} \in J.$$

Por consiguiente, $\dfrac{r}{s'} \in S^{-1}I$, lo cual nos permite concluir que $J \subset S^{-1}I$.

Finalmente, y dado que $S^{-1}I = J$, podemos afirmar que la aplicación en cuestión es sobreyectiva.

♦

Ejemplo 2.1.12. Los ideales primos de $\mathbb{Z}[x]$ son

(i) $\{0\}$;

(ii) $p\mathbb{Z}[x]$, donde $p \in \mathbb{Z}$ es primo;

(iii) $f(x)\mathbb{Z}[x]$, donde $f(x) \in \mathbb{Z}[x]$ es un polinomio irreducible sobre $\mathbb{Z}[x]$;

(iv) $p\mathbb{Z}[x] + f(x)\mathbb{Z}[x]$, donde $p \in \mathbb{Z}$ es primo y $f(x) \in \mathbb{Z}[x]$ es tal que su reducción módulo el ideal $p\mathbb{Z}[x]$ es no constante e irreducible sobre $(\mathbb{Z}/p\mathbb{Z})[x]$.

Es de rutina probar que todos los ideales de la lista anterior son efectivamente ideales primos. Por lo tanto, resta verificar que la lista anterior está completa. Para ello, llamemos $R = \mathbb{Z}[x]$ y sea P un ideal primo de R. Es evidente que $P \cap \mathbb{Z}$ es un ideal propio de $\mathbb{Z}$. Más aún, si elegimos $a, b \in \mathbb{Z}$ tales que $ab \in P \cap \mathbb{Z}$, entonces $ab \in P$. Como P es primo, concluimos que $a \in P$ o $b \in P$. Puesto que a y b son enteros, deducimos que $a \in P \cap \mathbb{Z}$ o $b \in P \cap \mathbb{Z}$, y $P \cap \mathbb{Z}$ es, de hecho, un ideal primo.

Por consiguiente, hay dos opciones para $P \cap \mathbb{Z}$.

1. Si $P \cap \mathbb{Z} = \{0\}$, entonces $P \cap S = \emptyset$, donde $S = \mathbb{Z} - \{0\}$. Dado que S es un conjunto multiplicativamente cerrado y sin divisores de cero, podemos construir el anillo de fracciones

$$S^{-1}R = S^{-1}\mathbb{Z}[x] = \left\{ \frac{f(x)}{n} \;\middle|\; f(x) \in \mathbb{Z}[x] \;\text{ y }\; n \in \mathbb{Z} - \{0\} \right\} = \mathbb{Q}[x].$$

   De la proposición 2.1.11, sabemos que existe una biyección entre los ideales primos P de R tales que $P \cap S = \emptyset$ y los ideales primos de $S^{-1}R = \mathbb{Q}[x]$ dada por $P \leftrightarrow S^{-1}P$.

   De esta manera, podemos distinguir dos casos.

   (i) $S^{-1}P = \{0\} \;\Leftrightarrow\; P = \{0\}$.

   (ii) $S^{-1}P = f(x)\mathbb{Q}[x]$, donde $f(x) \in \mathbb{Q}[x]$ es un polinomio no constante e irreducible en $\mathbb{Q}[x]$. Podemos asumir sin pérdida de generalidad que $f(x) \in \mathbb{Z}[x]$ y que el m.c.d. de todos los coeficientes de $f(x)$ es 1, ya que siempre es posible multiplicar $f(x)$ por alguna fracción apropiada para que ello suceda. Por el lema de Gauss (ver [4], página 303), tendremos que $f(x)$ será irreducible sobre $\mathbb{Z}[x]$.

   Observemos que $P = f(x)\mathbb{Z}[x]$ es un ideal primo de R. Además, dado que $f(x)$ es un

polinomio no constante, es directo que $P \cap S = \emptyset$. Por otro lado, notemos que

$$S^{-1}P = \left\{ \frac{f(x)g(x)}{n} \in \mathbb{Q}[x] \;\middle|\; g(x) \in \mathbb{Z}[x] \text{ y } n \in \mathbb{Z} - \{0\} \right\}$$

$$S^{-1}P = \{f(x)g(x) \in \mathbb{Q}[x] \mid g(x) \in \mathbb{Q}[x]\}$$

$$S^{-1}P = f(x)\mathbb{Q}[x].$$

Por lo tanto, $P = f(x)\mathbb{Z}[x]$ es aquel único ideal primo de R que satisface $P \cap S = \emptyset$ y que se encuentra en biyección con $S^{-1}P$.

2. $P \cap \mathbb{Z} = p\mathbb{Z}$, para algún $p \in \mathbb{Z}$ primo. Dado que $p \in P$ y P es un ideal de $\mathbb{Z}[x]$, podemos plantear que

$$p\mathbb{Z}[x] \subset P \subset \mathbb{Z}[x].$$

Según el corolario 2.1.6, sabemos que los ideales primos P que contienen a $p\mathbb{Z}[x]$ están en biyección con aquellos ideales primos del anillo $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong (\mathbb{Z}/p\mathbb{Z})[x]$ mediante la aplicación $P \leftrightarrow P/p\mathbb{Z}[x]$. Dado que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo y $(\mathbb{Z}/p\mathbb{Z})[x]$ es un dominio de ideales principales, nuevamente podemos distinguir dos casos.

(i) $P/p\mathbb{Z}[x] = \{0\} \Leftrightarrow P = p\mathbb{Z}[x]$.

(ii) $P/p\mathbb{Z}[x] = \overline{f(x)}\,(\mathbb{Z}/p\mathbb{Z})[x]$ para algún polinomio $\overline{f(x)} \in (\mathbb{Z}/p\mathbb{Z})[x]$ no constante e irreducible sobre $(\mathbb{Z}/p\mathbb{Z})[x]$. En este caso, aquel único ideal que satisface $p\mathbb{Z}[x] \subset P$ y que se encuentra en biyección con $\overline{f(x)}\,(\mathbb{Z}/p\mathbb{Z})[x]$ corresponde precisamente a $P = p\mathbb{Z}[x] + f(x)\mathbb{Z}[x]$, donde $f(x) \in \mathbb{Z}[x]$ es tal que su reducción módulo el ideal $p\mathbb{Z}[x]$ coincide con $\overline{f(x)}$.

2.2. La topología de Zariski

Podemos definir una topología sobre $\mathrm{Spec}(R)$ de la siguiente manera. Dado un ideal I de R definimos el subconjunto $V(I)$ de $\mathrm{Spec}(R)$ como

$$V(I) = \{P \in \mathrm{Spec}(R) \mid I \subset P\}.$$

Proposición 2.2.1. *Sea Λ algún conjunto de índices (posiblemente infinito). Si I, J e I_λ, con*

$\lambda \in \Lambda$, son ideales de R, entonces

(i) $V(\{0\}) = \mathrm{Spec}(R)$ *y* $V(R) = \emptyset$*;*

(ii) $V(I) \cup V(J) = V(I \cap J)$*;*

(iii) $\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V\Big(\sum_{\lambda\in\Lambda} I_\lambda\Big)$.

Acá, $\sum_{\lambda\in\Lambda} I_\lambda$ *corresponde al ideal generado por la colección de ideales* $\{I_\lambda\}_{\lambda\in\Lambda}$.

Demostración.

(i) Es directo de la definición.

$$V(\{0\}) = \{P \in \mathrm{Spec}(R) \mid \{0\} \subset P\} = \mathrm{Spec}(R)$$
$$V(R) = \{P \in \mathrm{Spec}(R) \mid R \subset P\} = \emptyset.$$

(ii) Sea $P \in V(I) \cup V(J)$. Luego, $P \in V(I)$ o $P \in V(J)$. Si sucede lo primero, entonces $I \cap J \subset I \subset P$. Si sucede lo segundo, entonces $I \cap J \subset J \subset P$. En cualquier caso sucede $I \cap J \subset P$, o dicho de manera equivalente, $P \in V(I \cap J)$.

Ahora elijamos $P \in V(I \cap J)$, es decir, $I \cap J \subset P$. Si $P \in V(I)$, entonces no hay nada que probar. Si $P \notin V(I)$, entonces $I \not\subset P$ y existirá $a \in I$ tal que $a \notin P$. Observemos que para cualquier elección de $r \in J$ tenemos que $ar \in I \cap J \subset P$. Dado que P es un ideal primo y $a \notin P$, necesariamente sucederá que $r \in P$. Por ende, $J \subset P$ y $P \in V(J)$. De esta manera concluimos que $P \in V(I) \cup V(J)$.

(iii) Sea $P \in \bigcap_{\lambda\in\Lambda} V(I_\lambda)$, es decir, para todo $\lambda \in \Lambda$ se cumple que $P \in V(I_\lambda)$. Lo anterior es equivalente a afirmar que para todo $\lambda \in \Lambda$ tenemos que $I_\lambda \subset P$. A su vez, esta proposición equivale a decir que el ideal generado por $\{I_\lambda\}_{\lambda\in\Lambda}$ también está contenido en P. En otras palabaras, $\sum_{\lambda\in\Lambda} I_\lambda \subset P$ y $P \in V\Big(\sum_{\lambda\in\Lambda} I_\lambda\Big)$. ♦

Gracias a la proposición 2.2.1, podemos construir una topología sobre $\mathrm{Spec}(R)$ al considerar que cualquier conjunto cerrado tenga la forma $V(I)$, donde I es algún ideal de R. Por consiguiente, los

conjuntos abiertos serán de la forma

$$D(I) = V(I)^c = \{P \in \text{Spec}(R) \mid I \not\subset P\}.$$

La topología recién descrita sobre $\text{Spec}(R)$ se conoce como *topología de Zariski*.

Proposición 2.2.2. *Sean $f \in R$ y $D(f) = \{P \in \text{Spec}(R) \mid f \notin P\}$. Luego, para cualquier ideal I de R,*

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

(ii) si $I = (f_1, f_2, \ldots, f_m)$, *entonces* $D(I) = \bigcup_{j=1}^{m} D(f_j)$.

Acá, $(f_1, f_2, \ldots, f_m)$ *denota el ideal de R generado por* $\{f_1, f_2, \ldots, f_m\}$.

Demostración.

(i) Sea $P \in D(I)$, es decir, $I \not\subset P$. Luego, existe un elemento $f \in I$ tal que $f \notin P$. De esta forma, $P \in D(f) \subset \bigcup_{f \in I} D(f)$.

A la inversa, sea $P \in \bigcup_{f \in I} D(f)$. Luego, existe $f \in I$ tal que $P \in D(f)$, o dicho de otra manera, $f \notin P$. Por ende, $I \not\subset P$ y $P \in D(I)$.

(ii) De la parte (i) es directo que $\bigcup_{j=1}^{m} D(f_j) \subset \bigcup_{f \in I} D(f) = D(I)$. Tomemos $P \in D(I)$, esto es, $I \not\subset P$. Necesariamente existirá algún $j \in \{1, 2, \ldots, m\}$ tal que $f_j \notin P$, ya que en caso contrario, si $f_j \in P$ para todo j, entonces $I \subset P$ y llegamos a una contradicción. De esta forma, $P \in D(f_j) \subset \bigcup_{j=1}^{m} D(f_j)$. ♦

La proposición 2.2.2 nos permite concluir que la familia de conjuntos abiertos $\{D(f) \mid f \in R\}$ forma una base para la topología de $\text{Spec}(R)$. Incluso, si R es un anillo noetheriano, entonces cualquier conjunto abierto puede ser recubierto por una cantidad finita de los abiertos basales $D(f)$.

Ejemplo 2.2.3. Describiremos la topología de Spec($\mathbb{Z}$). Sea $I = n\mathbb{Z}$ el ideal generado por $n \neq 0$ en $\mathbb{Z}$. Podemos descomponer n en factores primos distintos como $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Es así que

$$V(I) = \{P \in \text{Spec}(\mathbb{Z}) \mid I \subset P\} = \{p_1\mathbb{Z}, p_2\mathbb{Z}, \ldots, p_r\mathbb{Z}\}.$$

En otras palabras, cualquier conjunto cerrado en Spec($\mathbb{Z}$) está formado por una cantidad finita de puntos distintos de $\{0\}$. Sin embargo, $\{\{0\}\}$ no es cerrado, ya que si lo fuera, debería existir un ideal $I = m\mathbb{Z}$ tal que $V(I) = \{\{0\}\}$. Lo anterior implica que $m\mathbb{Z} \subset \{0\}$ y $m = 0$. Pero $V(\{0\}) = \text{Spec}(\mathbb{Z})$, una contradicción. Es más, la clausura de $\{\{0\}\}$ es Spec($\mathbb{Z}$) y $\{0\}$ es un punto denso en Spec($\mathbb{Z}$).

Cada vez que un punto sea denso en Spec(R) lo llamaremos *punto genérico*.

Ejemplo 2.2.4. Sea k un cuerpo algebraicamente cerrado. Describiremos la topología de Spec($k[x]$). Como $k[x]$ es un dominio de ideales principales, sea $I = p(x)k[x]$ el ideal generado por $p(x) \neq 0$ en $k[x]$. Podemos factorizar $p(x)$ como

$$p(x) = \beta(x - a_1)^{\alpha_1}(x - a_2)^{\alpha_2} \cdots (x - a_r)^{\alpha_r}.$$

Al igual que en el caso de Spec($\mathbb{Z}$), tendremos

$$V(I) = \{(x - a_1)k[x], (x - a_2)k[x], \ldots, (x - a_r)k[x]\}.$$

A cualquier elemento $a \in k$ podemos asociar el punto $(x - a)k[x] \in \text{Spec}(k[x])$ y el subconjunto $\{(x - a)k[x]\}$ será cerrado en Spec($k[x]$). No obstante, $\{\{0\}\}$ no es cerrado en Spec($k[x]$); de hecho es un punto genérico.

Proposición 2.2.5. *Un homomorfismo de anillos conmutativos $\varphi : R \to S$ induce una función*

$$\begin{array}{rccc} \varphi^{\#} : & \text{Spec}(S) & \to & \text{Spec}(R) \\ & P & \mapsto & \varphi^{-1}(P) \ , \end{array}$$

la cual es continua para la topología de Zariski.

Demostración. Dado que $\varphi^{-1}(P)$ es un ideal primo de R para cualquier ideal primo P de S, $\varphi^{\#}$ es una función bien definida (ver proposición 2.1.4).

Sea $V(I)$ un conjunto cerrado en $\mathrm{Spec}(R)$ donde I es algún ideal de R. Luego,

$$\begin{aligned}\left(\varphi^{\#}\right)^{-1}(V(I)) &= \{P \in \mathrm{Spec}(S) \mid \varphi^{\#}(P) \in V(I)\} \\ &= \{P \in \mathrm{Spec}(S) \mid \varphi^{-1}(P) \in V(I)\} \\ &= \{P \in \mathrm{Spec}(S) \mid I \subset \varphi^{-1}(P)\} \\ &= \{P \in \mathrm{Spec}(S) \mid \varphi(I) \subset P\}.\end{aligned}$$

Dado que $\varphi(I)$ no es necesariamente un ideal de S, podemos considerar J aquel ideal en S generado por $\varphi(I)$. Así, $\varphi(I) \subset P$ si y solamente si $J \subset P$ y

$$\left(\varphi^{\#}\right)^{-1}(V(I)) = \{P \in \mathrm{Spec}(S) \mid J \subset P\} = V(J).$$

Dicho de otra manera, la preimagen por $\varphi^{\#}$ de cualquier cerrado en $\mathrm{Spec}(R)$ es un cerrado en $\mathrm{Spec}(S)$. En consecuencia, $\varphi^{\#}$ es una función continua para la topología de Zariski. ♦

Ejemplo 2.2.6. Consideremos el homomorfismo de anillos $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ dado por $f(x) \mapsto f(1)$. Este homomorfismo inducirá la función

$$\begin{array}{rccc}\varphi^{\#}: & \mathrm{Spec}\,(\mathbb{Z}) & \to & \mathrm{Spec}\,(\mathbb{Z}[x]) \\ & P & \mapsto & \varphi^{-1}(P).\end{array}$$

Si consideramos $P = p\mathbb{Z} \subset \mathbb{Z}$, con $p \in \mathbb{Z}$ primo, entonces

$$\varphi^{-1}(P) = \{f(x) \in \mathbb{Z}[x] \mid f(1) \in p\mathbb{Z}\}.$$

Notemos que los polinomios $f(x) = p$ y $g(x) = x - 1$ satisfacen $f(1), g(1) \in p\mathbb{Z}$, por lo que $f(x), g(x) \in \varphi^{-1}(P)$. Como este último conjunto es un ideal primo de $\mathbb{Z}[x]$, por la caracterización realizada en el ejemplo 2.1.12 podemos concluir que

$$\varphi^{-1}(P) = p\mathbb{Z}[x] + (x-1)\mathbb{Z}[x].$$

Por otro lado, si consideramos $Q = \{0\} \subset \mathbb{Z}$, entonces

$$\varphi^{-1}(Q) = \{f(x) \in \mathbb{Z}[x] \mid f(1) = 0\}.$$

Podemos notar que ningún polinomio constante pertenece a $\varphi^{-1}(Q)$, salvo el polinomio nulo.

Además, $g(x) = x - 1$ satisface $g(1) = 0$, por lo que $g(x) \in \varphi^{-1}(Q)$. De esta manera,

$$\varphi^{-1}(Q) = (x-1)\mathbb{Z}[x].$$

Finalmente, podemos definir explícitamente la función $\varphi^{\#}$ como

$$\begin{array}{rccl} \varphi^{\#}: & \operatorname{Spec}(\mathbb{Z}) & \to & \operatorname{Spec}(\mathbb{Z}[x]) \\ & p\mathbb{Z} & \mapsto & p\mathbb{Z}[x] + (x-1)\mathbb{Z}[x] \\ & \{0\} & \mapsto & (x-1)\mathbb{Z}[x]. \end{array}$$

Según la proposición 2.2.5, esta función es continua para las respectivas topologías de Zariski de los espacios $\operatorname{Spec}(\mathbb{Z})$ y $\operatorname{Spec}(\mathbb{Z}[x])$.

Utilizaremos la siguiente notación. Si llamamos $X = \operatorname{Spec}(R)$ y elegimos $f \in R$, entonces X_f denotará el conjunto

$$X_f = D(f) = \{P \in \operatorname{Spec}(R) \mid f \notin P\}.$$

Proposición 2.2.7. *Dada una familia $\{f_\lambda\}_{\lambda\in\Lambda}$ de elementos en R, la igualdad*

$$X = \bigcup_{\lambda\in\Lambda} X_{f_\lambda}$$

se satisface si y solamente si el ideal generado por $\{f_\lambda\}_{\lambda\in\Lambda}$ coincide con R.

Demostración. Supongamos que la igualdad se cumple. Luego, para cualquier ideal primo $P \in X = \operatorname{Spec}(R)$, existirá algún $\lambda \in \Lambda$ tal que $P \in X_{f_\lambda} = D(f_\lambda)$, esto es, $f_\lambda \notin P$. De esta manera, el ideal J generado por $\{f_\lambda\}_{\lambda\in\Lambda}$ no puede estar contenido en ningún ideal primo P, lo cual implica que $J = R$.

Ahora a la inversa, supongamos que el ideal J generado por $\{f_\lambda\}_{\lambda\in\Lambda}$ coincide con R. Entonces, dado cualquier ideal primo $P \in X = \operatorname{Spec}(R)$, existirá algún $\lambda \in \Lambda$ tal que $f_\lambda \notin P$. Es decir, $P \in D(f_\lambda) = X_{f_\lambda}$ y se cumplirá que

$$X \subset X_{f_\lambda} \subset \bigcup_{\lambda\in\Lambda} X_{f_\lambda}.$$ ♦

Corolario 2.2.8. *El espacio topológico $X = \operatorname{Spec}(R)$ es casi−compacto. Es decir, dado un cubri-*

miento abierto de X de la forma

$$X = \bigcup_{\lambda \in \Lambda} U_\lambda$$

podemos extraer una cantidad finita de abiertos U_{λ_j} desde $\{U_\lambda\}_{\lambda \in \Lambda}$ de modo que

$$X = \bigcup_{j=1}^{m} U_{\lambda_j}.$$

Utilizamos la palabra "casi−compacto"porque X no es necesariamente Hausdorff.

Demostración. Por la proposición 2.2.2, cualquier conjunto abierto de X es unión de conjuntos de la forma $D(f) = X_f$. Luego, todo recubrimiento de X por conjuntos abiertos se podrá representar como

$$X = \bigcup_{\lambda \in \Lambda} X_{f_\lambda},$$

donde $f_\lambda \in R$ y Λ es algún conjunto de índices. Por la proposición 2.2.7, tendremos que R coincide con el ideal generado por $\{f_\lambda\}_{\lambda \in \Lambda}$. De esta manera, encontraremos $\lambda_1, \lambda_2, \ldots, \lambda_r \in \Lambda$ tales que

$$\sum_{j=1}^{r} g_{\lambda_j} f_{\lambda_j} = 1,$$

donde $g_{\lambda_1}, g_{\lambda_2}, \ldots, g_{\lambda_r} \in R$. Es por esto que R queda generado por $\{f_{\lambda_1}, f_{\lambda_2}, \ldots, f_{\lambda_r}\}$ y gracias a la proposición 2.2.2 podemos concluir que

$$D(R) = X = \bigcup_{j=1}^{r} D\left(f_{\lambda_j}\right) = \bigcup_{j=1}^{r} X_{f_{\lambda_j}}. \qquad \blacklozenge$$

Ejemplo 2.2.9. El conjunto $\{(0)\}$ no es cerrado en $\mathrm{Spec}(\mathbb{Z})$. Es por esto que $\mathrm{Spec}(\mathbb{Z})$ no es Hausdorff, ya que ni siquiera cumple con el axioma T_1 de separabilidad (ver [5], página 99).

De manera general, si $\mathrm{Spec}(R)$ contiene un punto genérico, entonces este espacio no será Hausdorff.

Ejemplo 2.2.10. Los únicos ideales propiamente contenidos en $\mathbb{Z}/6\mathbb{Z}$ son $\left\{\overline{0}\right\}$, $2\mathbb{Z}/6\mathbb{Z}$ y $3\mathbb{Z}/6\mathbb{Z}$. Además, los ideales $2\mathbb{Z}/6\mathbb{Z}$ y $3\mathbb{Z}/6\mathbb{Z}$ son maximales, y por ende, ellos también son primos. Sin embargo, el ideal $\left\{\overline{0}\right\}$ no es primo, ya que $\overline{2} \cdot \overline{3} = \overline{0}$. Luego,

$$\mathrm{Spec}\left(\mathbb{Z}/6\mathbb{Z}\right) = \left\{2\mathbb{Z}/6\mathbb{Z}, 3\mathbb{Z}/6\mathbb{Z}\right\}.$$

Observemos que $\{2\mathbb{Z}/6\mathbb{Z}\}$ es un conjunto cerrado en $\mathrm{Spec}\,(\mathbb{Z}/6\mathbb{Z})$, ya que

$$V\,(2\mathbb{Z}/6\mathbb{Z}) = \{P \in \mathrm{Spec}\,(\mathbb{Z}/6\mathbb{Z}) \mid 2\mathbb{Z}/6\mathbb{Z} \subset P\} = \{2\mathbb{Z}/6\mathbb{Z}\}\,.$$

Por razones análogas, podemos afirmar que $\{3\mathbb{Z}/6\mathbb{Z}\}$ es un conjunto cerrado en $\mathrm{Spec}\,(\mathbb{Z}/6\mathbb{Z})$. De esta manera, dado que $\mathrm{Spec}\,(\mathbb{Z}/6\mathbb{Z})$ es un conjunto finito en donde cada singletón es un conjunto cerrado, podemos concluir que él está dotado de la topología discreta y es, evidentemente, Hausdorff.

Por supuesto, podemos generalizar el resultado anterior. Afirmamos que para todo $n \in \mathbb{Z}$, $\mathrm{Spec}\,(\mathbb{Z}/n\mathbb{Z})$ es un espacio topológico discreto, y por ende, Hausdorff. Para probar esta afirmación, consideraremos dos casos.

- Si n fuera primo, entonces $\mathbb{Z}/n\mathbb{Z}$ sería un cuerpo y $\mathrm{Spec}\,(\mathbb{Z}/n\mathbb{Z}) = \left\{\left\{\overline{0}\right\}\right\}$, el cual es claramente discreto.
- Si n no fuera primo, entonces podemos descomponerlo en factores primos distintos como $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Los ideales primos de $\mathbb{Z}/n\mathbb{Z}$ corresponden precisamente a $p_1\mathbb{Z}/n\mathbb{Z}$, $p_2\mathbb{Z}/n\mathbb{Z}$, $\ldots$, $p_r\mathbb{Z}/n\mathbb{Z}$, por lo que

  $$\mathrm{Spec}\,(\mathbb{Z}/n\mathbb{Z}) = \{p_1\mathbb{Z}/n\mathbb{Z}\ ,\ p_2\mathbb{Z}/n\mathbb{Z}\ ,\ \ldots\ ,\ p_r\mathbb{Z}/n\mathbb{Z}\}\,.$$

  Observemos que $\{p_1\mathbb{Z}/n\mathbb{Z}\}$ es un conjunto cerrado en $\mathrm{Spec}\,(\mathbb{Z}/n\mathbb{Z})$, ya que

  $$V\,(p_1\mathbb{Z}/n\mathbb{Z}) = \{P \in \mathrm{Spec}\,(\mathbb{Z}/n\mathbb{Z}) \mid p_1\mathbb{Z}/n\mathbb{Z} \subset P\} = \{p_1\mathbb{Z}/n\mathbb{Z}\}\,.$$

  Por razones análogas, podemos concluir que $\{p_2\mathbb{Z}/n\mathbb{Z}\}$, $\ldots$, $\{p_r\mathbb{Z}/n\mathbb{Z}\}$ son todos conjuntos cerrados en $\mathrm{Spec}\,(\mathbb{Z}/n\mathbb{Z})$. Finalmente, dado que $\mathrm{Spec}\,(\mathbb{Z}/n\mathbb{Z})$ es un conjunto finito en donde cada singletón es cerrado, concluimos que la topología de Zariski coincide efectivamente con la topología discreta.

Proposición 2.2.11. *Sea J un ideal primo de R. Entonces, el conjunto $\{J\}$ es cerrado en $X = \mathrm{Spec}(R)$ si y solamente si J es un ideal maximal de R.*

Demostración. Supongamos que J es un ideal maximal de R. Dado que J también es un ideal primo, tenemos que

$$V(J) = \{P \in \mathrm{Spec}(R) \mid J \subset P\} = \{J\},$$

por lo que $\{J\}$ es un conjunto cerrado en $X = \mathrm{Spec}(R)$.

Supongamos ahora que J no es maximal. Elijamos arbitrariamente algún conjunto cerrado $V(I) \subset X$ tal que $J \in V(I)$, esto es, $I \subset J$. Dado que J no es maximal, existirá algún ideal maximal $M \subset R$ tal que $J \subset M$ y $J \neq M$. M también es un ideal primo, por lo que $I \subset J \subset M$ y $M \in V(I)$. En conclusión, cualquier conjunto cerrado que contenga a J deberá contener al menos dos elementos, y por ende $\{J\}$ no podrá ser un conjunto cerrado en X. ♦

2.3. Teoría básica de haces

Definición 2.3.1. Sea X un espacio topológico. Un *prehaz de anillos conmutativos* $\mathcal{F}$ sobre X es una regla que asocia a cada abierto $U \subset X$ un anillo conmutativo $\mathcal{F}(U)$, y cada inclusión de conjuntos abiertos $U \supset V$ va vinculada con un homomorfismo de anillos conmutativos $\rho_{U,V} : \mathcal{F}(U) \to \mathcal{F}(V)$. Esta construcción debe satisfacer los siguientes tres axiomas.

(i) $\mathcal{F}(\emptyset)$ es el anillo nulo;

(ii) Para todo abierto $U \subset X$, $\rho_{U,U} = \mathrm{id}_{\mathcal{F}(U)}$;

(iii) Para cualquier elección de abiertos $U \supset V \supset W$ de X, $\rho_{U,W} = \rho_{V,W} \circ \rho_{U,V}$.

Los elementos de $\mathcal{F}(U)$ se conocen como las *secciones* de $\mathcal{F}$ sobre U, mientras que los homomorfismos de anillos conmutativos $\rho_{U,V}$ se denominan *funciones de restricción*.

Ejemplo 2.3.2. Sea X cualquier espacio topológico. A cada abierto $U \subset X$ no vacío asociamos el anillo conmutativo con identidad

$$\mathcal{F}(U) = \{f : U \to \mathbb{R} \mid f \text{ es continua}\}.$$

Además, para cada inclusión de conjuntos abiertos no vacíos $U \supset V$ definimos

$$\begin{array}{rccc} \rho_{U,V} : & \mathcal{F}(U) & \to & \mathcal{F}(V) \\ & f & \mapsto & f|_V \, . \end{array}$$

Podemos verificar de manera directa que $\mathcal{F}$ es un prehaz de anillos conmutativos con identidad sobre X.

Motivados por este ejemplo utilizaremos una notación un poco más sugerente: dada la inclusión $U \supset V$, para cada $s \in \mathcal{F}(U)$ anotaremos $s|_V$ en lugar de $\rho_{U,V}(s)$.

Definición 2.3.3. Consideremos X un espacio topológico y $\mathcal{F}$ un prehaz de anillos conmutativos sobre X. Diremos que $\mathcal{F}$ es un *haz de anillos conmutativos* sobre X si se satisfacen los siguientes dos axiomas: dado un conjunto abierto $U \subset X$ y $\{U_i \mid i \in I\}$ un cubrimiento de U por conjuntos abiertos,

(i) si dos secciones $s, t \in \mathcal{F}(U)$ son tales que $s|_{U_i} = t|_{U_i}$ para todo $i \in I$, entonces $s = t$;

(ii) si $\{s_i \in \mathcal{F}(U_i) \mid i \in I\}$ es un sistema de secciones con la propiedad $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ para cada pareja $i, j \in I$, entonces existe una sección $s \in \mathcal{F}(U)$ tal que $s|_{U_i} = s_i$ para todo $i \in I$. Por el axioma (i), tal sección s es única.

Ejemplo 2.3.4. El prehaz del ejemplo 2.3.2 es, de hecho, un haz de anillos conmutativos con identidad sobre X. Consideremos un abierto no vacío $U \subset X$ y un cubrimiento de U por abiertos no vacíos $\{U_i \mid i \in I\}$. Si dos funciones continuas $f, g : U \to \mathbb{R}$ son tales que $f|_{U_i} = g|_{U_i}$ para todo $i \in I$, entonces ellas coinciden sobre todo U y $f = g$. Igualmente, si contamos con el sistema de funciones continuas $f_i : U_i \to \mathbb{R}$ tales que $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ cada vez que $U_i \cap U_j \neq \emptyset$, entonces podremos fabricar una nueva función f "pegando" de manera continua en aquellos abiertos donde ellas coincidan (ver [5], página 108). Más explícitamente, definimos $f(x) = f_i(x)$ cuando $x \in U_i$. Esta función está bien definida (no depende de la elección de U_i en caso que x pertenezca a dos o más abiertos del cubrimiento) y es continua.

Ejemplo 2.3.5. Si D es un abierto conexo de $\mathbb{C}$, podemos definir el *haz de funciones holomorfas* sobre D como el haz de anillos conmutativos con identidad $\mathcal{O}$ cuyas secciones sobre algún abierto $U \subset D$ no vacío son todas las funciones $f : U \to \mathbb{C}$ holomorfas.

En general, podemos seguir esta misma construcción sobre cualquier variedad compleja.

Ejemplo 2.3.6. Consideremos el conjunto $X = \{0, 1\}$ junto con la topología discreta y sea $\mathcal{F}$ un haz sobre X. Los abiertos $\{0\}$ y $\{1\}$ no nos aportan información acerca de $\mathcal{F}$, ya que cualquier cubrimiento de ellos por abiertos no vacíos es trivial.

Pues bien, consideremos el cubrimiento $\{\{0\},\{1\}\}$ de X. Sea $f_0 \in \mathcal{F}(\{0\})$ y $f_1 \in \mathcal{F}(\{1\})$. Dado que existe una única sección sobre el conjunto vacío, tenemos que

$$f_0|_{\{0\}\cap\{1\}} = f_0|_\emptyset = f_1|_\emptyset = f_1|_{\{0\}\cap\{1\}}\,.$$

Luego, por los axiomas de haz, existe una única sección g sobre X tal que $g|_{\{0\}} = f_0$ y $g|_{\{1\}} = f_1$. Es decir, $\mathcal{F}(X)$ es igual a $\mathcal{F}(\{0\}) \times \mathcal{F}(\{1\})$ y las funciones de restricción corresponden simplemente a las funciones de proyección en cada coordenada.

De manera más precisa, si elegimos R_0 y R_1 dos anillos conmutativos, podemos definir el haz $\mathcal{F}$ como

$$\mathcal{F}(\emptyset) = \{0\} \quad , \quad \mathcal{F}(\{0\}) = R_0 \quad , \quad \mathcal{F}(\{1\}) = R_1 \quad \text{y} \quad \mathcal{F}(\{0,1\}) = R_0 \times R_1,$$

mientras que las funciones de restricción corresponden a

$$\begin{array}{rccc} \rho_{\emptyset,\emptyset}: & \{0\} & \to & \{0\} \\ & 0 & \mapsto & 0 \end{array} \qquad \begin{array}{rccc} \rho_{\{0\},\emptyset}: & R_0 & \to & \{0\} \\ & a & \mapsto & 0 \end{array} \qquad \begin{array}{rccc} \rho_{\{1\},\emptyset}: & R_1 & \to & \{0\} \\ & b & \mapsto & 0 \end{array}$$

$$\begin{array}{rccc} \rho_{X,\emptyset}: & R_0 \times R_1 & \to & \{0\} \\ & (a,b) & \mapsto & 0 \end{array} \qquad \begin{array}{rccc} \rho_{\{0\},\{0\}}: & R_0 & \to & R_0 \\ & a & \mapsto & a \end{array} \qquad \begin{array}{rccc} \rho_{\{1\},\{1\}}: & R_1 & \to & R_1 \\ & b & \mapsto & b \end{array}$$

$$\begin{array}{rccc} \rho_{X,\{0\}}: & R_0 \times R_1 & \to & R_0 \\ & (a,b) & \mapsto & a \end{array} \qquad \begin{array}{rccc} \rho_{X,\{1\}}: & R_0 \times R_1 & \to & R_1 \\ & (a,b) & \mapsto & b \end{array} \qquad \begin{array}{rccc} \rho_{X,X}: & R_0 \times R_1 & \to & R_0 \times R_1 \\ & (a,b) & \mapsto & (a,b). \end{array}$$

En general, si Y es cualquier espacio topológico discreto, entonces $\mathcal{F}(Y) = \prod_{y\in Y} \mathcal{F}(\{y\})$, mientras que las funciones de restricción corresponden a todas las proyecciones en cada coordenada.

Observación 2.3.7. Podemos dar una definición paralela de prehaz como functor contravariante (ver Anexo A). Dado X un espacio topológico podemos considerar la categoría X_{Top} cuyos objetos son todos los abiertos $U \subset X$. Además, dados U y V abiertos de X definimos el conjunto

$$\mathrm{Hom}(U,V) = \begin{cases} \{\mathrm{incl} : V \to U\} & \text{si} \quad U \supset V \\ \emptyset & \text{si} \quad U \not\supset V, \end{cases}$$

donde incl es la función de inclusión. Así pues, un prehaz de anillos conmutativos sobre X es simplemente un functor contravariante $\mathcal{F}$ el cual a cada objeto U de la categoría X_{Top} le asocia un anillo conmutativo $\mathcal{F}(U)$, y en caso de que $U \supset V$, asocia al morfismo incl : $V \to U$ el homomorfismo

de anillos conmutativos $\rho_{U,V} : \mathcal{F}(U) \to \mathcal{F}(V)$.

2.4. El haz estructural sobre $X = \mathrm{Spec}(R)$

El objetivo de esta sección es construir un haz sobre el espacio topológico $X = \mathrm{Spec}(R)$.

Lema 2.4.1. *Sea $f \in R$. Luego,*

$$\sqrt{(f)} = \bigcap_{\substack{P \in Spec(R) \\ f \in P}} P.$$

Acá, $\sqrt{(f)}$ denota el radical del ideal generado por f, es decir,

$$\sqrt{(f)} = \{h \in R \mid h^n = af, \text{ para algunos } n \in \mathbb{N} \text{ y } a \in R\}.$$

Demostración. Sea $h \in \sqrt{(f)}$, es decir, existirán $n \in \mathbb{N}$ y $a \in R$ tales que $h^n = af$. Si elegimos cualquier ideal primo $P \subset R$ tal que $f \in P$, entonces $h^n \in P$. Como P es primo, necesariamente tendremos que $h \in P$. De esta manera, $h \in \bigcap_{\substack{P \in \mathrm{Spec}(R) \\ f \in P}} P$.

Ahora elijamos $h \in \bigcap_{\substack{P \in \mathrm{Spec}(R) \\ f \in P}} P$ y supongamos que ninguna potencia de h pertenece al ideal (f). Podemos construir la siguiente familia de ideales.

$$\mathcal{S} = \{I \subset R \mid I \text{ es un ideal de } R \text{ tal que } f \in I \text{ y } h^n \notin I, \forall n \in \mathbb{N}\}.$$

Observemos que $\mathcal{S} \neq \emptyset$ ya que $(f) \in \mathcal{S}$ según nuestra asunción inicial. Además, $\mathcal{S}$ es un conjunto parcialmente ordenado bajo la relación de inclusión. Si elegimos cualquier subconjunto totalmente ordenado $\mathcal{T}$ de $\mathcal{S}$, entonces se puede probar de manera rutinaria que $J = \bigcup_{I \in \mathcal{T}} I$ es una cota superior de $\mathcal{T}$ en $\mathcal{S}$. Por el lema de Zorn, deberá existir un elemeto maximal $Q \in \mathcal{S}$.

A continuación probaremos que este ideal Q debe ser primo. Supongamos que existen $a, b \in R$ tales que $a, b \notin Q$ y $ab \in Q$. Dado que Q es maximal en $\mathcal{S}$, los ideales (a, Q) y (b, Q) no pertenecen a $\mathcal{S}$. Por la definición de $\mathcal{S}$ existirán $n, m \in \mathbb{N}$ tales que $h^n \in (a, Q)$ y $h^m \in (b, Q)$. A su vez, existirán $r_1, r_2 \in R$ y $q_1, q_2 \in Q$ tales que $h^n = ar_1 + q_1$ y $h^m = br_2 + q_2$. En vista de que $ab \in Q$, podremos

concluir que

$$h^{n+m} = h^n \cdot h^m = (ar_1 + q_1)(br_2 + q_2) = abr_1r_2 + ar_1q_2 + br_2q_1 + q_1q_2 \in Q.$$

Hemos llegado a una contradicción, ya que Q es un elemento de $\mathcal{S}$ el cual no puede contener a ninguna potencia de h. Con ello probamos que Q es efectivamente un ideal primo.

Finalmente, y en vista de que Q es un ideal primo de R que contiene a f, concluimos que $h \in \bigcap_{\substack{P \in \mathrm{Spec}(R) \\ f \in P}} P \subset Q$, una nueva contradicción. En consecuencia, deberá existir alguna potencia de h que pertenezca a (f), es decir, $h \in \sqrt{(f)}$. ♦

Lema 2.4.2. *Sea $X = \mathrm{Spec}(R)$. Entonces, para todos $f, g \in R$ se cumple que*

(i) $X_f \cap X_g = X_{fg}$;

(ii) $X_f \supset X_g$ *si y solamente si* $g \in \sqrt{(f)}$.

Demostración.

(i) $P \in X_f \cap X_g$ es equivalente a decir que $f \notin P$ y $g \notin P$. Como P es un ideal primo de R, lo anterior se cumple si y solo si $fg \notin P$, esto es, si $P \in X_{fg}$.

(ii) Por el lema 2.4.1, la proposición $g \notin \sqrt{(f)}$ es equivalente a

$$g \notin \bigcap_{\substack{P \in \mathrm{Spec}(R) \\ f \in P}} P \;\Leftrightarrow\; g \in \bigcup_{\substack{P \in \mathrm{Spec}(R) \\ f \in P}} R - P.$$

Esta última afirmación equivale a aseverar que existe $P \in \mathrm{Spec}(R)$ tal que $f \in P$ y $g \notin P$. En otras palabras, existe $P \notin X_f$ tal que $P \in X_g$, vale decir, $X_f \not\supset X_g$. ♦

Ejemplo 2.4.3. En $X = \mathrm{Spec}(\mathbb{Z})$ tenemos que $X_{36} \supset X_{30}$, ya que

$$X_{36} = X - \{2\mathbb{Z}, 3\mathbb{Z}\} \quad \text{y} \quad X_{30} = X - \{2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}\}.$$

Además, $30 \in \sqrt{(36)} = 6\mathbb{Z}$, verificando el resultado del lema 2.4.2.

Observación 2.4.4. Si llamamos $X = \text{Spec}(R)$, tomemos $f \in R$ un elemento nilpotente. Entonces f está contenido en cualquier ideal primo P, ya que si $f \notin P$, entonces $f^m \notin P$ para todo $m \in \mathbb{N}$ y ninguna potencia de f será nula, llegando a una contradicción. Así, $X_f = \emptyset$.

Por otro lado, a partir del lema 2.4.1, tenemos que

$$\sqrt{(0)} = \{f \in R \mid f^n = 0 \text{ para algún } n \in \mathbb{N}\} = \bigcap_{P \in \text{Spec}(R)} P$$

y podemos observar que si f pertenece a todos los ideales primos $P \subset R$, entonces f debe ser nilpotente. O de manera equivalente, si f no es nilpotente, entonces existe algún ideal primo $P \subset R$ tal que $f \notin P$, y en consecuencia, $X_f \neq \emptyset$.

Proposición 2.4.5. *Si $f \in R$ es un elemento no nilpotente, entonces el conjunto*

$$S = \{f, f^2, f^3, \ldots, f^m, f^{m+1}, \ldots\}$$

es multiplicativamente cerrado.

Proposición 2.4.6. *Si P es un ideal primo de R, entonces $S = R - P$ es un conjunto multiplicativamente cerrado.*

Demostración. Si $a, b \notin P$, entonces $ab \notin P$, ya que P es un ideal primo de R. ♦

Definición 2.4.7. Sea $f \in R$ un elemento no nilpotente. Denotaremos por $\mathcal{R}_f$ al conjunto $S^{-1}R$ considerando el conjunto multiplicativamente cerrado $S = \{f, f^2, \ldots, f^m, f^{m+1}, \ldots\}$.

De manera análoga, si P es un ideal primo de R, denotaremos por $\mathcal{R}_P$ al conjunto $S^{-1}R$ considerando $S = R - P$.

Explícitamente,

$$\mathcal{R}_f = \left\{ \frac{r}{f^m} \;\middle|\; r \in R \text{ y } m \in \mathbb{N} \right\} \quad \text{y} \quad \mathcal{R}_P = \left\{ \frac{r}{s} \;\middle|\; r \in R \text{ y } s \notin P \right\}.$$

El anillo $\mathcal{R}_P$ se conoce comúnmente con la *localización de R en P*.

Ejemplo 2.4.8. En $X = \text{Spec}(\mathbb{Z})$ se tiene

$$\mathcal{R}_6 = \left\{ \frac{r}{6^m} \;\middle|\; r \in \mathbb{Z} \text{ y } m \in \mathbb{N} \right\} \quad \text{y} \quad \mathcal{R}_{36} = \left\{ \frac{s}{36^k} \;\middle|\; s \in \mathbb{Z} \text{ y } k \in \mathbb{N} \right\}.$$

Podemos notar que estos anillos son isomorfos, ya que la función

$$\begin{array}{rccc} \rho: & \mathcal{R}_6 & \to & \mathcal{R}_{36} \\ & \dfrac{r}{6^m} & \mapsto & \dfrac{r\cdot 6^m}{36^m} \end{array}$$

es un isomorfismo de anillos conmutativos con identidad. Para probar este hecho, tomemos dos elementos $\dfrac{r}{6^m}$ y $\dfrac{t}{6^n}$ en el anillo $\mathcal{R}_6$. Observemos que

$$\begin{aligned} \rho\left(\frac{r}{6^m}+\frac{t}{6^n}\right) &= \rho\left(\frac{r\cdot 6^n + t\cdot 6^m}{6^{m+n}}\right) \\ &= \frac{(r\cdot 6^n + t\cdot 6^m)\cdot 6^{m+n}}{36^{m+n}} \\ &= \frac{r\cdot 6^{m+2n} + t\cdot 6^{2m+n}}{36^{m+n}} \\ &= \frac{r\cdot 6^m\cdot 36^n}{36^m\cdot 36^n} + \frac{t\cdot 36^m\cdot 6^n}{36^m\cdot 36^n} \\ &= \frac{r\cdot 6^m}{36^m} + \frac{t\cdot 6^n}{36^n} \\ &= \rho\left(\frac{r}{6^m}\right) + \rho\left(\frac{t}{6^n}\right), \end{aligned}$$

mientras que

$$\begin{aligned} \rho\left(\frac{r}{6^m}\cdot\frac{t}{6^n}\right) &= \rho\left(\frac{r\cdot t}{6^{m+n}}\right) \\ &= \frac{r\cdot t\cdot 6^{m+n}}{36^{m+n}} \\ &= \frac{r\cdot 6^m}{36^m}\cdot\frac{t\cdot 6^n}{36^n} \\ &= \rho\left(\frac{r}{6^m}\right)\cdot\rho\left(\frac{t}{6^n}\right). \end{aligned}$$

Además, el elemento identidad en $\mathcal{R}_6$ se puede representar como $1=\dfrac{6}{6}$, por lo que

$$\rho(1)=\rho\left(\frac{6}{6}\right)=\frac{6\cdot 6}{36}=1.$$

Por otro lado, ρ es un homomorfismo inyectivo, ya que

$$\ker(\rho)=\left\{\frac{r}{6^m}\in\mathcal{R}_6 \;\middle|\; \rho\left(\frac{r}{6^m}\right)=0\right\}=\left\{\frac{r}{6^m}\in\mathcal{R}_6 \;\middle|\; \frac{r\cdot 6^m}{36^m}=0\right\}=\{0\},$$

y así también, ρ es un homomorfismo sobreyectivo, pues si elegimos $\frac{s}{36^k} \in \mathcal{R}_{36}$, entonces siempre existirá $\frac{s}{6^{2k}} \in \mathcal{R}_6$ de modo que

$$\rho\left(\frac{s}{6^{2k}}\right) = \frac{s \cdot 6^{2k}}{36^{2k}} = \frac{s \cdot 36^k}{36^k \cdot 36^k} = \frac{s}{36^k}.$$

Finalmente, observemos que la única acción del homomorfismo ρ sobre las fracciones de $\mathcal{R}_6$ es reescribirlas de manera equivalente.

Ejemplo 2.4.9. Nuevamente, en $X = \text{Spec}(\mathbb{Z})$ se tiene

$$\mathcal{R}_6 = \left\{ \frac{r}{6^m} \;\middle|\; r \in \mathbb{Z} \text{ y } m \in \mathbb{N} \right\} \quad \text{y} \quad \mathcal{R}_{30} = \left\{ \frac{s}{30^k} \;\middle|\; s \in \mathbb{Z} \text{ y } k \in \mathbb{N} \right\}.$$

La función

$$\begin{array}{rccc} \rho: & \mathcal{R}_6 & \to & \mathcal{R}_{30} \\ & \frac{r}{6^m} & \mapsto & \frac{r \cdot 5^m}{30^m} \end{array}$$

también es un homomorfismo inyectivo de anillos conmutativos con identidad. Sin embargo, ρ no es un homomorfismo sobreyectivo, ya que la fracción $\frac{1}{5} = \frac{6}{30} \in \mathcal{R}_{30}$ no tiene preimagen bajo ρ en $\mathcal{R}_6$.

Motivados por los ejemplos 2.4.8 y 2.4.9, supongamos que $X_f \supset X_g$. Por el lema 2.4.2, se tiene que $g \in \sqrt{(f)}$, es decir, $g^n = af$ para algún $n \in \mathbb{N}$ y algún $a \in R$. Esta observación inducirá el siguiente homomorfismo de anillos conmutativos.

$$\begin{array}{rccc} \rho_{X_f, X_g}: & \mathcal{R}_f & \to & \mathcal{R}_g \\ & \frac{r}{f^m} & \mapsto & \frac{a^m r}{g^{mn}}. \end{array}$$

Este homomorfismo queda únicamente determinado por f y g, ya que si elegimos otros candidatos $\hat{n} \in \mathbb{N}$ y $\hat{a} \in R$ tales que $g^{\hat{n}} = \hat{a}f$, entonces

$$\frac{\hat{a}^m r}{g^{m\hat{n}}} = \frac{a^m r}{g^{mn}}.$$

El homomorfismo ρ_{X_f, X_g} se conoce como *función de restricción*. Esta función tiene una propiedad similar a la noción usual de restringir una función a un dominio más pequeño. Esta caracerística queda de manifiesto en el siguiente lema.

Lema 2.4.10. *Si $X_f \supset X_g \supset X_h$, entonces $\rho_{X_g, X_h} \circ \rho_{X_f, X_g} = \rho_{X_f, X_h}$.*

Demostración. Por el lema 2.4.2, se tiene que $h \in \sqrt{(g)}$ y $g \in \sqrt{(f)}$. Dicho de otra manera, podremos encontrar $n_1, n_2 \in \mathbb{N}$ y $a, b \in R$ de modo que $h^{n_1} = ag$ y $g^{n_2} = bf$, por lo que $h^{n_1 n_2} = a^{n_2} bf$. Así, para $\dfrac{r}{f^m} \in \mathcal{R}_f$ se tiene que

$$\rho_{X_f, X_h}\left(\frac{r}{f^m}\right) = \frac{a^{mn_2} b^m r}{h^{mn_1 n_2}}.$$

Por otro lado,

$$\rho_{X_g, X_h} \circ \rho_{X_f, X_g}\left(\frac{r}{f^m}\right) = \rho_{X_g, X_h}\left(\frac{b^m r}{g^{mn_2}}\right) = \frac{a^{mn_2} b^m r}{h^{mn_1 n_2}}. \qquad \blacklozenge$$

Ejemplo 2.4.11. Sea $f \in R$ un elemento no nilpotente y $X = \operatorname{Spec}(R)$. Notemos que

$$X_f = \{P \in X \mid f \notin P\} \quad \text{y} \quad X_{f^2} = \left\{P \in X \mid f^2 \notin P\right\}.$$

Si elegimos cualquier elemento $P \in X$, y dado que P es un ideal primo de R, la proposición $f \notin P$ es equivalente a $f^2 \notin P$. Es por ello que $X_f = X_{f^2}$. Más aún, para todo $n \in \mathbb{N}$ se cumple $X_f = X_{f^n}$.

Al igual como se probó en el ejemplo 2.4.8, podemos observar que el homomorfismo

$$\begin{array}{rccc} \rho_{X_f, X_{f^2}}: & \mathcal{R}_f & \to & \mathcal{R}_{f^2} \\ & \dfrac{r}{f^m} & \mapsto & \dfrac{r \cdot f^m}{f^{2m}} \end{array}$$

es de hecho una biyección. Es así que $\mathcal{R}_f \cong \mathcal{R}_{f^2}$, e incluso, para todo $n \in \mathbb{N}$ se cumple $\mathcal{R}_f \cong \mathcal{R}_{f^n}$.

Lema 2.4.12. *Si* $X_f = \bigcup_{\lambda \in \Lambda} X_{f_\lambda}$ *y si para* $a \in \mathcal{R}_f$ *se cumple que*

$$\rho_{X_f, X_{f_\lambda}}(a) = 0 \text{ para todo } \lambda \in \Lambda,$$

entonces $a = 0$.

Demostración. Si escribimos $a = \dfrac{r}{f^m}$, entonces afirmar que $a = 0$ en $\mathcal{R}_f$ es equivalente a decir que existe algún entero $n \in \mathbb{N}$ tal que $f^n r = 0$ en R. Definamos

$$A = \{h \in R \mid hr = 0\}.$$

Es de rutina probar que A es un ideal de R. De esta manera,

$$a = 0 \text{ en } \mathcal{R}_f \;\Leftrightarrow\; f^n \in A, \text{ para algún } n \in \mathbb{N} \;\Leftrightarrow\; f \in \sqrt{A}.$$

Por otro lado, podemos generalizar el resultado del lema 2.4.1 como

$$\sqrt{A} = \bigcap_{\substack{P \in \mathrm{Spec}(R) \\ P \supset A}} P.$$

Así, afirmar que $a = 0$ en $\mathcal{R}_f$ es equivalente a decir que $f \in P$ para todo ideal primo P de R tal que $P \supset A$.

Supongamos que $a \neq 0$. Luego, existirá un ideal primo P de R tal que $P \supset A$ y $f \notin P$. Como $P \in X_f = \bigcup_{\lambda \in \Lambda} X_{f_\lambda}$, existirá algún $\lambda \in \Lambda$ tal que $P \in X_{f_\lambda}$, esto es, $f_\lambda \notin P$.

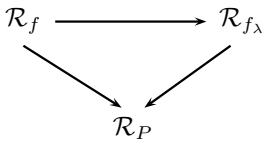
Como $X_f \supset X_{f_\lambda}$, por el lema 2.4.2 se tendrá que $f_\lambda \in \sqrt{(f)}$, o sea, existirán $b \in R$ y $n \in \mathbb{N}$ de modo que $f_\lambda^n = bf$. Luego, podremos construir el homomorfismo de anillos conmutativos

$$\begin{array}{rccc} \rho_{X_f, X_{f_\lambda}} : & \mathcal{R}_f & \to & \mathcal{R}_{f_\lambda} \\ & \dfrac{r}{f^m} & \mapsto & \dfrac{rb^m}{f_\lambda^{mn}}. \end{array}$$

Así también, dado que $f \notin P$ y $f_\lambda \notin P$, $\mathcal{R}_f$ y $\mathcal{R}_{f_\lambda}$ aparecen como subanillos de

$$\mathcal{R}_P = \left\{ \frac{r}{s} \;\middle|\; r, s \in R \text{ y } s \notin P \right\}.$$

Podremos formar el siguiente diagrama de homomorfismos de anillos conmutativos.



Los homomorfismos $\mathcal{R}_f \to \mathcal{R}_P$ y $\mathcal{R}_{f_\lambda} \to \mathcal{R}_P$ corresponden simplemente a las inclusiones de $\mathcal{R}_f$ y $\mathcal{R}_{f_\lambda}$ en $\mathcal{R}_P$. Notemos que el diagrama anterior es conmutativo, ya que se puede verificar de manera directa que

$$\frac{r}{f^m} = \frac{rb^m}{f_\lambda^{mn}}$$

en $\mathcal{R}_P$.

Ahora bien, como $\rho_{X_f, X_{f_\lambda}}(a) = 0$, la imagen de $a \in \mathcal{R}_f$ sobre $\mathcal{R}_P$ deberá ser 0. Por lo tanto, la

imagen de $r = f^m a \in \mathcal{R}_f$ sobre $\mathcal{R}_P$ también deberá ser 0. Lo anterior significa que existirá $s \in R - P$ de modo que $rs = 0$. Por esta razón, $s \in A$ y como $P \supset A$, necesariamente se tiene que $s \in P$. Esto es una contradicción, ya que $s \in R - P$.

Finalmente, concluimos que $a = 0$ en $\mathcal{R}_f$. ♦

Un resultado importante en topología es el lema del pegado (ver [5], página 108), el cual nos permite extender continuamente funciones continuas. De manera muy sencilla, este lema nos indica que si $A, B \subset X$ son conjuntos abiertos en algún espacio topológico X y $g_A : A \to Y$, $g_B : B \to Y$ son funciones continuas tales que $g_A(x) = g_B(x)$, $\forall x \in A \cap B$, entonces siempre es posible construir una función continua $g : A \cup B \to Y$ de modo que $g|_A = g_A$ y $g|_B = g_B$. Esta misma idea es la que se persigue en el lema que se enuncia a continuación.

Lema 2.4.13. *Supongamos que* $X_f = \bigcup_{\lambda \in \Lambda} X_{f_\lambda}$ *y que para cualquier elección de* $g_\alpha \in \mathcal{R}_{f_\alpha}$ *y* $g_\beta \in \mathcal{R}_{f_\beta}$, *donde* $\alpha, \beta \in \Lambda$ *son arbitarios, se cumple que*

$$\rho_{X_{f_\alpha}, X_{f_\alpha f_\beta}}(g_\alpha) = \rho_{X_{f_\beta}, X_{f_\alpha f_\beta}}(g_\beta),$$

entonces existirá $g \in \mathcal{R}_f$ *que satisface*

$$g_\lambda = \rho_{X_f, X_{f_\lambda}}(g), \text{ para todo } \lambda \in \Lambda.$$

Demostración. Ver [3], página 65. ♦

Ahora que contamos con varios resultados acerca del espacio topológico $X = \mathrm{Spec}(R)$, podremos definir el haz estructural $\mathcal{O}_X$ sobre X. Según la proposición 2.2.2, X tiene como base al conjunto

$$\mathcal{B}_X = \{X_f \subset X \mid f \in R\}.$$

Es por ello que definimos

$$\mathcal{O}_X(X_f) = \mathcal{R}_f.$$

Además, dada la inclusión de abiertos basales $X_f \supset X_g$ (es decir, existen $a \in R$ y $n \in \mathbb{N}$ tales que $g^n = af$), elegiremos como función de restricción del haz $\mathcal{O}_X$ al homomorfismo de anillos

conmutativos

$$\begin{array}{rccc} \rho_{X_f,X_g}: & \mathcal{R}_f & \to & \mathcal{R}_g \\ & \dfrac{r}{f^m} & \mapsto & \dfrac{ra^m}{g^{mn}}. \end{array}$$

Por los lemas 2.4.10, 2.4.12 y 2.4.13, esta construcción efectivamente cumple con las características de un haz de anillos conmutativos.

Sin embargo, si elegimos algún abierto arbitrario $U \subset X$, este abierto no necesariamente pertenecerá a $\mathcal{B}_X$. En este caso, definimos

$$\mathcal{O}_X(U) = \left\{ s \in \prod_{X_f \subset U} \mathcal{R}_f \;\middle|\; \begin{array}{l} \text{para todos } X_f, X_g \text{ tales que } U \supset X_f \supset X_g, \\ \text{se cumple que } \rho_{X_f,X_g}\left(s_{X_f}\right) = s_{X_g} \end{array} \right\}.$$

Acá, $\prod_{X_f \subset U} \mathcal{R}_f$ denota el producto cartesiano de todos los anillos $\mathcal{R}_f$ tales que $X_f \subset U$, mientras que s_{X_f} y s_{X_g} representan las coordenadas X_f-ésima y X_g-ésima de s, respectivamente.

Además, dados dos abiertos $U, V \subset X$, tales que $U \supset V$ podemos definir la función de restricción $\rho_{U,V} : \mathcal{O}_X(U) \to \mathcal{O}_X(V)$ simplemente restringiendo coordenada a coordenada.

Se puede probar (ver [2], página 17) que esta forma de definir los anillos conmutativos $\mathcal{O}_X(U)$ y las funciones de restricción $\rho_{U,V}$ para abiertos arbitrarios $U \supset V$ de $X = \operatorname{Spec}(R)$ da lugar efectivamente a un haz de anillos conmutativos sobre el espacio topológico X. Además, estas definiciones son consistentes con la construcción inicial del haz sobre abiertos basales.

Ejemplo 2.4.14. En $\mathbb{Z}$ elijamos el ideal $I = (36)$. En $X = \operatorname{Spec}(\mathbb{Z})$, construyamos el abierto

$$U = D(I) = \{P \in \operatorname{Spec}(\mathbb{Z}) \mid I \not\subset P\} = X - \{(2), (3)\}.$$

Con respecto a la definición anterior, podemos notar que $X_f \subset U$ si y solamente si $(2) \notin X_f$ y

$(3) \notin X_f$. Los únicos abiertos basales que cumplen con estas condiciones son

$$\begin{aligned}
X_6 &= \{P \in X \mid 6 \notin P\} = X - \{(2),(3)\} \\
X_{12} &= \{P \in X \mid 12 \notin P\} = X - \{(2),(3)\} \\
X_{18} &= \{P \in X \mid 18 \notin P\} = X - \{(2),(3)\} \\
X_{24} &= \{P \in X \mid 24 \notin P\} = X - \{(2),(3)\} \\
X_{30} &= \{P \in X \mid 30 \notin P\} = X - \{(2),(3),(5)\} \\
&\vdots
\end{aligned}$$

De esta manera, el anillo conmutativo $\mathcal{O}_X(U)$ corresponde al subanillo del producto cartesiano

$$\mathcal{R}_6 \times \mathcal{R}_{12} \times \mathcal{R}_{18} \times \mathcal{R}_{24} \times \mathcal{R}_{30} \times \cdots = \prod_{n \in \mathbb{N}} \mathcal{R}_{6n}$$

dado por

$$\mathcal{O}_X(U) = \left\{ \left(\frac{r}{6^m}, \frac{r \cdot 2^m}{12^m}, \frac{r \cdot 3^m}{18^m}, \frac{r \cdot 4^m}{24^m}, \frac{r \cdot 5^m}{30^m}, \cdots \right) \;\middle|\; r \in \mathbb{Z} \text{ y } m \in \mathbb{N} \right\}.$$

Observemos que el conjunto abierto $U = X - \{(2),(3)\}$ corresponde simplemente a X_6. De forma paralela, podemos encontrar el anillo conmutativo $\mathcal{O}_X(U)$ sencillamente como

$$\mathcal{O}_X(U) = \mathcal{O}_X\left(X_6\right) = \mathcal{R}_6 = \left\{ \frac{r}{6^m} \;\middle|\; r \in \mathbb{Z} \text{ y } m \in \mathbb{N} \right\}.$$

Ambas maneras de hallar $\mathcal{O}_X(U)$ son consistentes entre sí, ya que los anillos construidos en cada caso son isomorfos mediante el isomorfismo

$$\frac{r}{6^m} \mapsto \left(\frac{r}{6^m}, \frac{r \cdot 2^m}{12^m}, \frac{r \cdot 3^m}{18^m}, \frac{r \cdot 4^m}{24^m}, \frac{r \cdot 5^m}{30^m}, \cdots \right).$$

Por otro lado, elijamos el ideal $J = (30) \subset \mathbb{Z}$ y construyamos el siguiente conjunto abierto en $X = \operatorname{Spec}(\mathbb{Z})$.

$$V = D(J) = \{P \in \operatorname{Spec}(\mathbb{Z}) \mid J \not\subset P\} = X - \{(2),(3),(5)\}.$$

En este caso, el anillo conmutativo $\mathcal{O}_X(V)$ corresponde al subanillo del producto cartesiano

$$\mathcal{R}_{30} \times \mathcal{R}_{60} \times \mathcal{R}_{90} \times \mathcal{R}_{120} \times \mathcal{R}_{150} \times \cdots = \prod_{n \in \mathbb{N}} \mathcal{R}_{30n}$$

dado por

$$\mathcal{O}_X(V) = \left\{ \left(\frac{r}{30^m}, \frac{r \cdot 2^m}{60^m}, \frac{r \cdot 3^m}{90^m}, \frac{r \cdot 4^m}{120^m}, \frac{r \cdot 5^m}{150^m}, \cdots \right) \;\middle|\; r \in \mathbb{Z} \text{ y } m \in \mathbb{N} \right\}.$$

Dado que $U \supset V$, la función de restricción $\rho_{U,V} : \mathcal{O}_X(U) \to \mathcal{O}_X(V)$ se obtiene restringiendo la fracción $\dfrac{r}{6^m}$ en cada coordenada del producto $\mathcal{R}_{30} \times \mathcal{R}_{60} \times \mathcal{R}_{90} \times \mathcal{R}_{120} \times \mathcal{R}_{150} \times \cdots$. Explícitamente,

$$\left(\frac{r}{6^m}, \frac{r \cdot 2^m}{12^m}, \frac{r \cdot 3^m}{18^m}, \frac{r \cdot 4^m}{24^m}, \frac{r \cdot 5^m}{30^m}, \cdots \right) \xmapsto{\rho_{U,V}} \left(\frac{r \cdot 5^m}{30^m}, \frac{r \cdot 10^m}{60^m}, \frac{r \cdot 15^m}{90^m}, \frac{r \cdot 20^m}{120^m}, \frac{r \cdot 25^m}{150^m}, \cdots \right).$$

Finalmente, dado que $\mathcal{O}_X(U) \cong \mathcal{R}_6$ y $\mathcal{O}_X(V) \cong \mathcal{R}_{30}$ bajo los isomorfismos

$$\frac{r}{6^m} \xmapsto{\varphi} \left(\frac{r}{6^m}, \frac{r \cdot 2^m}{12^m}, \frac{r \cdot 3^m}{18^m}, \frac{r \cdot 4^m}{24^m}, \frac{r \cdot 5^m}{30^m}, \cdots \right)$$
$$\text{y} \quad \frac{r}{30^m} \xmapsto{\psi} \left(\frac{r}{30^m}, \frac{r \cdot 2^m}{60^m}, \frac{r \cdot 3^m}{90^m}, \frac{r \cdot 4^m}{120^m}, \frac{r \cdot 5^m}{150^m}, \cdots \right),$$

podemos construir el siguiente diagrama conmutativo.

$$\begin{array}{ccc} \mathcal{R}_6 & \xrightarrow{\quad\varphi\quad} & \mathcal{O}_X(U) \\ {\scriptstyle \rho_{X_6,X_{30}}}\downarrow & & \downarrow{\scriptstyle \rho_{U,V}} \\ \mathcal{R}_{30} & \xrightarrow{\quad\psi\quad} & \mathcal{O}_X(V) \end{array}$$

En cierto sentido, los homomorfismos de anillos conmutativos $\rho_{X_6,X_{30}}$ y $\rho_{U,V}$ son equivalentes.

Definición 2.4.15. Sea $X = \operatorname{Spec}(R)$ y $\mathcal{O}_X$ el haz estructural de anillos conmutativos construido anteriormente. El par $(X, \mathcal{O}_X)$ es llamado *esquema afín* asociado al anillo conmutativo con identidad R.

Capítulo 3

Interacciones con geometría algebraica y teoría de números

3.1. Curvas algebraicas

En esta sección expondremos varios ejemplos relacionados con el estudio de curvas algebraicas desde el punto de vista clásico. Además, implementaremos algunos resultados de la teoría de los esquemas en cada caso.

Definición 3.1.1. Sea R un anillo conmutativo con identidad. Diremos que R es un *anillo local* si él contiene un único ideal maximal.

Ejemplo 3.1.2.

(i) Cualquier cuerpo es un anillo local, ya que su único ideal maximal es $\{0\}$.

(ii) Sea $p \in \mathbb{Z}$ algún entero primo. El anillo

$$\mathbb{Z}_{(p)} = \left\{ \frac{r}{s} \;\middle|\; r \in \mathbb{Z} \text{ y } s \in \mathbb{Z} - (p) \right\} = \left\{ \frac{r}{s} \;\middle|\; r, s \in \mathbb{Z} \text{ y } s \text{ no es divisible por } p \right\} \subset \mathbb{Q}$$

es un anillo local. Su único ideal maximal está generado por la fracción $p = \dfrac{p}{1} \in \mathbb{Z}_{(p)}$.

Explícitamente, este ideal maximal corresponde a

$$p\mathbb{Z}_{(p)} = \left\{ \frac{rp}{s} \;\middle|\; r, s \in \mathbb{Z} \text{ y } s \text{ no es divisible por } p \right\}.$$

(iii) De manera general, si R es un anillo conmutativo con identidad, $P \subset R$ algún ideal primo y $S = R - P$, entonces el anillo

$$\mathcal{R}_P = S^{-1}R = \left\{ \frac{r}{s} \;\middle|\; r \in R \text{ y } s \in S \right\}$$

es un anillo local cuyo único ideal maximal es $S^{-1}P$.

Proposición 3.1.3. *Un anillo conmutativo con identidad R es un anillo local si y solamente si el conjunto de todos sus elementos no invertibles forman un ideal de R.*

Demostración. Supongamos que R es un anillo local y sea $M \subset R$ su único ideal maximal. Supongamos además que existe algún elemento $r \in R - M$ no invertible. Luego, el ideal (r) debe estar propiamente contenido en R, ya que en caso contrario, existiría $s \in R$ tal que $rs = 1$, una contradicción. Como M es el único ideal maximal de R, cualquier otro ideal de R deberá estar contenido en M, y en particular, $(r) \subset M$. Lo anterior implica que $r \in M$, una contradicción.

Ahora a la inversa. Supongamos que

$$M = \{r \in R \mid r \text{ no es invertible}\}$$

es un ideal de R. M es efectivamente un ideal maximal de R, ya que si existiese otro ideal $N \supset M$, $N \neq M$, entonces N debiese contener algún elemento invertible y necesariamente $N = R$. Para probar la unicidad de M, supongamos que existe otro ideal maximal $I \subset R$ tal que $I \neq M$. Por razones análogas, I deberá contener algún elemento invertible, concluyendo finalmente que $I = R$, una contradicción. ⧫

La proposición 3.1.3 nos permite caracterizar el ideal maximal de un anillo local R como aquel conjunto que contiene a todos los elementos no invertibles de R.

Ejemplo 3.1.4. En este ejemplo intentaremos explicar las razones por las cuales utilizamos el adjetivo "local" para designar a este tipo de anillos.

Consideremos el anillo conmutativo con identidad

$$R = \left\{ f : \left[-1, 1 \right] \to \mathbb{R} \mid f \text{ es continua} \right\}.$$

Sobre R definimos la relación de equivalencia

$$f \sim g \;\Leftrightarrow\; \text{existe } 0 < \varepsilon \leq 1 \text{ tal que } f(x) = g(x), \text{ para todo } x \in \left] -\varepsilon, \varepsilon \right[.$$

En otras palabras, dos funciones están relacionadas bajo $\sim$ si ellas tienen el mismo comportamiento en algún entorno abierto de 0. Realizamos esta identificación porque solamente nos interesa estudiar las características locales de las funciones continuas en torno a 0.

El conjunto $\mathcal{R} = R/\sim$ puede ser dotado con estructura de anillo conmutativo con identidad de manera natural. Si $\left[f\right]$ y $\left[g\right]$ representan las clases de equivalencia de $f \in R$ y $g \in R$, respectivamente, entonces

$$\left[f\right] + \left[g\right] = \left[f + g\right] \quad \text{y} \quad \left[f\right] \cdot \left[g\right] = \left[f \cdot g\right].$$

Se puede probar de manera rutinaria que estas operaciones están bien definidas (no dependen del representante de cada clase de equivalencia) y proporcionan a $\mathcal{R}$ la estructura de anillo conmutativo con identidad. $\mathcal{R}$ se conoce comúnmente como el *anillo de los gérmenes* de R en 0.

Un gérmen $\left[f\right]$ será invertible en $\mathcal{R}$ si y solamente si $f(0) \neq 0$. Lo anterior se explica porque si una función continua satisface $f(0) \neq 0$, entonces $f(x) \neq 0$ para todo x en alguna vecindad de 0. Así, en aquella vecindad podremos definir la función $g(x) = \dfrac{1}{f(x)}$, la cual cumplirá con $\left[f\right] \cdot \left[g\right] = \left[1\right]$.

Es claro que el conjunto de todos los gérmenes no invertibles constituye un ideal de $\mathcal{R}$. Explícitamente, este ideal corresponde a

$$\mathcal{M} = \left\{ \left[f\right] \in \mathcal{R} \mid f(0) = 0 \right\}.$$

Finalmente, por la proposición 3.1.3, $\mathcal{R}$ es efectivamente un anillo local.

Podemos generalizar exactamente la misma construcción realizada anteriormente y definir, por ejemplo, el anillo de los gérmenes de todas las funciones reales sobre algún espacio topológico en

algún punto dado, así como también, el anillo de los gérmenes de todas las funciones racionales sobre alguna variedad algebraica en algún punto dado, entre otros.

Definición 3.1.5. Un dominio de integridad R se denomina *anillo de valuación discreta* si R es un anillo noetheriano, R no es un cuerpo, R es un anillo local, y además, su único ideal maximal es principal.

Ejemplo 3.1.6. Con respecto al ejemplo 3.1.2, el anillo

$$\mathbb{Z}_{(p)} = \left\{ \frac{r}{s} \;\middle|\; r, s \in \mathbb{Z} \text{ y } s \text{ no es divisible por } p \right\}$$

es un anillo de valuación discreta. Su único ideal maximal está generado por la fracción $p = \dfrac{p}{1} \in \mathbb{Z}_{(p)}$ y cualquier otro ideal propio de $\mathbb{Z}_{(p)}$ está generado por la fracción $p^n = \dfrac{p^n}{1}$, para algún entero $n \geq 2$.

Proposición 3.1.7. *Un dominio de integridad R es un anillo de valuación discreta si y solamente si existe un elemento $t \in R$ irreducible tal que todo elemento $r \in R$ no nulo se puede escribir de manera única como $r = ut^n$, donde $u \in R$ es invertible y $n \geq 0$ es un entero.*

Demostración. Supongamos que R es un anillo de valuación discreta y sea $M = (t)$ su único ideal maximal, donde $t \in R$ es algún generador de M. Luego, por la proposición 3.1.3,

$$M = \{r \in R \mid r \text{ no es invertible}\} = (t).$$

Sea $r \in R$ algún elemento no nulo y consideremos dos casos. El primero, si $r \notin M$, entonces r es invertible y se puede escribir como $r = rt^0$. El segundo, si $r \in M$, entonces r no es invertible y se puede escribir como $r = a_1 t$, para algún $a_1 \in R$. Si a_1 fuera invertible, entonces la demostración está completa; si a_1 no fuera invertible, entonces $a_1 \in M$ y $a_1 = a_2 t$, para algún $a_2 \in R$. Supongamos que repetimos este proceso de manera indefinida sin que ningún elemento $a_1, a_2, a_3, \ldots$ sea invertible. Entonces, habremos encontrado $a_1, a_2, a_3, \ldots \in M$ tales que

$$a_1 = a_2 t$$

$$a_2 = a_3 t$$

$$\vdots$$

De esta manera, podremos formar la siguiente cadena ascendente de ideales.

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots$$

Dado que R es un anillo noetheriano, la cadena anteriormente construida debe ser estacionaria, es decir, existirá $m \in \mathbb{N}$ tal que $(a_m) = (a_{m+1}) = \cdots$. Por lo tanto, podremos encontrar $s \in R$ tal que $a_{m+1} = a_m s$. Según la construcción descrita anteriormente, tenemos además que $a_m = a_{m+1}t$, y en consecuencia, $a_m = a_m st$. Dado que R es un dominio de integridad y $a_m \neq 0$, necesariamente tendremos que $st = 1$, lo cual es una contradicción, ya que t no puede ser invertible.

Es por esto que el proceso descrito en los párrafos anteriores deberá terminar en una cantidad finita de pasos. En otras palabras, existirá algún entero $n \geq 1$ tal que $a_1, a_2, \ldots, a_{n-1} \in M$ y además $a_n \notin M$. Luego,

$$r = a_1 t = a_2 t^2 = \ldots = a_{n-1} t^{n-1} = a_n t^n,$$

donde $a_n \in R$ es invertible.

Para probar la unicidad de esta representación, supongamos que $r = ut^n = vt^m$, donde $u, v \in R$ son invertibles y $n \geq 0$, $m \geq 0$ son enteros. Sin perdida de generalidad, podemos asumir que $n \geq m$. Así, podemos concluir que

$$ut^n - vt^m = 0 \;\Leftrightarrow\; t^m \left(ut^{n-m} - v\right) = 0.$$

Dado que $t \neq 0$ y R es un dominio de integridad, necesariamente tenemos que

$$ut^{n-m} - v = 0 \;\Leftrightarrow\; ut^{n-m} = v \;\Leftrightarrow\; t^{n-m} = u^{-1}v.$$

Notemos que t^{n-m} no es un elemento invertible, a menos que $n = m$, en cuyo caso $t^{n-m} = t^0 = 1$ y $u = v$.

Ahora a la inversa. Supongamos que existe $t \in R$ irreducible tal que cualquier elemento $r \in R$ no nulo se puede escribir de manera única como $r = ut^n$, donde $u \in R$ es invertible y $n \geq 0$ es un entero. Podemos notar que el ideal $M = (t)$ es maximal, ya que cualquier elemento $r \in R - M$ no puede ser múltiplo de t y la única manera de representarlo será $r = rt^0$. Luego, r debe ser invertible en R y $M = (t)$ tiene que ser un ideal maximal. De hecho, M es el ideal formado por todos los elementos no invertibles, por lo que M es un anillo local. Por último, los únicos ideales propios de R son aquellos generados por t^n, para algún entero $n \geq 1$, por lo que R es un dominio de ideales principales, y por ende, también es noetheriano. ♦

Ejemplo 3.1.8. Continuando con el ejemplo 3.1.6, cualquier elemento $\frac{r}{s} \in \mathbb{Z}_{(p)}$ no nulo se puede representar como

$$\frac{r}{s} = \frac{up^n}{s} = \frac{u}{s}\, p^n,$$

donde u y s son enteros no nulos y no divisibles por p. Así, la fracción $\frac{u}{s}$ es invertible en $\mathbb{Z}_{(p)}$ y se verifica la caracterización de los anillos de valuación discreta expuesta en la proposición 3.1.7.

Ejemplo 3.1.9. Sea k un cuerpo algebraicamente cerrado. Sobre $k[x, y]$ consideremos la curva algebraica con ecuación $x = y$, la cual sabemos representa una recta. Su anillo de coordenadas corresponde a $k[x, y]/(x - y)$, el cual es isomorfo a $R = k[x]$. Según lo expuesto en el ejemplo 2.1.3, tenemos que

$$X = \operatorname{Spec}(R) = \{\{0\}\} \cup \{(x - \alpha)k[x] \mid \alpha \in k\}.$$

Supongamos que deseamos buscar información acerca del comportamiento de esta curva algebraica en torno al punto $(x, y) = (0, 0)$. Para ello, desde anillo de coordenadas $k[x, y]/(x - y)$ elegimos el ideal (x, y). Si traspasamos esta información al anillo $R = k[x]$, entonces estaremos observando el ideal primo $P = xk[x] \in X$. Con él podemos formar el conjunto abierto

$$U = D(P) = \{Q \in X \mid P \not\subset Q\} = X - \{xk[x]\},$$

el cual coincide con el abierto basal

$$X_x = \{Q \in X \mid x \notin Q\} = X - \{xk[x]\}.$$

Por lo tanto,

$$\mathcal{O}_X(U) = \mathcal{O}_X\left(X_x\right) = \mathcal{R}_x = \left\{ \frac{r}{x^m} \;\middle|\; r \in R \text{ y } m \in \mathbb{N} \right\}.$$

El resultado anterior se puede interpretar como el anillo de todas las funciones racionales definidas en cualquier punto de la curva con ecuación $x = y$, excepto en el punto $(0, 0)$. De manera informal, la operación anterior consiste en eliminar el punto $(0, 0)$ de esta curva.

$\mathcal{R}_x$ no es un anillo local, ya que sus ideales maximales tienen la forma $(x-\alpha)\mathcal{R}_x$, donde $\alpha \in k-\{0\}$. En otras palabras, todos los puntos sobre la curva con ecuación $x = y$, exceptuando el punto $(0, 0)$, están relacionados con los ideales maximales de $\mathcal{R}_x$.

Por otro lado, si localizamos el anillo R en el ideal P, obtendremos

$$\mathcal{R}_P = \left\{ \frac{f}{g} \;\middle|\; f \in R \text{ y } g \in R - P \right\} = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in k[x] \text{ y } g(0) \neq 0 \right\}.$$

Este anillo corresponde al conjunto de todas las funciones racionales definidas sobre el punto $(x, y) = (0, 0)$ de la curva con ecuación $x = y$. Además, es un anillo de valuación discreta cuyo único ideal maximal es $P\mathcal{R}_P$, el cual queda generado por la fracción $x = \dfrac{x}{1} \in \mathcal{R}_P$.

Ejemplo 3.1.10. Sea k un cuerpo algebraicamente cerrado. Sobre $k[x, y]$ consideremos ahora la curva algebraica con ecuación $x^3 = y^2$, la cual sabemos es una curva suave en cualquiera de sus puntos, excepto en el punto $(x, y) = (0, 0)$, en donde ella presenta una singularidad de tipo cúspide. Su anillo de coordenadas corresponde a $R = k[x, y]/\left(x^3 - y^2\right)$. Un elemento típico en este anillo se puede escribir de la forma $p(x) + yq(x)$, donde $p(x), q(x) \in k[x]$. Las operaciones entre estos polinomios se deben reducir módulo el ideal $(x^3 - y^2)$.

Imaginemos que buscamos información acerca del comportamiento de esta curva en torno al punto $(0, 0)$. Al igual que en el ejemplo 3.1.9, elegimos el ideal

$$P = (x, y)R = \{f(x, y) \in R \mid f(0, 0) = 0\}.$$

Notemos que $R/P \cong k$, por lo que P es un ideal maximal de R, y por lo tanto también es primo. La localización de R en P corresponde a

$$\mathcal{R}_P = \left\{ \frac{f}{g} \;\middle|\; f \in R \text{ y } g \in R - P \right\}.$$

Un elemento típico en este anillo se puede escribir de la forma $\dfrac{p(x) + yq(x)}{r(x) + ys(x)}$, donde $p(x), q(x), r(x)$, $s(x) \in k[x]$ y $r(0) \neq 0$. Además, las operaciones entre estas fracciones se deben reducir módulo el ideal $(x^3 - y^2)$.

Notemos que $\mathcal{R}_P$ es un anillo local cuyo único ideal maximal es $(x, y)\mathcal{R}_P$. Sin embargo, $\mathcal{R}_P$ no es un anillo de valuación discreta, ya que su ideal maximal no es principal.

Por otro lado, supongamos ahora que buscamos información sobre el comportamiento de esta curva

en torno al punto $(x, y) = (1, 1)$. En este caso, escogemos el ideal

$$Q = (x-1, y-1)R = \{f(x,y) \in R \mid f(1,1) = 0\}.$$

Podemos observar nuevamente que $R/Q \cong k$, por lo que Q es un ideal maximal, y por ende también es primo. La localización de R en Q es

$$\mathcal{R}_Q = \left\{ \frac{f}{g} \;\middle|\; f \in R \text{ y } g \in R - Q \right\}.$$

Un elemento típico en este anillo se puede escribir de la forma $\dfrac{p(x) + yq(x)}{r(x) + ys(x)}$, donde $p(x), q(x), r(x)$, $s(x) \in k[x]$ y $r(1)+s(1) \neq 0$. Además, las operaciones entre estas fracciones se deben reducir módulo el ideal $(x^3 - y^2)$.

De manera similar, $\mathcal{R}_Q$ es un anillo local cuyo único ideal maximal es $(x-1, y-1)\mathcal{R}_Q$. A pesar de que las apariencias podrían engañarnos, $(x-1, y-1)\mathcal{R}_Q$ sí es un ideal principal de $\mathcal{R}_Q$, ya que en este anillo contamos con las siguientes relaciones.

$$\begin{aligned} y^2 - 1 &= x^3 - 1 \\ (y-1)(y+1) &= (x-1)\left(x^2 + x + 1\right) \\ y - 1 &= \frac{(x-1)\left(x^2 + x + 1\right)}{y+1} \in \mathcal{R}_Q. \end{aligned}$$

De esta manera, $(x-1, y-1)\mathcal{R}_Q = (x-1)\mathcal{R}_Q$ y $\mathcal{R}_Q$ es de hecho un anillo de valuación discreta.

En resumen, muchos resultados tradicionales de la teoría clásica sobre curvas algebraicas también se pueden encontrar utilizando la teoría los esquemas. Como un ejemplo particular de ello, con la teoría de los esquemas podemos detectar y estudiar puntos suaves y puntos singulares sobre curvas algebraicas.

3.2. Puntos dobles

En esta sección utilizaremos algunas herramientas de la teoría de los esquemas para analizar puntos con multiplicidad en una variedad algebraica.

Proposición 3.2.1. *Sea R un anillo conmutativo con identidad, $X = \mathrm{Spec}(R)$ y $\mathcal{O}_X$ el haz estructural de anillos conmutativos sobre X. Entonces*

$$\mathcal{O}_X(X) \cong R.$$

Demostración. Notemos que

$$X_1 = \{P \in \mathrm{Spec}(R) \mid 1 \notin P\} = \mathrm{Spec}(R) = X.$$

Por la definición del haz estructural $\mathcal{O}_X$, tenemos que

$$\mathcal{O}_X(X) = \mathcal{O}_X(X_1) = \mathcal{R}_1 = \left\{ \frac{r}{1^m} \;\middle|\; r \in R \text{ y } m \in \mathbb{N} \right\} \cong R. \qquad \blacklozenge$$

Ejemplo 3.2.2. Consideremos k un cuerpo algebraicamente cerrado. Observemos que

$$R = k[x]/(x) \cong k,$$

por lo que el único ideal primo en R es el trivial y $\mathrm{Spec}(R)$ contiene un único punto.

Examinemos ahora el anillo $S = k[x]/(x^2)$. Sea P un ideal primo de S. Dado que en S contamos con la relación $x \cdot x = x^2 = 0$, podemos concluir que $x \in P$ y $xS \subset P$. Además, ningún polinomio constante (salvo el polinomio nulo) puede estar contenido en P, pues P no puede admitir elementos invertibles. Por esta razón, concluimos que $P = xS$ y $\mathrm{Spec}(S)$ también contiene solamente un punto.

Ahora bien, aun cuando $X = \mathrm{Spec}(R)$ e $Y = \mathrm{Spec}(S)$ tienen ambos un único elemento, estos esquemas son distintos, ya que, según la proposición 3.2.1,

$$\mathcal{O}_X(X) \cong R \quad \text{y} \quad \mathcal{O}_Y(Y) \cong S.$$

Podemos notar que 0 es una raíz simple del polinomio $f(x) = x$ y doble del polinomio $g(x) = x^2$. Esta diferencia queda de manifiesto en que R es un $k-$espacio vectorial de dimensión 1, mientras que S es un $k-$espacio vectorial de dimensión 2. Intuitivamente, los haces $\mathcal{O}_X$ y $\mathcal{O}_Y$ albergan toda la información de sus respectivos anillos.

De manera general, para todo $n \in \mathbb{N}$, si elegimos el anillo $S = k[x]/(x^n)$, entonces $Y = \text{Spec}(S) = \{xS\}$ contiene un único punto y $\mathcal{O}_Y(Y) \cong S$ es un $k-$espacio vectorial de dimensión n.

Ejemplo 3.2.3. Al igual que en ejemplo 3.2.2, consideremos k un cuerpo algebraicamente cerrado. Observemos que

$$R = k[x, y]/(x, y) \cong k,$$

por lo que el único ideal primo de R es el trivial y $X = \text{Spec}(R)$ contiene un único punto.

Por un lado, notemos que el anillo $S = k[x, y]/(x^2, y)$ es isomorfo a aquel del ejemplo 3.2.2. Deducimos inmediatamente que $Y = \text{Spec}(S) = \{xS\}$, el cual también contiene un único punto.

Por otro lado, analicemos el anillo $T = k[x, y]/(x^2, xy, y^2)$. Sea P algún ideal primo de T. Dado que en T contamos con la relación $x \cdot x = x^2 = 0 \in P$, tenemos que $x \in P$ y $xT \subset P$. Por razones análogas, $yT \subset P$. Dado que ningún polinomio constante (salvo el polinomio nulo) puede estar contenido en P, concluimos que $P = (x, y)T$. De esta manera, $Z = \text{Spec}(T)$ también contiene un único punto.

Sin embargo, aun cuando X, Y y Z contienen todos un único punto, tenemos que

$$\mathcal{O}_X(X) \cong R \quad , \quad \mathcal{O}_Y(Y) \cong S \quad \text{y} \quad \mathcal{O}_Z(Z) \cong T.$$

Es más, R, S y T son $k-$espacios vectoriales de dimensiones 1, 2 y 3, respectivamente. Es por esta razón que no basta con estudiar los esquemas simplemente como espacios topológicos. Si queremos transferir toda la información contenida en un anillo hacia un esquema, es indispensable tratarlo como un haz.

Observemos además que podemos construir la cadena de homomorfismos de anillos

$$R \quad \hookrightarrow \quad S \quad \hookrightarrow \quad T,$$

que consiste simplemente en las inclusiones de R en S, y S en T. Tal y como se indica en la proposición 2.2.5, estos homomorfismos inducirán una cadena de funciones continuas entre sus

respectivos esquemas. Explícitamente,

$$\begin{array}{ccccc} Z & \to & Y & \to & X \\ (x,y)T & \mapsto & xS & \mapsto & \{0\}. \end{array}$$

En este caso, estas funciones son evidentemente continuas, ya que tanto X como Y y Z son espacios topológicos con un único punto y están dotados con la topología discreta.

Nuevamente, la teoría de los esquemas nos permite generalizar los mismos conceptos de la geometría algebraica clásica. Podemos identificar puntos simples, dobles, y en general, múltiples. Incluso nos permite expandir la noción de tangencia entre dos o más variedades algebraicas.

3.3. Anillo de los enteros en un cuerpo de números

El objetivo de esta sección es analizar el esquema Spec $\left(\mathbb{Z}\left[\sqrt{3}\right]\right)$.

Ejemplo 3.3.1. Sea I el ideal del anillo $\mathbb{Z}[x]$ generado por el polinomio x^2-3, es decir, $I = \left(x^2-3\right)\mathbb{Z}[x]$. El propósito de este ejemplo es buscar todos los ideales primos P de $\mathbb{Z}[x]$ tales que $I \subset P$.

Del ejemplo 2.1.12, sabemos que los ideales primos de $\mathbb{Z}[x]$ son

(i) $\{0\}$;

(ii) $p\mathbb{Z}[x]$, donde $p \in \mathbb{Z}$ es primo;

(iii) $f(x)\mathbb{Z}[x]$, donde $f(x) \in \mathbb{Z}[x]$ es un polinomio irreducible sobre $\mathbb{Z}[x]$;

(iv) $p\mathbb{Z}[x] + f(x)\mathbb{Z}[x]$, donde $p \in \mathbb{Z}$ es primo y $f(x) \in \mathbb{Z}[x]$ es tal que su reducción módulo el ideal $p\mathbb{Z}[x]$ es no constante e irreducible sobre $(\mathbb{Z}/p\mathbb{Z})[x]$.

Ahora bien, denotemos por P a alguno de los ideales primos de $\mathbb{Z}[x]$ incluido en la lista anterior. De todas estas opciones para P, debemos buscar cuáles cumplen con la condición $I \subset P$.

(i) Si $P = \{0\}$, entonces es evidente que $I \not\subset P$.

(ii) Si $P = p\mathbb{Z}[x]$, donde $p \in \mathbb{Z}$ es primo, entonces $I \not\subset P$, ya que el polinomio $x^2 - 3 \in I$ y $x^2 - 3 \notin p\mathbb{Z}[x]$.

(iii) Si $P = f(x)\mathbb{Z}[x]$, donde $f(x) \in \mathbb{Z}[x]$ es un polinomio irreducible sobre $\mathbb{Z}[x]$, entonces la inclusión $I \subset P$ es válida si y solamente si $I = P$. Para probar este hecho, supongamos que $I \subset P$. Dado que $x^2 - 3 \in I \subset P$, existirá un polinomio $g(x) \in \mathbb{Z}[x]$ tal que $x^2 - 3 = f(x)g(x)$. Puesto que los polinomios $f(x)$ y $x^2 - 3$ son irreducibles sobre $\mathbb{Z}[x]$, necesariamente tendremos que $f(x) = \pm\left(x^2 - 3\right)$. En cualquier caso concluimos que $I = P$.

(iv) Si $P = p\mathbb{Z}[x] + f(x)\mathbb{Z}[x]$, donde $p \in \mathbb{Z}$ es primo y $f(x) \in \mathbb{Z}[x]$ es tal que su reducción módulo el ideal $p\mathbb{Z}[x]$ es no constante e irreducible sobre $(\mathbb{Z}/p\mathbb{Z})[x]$, entonces la inclusión $I \subset P$ será válida solo en algunos casos muy particulares. Analizaremos detenidamente estos casos a continuación.

- Estudiemos el caso en que $p = 2$. Nuestra misión consistirá en buscar todos los posibles polinomios $f(x)$ de modo que $I \subset P = 2\mathbb{Z}[x] + f(x)\mathbb{Z}[x]$. Dado que $x^2 - 3 \in I \subset P$, existirán $p(x), q(x) \in \mathbb{Z}[x]$ tales que

$$x^2 - 3 = 2p(x) + f(x)q(x).$$

Si reducimos la ecuación anterior módulo el ideal $2\mathbb{Z}[x]$, obtendremos

$$x^2 + 1 = \overline{f(x)}\ \overline{q(x)}$$
$$(x+1)^2 = \overline{f(x)}\ \overline{q(x)}.$$

Dado que $\overline{f(x)}$ es un polinomio irreducible, concluimos que $\overline{f(x)} = \pm(x+1)$. Por lo tanto, el polinomio $f(x)$ se podrá escribir de la forma

$$f(x) = \pm(x+1) + 2r(x),$$

para algún polinomio $r(x) \in \mathbb{Z}[x]$. Recordemos que estamos buscando un polinomio $f(x)$ tal que $P = 2\mathbb{Z}[x] + f(x)\mathbb{Z}[x]$, por lo que podemos elegir simplemente $f(x) = x + 1$. Notemos que

$$x^2 - 3 = 2(-1) + (x+1)(x-1) \in 2\mathbb{Z}[x] + (x+1)\mathbb{Z}[x],$$

por lo que la inclusión $I \subset P$ es válida en este caso si y solamente si

$$P = 2\mathbb{Z}[x] + (x+1)\mathbb{Z}[x].$$

- Examinemos ahora el caso en que $p = 3$. Dado que $x^2 - 3 \in I \subset P$, existirán $p(x), q(x) \in \mathbb{Z}[x]$ tales que

$$x^2 - 3 = 3p(x) + f(x)q(x).$$

Si reducimos la ecuación anterior módulo el ideal $3\mathbb{Z}[x]$, obtendremos

$$x^2 = \overline{f(x)}\ \overline{q(x)}.$$

Dado que $\overline{f(x)}$ es un polinomio irreducible, concluimos que $\overline{f(x)} = \pm x$. Por las mismas razones expuestas en el caso anterior, podemos elegir simplemente $f(x) = x$. Notemos además que

$$x^2 - 3 = 3(-1) + x \cdot x \in 3\mathbb{Z}[x] + x\mathbb{Z}[x],$$

por lo que la inclusión $I \subset P$ es válida en este caso si y solamente si

$$P = 3\mathbb{Z}[x] + x\mathbb{Z}[x].$$

- Analicemos ahora el caso en que $p = 5$. Dado que $x^2 - 3 \in I \subset P$, existirán $p(x), q(x) \in \mathbb{Z}[x]$ tales que

$$x^2 - 3 = 5p(x) + f(x)q(x).$$

Si reducimos la ecuación anterior módulo el ideal $5\mathbb{Z}[x]$, obtendremos

$$x^2 - 3 = \overline{f(x)}\ \overline{q(x)}.$$

En este punto hay una diferencia importante respecto a los dos casos anteriores. Acá, el polinomio $x^2 - 3$ no tiene raíces en $\mathbb{Z}/5\mathbb{Z}$, por lo que es irreducible sobre $(\mathbb{Z}/5\mathbb{Z})[x]$. Dado que $\overline{f(x)}$ es también un polinomio irreducible, concluimos que $\overline{f(x)} = \pm\left(x^2 - 3\right)$. Al igual que en los casos anteriores, podemos elegir simplemente $f(x) = x^2 - 3$. Podemos notar que

$$x^2 - 3 = 5 \cdot 0 + \left(x^2 - 3\right) \in 5\mathbb{Z}[x] + \left(x^2 - 3\right)\mathbb{Z}[x],$$

por lo que la inclusión $I \subset P$ es válida en este caso si y solamente si

$$P = 5\mathbb{Z}[x] + \left(x^2 - 3\right)\mathbb{Z}[x].$$

- Consideremos ahora el caso en que $p = 7$. Dado que $x^2 - 3 \in I \subset P$, existirán $p(x), q(x) \in \mathbb{Z}[x]$ tales que

$$x^2 - 3 = 7p(x) + f(x)q(x).$$

Si reducimos la ecuación anterior módulo el ideal $7\mathbb{Z}[x]$, obtendremos

$$x^2 - 3 = \overline{f(x)}\ \overline{q(x)}.$$

Nuevamente, el polinomio $x^2 - 3$ no tiene raíces en $\mathbb{Z}/7\mathbb{Z}$, y podremos concluir que $\overline{f(x)} = \pm\left(x^2 - 3\right)$. Por supuesto, elegimos simplemente $f(x) = x^2 - 3$. Podemos notar que

$$x^2 - 3 = 7 \cdot 0 + \left(x^2 - 3\right) \in 7\mathbb{Z}[x] + \left(x^2 - 3\right)\mathbb{Z}[x],$$

por lo que la inclusión $I \subset P$ es válida en este caso si y solamente si

$$P = 7\mathbb{Z}[x] + \left(x^2 - 3\right)\mathbb{Z}[x].$$

- Examinemos ahora el caso en que $p = 11$. Dado que $x^2 - 3 \in I \subset P$, existirán $p(x), q(x) \in \mathbb{Z}[x]$ tales que

$$x^2 - 3 = 11p(x) + f(x)q(x).$$

Si reducimos la ecuación anterior módulo el ideal $11\mathbb{Z}[x]$, obtendremos

$$\begin{aligned} x^2 - 3 &= \overline{f(x)}\ \overline{q(x)} \\ (x-5)(x+5) &= \overline{f(x)}\ \overline{q(x)}. \end{aligned}$$

En esta oportunidad, se produce otra diferencia importante con respecto a todos los casos estudiados anteriormente. Acá, el polinomio $x^2 - 3$ tiene dos raíces distintas en $\mathbb{Z}/11\mathbb{Z}$. Como $\overline{f(x)}$ es un polinomio irreducible, concluimos que $\overline{f(x)} = \pm(x - 5)$ o $f(x) = \pm(x + 5)$. Desde luego, podemos elegir simplemente $f(x) = x - 5$ o $f(x) = x + 5$.

Notemos además que

$$x^2 - 3 = 11 \cdot 2 + (x-5)(x+5) \in 11\mathbb{Z}[x] + (x-5)\mathbb{Z}[x]$$
$$\text{y} \quad x^2 - 3 = 11 \cdot 2 + (x+5)(x-5) \in 11\mathbb{Z}[x] + (x+5)\mathbb{Z}[x],$$

por lo que la inclusión $I \subset P$ es válida en este caso si y solamente si

$$P = 11\mathbb{Z}[x] + (x-5)\mathbb{Z}[x] \quad \text{o} \quad P = 11\mathbb{Z}[x] + (x+5)\mathbb{Z}[x].$$

Si repetimos los mismos argumentos anteriores para distintos valores de p, encontraremos una dualidad de comportamiento. Para algunos primos p, el polinomio $x^2 - 3$ es irreducible sobre $(\mathbb{Z}/p\mathbb{Z})[x]$, mientras que para otros valores de p, este polinomio sí se puede factorizar. En la tabla 3.1 resumimos algunos de estos casos.

Tabla 3.1: Factorización del polinomio $x^2 - 3$ en $(\mathbb{Z}/p\mathbb{Z})[x]$.

p	$x^2 - 3$
2	$(x-1)(x+1)$
3	x^2
5	Irreducible
7	Irreducible
11	$(x-5)(x+5)$
13	$(x-4)(x+4)$
17	Irreducible
19	Irreducible
23	$(x-7)(x+7)$

En caso de que el polinomio $x^2 - 3$ fuera irreducible sobre $(\mathbb{Z}/p\mathbb{Z})[x]$, entonces la inclusión $I \subset P$ será valida si y solamente si

$$P = p\mathbb{Z}[x] + (x^2 - 3)\mathbb{Z}[x].$$

Por otro lado, si $x^2 - 3$ fuera reducible sobre $(\mathbb{Z}/p\mathbb{Z})[x]$, entonces existirá $\alpha \in \mathbb{Z}/p\mathbb{Z}$ tal que $\alpha^2 \equiv 3 \mod p$. Por lo tanto el polinomio $x^2 - 3$ se podrá factorizar como $(x-\alpha)(x+\alpha)$ en

$(\mathbb{Z}/p\mathbb{Z})[x]$ y la inclusión $I \subset P$ será válida si y solamente si

$$P = p\mathbb{Z}[x] + (x-\alpha)\mathbb{Z}[x] \quad \text{o} \quad P = p\mathbb{Z}[x] + (x+\alpha)\mathbb{Z}[x].$$

Solo en caso de que $p = 2$ o $p = 3$, las raíces del polinomio $x^2 - 3$ coinciden y los dos posibles ideales descritos anteriormente también coinciden.

En la tabla 3.2 exhibimos algunos de los posibles ideales primos $P \subset \mathbb{Z}[x]$ tales que $I \subset P$.

Tabla 3.2: Algunos ideales primos del anillo $\mathbb{Z}[x]$ que contienen al polinomio $x^2 - 3$.

p	$P = p\mathbb{Z}[x] + f(x)\mathbb{Z}[x]$
0	$\left(x^2-3\right)\mathbb{Z}[x]$
2	$2\mathbb{Z}[x] + (x+1)\mathbb{Z}[x]$
3	$3\mathbb{Z}[x] + x\mathbb{Z}[x]$
5	$5\mathbb{Z}[x] + \left(x^2-3\right)\mathbb{Z}[x]$
7	$7\mathbb{Z}[x] + \left(x^2-3\right)\mathbb{Z}[x]$
11	$11\mathbb{Z}[x] + (x-5)\mathbb{Z}[x]$ o $11\mathbb{Z}[x] + (x+5)\mathbb{Z}[x]$
13	$13\mathbb{Z}[x] + (x-4)\mathbb{Z}[x]$ o $13\mathbb{Z}[x] + (x+4)\mathbb{Z}[x]$
17	$17\mathbb{Z}[x] + \left(x^2-3\right)\mathbb{Z}[x]$
19	$19\mathbb{Z}[x] + \left(x^2-3\right)\mathbb{Z}[x]$
23	$23\mathbb{Z}[x] + (x-7)\mathbb{Z}[x]$ o $23\mathbb{Z}[x] + (x+7)\mathbb{Z}[x]$

Observación 3.3.2. Sea $I = \left(x^2 - d\right)\mathbb{Z}[x]$, donde $d \in \mathbb{Z}$ es un entero libre de cuadrados. Podemos imitar exactamente los mismos razonamientos expuestos en el ejemplo 3.3.1 para encontrar todos los ideales primos P de $\mathbb{Z}[x]$ tales que $I \subset P$. Quizás el asunto más importante en todo este análisis corresponde a decidir si el polinomio $x^2 - d$ es irreducible o no sobre el anillo $(\mathbb{Z}/p\mathbb{Z})[x]$.

Ejemplo 3.3.3. Una vez más, anotaremos $I = \left(x^2 - 3\right)\mathbb{Z}[x]$. En esta ocasión buscaremos los ideales primos del anillo $\mathbb{Z}\left[\sqrt{3}\right]$. Recordemos que este anillo es isomorfo a $\mathbb{Z}[x]/I$ bajo el isomorfismo $a + b\sqrt{3} \mapsto a + bx$. En el ejemplo 3.3.1 ya hemos encontrado todos los ideales primos de P de $\mathbb{Z}[x]$ tales que $I \subset P$. Gracias al corolario 2.1.6, los ideales primos de $\mathbb{Z}[x]/I$ corresponden simplemente a P/I. En la tabla 3.3 exhibimos algunos de estos ideales.

Tabla 3.3: Algunos ideales primos del anillo $\mathbb{Z}\left[\sqrt{3}\right]$.

p	P/I
0	$\{0\}$
2	$2\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}+1\right)\mathbb{Z}\left[\sqrt{3}\right]$
3	$3\mathbb{Z}\left[\sqrt{3}\right] + \sqrt{3}\mathbb{Z}\left[\sqrt{3}\right]$
5	$5\mathbb{Z}\left[\sqrt{3}\right]$
7	$7\mathbb{Z}\left[\sqrt{3}\right]$
11	$11\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}-5\right)\mathbb{Z}\left[\sqrt{3}\right]$ o $11\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}+5\right)\mathbb{Z}\left[\sqrt{3}\right]$
13	$13\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}-4\right)\mathbb{Z}\left[\sqrt{3}\right]$ o $13\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}+4\right)\mathbb{Z}\left[\sqrt{3}\right]$
17	$17\mathbb{Z}\left[\sqrt{3}\right]$
19	$19\mathbb{Z}\left[\sqrt{3}\right]$
23	$23\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}-7\right)\mathbb{Z}\left[\sqrt{3}\right]$ o $23\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}+7\right)\mathbb{Z}\left[\sqrt{3}\right]$

En definitiva para encontrar cualquier ideal primo del anillo $\mathbb{Z}\left[\sqrt{3}\right]$ basta con elegir un entero primo $p \in \mathbb{Z}$ (incluyendo $p = 0$).

(i) Si el polinomio $x^2 - 3$ no tiene raíces en $\mathbb{Z}/p\mathbb{Z}$, entonces p va asociado con el ideal primo $p\mathbb{Z}\left[\sqrt{3}\right]$.

(ii) Si el polinomio $x^2 - 3$ tiene raíces en $\mathbb{Z}/p\mathbb{Z}$, entonces existirá $\alpha \in \mathbb{Z}/p\mathbb{Z}$ tal que $\alpha^2 \equiv 3 \mod p$. En este caso, p va asociado con los ideales primos $p\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}-\alpha\right)\mathbb{Z}\left[\sqrt{3}\right]$ y con $p\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}+\alpha\right)\mathbb{Z}\left[\sqrt{3}\right]$.

Solo en caso de que $p = 2$ o $p = 3$, los dos ideales descritos anteriormente coinciden.

Para continuar con el estudio del espacio Spec $\left(\mathbb{Z}\left[\sqrt{3}\right]\right)$, haremos uso de los siguientes resultados.

Lema 3.3.4. *Sean $p, q \in \mathbb{Z}$ dos enteros primos distintos e I algún ideal del anillo $\mathbb{Z}\left[\sqrt{3}\right]$. Si $p, q \in I$, entonces $I = \mathbb{Z}\left[\sqrt{3}\right]$.*

Demostración. Dado que p y q son coprimos, existirán $a, b \in \mathbb{Z}$ tales que $ap + bq = 1$. Si $p, q \in I$, entonces $1 \in I$ y necesariamente $I = \mathbb{Z}\left[\sqrt{3}\right]$. ♦

Corolario 3.3.5. *Todo ideal primo no nulo en* $\mathbb{Z}\left[\sqrt{3}\right]$ *contiene a un único entero primo.*

Demostración. Es una consecuencia directa del lema 3.3.4 y de la caracterización de los ideales primos en $\mathbb{Z}\left[\sqrt{3}\right]$ realizada en el ejemplo 3.3.3. ♦

Proposición 3.3.6. *Todo ideal primo no nulo en* $\mathbb{Z}\left[\sqrt{3}\right]$ *también es maximal.*

Demostración. Supongamos que existe un ideal primo P de $\mathbb{Z}\left[\sqrt{3}\right]$ que no es maximal. Como consecuencia del lema de Zorn, existirá un ideal maximal M de $\mathbb{Z}\left[\sqrt{3}\right]$ que contendrá propiamente a P. El ideal M también es primo, y por el corolario 3.3.5, existirá un único entero primo $p \in \mathbb{Z}$ tal que $p \in P \subset M$. Podemos estudiar dos casos.

- Si el polinomio $x^2 - 3$ no tiene raíces en $\mathbb{Z}/p\mathbb{Z}$, entonces el único ideal primo que contiene a p es $p\mathbb{Z}\left[\sqrt{3}\right]$. En este caso concluimos que $P = M = p\mathbb{Z}\left[\sqrt{3}\right]$, una contradicción.
- Si el polinomio $x^2 - 3$ tiene a $\alpha \in \mathbb{Z}/p\mathbb{Z}$ como raíz, entonces existen solamente dos ideales primos que contienen a p, a saber

$$p\mathbb{Z}[\sqrt{3}] + (\sqrt{3} - \alpha)\mathbb{Z}[\sqrt{3}] \quad \text{y} \quad p\mathbb{Z}[\sqrt{3}] + (\sqrt{3} + \alpha)\mathbb{Z}[\sqrt{3}].$$

  Ninguno de estos ideales contiene al otro, por lo que llegamos nuevamente a una contradicción.

♦

Ejemplo 3.3.7. En seguida estudiaremos $X = \operatorname{Spec}\left(\mathbb{Z}\left[\sqrt{3}\right]\right)$ como espacio topológico. Puesto que todo ideal primo P no nulo de $\mathbb{Z}\left[\sqrt{3}\right]$ también es maximal, por la proposición 2.2.11, el singletón $\{P\}$ es un conjunto cerrado en X. En otras palabras, este último espacio topológico tiene características similares a $\operatorname{Spec}(\mathbb{Z})$, ya que contiene dos tipos de puntos. Puntos cerrados, correspondientes a cada ideal no nulo de X, y un punto genérico correspondiente al ideal $\{0\}$.

Otro camino para estudiar a X como espacio topológico es, por ejemplo, considerar el homomorfismo de anillos

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & \mathbb{Z}\left[\sqrt{3}\right] \\ & a & \mapsto & a. \end{array}$$

Este homomorfismo inducirá la función

$$\begin{array}{rccc} \varphi^{\#}: & \operatorname{Spec}\left(\mathbb{Z}\left[\sqrt{3}\right]\right) & \to & \operatorname{Spec}\left(\mathbb{Z}\right) \\ & P & \mapsto & \varphi^{-1}(P), \end{array}$$

la cual, según la proposición 2.2.5, es una función continua con respecto a la topología de Zariski. En este caso, podemos explicitar aún más esta función.

$$\varphi^{\#}(P) = \varphi^{-1}(P) = \{a \in \mathbb{Z} \mid \varphi(a) \in P\} = \{a \in \mathbb{Z} \mid a \in P\} = P \cap \mathbb{Z}.$$

Como ya fue expuesto en el ejemplo 3.3.3, cualquier ideal primo P de $\mathbb{Z}\left[\sqrt{3}\right]$ se puede construir a partir de algún primo $p \in \mathbb{Z}$ como

$$P = \begin{cases} p\mathbb{Z}\left[\sqrt{3}\right] & \text{si} \quad x^2 - 3 \text{ no tiene raíces en } \mathbb{Z}/p\mathbb{Z}; \\ p\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3} \pm \alpha\right)\mathbb{Z}\left[\sqrt{3}\right] & \text{si} \quad x^2 - 3 \text{ tiene a } \alpha \in \mathbb{Z}/p\mathbb{Z} \text{ como raíz.} \end{cases}$$

En cualquier caso tenemos $\varphi^{\#}(P) = P \cap \mathbb{Z} = p\mathbb{Z}$.

Si $p \neq 0$, sabemos que cada singletón $\{p\mathbb{Z}\}$ es un conjunto cerrado en $\mathrm{Spec}(\mathbb{Z})$, por lo que su preimagen bajo $\varphi^{\#}$ también es un conjunto cerrado en $X = \mathrm{Spec}\left(\mathbb{Z}\left[\sqrt{3}\right]\right)$. Esta observación generará dos tipos de conjuntos cerrados en X, los cuales dependen de p.

- Si $x^2 - 3$ no tiene raíces en $\mathbb{Z}/p\mathbb{Z}$, entonces la preimagen de $\{p\mathbb{Z}\}$ bajo $\varphi^{\#}$ corresponde al singletón $\{p\mathbb{Z}\left[\sqrt{3}\right]\}$.
- Si $x^2 - 3$ tiene a $\alpha \in \mathbb{Z}/p\mathbb{Z}$ como raíz, entonces la preimagen de $\{p\mathbb{Z}\}$ bajo $\varphi^{\#}$ corresponde al siguiente conjunto con dos puntos.

  $$\left\{p\mathbb{Z}[\sqrt{3}] + (\sqrt{3} - \alpha)\mathbb{Z}[\sqrt{3}] \ , \ p\mathbb{Z}[\sqrt{3}] + (\sqrt{3} + \alpha)\mathbb{Z}[\sqrt{3}]\right\}.$$

  Por ahora designemos por Q y $\overline{Q}$ a los ideales primos $p\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3} - \alpha\right)\mathbb{Z}\left[\sqrt{3}\right]$ y $p\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3} + \alpha\right)\mathbb{Z}\left[\sqrt{3}\right]$, respectivamente. Recordemos que

  $$V(Q) = \{P \in X \mid Q \subset P\}$$

  es un conjunto cerrado en $X = \mathrm{Spec}\left(\mathbb{Z}\left[\sqrt{3}\right]\right)$. Dado que los únicos ideales primos que contienen a p son precisamente Q y $\overline{Q}$, pero ninguno de ellos contiene al otro, la afirmación $Q \subset P$ será verdadera si y solamente si $P = Q$. De esta manera, $V(Q) = \{Q\}$ y el singletón $\{Q\}$ será cerrado en X. De manera análoga podemos advertir que el singletón $\left\{\overline{Q}\right\}$ también es cerrado en X.

En cualquier caso podremos concluir que cada singletón $\{P\}$ es cerrado en X siempre y cuando $P \neq \{0\}$.

Ejemplo 3.3.8. En este ejemplo investigaremos algunas características del espacio $X = \operatorname{Spec}\left(\mathbb{Z}\left[\sqrt{3}\right]\right)$ junto con su haz estructural $\mathcal{O}_X$. Para tal efecto, consideremos $p = 2$ y el ideal primo asociado a p, es decir,

$$Q = 2\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}+1\right)\mathbb{Z}\left[\sqrt{3}\right].$$

Notemos que $2 = \left(\sqrt{3}+1\right)\left(\sqrt{3}-1\right)$, por lo que de hecho Q es un ideal principal generado por $\sqrt{3}+1$. Si denotamos por $R = \mathbb{Z}\left[\sqrt{3}\right]$ y $X = \operatorname{Spec}(R)$, recordemos que

$$X_{\sqrt{3}+1} = \left\{P \in X \mid \sqrt{3}+1 \notin P\right\}$$

es un abierto basal de X con respecto a la topología de Zariski. Es claro que $\sqrt{3}+1 \in Q$. Supongamos que existe otro ideal primo $P \in X$ tal que $\sqrt{3}+1 \in P$. Luego $\left(\sqrt{3}+1\right)\left(\sqrt{3}-1\right) = 2 \in P$. Por el corolario 3.3.5 y la caracterización de los ideales primos de $\mathbb{Z}\left[\sqrt{3}\right]$ expuesta en el ejemplo 3.3.3, el único ideal primo de R que contiene a 2 es precisamente Q, por lo que concluimos que $P = Q$. De esta manera,

$$X_{\sqrt{3}+1} = X - \{Q\}.$$

Por razones análogas, podemos afirmar que

$$X_2 = \{P \in X \mid 2 \notin P\} = X - \{Q\},$$

por lo que $X_{\sqrt{3}+1}$ y X_2 representan exactamente el mismo abierto basal de X.

Según la definición del haz estructural sobre X, tenemos

$$\mathcal{O}_X\left(X_{\sqrt{3}+1}\right) = \mathcal{R}_{\sqrt{3}+1} = \left\{\frac{r}{\left(\sqrt{3}+1\right)^m} \;\middle|\; r \in R \text{ y } m \in \mathbb{N}\right\}$$

$$\mathcal{O}_X\left(X_2\right) = \mathcal{R}_2 = \left\{\frac{r}{2^m} \;\middle|\; r \in R \text{ y } m \in \mathbb{N}\right\}.$$

Si bien estos anillos lucen distintos, en realidad coinciden, ya que

$$\frac{1}{\sqrt{3}+1} = \frac{\sqrt{3}-1}{2} \in \mathcal{R}_2 \quad \text{y} \quad \frac{1}{2} = \frac{\sqrt{3}+2}{\left(\sqrt{3}+1\right)^2} \in \mathcal{R}_{\sqrt{3}+1}.$$

Ejemplo 3.3.9. Otro ejemplo interesante ocurre si elegimos $p = 11$. En este caso, los ideales primos de $R = \mathbb{Z}\left[\sqrt{3}\right]$ asociados a p corresponden a

$$Q = 11\mathbb{Z}\big[\sqrt{3}\big] + \big(\sqrt{3}-5\big)\mathbb{Z}\big[\sqrt{3}\big] \quad \text{y} \quad \overline{Q} = 11\mathbb{Z}\big[\sqrt{3}\big] + \big(\sqrt{3}+5\big)\mathbb{Z}\big[\sqrt{3}\big].$$

En este punto podemos notar que

$$\begin{aligned} 11 &= \big(2\sqrt{3}+1\big)\big(2\sqrt{3}-1\big) \\ \sqrt{3}-5 &= \big(2\sqrt{3}+1\big)\big(1-\sqrt{3}\big) \\ \sqrt{3}+5 &= \big(2\sqrt{3}-1\big)\big(1+\sqrt{3}\big). \end{aligned}$$

Luego, los ideales Q y $\overline{Q}$ son principales. Explícitamente,

$$Q = \big(2\sqrt{3}+1\big)\mathbb{Z}\big[\sqrt{3}\big] \quad \text{y} \quad \overline{Q} = \big(2\sqrt{3}-1\big)\mathbb{Z}\big[\sqrt{3}\big].$$

Se puede probar de manera rutinaria que estos ideales son distintos, ya que, por ejemplo, $2\sqrt{3}+1 \notin \overline{Q}$. Más aún, Q es el único ideal primo que contiene a $2\sqrt{3}+1$. Para probar este hecho, supongamos que P es algún ideal primo tal que $2\sqrt{3}+1 \in P$. Luego $\left(2\sqrt{3}+1\right)\left(2\sqrt{3}-1\right) = 11 \in P$ y por el corolario 3.3.5 y el ejemplo 3.3.3, los únicos ideales primos que contienen a 11 son Q y $\overline{Q}$. Como este último ideal no contiene a $2\sqrt{3}+1$, concluimos que $P = Q$.

De esta manera, sobre el espacio topológico $X = \operatorname{Spec}\left(\mathbb{Z}\left[\sqrt{3}\right]\right)$ podemos construir el abierto basal

$$X_{2\sqrt{3}+1} = \left\{P \in X \mid 2\sqrt{3}+1 \notin P\right\} = X - \{Q\},$$

el cual va asociado con el anillo conmutativo

$$\mathcal{O}_X\left(X_{2\sqrt{3}+1}\right) = \mathcal{R}_{2\sqrt{3}+1} = \left\{ \frac{r}{\left(2\sqrt{3}+1\right)^m} \;\middle|\; r \in R \text{ y } m \in \mathbb{N} \right\}.$$

Por otro lado, podemos considerar el abierto basal

$$X_{11} = \{P \in X \mid 11 \notin P\} = X - \left\{Q, \overline{Q}\right\},$$

el cual va asociado con el anillo conmutativo

$$\mathcal{O}_X\left(X_{11}\right) = \mathcal{R}_{11} = \left\{ \frac{r}{11^m} \;\middle|\; r \in R \text{ y } m \in \mathbb{N} \right\}.$$

Notemos en este caso que $X_{2\sqrt{3}+1} \supset X_{11}$ y la función de restricción corresponde a

$$\begin{array}{rccc} \rho_{X_{2\sqrt{3}+1}, X_{11}}: & \mathcal{R}_{2\sqrt{3}+1} & \to & \mathcal{R}_{11} \\ & \dfrac{r}{\left(2\sqrt{3}+1\right)^m} & \mapsto & \dfrac{r\left(2\sqrt{3}-1\right)^m}{11^m}. \end{array}$$

Antes de exponer el último ejemplo correspondiente a esta sección, utilizaremos los siguientes resultados.

Proposición 3.3.10. *Sean R y R' dos anillos conmutativos con identidad, $S \subset R$ un conjunto multiplicativamente cerrado y $\varphi : R \to R'$ un homomorfismo de anillos conmutativos con identidad. Si $\varphi(S)$ solamente contiene elementos invertibles en R', entonces existe un único homomorfismo de anillos conmutativos con identidad $\overline{\varphi} : S^{-1}R \to R'$ que satisface $\overline{\varphi}\left(\frac{r}{1}\right) = \varphi(r)$ para todo $r \in R$.*

Demostración. Supongamos que existe tal homomorfismo $\overline{\varphi}$. En particular, deberá cumplirse $\overline{\varphi}\left(\frac{s}{1}\right) = \varphi(s)$ para todo $s \in S$. Dado que $\overline{\varphi}$ es un homomorfismo de anillos conmutativos con identidad, tendremos que

$$\begin{aligned} \overline{\varphi}\left(1\right) &= 1 \\ \overline{\varphi}\left(\frac{s}{s}\right) &= 1 \\ \overline{\varphi}\left(\frac{s}{1} \cdot \frac{1}{s}\right) &= 1 \\ \overline{\varphi}\left(\frac{s}{1}\right) \cdot \overline{\varphi}\left(\frac{1}{s}\right) &= 1 \\ \varphi(s) \cdot \overline{\varphi}\left(\frac{1}{s}\right) &= 1. \end{aligned}$$

Como $\varphi(s)$ es un elemento invertible en R', obtenemos

$$\overline{\varphi}\left(\frac{1}{s}\right) = \varphi(s)^{-1}.$$

De esta manera, podemos construir un único homomorfismo de anillos conmutativos con identidad con las características solicitadas a partir de φ. Este homomorfismo viene dado por

$$\overline{\varphi}\left(\frac{r}{s}\right) = \overline{\varphi}\left(\frac{r}{1}\cdot\frac{1}{s}\right) = \overline{\varphi}\left(\frac{r}{1}\right)\cdot\overline{\varphi}\left(\frac{1}{s}\right) = \varphi(r)\cdot\varphi(s)^{-1}.$$

Es sencillo probar que $\overline{\varphi}$ es efectivamente un homomorfismo de anillos conmutativos con identidad, es decir, que para todos $r,t \in R$ y $s,u \in S$ se cumple

$$\overline{\varphi}\left(\frac{r}{s}+\frac{t}{u}\right) = \overline{\varphi}\left(\frac{r}{s}\right)+\overline{\varphi}\left(\frac{t}{u}\right) \quad \text{y} \quad \overline{\varphi}\left(\frac{r}{s}\cdot\frac{t}{u}\right) = \overline{\varphi}\left(\frac{r}{s}\right)\cdot\overline{\varphi}\left(\frac{t}{u}\right). \qquad \blacklozenge$$

Proposición 3.3.11. *Sea R un anillo conmutativo con identidad, M algún ideal maximal de R y $S = R - M$, el cual es un conjunto multiplicativamente cerrado. Entonces*

$$\left(S^{-1}R\right) / \left(S^{-1}M\right) \cong R/M.$$

Demostración. Consideremos

$$\begin{array}{rccc} \pi: & R & \to & R/M \\ & r & \mapsto & r+M \end{array}$$

la función sobreyectiva de proyección natural. En este caso, $\ker(\pi) = M$ y el conjunto $\pi(S) = \pi(R-M)$ contiene a todos los elementos no nulos del anillo R/M. Dado que M es un ideal maximal en R, R/M es un cuerpo y $\pi(S)$ está constituido por todos los elementos invertibles de R/M. Por la proposición 3.3.10, podemos construir el siguiente homomorfismo de anillos conmutativos con identidad.

$$\begin{array}{rccc} \overline{\pi}: & S^{-1}R & \to & R/M \\ & \dfrac{r}{s} & \mapsto & \pi(r)\pi(s)^{-1} = (r+M)(s+M)^{-1}. \end{array}$$

Además, notemos que

$$\begin{aligned} \ker(\overline{\pi}) &= \left\{ \frac{r}{s} \in S^{-1}R \;\middle|\; (r+M)(s+M)^{-1} = 0+M \right\} \\ &= \left\{ \frac{r}{s} \in S^{-1}R \;\middle|\; r+M = 0+M \right\} \\ &= \left\{ \frac{r}{s} \in S^{-1}R \;\middle|\; r \in M \right\} \\ &= S^{-1}M. \end{aligned}$$

Finalmente, dado que $\overline{\pi}$ es una función sobreyectiva, el resultado de la proposición se obtiene

directamente del primer teorema del isomorfismo de anillos (ver [4], página 243).

$$\left(S^{-1}R\right)/\ker\left(\overline{\pi}\right) \cong \overline{\pi}\left(S^{-1}R\right) \quad \Leftrightarrow \quad \left(S^{-1}R\right)/\left(S^{-1}M\right) \cong R/M. \qquad \blacklozenge$$

Observación 3.3.12. Con respecto a la proposición 3.3.11, es indispensable que M sea un ideal maximal de R. En general, si P es algún ideal primo de R y $S = R - P$, entonces $\mathcal{R}_P = S^{-1}R$ es un anillo local cuyo único ideal maximal es $S^{-1}P$ (ver ejemplo 3.1.2). Por esta razón, $\left(S^{-1}R\right)/\left(S^{-1}P\right)$ siempre será un cuerpo. Sin embargo, R/P es apenas un dominio de integridad, el cual será isomorfo a $\left(S^{-1}R\right)/\left(S^{-1}P\right)$ solamente en caso de que P sea un ideal maximal de R.

Ejemplo 3.3.13. Sea $R = \mathbb{Z}\left[\sqrt{3}\right]$. En este último ejemplo estudiaremos algunas características locales del esquema $X = \mathrm{Spec}(R)$.

En primer lugar, consideremos $p = 2$ y P su respectivo ideal primo asociado en R, es decir,

$$P = 2\mathbb{Z}\left[\sqrt{3}\right] + \left(\sqrt{3}+1\right)\mathbb{Z}\left[\sqrt{3}\right] = \left(\sqrt{3}+1\right)\mathbb{Z}\left[\sqrt{3}\right].$$

La localización de R en P corresponde a

$$\mathcal{R}_P = \left\{ \frac{r}{s} \;\middle|\; r \in R \text{ y } s \in R - P \right\}.$$

Según lo expuesto en el ejemplo 3.1.2, el anillo anterior es un anillo local cuyo único ideal maximal es

$$P\mathcal{R}_P = \left\{ \frac{r}{s} \;\middle|\; r \in P \text{ y } s \in R - P \right\} = \left\{ \frac{\left(\sqrt{3}+1\right) r}{s} \;\middle|\; r \in R \text{ y } s \in R - P \right\}.$$

Dado que P es también un ideal maximal de R, gracias a la proposición 3.3.11 tenemos que

$$\mathcal{R}_P/P\mathcal{R}_P \cong R/P.$$

Notemos que cualquier elemento en R se puede representar como

$$r = a + b\sqrt{3} = a + b\left(\sqrt{3} + 1 - 1\right) = a - b + b\left(\sqrt{3}+1\right),$$

donde $a, b \in \mathbb{Z}$. Por lo tanto $r \in R$ y $a - b \in \mathbb{Z}$ pertenecen a la misma clase de equivalencia en el cuerpo R/P. Como además P contiene a todos los múltiplos de 2 en R, R/P contiene únicamente

dos clases de equivalencia y por ende

$$\mathcal{R}_P/P\mathcal{R}_P \cong R/P \cong \mathbb{F}_2.$$

En segundo lugar, consideremos ahora $p = 5$ y P su respectivo ideal primo asociado en R, es decir, $P = 5\mathbb{Z}\left[\sqrt{3}\right]$. En este caso, la localización de R en P es

$$\mathcal{R}_P = \left\{ \frac{r}{s} \;\middle|\; r \in R \text{ y } s \in R - P \right\},$$

el cual también es un anillo local y su único ideal maximal corresponde a

$$P\mathcal{R}_P = \left\{ \frac{r}{s} \;\middle|\; r \in P \text{ y } s \in R - P \right\} = \left\{ \frac{5r}{s} \;\middle|\; r \in R \text{ y } s \in R - P \right\}.$$

Puesto que P nuevamente es un ideal maximal de R, tenemos

$$\mathcal{R}_P/P\mathcal{R}_P \cong R/P.$$

Ahora bien, cualquier elemento en R se puede representar como $r = a + b\sqrt{3}$, donde $a, b \in \mathbb{Z}$. Pero además, al identificar módulo 5 aparecerán solo 25 clases de equivalencia en el cuerpo cociente R/P, a saber,

$$R/P = \left\{ \left(a + b\sqrt{3}\right) + P \;\middle|\; a, b \in \{0, 1, 2, 3, 4\} \right\}.$$

El único cuerpo con 25 elementos es la extensión cuadrática de $\mathbb{Z}/5\mathbb{Z}$, por lo que concluimos que

$$\mathcal{R}_P/P\mathcal{R}_P \cong R/P \cong \mathbb{F}_{25}.$$

Podemos generalizar estos resultados. Si elegimos cualquier entero primo $p \in \mathbb{Z}$, entonces existen dos opciones.

- Si el polinomio $x^2 - 3$ no tiene raíces en $\mathbb{Z}/p\mathbb{Z}$, entonces el único ideal primo asociado a p es $P = p\mathbb{Z}\left[\sqrt{3}\right]$ y
$$\mathcal{R}_P/P\mathcal{R}_P \cong R/P \cong \mathbb{F}_{p^2}.$$
- Si el polinomio $x^2 - 3$ tiene a $\alpha \in \mathbb{Z}/p\mathbb{Z}$ como raíz, entonces existen solo dos ideales primos

asociado a p. Ellos son

$$P = p\mathbb{Z}\big[\sqrt{3}\big] + \big(\sqrt{3} - \alpha\big)\mathbb{Z}\big[\sqrt{3}\big] \quad \text{y} \quad \overline{P} = p\mathbb{Z}\big[\sqrt{3}\big] + \big(\sqrt{3} + \alpha\big)\mathbb{Z}\big[\sqrt{3}\big].$$

Estos ideales coincidirán solamente si $p = 2$ o $p = 3$. Independiente de ello, siempre se cumplirá que

$$\mathcal{R}_P/P\mathcal{R}_P \cong \mathcal{R}_{\overline{P}}/\overline{P}\mathcal{R}_{\overline{P}} \cong R/P \cong R/\overline{P} \cong \mathbb{F}_p.$$

Por último, estudiemos el comportamiento local del esquema $X = \mathrm{Spec}(R)$ en torno al ideal primo $P = \{0\}$. En este caso, la localización de R en P corresponde a

$$\mathcal{R}_P = \left\{ \frac{r}{s} \;\middle|\; r \in R \text{ y } s \in R - \{0\} \right\} \cong \mathbb{Q}\big[\sqrt{3}\big].$$

Este anillo de hecho es un cuerpo, por lo que su único ideal propio es $P\mathcal{R}_P = \{0\}$, el cual también es maximal. Por esta razón es evidente que

$$\mathcal{R}_P/P\mathcal{R}_P \cong \mathbb{Q}\big[\sqrt{3}\big].$$

Conclusiones y proyecciones

Al finalizar el capítulo 1, dimos la definición de un *esquema afín*, la cual toma como punto de partida un anillo conmutativo con identidad R, el espacio topológico $X = \mathrm{Spec}(R)$ y el haz estructural de anillos conmutativos $\mathcal{O}_X$ construido y detallado en ese capítulo. En resumen, un esquema afín se construye a partir de un anillo conmutativo con identidad R.

Sin embargo, podemos ampliar nuestra visión. Para tal efecto, la idea consiste en tomar como punto de partida cualquier espacio topológico X y así poder definir un esquema de manera general (no necesariamente un esquema afín). De esta forma, si nuestro objetivo fuese estudiar esquemáticamente algún espacio topológico, entonces no sería primordial el hecho de contar con un anillo conmutativo con identidad R como base de nuestro análisis. Ante esta situación, podría surgirnos la siguiente inquietud. Si el asunto sobre los esquemas afines ya es bastante complejo de digerir, ¿para qué seguir complicándolo aún más? Existen varias razones.

(i) Los esquemas afines tienen el siguiente problema. Si restringimos un esquema afín a algún subconjunto abierto de él, entonces el esquema resultante podría no ser afín. Por lo tanto, la noción de un esquema en general nos entregará mucha más flexibilidad.

(ii) Existen muchos ejemplos interesantes de esquemas que no son afines, como por ejemplo los esquemas proyectivos y los espacios con puntos dobles.

(iii) Probablemente la razón más importante para estudiar los esquemas de manera general es que no ganamos absolutamente nada con quedarnos solo con la teoría de los esquemas afines. La categoría de los esquemas afines es anti-equivalente a la categoría de los anillos conmutativos con identidad (ver [2], página 30), por lo que cualquier estudio que queramos realizar sobre

los esquemas afines, podremos hacerlo igual de bien solamente con la teoría de los anillos conmutativos con identidad.

De manera rudimentaria, un esquema en general consiste en un espacio topológico X junto con un haz de anillos conmutativos con identidad $\mathcal{O}_X$ sobre X de tal manera que la pareja $(X, \mathcal{O}_X)$ es localmente afín. Esto último significa que X se puede recubrir mediante abiertos U_i tales que la restricción del haz $\mathcal{O}_X$ sobre cada abierto U_i es ahora un esquema afín, es decir, existen anillos conmutativos con identidad R_i tales que los esquemas $\left(U_i, \mathcal{O}_X|_{U_i}\right)$ y $\left(\operatorname{Spec}(R_i), \mathcal{O}_{\operatorname{Spec}(R_i)}\right)$ son isomorfos.

Este enfoque más extenso nos entregará herramientas contundentes que permiten estudiar variedades algebraicas afines y proyectivas, e incluso podremos utilizar estos nuevos conceptos para analizar algunos problemas relacionados con geometría aritmética. En conclusión la teoría de los esquemas es una amalgama de métodos aplicables a varios problemas que nacen desde la geometría algebraica y la teoría de números, y que además utiliza ingredientes de diversas áreas de la matemática, como el álgebra conmutativa, la topología y la teoría de categorías.

Bibliografía

[1] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[2] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197. Springer Science & Business Media, 2006.

[3] Kenji Ueno. *Algebraic Geometry: From algebraic varieties to schemes*, volume 1. American Mathematical Soc., 1999.

[4] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[5] James Munkres. *Topology*. Pearson Education, 2014.

[6] Daniel A Marcus. *Number fields*, volume 8. Springer, 1977.

Anexo A

Nociones sobre la teoría de categorías

Definición A.1. Una *categoría* consiste en una colección de *objetos* junto con *morfismos* entre cada pareja de objetos. Más específicamente, dados dos objetos A y B en la categoría $\mathcal{C}$, los morfismos entre A y B forman un conjunto denotado por $\mathrm{Hom}(A, B)$, los cuales deben satisfacer las siguientes propiedades.

(i) Para cualquier objeto A, el conjunto $\mathrm{Hom}(A, A)$ debe contener un elemento llamado *morfismo identidad* y denotado por id_A;

(ii) Dados dos morfismos $\varphi \in \mathrm{Hom}(B, C)$ y $\psi \in \mathrm{Hom}(A, B)$, debe existir el *morfismo composición* de φ con ψ, el cual se denotará por $\varphi \circ \psi \in \mathrm{Hom}(A, C)$. La composición de morfismos debe satisfacer dos axiomas naturales.

- Para todo $\varphi \in \mathrm{Hom}(A, B)$ se cumple que $\varphi \circ \mathrm{id}_A = \mathrm{id}_B \circ \varphi = \varphi$;
- Para todos $\chi \in \mathrm{Hom}(A, B)$, $\psi \in \mathrm{Hom}(B, C)$ y $\varphi \in \mathrm{Hom}(C, D)$ se cumple que $(\varphi \circ \psi) \circ \chi = \varphi \circ (\psi \circ \chi)$.

Un morfismo $\varphi \in \mathrm{Hom}(A, B)$ se llama *isomorfismo* si es que existe un segundo morfismo $\psi \in \mathrm{Hom}(B, A)$ de modo que $\psi \circ \varphi = \mathrm{id}_A$ y $\varphi \circ \psi = \mathrm{id}_B$. Denotaremos al conjunto de todos los isomorfismos entre los objetos A y B por $\mathrm{Isom}(A, B)$.

Una *subcategoría* de una categoría $\mathcal{C}$ es simplemente una categoría $\mathcal{D}$ la cual consta de algunos objetos y algunos morfismos de $\mathcal{C}$. La subcategoría se llamará *completa* si dados dos objetos A y B en $\mathcal{D}$, todos los $\mathcal{C}-$morfismos entre A y B también son morfismos en $\mathcal{D}$.

Ejemplo A.2. Algunas categorías comunes y sencillas son las siguientes.

(i) **Con** es la categoría de los conjuntos. Dados dos conjuntos A y B, $\mathrm{Hom}(A, B)$ es el conjunto de todas las funciones con dominio A y codominio B.

(ii) **Gr** es la categoría de los grupos. Dados dos grupos A y B, $\mathrm{Hom}(A, B)$ es el conjunto de todos los homomorfismos de grupo $h : A \to B$.

(iii) **Ab** es la categoría de grupos abelianos, la cual es una subcategoría completa de **Gr**.

(iv) **Top** es la categoría de los espacios topológicos. Dados dos espacios topológicos X e Y, $\mathrm{Hom}(X, Y)$ es el conjunto de todas las funciones continuas $f : X \to Y$.

Definición A.3. Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ dos categorías. Un *functor covariante* F desde $\mathcal{C}_1$ a $\mathcal{C}_2$ es un regla que

(i) asocia a cada objeto A en $\mathcal{C}_1$ un objeto $F(A)$ en $\mathcal{C}_2$;

(ii) asocia a cada morfismo $\varphi \in \mathrm{Hom}(A, B)$ en $\mathcal{C}_1$ un morfismo $F(\varphi) \in \mathrm{Hom}(F(A), F(B))$ en $\mathcal{C}_2$ de manera tal que se verifican las siguientes propiedades.

- Para cada objeto A en $\mathcal{C}_1$ se cumple que $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$;
- Para cualquier pareja de morfismos $\psi \in \mathrm{Hom}(A, B)$ y $\varphi \in \mathrm{Hom}(B, C)$, ambos en $\mathcal{C}_1$, se cumple que $F(\varphi \circ \psi) = F(\varphi) \circ F(\psi)$.

Ejemplo A.4. Consideremos la categoría **Gr** de los grupos junto con los homomorfismos de grupos y la categoría **Con** de los conjuntos con las funciones entre conjuntos. Podemos construir un functor covariante F desde **Gr** a **Con** de manera muy simple. Dado un grupo G, definimos $F(G)$ como aquel conjunto formado por los elementos de G, y dado cualquier homomorfismo $\varphi \in \mathrm{Hom}(G, H)$, definimos $F(\varphi)$ como la misma función subyacente entre los conjuntos $F(G)$ y $F(H)$. En cierto sentido, el functor F nos muestra algo muy obvio; nos indica que cualquier grupo es en realidad un conjunto con un poco de estructura adicional, mientras que cualquier homomorfismo de grupos es simplemente una función entre dos conjuntos con algunas propiedades extras. Informalmente, podemos pensar que F se olvida de la estructura de grupo, y en su lugar trata a estos objetos como simples conjuntos. Por esta razón, a esta clase de functores se les denomina *functores olvidadizos*.

Definición A.5. Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ dos categorías. Un *functor contravariante* F desde $\mathcal{C}_1$ a $\mathcal{C}_2$ es un regla que

(i) asocia a cada objeto A en $\mathcal{C}_1$ un objeto $F(A)$ en $\mathcal{C}_2$;

(ii) asocia a cada morfismo $\varphi \in \mathrm{Hom}(A, B)$ en $\mathcal{C}_1$ un morfismo $F(\varphi) \in \mathrm{Hom}(F(B), F(A))$ en $\mathcal{C}_2$ de manera tal que se verifican las siguientes propiedades.

- Para cada objeto A en $\mathcal{C}_1$ se cumple que $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$;
- Para cualquier pareja de morfismos $\psi \in \mathrm{Hom}(A, B)$ y $\varphi \in \mathrm{Hom}(B, C)$, ambos en $\mathcal{C}_1$, se cumple que $F(\varphi \circ \psi) = F(\psi) \circ F(\varphi)$.

Ejemplo A.6. Sea $\mathbf{Vec}_k$ la categoría de todos los espacios vectoriales sobre un cuerpo fijo k. La regla que asigna a cada espacio vectorial V su espacio dual V^* y a cada transformación lineal $T : V \to W$ la transformación lineal dual $T^* : W^* \to V^*$ es un functor contravariante desde $\mathbf{Vec}_k$ sobre sí misma.

Definición A.7. Sean F y G dos functores covariantes entres las categorías $\mathcal{C}_1$ y $\mathcal{C}_2$. Un *morfismo de functores covariantes* Φ entre F y G es una colección de morfismos $\Phi_A : F(A) \to G(A)$ en $\mathcal{C}_2$ para todo objeto A en $\mathcal{C}_1$ de modo que para cualquier morfismo $\varphi : A \to B$ en $\mathcal{C}_1$ el siguiente diagrama conmuta.

$$\begin{array}{ccc} F(A) & \xrightarrow{\Phi_A} & G(A) \\ {\scriptstyle F(\varphi)}\downarrow & & \downarrow{\scriptstyle G(\varphi)} \\ F(B) & \xrightarrow[\Phi_B]{} & G(B) \end{array}$$

Además, el morfismo Φ es un *isomorfismo de functores covariantes* si cada Φ_A es un isomorfismo. En este caso anotaremos $F \cong G$.

Si ahora F y G son functores contravariantes, un *morfismo* (*isomorfismo*, resp.) *de functores contravariantes* se definirá de manera similar, con el reparo de que ahora es el siguiente diagrama el que conmutará.

$$\begin{array}{ccc} F(B) & \xrightarrow{\Phi_B} & G(B) \\ {\scriptstyle F(\varphi)}\downarrow & & \downarrow{\scriptstyle G(\varphi)} \\ F(A) & \xrightarrow[\Phi_A]{} & G(A) \end{array}$$

Ejemplo A.8. Dado R cualquier anillo conmutativo con identidad podemos construir el grupo de matrices invertibles de tamaño $n \times n$ con entradas en R, al cual denotaremos por $GL_n(R)$.

Ahora bien, cualquier homomorfismo de anillos conmutativos con identidad $f : R \to S$ inducirá un homomorfismo de grupos $GL_n(f) : GL_n(R) \to GL_n(S)$ dado por

$$(a_{ij})_{1\leq i,j\leq n} \mapsto (f\,(a_{ij}))_{1\leq i,j\leq n}\,.$$

Por otro lado, si denotamos por R^* al grupo de elementos invertibles de R, entonces el homomorfismo de anillos conmutativos con identidad $f : R \to S$ induce también un homomorfismo de grupos $f^* : R^* \to S^*$ el cual está dado por la restricción de f a R^*.

De hecho, GL_n y * son functores entre la categoría de los anillos conmutativos con identidad y la categoría de los grupos. Más aún, existe un morfismo entre estos functores conocido como *determinante*. El determinante de una matriz A con entradas en R se obtiene mediante la fórmula habitual (como sumas y productos de sus entradas).

Notemos que dada una matriz $A \in GL_n(R)$, entonces existe $B \in GL_n(R)$ de modo que $AB = I_R$. Por la propiedad multiplicativa del determinante (la cual sigue siendo válida para esta construcción generalizada), tenemos que

$$\det_R(AB) = \det_R(I_R) \Rightarrow\ \det_R(A) \cdot \det_R(B) = 1_R$$

Luego, $\det_R(A)$ es un elemento invertible en R cuyo inverso es $\det_R(B)$. Incluso es más, $\det_R : GL_n(R) \to R^*$ es un homomorfismo de grupos y se puede verificar que el siguiente diagrama conmuta.

$$\begin{array}{ccc} GL_n(R) & \xrightarrow{\det_R} & R^* \\ {\scriptstyle GL_n(f)}\downarrow & & \downarrow{\scriptstyle f^*} \\ GL_n(S) & \xrightarrow[\det_S]{} & S^* \end{array}$$

Observación A.9. Dadas dos categorías $\mathcal{C}_1$ y $\mathcal{C}_2$ podemos definir la *categoría de functores covariantes* del par $(\mathcal{C}_1, \mathcal{C}_2)$, cuyos objetos son los functores covariantes entre $\mathcal{C}_1$ y $\mathcal{C}_2$ y cuyos morfismos son los morfismos de functores covariantes. Cabe especificar que la regla de composición de dos morfismos de functores Φ y Ψ queda inducida por la composición de los morfismos Φ_A y Ψ_A para cada objeto A en $\mathcal{C}_1$. Más específicamente, si el morfismo Ψ corresponde a la colección $\Psi_A : F(A) \to G(A)$ y el morfismo Φ corresponde a la colección $\Phi_A : G(A) \to H(A)$, entonces el morfismo $\Phi \circ \Psi$ corresponde a la colección $\Phi_A \circ \Psi_A : F(A) \to H(A)$.

Definición A.10. Dos categorías $\mathcal{C}_1$ y $\mathcal{C}_2$ son *equivalentes* si existe un functor covariante F de $\mathcal{C}_1$ en $\mathcal{C}_2$ y un functor covariante G de $\mathcal{C}_2$ en $\mathcal{C}_1$ de modo que $F \circ G \cong \mathrm{id}_{\mathcal{C}_2}$ y $G \circ F \cong \mathrm{id}_{\mathcal{C}_1}$.

Si denotamos por Φ y Ψ a los isomorfismos entre $F \circ G$ e $\mathrm{id}_{\mathcal{C}_2}$ y $G \circ F$ e $\mathrm{id}_{\mathcal{C}_1}$ respectivamente, entonces diremos que G es el *functor casi-inverso* de F (y vice versa).

Más aún, si es posible encontrar functores covariantes F y G con $F \circ G = \mathrm{id}_{\mathcal{C}_2}$ y $G \circ F = \mathrm{id}_{\mathcal{C}_1}$, diremos que las categorías $\mathcal{C}_1$ y $\mathcal{C}_2$ son *isomorfas*.

Por último, definiremos categorías $\mathcal{C}_1$ y $\mathcal{C}_2$ *anti-equivalentes* (*anti-isomorfas, resp.*) de manera similar, pero ahora considerando functores F y G contravariantes. Notemos que en este caso los functores $F \circ G$ y $G \circ F$ son covariantes y esta definición adquiere sentido en comparación con lo estipulado anteriormente.

Observación A.11. Notemos que la definición de categorías equivalentes es por supuesto una relación de equivalencia. La antiequivalencia de categorías también es una relación de equivalencia, a pesar de que el nombre nos podría llevar a pensar de manera engañosa que esta relación es antisimétrica.

Ejemplo A.12. Sea k un cuerpo fijo. Las siguientes categorías son equivalentes.

(i) $\mathbf{Mat}_k$ cuyos objetos son los números naturales. Además, dados $m, n \in \mathbb{N}$, los morfismos entre

m y n corresponden a todas las matrices de tamaño $n \times m$ con entradas en k. En este caso anotamos $A \in \mathrm{Hom}(m, n)$.

(ii) $\mathbf{Vec}_k^F$ cuyos objetos son todos los espacios vectoriales sobre k de dimensión finita. Además, dados U y V dos espacios vectoriales sobre k de dimensión finita, los morfismos entre U y V corresponden a todas las transformaciones lineales $f : U \to V$. En este caso anotamos $f \in \mathrm{Hom}(U, V)$.

Podemos construir un functor covariante F entre $\mathbf{Mat}_k$ y $\mathbf{Vec}_k^F$ de la siguiente manera. Para cada objeto $n \in \mathbb{N}$ definimos $F(n) = k^n$. Además, dada $A \in \mathrm{Hom}(m, n)$, definimos $F(A)$ como aquella transformación lineal $F(A) : k^m \to k^n$ tal que $v \mapsto Av$.

Análogamente, podemos constuir un segundo functor covariante G entre $\mathbf{Vec}_k^F$ y $\mathbf{Mat}_k$. Para cada espacio vectorial sobre k de dimensión finita U definimos $G(U) = \dim_k(U)$. Además, dada $f \in \mathrm{Hom}(U, V)$, definimos $G(f)$ como la matriz asociada a f en algunas bases fijas $\mathcal{B}_U$ de U y $\mathcal{B}_V$ de V.

Se puede probar formalmente que los functores F y G dan origen a una equivalencia entre las categorías $\mathbf{Mat}_k$ y $\mathbf{Vec}_k^F$.

Ejemplo A.13. En general no es tarea fácil demostrar la equivalencia o anti-equivalencia de categorías. Es por esto que consideraremos un caso muy sencillo de estudiar.

Sea $\mathcal{C}_1$ una categoría con un único objeto denominado A, junto con un único morfismo, el cual no puede ser sino el morfismo identidad id_A.

Sea $\mathcal{C}_2$ una categoría con dos objetos distintos X e Y, junto con cuatro morfismos distintos: id_X, id_Y y dos isomorfismos $f : X \to Y$ y $g : Y \to X$ tales que $g \circ f = \mathrm{id}_X$ y $f \circ g = \mathrm{id}_Y$.

Probaremos que $\mathcal{C}_1$ y $\mathcal{C}_2$ no son categorías isomorfas, pero sí son equivalentes. Para tal efecto, construimos el siguiente functor covariante F entre $\mathcal{C}_1$ y $\mathcal{C}_2$.

$$F(A) = X \quad \text{y} \quad F(\mathrm{id}_A) = \mathrm{id}_X .$$

Asimismo, podemos construir el siguiente functor covariante G entre las categorías $\mathcal{C}_2$ y $\mathcal{C}_1$.

$$G(X) = G(Y) = A \quad \text{y} \quad G(\mathrm{id}_X) = G(\mathrm{id}_Y) = G(f) = G(g) = \mathrm{id}_A .$$

Notemos que

$$(G \circ F)(A) = A \quad \text{y} \quad (G \circ F)\left(\mathrm{id}_A\right) = \mathrm{id}_A,$$

y en consecuencia, $G \circ F = \mathrm{id}_{\mathcal{C}_1}$. Por otro lado, observemos que

$$\begin{aligned} &(F \circ G)(X) = (F \circ G)(Y) = X \\ \text{y} \quad &(F \circ G)\left(\mathrm{id}_X\right) = (F \circ G)(\mathrm{id}_Y) = (F \circ G)(f) = (F \circ G)(g) = \mathrm{id}_X, \end{aligned}$$

por lo que $F \circ G \neq \mathrm{id}_{\mathcal{C}_2}$. Sin embargo, podemos definir el siguiente morfismo Φ entre los functores covariantes $F \circ G$ e $\mathrm{id}_{\mathcal{C}_2}$.

$$\Phi_X = \mathrm{id}_X \quad \text{y} \quad \Phi_Y = f.$$

De hecho, Φ es un isomorfismo entre los functores $F \circ G$ e $\mathrm{id}_{\mathcal{C}_2}$. Esta construcción hace que los siguientes diagramas conmuten.

$$\begin{array}{ccc} (F \circ G)(X) & \xrightarrow{\Phi_X} & \mathrm{id}_{C_2}(X) \\ {\scriptstyle (F \circ G)(\mathrm{id}_X)}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{C_2}(\mathrm{id}_X)} \\ (F \circ G)(X) & \xrightarrow{\Phi_X} & \mathrm{id}_{C_2}(X) \end{array} \qquad \begin{array}{ccc} (F \circ G)(Y) & \xrightarrow{\Phi_Y} & \mathrm{id}_{C_2}(Y) \\ {\scriptstyle (F \circ G)(\mathrm{id}_Y)}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{C_2}(\mathrm{id}_Y)} \\ (F \circ G)(Y) & \xrightarrow{\Phi_Y} & \mathrm{id}_{C_2}(Y) \end{array}$$

$$\begin{array}{ccc} (F \circ G)(X) & \xrightarrow{\Phi_X} & \mathrm{id}_{C_2}(X) \\ {\scriptstyle (F \circ G)(f)}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{C_2}(f)} \\ (F \circ G)(Y) & \xrightarrow{\Phi_Y} & \mathrm{id}_{C_2}(Y) \end{array} \qquad \begin{array}{ccc} (F \circ G)(Y) & \xrightarrow{\Phi_Y} & \mathrm{id}_{C_2}(Y) \\ {\scriptstyle (F \circ G)(g)}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{C_2}(g)} \\ (F \circ G)(X) & \xrightarrow{\Phi_X} & \mathrm{id}_{C_2}(X) \end{array}$$

De esta manera, $F \circ G \cong \mathrm{id}_{\mathcal{C}_2}$ y efectivamente las categorías $\mathcal{C}_1$ y $\mathcal{C}_2$ son equivalentes.

Ejemplo A.14. Al igual que en el ejemplo A.13, consideremos $\mathcal{C}_1$ una categoría con un único objeto A, junto con el morfismo identidad id_A. Sea $\mathcal{C}_2$ una categoría con dos objetos distintos X e Y, pero ahora solamente consideraremos los morfismos id_X e id_Y. Es evidente que estas categorías no pueden ser equivalentes. Según lo expuesto en el ejemplo A.13, $\mathcal{C}_1$ y $\mathcal{C}_2$ podrían ser eventualmente equivalentes solamente en caso de que los objetos X e Y sean isomorfos.

Anexo B

Cuerpos de números

Definición B.1. Un *cuerpo de números* es un subcuerpo de $\mathbb{C}$ de grado finito sobre $\mathbb{Q}$.

Ejemplo B.2. $\mathbb{Q}$, $\mathbb{Q}\left(\sqrt{2}\right)$ y $\mathbb{Q}(i)$ son cuerpos de números. Por el teorema del elemento primitivo (ver [4], página 595), todos los cuerpos de números son de la forma $\mathbb{Q}(\alpha)$, donde $\alpha \in \mathbb{C}$ es un número algebraico.

Definición B.3. Sea $w = e^{2\pi i/m}$, donde $m \in \mathbb{N}$. El cuerpo $\mathbb{Q}(w)$ se conoce como *$m-$ésimo cuerpo ciclotómico.*

Ejemplo B.4.

Tabla B.1: Algunos cuerpos ciclotómicos.

m	$w = e^{2\pi i/m}$	$\mathbb{Q}(w)$
1	1	$\mathbb{Q}$
2	-1	$\mathbb{Q}$
3	$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$	$\mathbb{Q}\left(i\sqrt{3}\right)$
4	i	$\mathbb{Q}(i)$
5	$\frac{\sqrt{5}-1}{4} + i\frac{\sqrt{10+2\sqrt{5}}}{4}$	$\mathbb{Q}\left(\sqrt{5} + i\sqrt{10+2\sqrt{5}}\right)$
6	$\frac{1}{2} + i\frac{\sqrt{3}}{2}$	$\mathbb{Q}\left(i\sqrt{3}\right)$

En general, para m impar, el $m-$ésimo cuerpo ciclotómico coincide con el $2m-$ésimo, es decir, $\mathbb{Q}\left(e^{2\pi i/m}\right) = \mathbb{Q}\left(e^{\pi i/m}\right)$. Para probar este hecho, llamemos $\alpha = e^{\pi i/m}$. Es evidente que $\mathbb{Q}\left(\alpha^2\right) \subseteq$

$\mathbb{Q}(\alpha)$. Además, como m es impar, $\alpha = -\alpha^{m+1} = -\left(\alpha^2\right)^{\frac{m+1}{2}}$, por lo que $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}\left(\alpha^2\right)$.

Se puede probar que para m par, los $m-$ésimos cuerpos ciclotómicos son todos distintos (ver [6], página 27).

Definición B.5. Sea d un número entero no cuadrado perfecto. El cuerpo $\mathbb{Q}\left(\sqrt{d}\right)$ se conoce como *cuerpo cuadrático*. Si $d > 0$, este cuerpo se denomina *cuerpo cuadrático real*; si $d < 0$ se denomina *cuerpo cuadrático complejo*.

Ejemplo B.6. Los cuerpos $\mathbb{Q}\left(\sqrt{-3}\right)$ y $\mathbb{Q}(i)$ son cuerpos ciclotómicos y cuerpos cuadráticos complejos.

Definición B.7. Un número complejo se denomina *entero algebraico* si éste es raíz de algún polinomio mónico $p(x) \in \mathbb{Z}[x]$.

Ejemplo B.8.

(i) Si $n \in \mathbb{Z}$, entonces n es un entero algebraico, ya que n es raíz del polinomio mónico $x - n \in \mathbb{Z}[x]$.

(ii) Si d es un entero no cuadrado perfecto, entonces $\sqrt{d}$ es un entero algebraico, ya que éste es raíz del polinomio mónico $x^2 - d \in \mathbb{Z}[x]$.

(iii) Sea $m \in \mathbb{N}$. El número $w = e^{2\pi i/m}$ es un entero algebraico, ya que éste es raíz del polinomio mónico $x^m - 1 \in \mathbb{Z}[x]$.

Proposición B.9. *Los únicos enteros algebraicos en $\mathbb{Q}$ son precisamente los enteros.*

Demostración. Sea $\dfrac{m}{n} \in \mathbb{Q}$ un entero algebraico. Sin pérdida de generalidad, podemos asumir que m y n son relativamente primos. Sea $p(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ algún polinomio mónico tal que $p\left(\dfrac{m}{n}\right) = 0$. Luego,

$$\begin{aligned}
&\frac{m^r}{n^r} + a_{r-1}\frac{m^{r-1}}{n^{r-1}} + \cdots + a_1\frac{m}{n} + a_0 = 0 \\
&m^r + a_{r-1}m^{r-1}n + \cdots + a_1 mn^{r-1} + a_0 n^r = 0 \\
&m^r = -n\left(a_{r-1}m^{r-1} + \cdots + a_1 mn^{r-2} + a_0 n^{r-1}\right).
\end{aligned}$$

De este resultado, podemos deducir que n debe dividir a m^r. Dado que m.c.d.$(m, n) = 1$, necesariamente deberá suceder que $n = \pm 1$. ♦

Lema B.10. *Sea $f(x) \in \mathbb{Z}[x]$ un polinomio mónico y supongamos que $f(x) = g(x)h(x)$, donde $g(x)$ y $h(x)$ son polinomios mónicos en $\mathbb{Q}[x]$. Entonces, $g(x)$ y $h(x)$ pertencen a $\mathbb{Z}[x]$.*

Demostración. Sea m el mínimo común múltiplo de los denominadores de todos los coeficientes que aparece en $g(x)$. Entonces $mg(x) \in \mathbb{Z}[x]$ y los coeficientes de este polinomio no tienen ningún factor en común. Repetimos este mismo proceso con $h(x)$ para obtener $nh(x) \in \mathbb{Z}[x]$ con coeficientes sin factores en común. Mostraremos que $mn = 1$.

Supongamos que $mn > 1$. Elijamos cualquier entero primo p que divida a mn y notemos que $mnf(x) = mg(x) \cdot nh(x) \in \mathbb{Z}[x]$. Al reducir este polinomio módulo p, obtendremos $\overline{0} = \overline{mg(x)} \cdot \overline{nh(x)}$. Además, el anillo $(\mathbb{Z}/p\mathbb{Z})[x]$ es un dominio de integridad, por lo que $\overline{mg(x)} = \overline{0}$ o $\overline{nh(x)} = \overline{0}$. Esto nos dice que todos los coeficientes de $mg(x)$ son divisibles por p, o todos los coeficientes de $nh(x)$ son divisibles por p, lo cual es una contradicción.

Finalmente, como $mn = 1$, necesariamente $m = 1$ y $n = 1$. Concluimos que $g(x), h(x) \in \mathbb{Z}[x]$. ♦

Proposición B.11. *Sea α un entero algebraico y $f(x) \in \mathbb{Z}[x]$ un polinomio mónico de grado minimal que tenga a α como raíz. Entonces $f(x)$ es irreducible sobre $\mathbb{Q}[x]$.*

Demostración. Supongamos que $f(x)$ es reducible sobre $\mathbb{Q}[x]$, es decir, $f(x) = g(x)h(x)$, donde $g(x), h(x) \in \mathbb{Q}[x]$ son polinomios no constantes. Sin pérdida de generalidad, podemos asumir que tanto $g(x)$ como $h(x)$ son mónicos, ya que $f(x)$ lo es. Por el lema B.10, $g(x), h(x) \in \mathbb{Z}[x]$. Por lo tanto, α deberá ser, o raíz de $g(x)$, o raíz de $h(x)$, ambos con grado menor al grado de $f(x)$. Esto contradice la minimalidad del grado de $f(x)$. ♦

Corolario B.12. *Sea d un entero libre de cuadrados. El conjunto de enteros algebraicos en el cuerpo cuadrático $\mathbb{Q}(\sqrt{d})$ es*

(i) $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ *si* $d \equiv 2 \mod 4$ *o* $d \equiv 3 \mod 4$*;*

(ii) $\mathbb{Z} + \mathbb{Z}\dfrac{1+\sqrt{d}}{2}$ *si* $d \equiv 1 \mod 4$*.*

Demostración. Como d es un entero libre de cuadrados, d no puede ser múltiplo de 4. Es por esto que distinguimos los casos $d \equiv 1 \mod 4$, $d \equiv 2 \mod 4$ y $d \equiv 3 \mod 4$. Llamaremos R al conjunto de todos los enteros algebraicos contenidos en $\mathbb{Q}(\sqrt{d})$.

En primer lugar, probaremos que los anillos $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ y $\mathbb{Z} + \dfrac{1+\sqrt{d}}{2}\mathbb{Z}$ están contenidos en R, según sea el caso. Para tal efecto, basta con demostrar que $\beta = \sqrt{d} \in R$ si $d \equiv 2 \mod 4$ o $d \equiv 3 \mod 4$, y que $\gamma = \dfrac{1+\sqrt{d}}{2} \in R$ si $d \equiv 1 \mod 4$, esto pues R es un anillo. En el primer caso, notemos que β es

raíz del polinomio mónico $x^2 - d \in \mathbb{Z}[x]$. En el segundo caso, observemos que γ es raíz del polinomio mónico $x^2 - x - \dfrac{d-1}{4}$. Este último polinomio tiene coeficientes enteros, ya que $d \equiv 1 \mod 4$.

En segundo lugar, probaremos que el conjunto R formado por todos los enteros algebraicos en $\mathbb{Q}\big(\sqrt{d}\big)$ está contenido en $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ o $\mathbb{Z} + \dfrac{1+\sqrt{d}}{2}\mathbb{Z}$, según sea el caso. Sea $\alpha \in R$. Como $\alpha \in \mathbb{Q}\big(\sqrt{d}\big)$ existen $a, b \in \mathbb{Q}$ tales que $\alpha = a + b\sqrt{d}$. Si $b = 0$, entonces $\alpha = a \in \mathbb{Q}$ y dado que α es un entero algebraico, por la proposición B.9, se requiere $\alpha \in \mathbb{Z}$. En caso contrario, si $b \neq 0$, entonces el polinomio minimal de α en $\mathbb{Q}[x]$ es

$$f(x) = \big(x - \big(a + b\sqrt{d}\big)\big)\big(x - \big(a - b\sqrt{d}\big)\big) = x^2 - 2ax + a^2 - b^2 d \in \mathbb{Q}[x].$$

Además, dado que α es un entero algebraico, existe un polinomio $p(x) \in \mathbb{Z}[x]$ mónico tal que $p(\alpha) = 0$. Como $f(x)$ es el polinomio minimal de α en $\mathbb{Q}[x]$, podemos factorizar $p(x)$ como $p(x) = f(x)g(x)$, donde $g(x) \in \mathbb{Q}[x]$ también es un polinomio mónico. Por el lema B.10, $f(x) \in \mathbb{Z}[x]$, es decir,

$$2a \in \mathbb{Z} \quad \text{y} \quad a^2 - b^2 d \in \mathbb{Z}.$$

Estas condiciones se satisfacen, por supuesto, cuando $a, b \in \mathbb{Z}$.

Sin embargo, dado que $2a \in \mathbb{Z}$, también es posible que a admita la forma $a = m + \dfrac{1}{2}$, con $m \in \mathbb{Z}$. Probaremos que esta representación es posible única y exclusivamente cuando $d \equiv 1 \mod 4$.

Pues bien, sea $m \in \mathbb{Z}$ y $a = m + \dfrac{1}{2}$. De la segunda condición podemos concluir que

$$a^2 - b^2 d = \left(m + \frac{1}{2}\right)^2 - b^2 d = m^2 + m + \frac{1}{4} - b^2 d \in \mathbb{Z}.$$

Dado que $m^2 + m \in \mathbb{Z}$, deducimos que

$$\frac{1}{4} - b^2 d \in \mathbb{Z} \;\Leftrightarrow\; \frac{1 - 4b^2 d}{4} \in \mathbb{Z} \;\Leftrightarrow\; 1 - 4b^2 d \equiv 0 \mod 4 \;\Leftrightarrow\; 4b^2 d \equiv 1 \mod 4.$$

Si escribimos $b \in \mathbb{Q}$ como una fracción irreducible de la forma $b = \dfrac{r}{s}$, entonces

$$4b^2 d = \frac{4r^2 d}{s^2} \in \mathbb{Z}.$$

Como d es un entero libre de cuadrados, la fracción anterior será un entero solamente cuando s^2 divida a 4, esto es, $s = \pm 2$. De esta manera, b admite la forma $b = n + \frac{1}{2}$, donde $n \in \mathbb{Z}$. Luego, la condición $4b^2 d \equiv 1 \mod 4$ equivale a

$$4\left(n + \frac{1}{2}\right)^2 d \equiv 1 \mod 4 \Leftrightarrow 4n^2 d + 4nd + d \equiv 1 \mod 4 \Leftrightarrow d \equiv 1 \mod 4.$$

Bajo esta última condición para d, concluimos que

$$\alpha = a + b\sqrt{d} = m + \frac{1}{2} + \left(n + \frac{1}{2}\right)\sqrt{d} = (m-n) + (2n+1)\frac{1+\sqrt{d}}{2} \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}.$$

En caso de que $d \equiv 2 \mod 4$ o $d \equiv 3 \mod 4$, la única opción es que a y b sean ambos enteros. En este caso, $\alpha = a + b\sqrt{d} \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$. ♦

Proposición B.13. *Sea $\alpha \in \mathbb{C}$. Las siguientes proposiciones son equivalentes.*

(i) α es un entero algebraico;

(ii) el grupo aditivo del anillo $\mathbb{Z}[\alpha]$ es finitamente generado;

(iii) α pertenece a algún subanillo no nulo de $\mathbb{C}$ cuyo grupo aditivo es finitamente generado;

(iv) existe un subgrupo aditivo no nulo $A \subset \mathbb{C}$ finitamente generado tal que $\alpha A \subset A$.

Demostración.

$(i) \Rightarrow (ii)$ Si α es un entero algebraico, entonces α es raíz de algún polinomio mónico $p(x) \in \mathbb{Z}[x]$ de grado $n \geq 1$. De esta manera, el grupo aditivo $\mathbb{Z}[\alpha]$ queda generado por $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

$(ii) \Rightarrow (iii)$ Trivial. El mismo conjunto $\mathbb{Z}[\alpha]$ es un subanillo no nulo de $\mathbb{C}$ que contiene a α y su grupo aditivo es finitamente generado.

$(iii) \Rightarrow (iv)$ Trivial. Por hipótesis, existe un subanillo no nulo $A \subset \mathbb{C}$ con grupo aditivo finitamente generado tal que $\alpha \in A$. Como A tiene estructura de anillo, se tiene que $\alpha A \subset A$.

$(iv) \Rightarrow (i)$ Supongamos que A es un subgrupo aditivo no nulo de $\mathbb{C}$ generado por $\{a_1, a_2, \ldots, a_n\} \subset \mathbb{C}$ y que además satistace $\alpha A \subset A$. Podemos expresar cada αa_i como combinación lineal de

$a_1, a_2, \ldots, a_n$ con coeficientes en $\mathbb{Z}$.

$$\begin{cases} \alpha a_1 = \beta_{11}a_1 + \beta_{12}a_2 + \cdots + \beta_{1n}a_n \\ \alpha a_2 = \beta_{21}a_1 + \beta_{22}a_2 + \cdots + \beta_{2n}a_n \\ \quad \vdots \\ \alpha a_n = \beta_{n1}a_1 + \beta_{n2}a_2 + \cdots + \beta_{nn}a_n. \end{cases}$$

Reacomodando los términos, podemos plantear

$$\begin{pmatrix} \beta_{11} - \alpha & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} - \alpha & \cdots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} - \alpha \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Como los elementos $a_1, a_2, \ldots, a_n$ no son todos nulos, este sistema de ecuaciones en $\mathbb{C}$ debe tener infinitas soluciones. De esta manera,

$$\begin{vmatrix} \beta_{11} - \alpha & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} - \alpha & \cdots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} - \alpha \end{vmatrix} = 0.$$

Al desarrollar este determinante, obtendremos una ecuación del estilo

$$(-1)^n \alpha^n + \text{términos de orden inferior} = 0.$$

Finalmente, α es raíz de un polinimio mónico con coeficientes en $\mathbb{Z}$, es decir, α es un entero algebraico. ♦

Corolario B.14. *Si α y β son enteros algebraicos, entonces $\alpha + \beta$ y $\alpha\beta$ también lo son.*

Demostración. Sabemos que los grupos aditivos $\mathbb{Z}[\alpha]$ y $\mathbb{Z}[\beta]$ son finitamente generados. Si $\mathbb{Z}[\alpha] = \langle a_1, \ldots, a_m \rangle$ y $\mathbb{Z}[\beta] = \langle b_1, \ldots, b_n \rangle$, entonces $\mathbb{Z}[a, b] = \langle a_1 b_1, \ldots, a_m b_n \rangle$ también es un grupo aditivo finitamente generado. Finalmente, $\mathbb{Z}[\alpha, \beta]$ es un subanillo de $\mathbb{C}$ con grupo aditivo finitamente generado que contiene tanto a $\alpha + \beta$ como a $\alpha\beta$, y por la caracterización (iii) de la proposición B.13, $\alpha + \beta$ y $\alpha\beta$ son enteros algebraicos. ♦

Definición B.15. Denotaremos por $\mathbb{A}$ al subconjunto de $\mathbb{C}$ formado por todos los enteros algebraicos. Más aún, por el corolario B.14, $\mathbb{A}$ es un subanillo de $\mathbb{C}$.

Si K es cualquier cuerpo de números, entonces $\mathcal{O}_K = \mathbb{A} \cap K$ también es un subanillo de $\mathbb{C}$, el cual se conoce como el anillo de los enteros de K.