

# Notas de Geometría Algebraica

## Introducción a la Geometría de Esquemas.

Luis Manuel Reyes de la Luz

Mayo 2026

### Resumen

Segundo tema del parcial 4.

## Índice

|                                       |    |
|---------------------------------------|----|
| 1. Introducción                       | 1  |
| 2. El espectro de un anillo.          | 2  |
| 3. Ejemplos.                          | 4  |
| 3.1. Espacio Afin $K^n$ .             | 4  |
| 3.2. Spectro de $\mathbb{Z}$          | 6  |
| 3.3. Topología de Curvas Elípticas.   | 8  |
| 3.4. Los numeros Duales               | 9  |
| 4. La categoría de variedades afines. | 10 |
| A. Algunos lemas técnicos.            | 12 |

## 1. Introducción

La geometría algebraica que se ha construido hasta el momento, ha resultado de un diccionario entre los objetos algebraicos que son el conjunto de ceros de un polinomio y objetos geométricos que son  $k$ -álgebras finitas y reducidas. Todo ese diccionario se resume en el siguiente funtor

$$K[-]: \mathbf{Var}_K \longrightarrow K\text{-}\mathbf{Alg}^{f.r.}, X \mapsto K[X] := K[x_1, \dots, x_n]/I(X)$$

que genera una equivalencia de categorías. Este funtor establece un diccionario natural que permite traducir conceptos y problemas geométricos al lenguaje del álgebra. Con el tiempo, la teoría evolucionó para abordar cuestiones más generales, extendiendo su alcance hacia áreas que originalmente parecían ajenas al marco geométrico clásico. El paso decisivo para esta expansión fue replantear la noción central de este funtor a través de la siguiente interrogante:

**Cuestión 1.1 — Problema de la noción de Esquema.** Si  $R$  es un anillo conmutativo ¿Cual es el espacio geométrico cuyo anillo de funciones regulares es  $R$ ?

La respuesta a esta pregunta fue articulada por Alexander Grothendieck, transformando la estructura de la disciplina. Hasta ese momento, la geometría algebraica clásica exigía que los espacios estudiados (las variedades) estuvieran definidos sobre campos algebraicamente cerrados. Esta condición representaba un obstáculo para otras ramas de las matemáticas, particularmente para la teoría de números, donde el interés principal radica en el estudio de ecuaciones sobre campos finitos o sobre anillos no cerrados, como los números enteros.

La propuesta de Grothendieck consistió en postular que la pregunta anterior siempre admite una respuesta afirmativa: a todo anillo conmutativo, sin importar su naturaleza geométrica o aritmética, se le puede asociar un espacio intrínseco. Al introducir esta nueva generalización, se eliminó la dependencia de un campo base específico.

Como resultado, se logró unificar bajo un mismo marco teórico fenómenos que antes se trataban por separado: el estudio de las congruencias aritméticas y la geometría espacial se volvieron dos manifestaciones de la misma teoría de anillos. Esta síntesis proporcionó el lenguaje estructural que la comunidad matemática necesitaba para atacar problemas aritméticos y analíticos desde una perspectiva unificada. Gracias a esta base, fue posible formular y resolver cuestiones matemáticas profundas, destacando:

- *Las Conjeturas de Weil*: El problema clásico de contar el número de soluciones de ecuaciones sobre campos finitos requería una nueva topología. El marco de los esquemas permitió desarrollar la cohomología étale, la herramienta clave que finalmente demostró la análoga a la Hipótesis de Riemann en este contexto.
- *El Último Teorema de Fermat*: La demostración de Andrew Wiles no habría sido posible abordando el problema únicamente sobre los números racionales. Requirió estudiar las curvas elípticas y sus simetrías sobre anillos locales de enteros, utilizando esquemas de grupos y teoría de deformación geométrica.
- *La Conjetura de Mordell (Teorema de Faltings)*: Para probar que ciertas curvas polinomiales tienen un número finito de soluciones racionales, fue indispensable extender el estudio de estas curvas hacia "modelos" definidos sobre anillos de enteros (modelos de Néron), un enfoque exclusivo de la teoría de esquemas.
- *Los Teoremas GAGA (Geometría Algebraica y Geometría Analítica)*: Este principio estableció una equivalencia formal y rigurosa entre espacios algebraicos y espacios analíticos complejos compactos. Facilitó un diccionario donde teoremas difíciles de álgebra podían demostrarse usando herramientas sólidas del análisis funcional y diferencial.
- *La Geometría Rígida*: Para estudiar el análisis métrico sobre números  $p$ -ádicos (donde la topología clásica falla de forma contraintuitiva), los esquemas formales proporcionaron la base correcta. Esto permitió construir espacios analíticos rigurosos sobre campos no arquimedianos, abriendo una rama entera de la teoría de números contemporánea.

Es importante notar que el fundamento técnico de esta construcción descansa sobre la teoría de gavillas y espacios anillados. No obstante, para mantener el carácter pedagógico de esta introducción, prescindiremos inicialmente de esa maquinaria formal para centrarnos de lleno en los esquemas y su intuición algebraica.

## 2. El espectro de un anillo.

Si  $K$  es un campo algebraicamente cerrado, gracias al Nullstellensatz débil A.1 se tiene el siguiente resultado que clasifica las subvariedades con ideales del anillo de polinomios.

**Teorema 2.1 — Correspondencia Ideales y Conjuntos Algebraicos.** Sea  $k$  un campo algebraicamente cerrado entonces se tienen la siguiente biyección antitona

$$\begin{array}{ccc}
 \{ \text{Ideales Radicales.} \} & \xrightarrow{\sim} & \{ \text{Conjuntos Algebraicos.} \} \\
 \uparrow & & \uparrow \\
 \{ \text{Ideales primos.} \} & \xrightarrow{\sim} & \{ \text{Conjuntos Algebraicos Irreducibles.} \} \\
 \uparrow & & \uparrow \\
 \{ \text{Ideales maximales.} \} & \xrightarrow{\sim} & \{ \text{Puntos.} \}
 \end{array}$$

Sin embargo, cuando  $K$  no es algebraicamente cerrado, entonces esta biyección se puede rescatar como una inclusión, indicando que hay mas puntos que no son detectados por  $K^n$ . Específicamente, para un ideal  $J \subseteq K[x_1, \dots, x_n]$ , la correspondencia estricta falla y se debilita a la contención:

$$I(V(J)) \supseteq \sqrt{J}.$$

Debido a que la igualdad no está garantizada, la aplicación  $J \mapsto V(J)$  deja de ser inyectiva sobre el conjunto de ideales radicales. Diferentes ideales radicales pueden definir el mismo conjunto algebraico en  $K^n$ .

**Definición 2.1 — Espectro de un anillo.** Sea  $R$  un anillo, definimos su espectro como el espacio topológico:

$$X = \text{Spec}(R)$$

dotado de una conexión de Galois antitona

$$(I, V): \mathbf{P}(X) \longleftrightarrow \text{Id}(R)$$

donde

$$V(J) = \{ \mathfrak{p} \in X \mid I \subseteq \mathfrak{p} \}, J \trianglelefteq R$$

$$I(E) := \bigcap_{\mathfrak{p} \in E} \mathfrak{p}, E \subseteq X$$

y la topología de Zariski está dado por los conjuntos cerrados  $\{V(J)\}_{J \trianglelefteq R}$ .

Vamos a analizar como funciona este objeto geométrico para pensar a los elementos de  $R$  como el espacio de funciones de  $X$ .

Dado  $\mathfrak{p} \in R$  entonces su localización  $R_{\mathfrak{p}}$  es un anillo local con ideal maximal  $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ . Definimos su *campo de fracciones* como  $k(\mathfrak{p}) := \text{Frac}(R_{\mathfrak{p}})$ . Notemos que

$$k(\mathfrak{p}) \cong R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}.$$

Sea  $x = \mathfrak{p} \in X$  y  $f \in R$  definimos

$$f(x) := f + \mathfrak{m}_{\mathfrak{p}} \in A/\mathfrak{p}.$$

Esto define una función, que por abuso de notación denotamos  $f$  a

$$f: X \longrightarrow \prod_{x \in X} R/\mathfrak{p}_x \subseteq \prod_{x \in X} k(x)$$

**Observación 2.2** Las siguientes observaciones se cumplen:

1.  $f(x) = 0$  si y sólo si  $f \in \mathfrak{p}_x$
2.  $V(E) = \{x \in X \mid f(x) = 0 \forall f \in E\}$ ,  $E \subseteq R$  obteniendo  $V(E) = V(\langle E \rangle)$ .
3.  $I(Y) = \{f \in R \mid f(y) = 0, \forall y \in Y\}$ .
4.  $I(V(J)) = \text{rad}(J)$ .

gracias al teorema A.2 tenemos

**Proposición 2.3** Las siguientes afirmaciones son válidas:

1. Para  $x \in X$ , se tiene  $V(x) = \overline{\{x\}}$ .
2.  $x \in X$  es cerrado si y sólo si  $x$  es un ideal maximal en  $R$ .
3. La conexión antitona induce una biyección antitona entre

$$\{\text{Conjuntos cerrados en } X\} \cong \{J \subseteq R, J = \text{rad } J\}.$$

**Proposición 2.4** Sea  $f: R \rightarrow S$  un homomorfismo de anillos entonces la función

$$f^*: \text{Spec}(S) \longrightarrow \text{Spec}(R), \mathfrak{p} \mapsto f^{-1}(\mathfrak{p}).$$

es continua.

**Proposición 2.5** Las siguientes afirmaciones son válidas:

1. Para cada  $g \in R$  entonces el conjunto  $D(g) = X - V(g)$  es abierto y compacto.
2. Para cada ideal  $J \trianglelefteq R$  existe un homeomorfismo  $V(J) \cong \text{Spec}(R/J)$ .
3. Existe un homeomorfismo canonico  $\text{Spec} R \cong \text{Spec}(R/\text{rad } R)$ .

### 3. Ejemplos.

#### 3.1. Espacio Afín $K^n$ .

Consideremos un campo arbitrario  $K$  y sea  $X = \text{Spec}(K[x_1, \dots, x_n])$ . Consideremos la función

$$\phi: K^n \longrightarrow X, (a_1, \dots, a_n) \mapsto \langle x_1 - a_1, \dots, x_n - a_n \rangle.$$

Para entender la naturaleza de esta función, consideremos el grupo absoluto de Galois  $G_K := \text{Gal}(K^{\text{alg}}/K)$ . Cada elemento  $\sigma \in G_K$  induce el siguiente diagrama conmutativo:

$$\begin{array}{ccc} K^{\text{alg}} & \xrightarrow{\sigma} & K^{\text{alg}} \\ & \searrow & \nearrow \\ & K & \end{array}.$$

Por la propiedad universal de los anillos de polinomios, esto se extiende a un automorfismo de anillos que denotaremos como  $\tilde{\sigma}$ :

$$\begin{array}{ccc} K^{\text{alg}}[x_1, \dots, x_n] & \xrightarrow{\tilde{\sigma}} & K^{\text{alg}}[x_1, \dots, x_n] \\ & \nwarrow \quad \nearrow & \\ & K[x_1, \dots, x_n] & \end{array}.$$

Denotando  $X_{K^{\text{alg}}} := \text{Spec}(K^{\text{alg}}[x_1, \dots, x_n])$  y usando la contravarianza del funtor  $\text{Spec}$  (Proposición 2.4), obtenemos una acción por la izquierda de Galois sobre el espacio topológico subyacente dada por:

$$\rho: G_K \longrightarrow \text{Aut}_{\text{Top}}(X_{K^{\text{alg}}}), \sigma \mapsto \rho_\sigma := (\tilde{\sigma}^{-1})^*.$$

Esta definición asegura que la biyección  $\phi_{K^{\text{alg}}}$ , garantizada por el Nullstellensatz débil (A.1), sea  $G_K$ -equivariante. Todo esto se resume en el siguiente diagrama conmutativo de funciones  $G_K$ -equivariantes:

$$\begin{array}{ccc} K^n & \xrightarrow{\phi} & X \\ i \downarrow & & \uparrow i^* \\ (K^{\text{alg}})^n & \xrightarrow{\phi_{K^{\text{alg}}}} & X_{K^{\text{alg}}} \end{array}$$

donde  $G_K$  actúa de manera trivial sobre las entradas de la fila superior, e  $i^*$  es la función continua inducida por la inclusión de anillos.

**Lema 3.1 — Fibra de un morfismo afín.** Sea  $\varphi: A \rightarrow B$  un homomorfismo de anillos conmutativos y  $f: \text{Spec}(B) \rightarrow \text{Spec}(A)$  la función continua inducida. Para cualquier ideal primo  $\mathfrak{p} \in \text{Spec}(A)$ , sea  $\kappa(\mathfrak{p}) := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$  su campo residual. Entonces, existe un homeomorfismo canónico

$$f^{-1}(\mathfrak{p}) \cong \text{Spec}(B \otimes_A \kappa(\mathfrak{p})).$$

*Demostración.* Un ideal primo  $\mathfrak{q} \in \text{Spec}(B)$  pertenece a la fibra  $f^{-1}(\mathfrak{p})$  si y solo si  $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ . Esta igualdad se descompone en dos condiciones equivalentes:

1.  $\mathfrak{p} \subseteq \varphi^{-1}(\mathfrak{q})$ , lo cual ocurre si y solo si  $\varphi(\mathfrak{p})B \subseteq \mathfrak{q}$ . Por la correspondencia de ideales, tales  $\mathfrak{q}$  se identifican con los ideales primos del anillo cociente  $B/\varphi(\mathfrak{p})B$ . Notemos que existe un isomorfismo canónico  $B/\varphi(\mathfrak{p})B \cong B \otimes_A (A/\mathfrak{p})$ .
2.  $\varphi^{-1}(\mathfrak{q}) \cap (A \setminus \mathfrak{p}) = \emptyset$ , lo cual significa que la imagen del conjunto multiplicativo  $S := A \setminus \mathfrak{p}$  bajo  $\varphi$  no interseca a  $\mathfrak{q}$ . En el anillo cociente, esto equivale a decir que el ideal primo sobrevive a la localización por el conjunto  $\varphi(S)$ .

Por las propiedades universales de la localización y el producto tensorial, los ideales primos que satisfacen ambas condiciones están en correspondencia biyectiva con el espectro de la localización del cociente:

$$\text{Spec}\left((B/\varphi(\mathfrak{p})B)_{\varphi(S)}\right).$$

Utilizando la conmutatividad entre el funtor de localización y el producto tensorial, obtenemos el isomorfismo de anillos:

$$(B/\varphi(\mathfrak{p})B)_{\varphi(S)} \cong B \otimes_A (A/\mathfrak{p})_S = B \otimes_A A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = B \otimes_A \kappa(\mathfrak{p}).$$

Dado que estas correspondencias preservan las contenciones de ideales primos, inducen el

homeomorfismo topológico deseado. ■

**Proposición 3.2** Sea  $\mathfrak{m} \in X$  un punto cerrado. La preimagen de  $\mathfrak{m}$  bajo la función continua  $i^*: X_{K^{\text{alg}}} \rightarrow X$  corresponde exactamente a una única órbita bajo la acción de  $G_K$  en los puntos cerrados de  $X_{K^{\text{alg}}}$ .

*Demostración.* Dado el punto cerrado  $\mathfrak{m} \in X$ , por el Lema de Zariski A.3, el campo residual  $L := K[x_1, \dots, x_n]/\mathfrak{m}$  es una extensión finita de  $K$ . La fibra de la aplicación  $i^*$  sobre  $\mathfrak{m}$  se identifica por el lema 3.1 con el espectro del producto tensorial:

$$(i^*)^{-1}(\mathfrak{m}) \cong \text{Spec}(K^{\text{alg}} \otimes_K L).$$

Los puntos de esta fibra están en correspondencia biyectiva con los  $K$ -morfismos de álgebras  $\tau: L \rightarrow K^{\text{alg}}$ . Para cada uno de estos morfismos, la evaluación en las clases de equivalencia de las variables  $\bar{x}_j := x_j \pmod{\mathfrak{m}}$  define una  $n$ -tupla:

$$P_\tau := (\tau(\bar{x}_1), \dots, \tau(\bar{x}_n)) \in (K^{\text{alg}})^n.$$

Por la teoría de Galois, el grupo absoluto  $G_K$  actúa de manera transitiva sobre el conjunto de inmersiones  $\text{Hom}_K(L, K^{\text{alg}})$ . Cualquier par de  $K$ -inmersiones  $\tau, \tau'$  difieren por un automorfismo  $\sigma \in G_K$ , cumpliendo  $\tau' = \sigma \circ \tau$ . En coordenadas, esto se traduce en:

$$P_{\tau'} = (\sigma(\tau(\bar{x}_1)), \dots, \sigma(\tau(\bar{x}_n))) = \rho_\sigma(P_\tau).$$

En consecuencia, bajo la identificación  $\phi_{K^{\text{alg}}}$ , el conjunto de puntos en  $(K^{\text{alg}})^n$  que se proyectan a  $\mathfrak{m}$  constituye de manera precisa la órbita de  $P_\tau$  bajo  $G_K$ . ■

Este resultado fundamenta de forma explícita que el esquema  $X = \text{Spec}(K[x_1, \dots, x_n])$  posee una estructura topológica significativamente mayor a la del espacio afín clásico  $K^n$  cuando  $K$  no es algebraicamente cerrado:

1. **Puntos cerrados de grado superior:** Si  $K \neq K^{\text{alg}}$ , existe al menos una extensión algebraica finita  $L/K$  de grado  $d > 1$ . Todo punto cerrado  $\mathfrak{m} \in X$  cuyo campo residual sea isomorfo a  $L$  corresponde a una órbita de Galois de longitud  $d$  en  $(K^{\text{alg}})^n$ . Estos puntos están formados por coordenadas que no pertenecen simultáneamente a  $K$ , por lo que no intersecan al conjunto  $K^n$ . La imagen de la función  $\phi: K^n \rightarrow X$  captura los puntos cerrados con campo residual trivial ( $L = K$ ).
2. **Puntos genéricos (no cerrados):** Para  $n \geq 1$ , el anillo  $K[x_1, \dots, x_n]$  contiene ideales primos  $\mathfrak{p}$  que no son maximales (como el ideal nulo  $\langle 0 \rangle$ , correspondiente al punto genérico de todo el espacio). Las aplicaciones  $\phi$  y  $\phi_{K^{\text{alg}}}$  mapean tuplas únicamente a ideales maximales. Por consiguiente, los puntos genéricos del espectro, los cuales codifican subvariedades irreducibles enteras en un solo punto topológico, representan una dimensión geométrica completamente ausente en el espacio afín clásico  $K^n$ .

### 3.2. Espectro de $\mathbb{Z}$

El anillo  $\mathbb{Z}$  es un dominio de ideales principales (DIP). La clasificación de sus ideales primos determina los puntos del espacio topológico.

**Proposición 3.3 — Topología de  $\text{Spec}(\mathbb{Z})$ .** El conjunto subyacente de  $\text{Spec}(\mathbb{Z})$  consiste en:

1. El ideal nulo  $\langle 0 \rangle$ .
2. Los ideales generados por números primos  $\langle p \rangle$ .

Los conjuntos cerrados en la topología de Zariski son exactamente  $\text{Spec}(\mathbb{Z})$  y los subconjuntos finitos que no contienen a  $\langle 0 \rangle$ .

*Demostración.* Sea  $I \subseteq \mathbb{Z}$  un ideal. Si  $I = \langle 0 \rangle$ , entonces  $V(\langle 0 \rangle) = \text{Spec}(\mathbb{Z})$ . Si  $I \neq \langle 0 \rangle$ , entonces  $I = \langle n \rangle$  para algún entero  $n > 1$ . Por el teorema fundamental de la aritmética,  $n$  tiene una factorización única  $n = p_1^{a_1} \cdots p_k^{a_k}$  con  $p_i$  primos distintos. El radical del ideal es  $\sqrt{\langle n \rangle} = \langle p_1 \cdots p_k \rangle$ . En consecuencia, el conjunto cerrado definido por  $I$  es:

$$V(\langle n \rangle) = V(\sqrt{\langle n \rangle}) = \langle p_1 \rangle, \dots, \langle p_k \rangle.$$

Cualquier conjunto cerrado propio de  $\text{Spec}(\mathbb{Z})$  es, por lo tanto, una colección finita de ideales maximales. ■

Topológicamente,  $\text{Spec}(\mathbb{Z})$  posee la topología cofinita sobre sus puntos cerrados, equipada adicionalmente con un punto genérico  $\langle 0 \rangle$ , cuya clausura es el espacio total  $\overline{\{\langle 0 \rangle\}} = \text{Spec}(\mathbb{Z})$ .

El anillo  $\mathbb{Z}[x]$  tiene dimensión de Krull 2. El análisis de su espectro requiere clasificar sus ideales primos por su altura topológica.

**Proposición 3.4 — Clasificación de ideales primos en  $\text{Spec}(\mathbb{Z}[x])$ .** Los puntos de  $\text{Spec}(\mathbb{Z}[x])$  se dividen en tres clases según su altura (codimensión topológica del cierre):

- **Altura 0 (Punto genérico):** El ideal  $\langle 0 \rangle$ . Su clausura es todo el espacio.
- **Altura 1 (Curvas):** Consiste en dos familias disjuntas de ideales principales:
  1. Ideales  $\langle p \rangle$ , donde  $p \in \mathbb{Z}$  es un número primo.
  2. Ideales  $\langle f(x) \rangle$ , donde  $f(x) \in \mathbb{Z}[x]$  es un polinomio irreducible con coeficientes coprimos (contenido igual a 1).
- **Altura 2 (Puntos cerrados):** Ideales de la forma  $\mathfrak{m} = \langle p, f(x) \rangle$ , donde  $p \in \mathbb{Z}$  es primo y  $f(x) \in \mathbb{Z}[x]$  es un polinomio cuya reducción módulo  $p$ , denotada como  $\bar{f}(x) \in \mathbb{F}_p[x]$ , es irreducible.

Para entender la geometría de este espacio, utilizamos el morfismo estructural. La inclusión natural de anillos  $\varphi: \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$  induce un morfismo continuo de esquemas afines:

$$\pi: \text{Spec}(\mathbb{Z}[x]) \rightarrow \text{Spec}(\mathbb{Z}).$$

Utilizando el Lema de la fibra topológica de un morfismo (Lema 3.1), podemos describir el espacio  $\text{Spec}(\mathbb{Z}[x])$  como un haz de esquemas sobre  $\text{Spec}(\mathbb{Z})$ :

1. **Fibra genérica:** La preimagen del punto genérico  $\langle 0 \rangle \in \text{Spec}(\mathbb{Z})$  es:

$$\pi^{-1}(\langle 0 \rangle) \cong \text{Spec}(\mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Q}) \cong \text{Spec}(\mathbb{Q}[x]).$$

Los puntos cerrados de esta fibra corresponden a los ideales de altura 1 de la forma  $\langle f(x) \rangle \in \text{Spec}(\mathbb{Z}[x])$ . Un punto de altura 1 se esparce por el espacio; su conjunto cerrado  $V(\langle f(x) \rangle)$  representa una curva horizontal.

2. **Fibras especiales:** Para cada punto cerrado  $\langle p \rangle \in \text{Spec}(\mathbb{Z})$ , la preimagen es:

$$\pi^{-1}(\langle p \rangle) \cong \text{Spec}(\mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{F}_p) \cong \text{Spec}(\mathbb{F}_p[x]).$$

Estas son las rectas afines sobre los campos finitos. El punto genérico de cada fibra especial es el ideal  $\langle p \rangle \in \text{Spec}(\mathbb{Z}[x])$  (altura 1), y sus puntos cerrados corresponden a los ideales maximales de la forma  $\langle p, f(x) \rangle$  (altura 2). Estas fibras constituyen curvas verticales en el esquema.

La topología dicta la intersección de estas curvas. La intersección formal de una curva horizontal  $V(\langle f(x) \rangle)$  con una fibra vertical  $\pi^{-1}(\langle p \rangle)$  es el esquema afín dado por el cociente:

$$\text{Spec} \left( \frac{\mathbb{Z}[x]}{\langle p, f(x) \rangle} \right) \cong \text{Spec} \left( \frac{\mathbb{F}_p[x]}{\langle \bar{f}(x) \rangle} \right).$$

Geoméricamente, la curva definida por las raíces de un polinomio irreducible sobre  $\mathbb{Q}$  corta la fibra característica  $p$  en los puntos determinados por la factorización de  $\bar{f}(x)$  en el anillo  $\mathbb{F}_p[x]$ .

### 3.3. Topología de Curvas Elípticas.

Supongamos que  $f$  define una curva elíptica (por ejemplo, en forma de Weierstrass  $f(x, y) = y^2 - x^3 - ax - b$  con discriminante  $\Delta \neq 0$ ), el polinomio  $f$  es absolutamente irreducible. Por lo tanto, el ideal  $\langle f \rangle$  es primo y el anillo cociente  $A := K[x, y]/\langle f \rangle$  es un dominio entero. Denotemos  $X = \text{Spec} A$ , entonces:

1. La dimensión de Krull del anillo  $A$  es 1 (es una curva).
2. **Punto Genérico (Altura 0):** Al ser  $A$  un dominio, posee un único ideal primo nulo  $\eta = \langle 0 \rangle$ . Según la Proposición 2.3 (1), su clausura topológica es  $V(\eta) = X$ . Este punto domina toda la curva y representa la subvariedad irreducible en su totalidad. Su campo residual es el campo de funciones racionales de la curva,  $K(X) = \text{Frac}(A)$ .
3. **Puntos Cerrados (Altura 1):** Según la Proposición 2.3(2), los puntos cerrados corresponden biyectivamente a los ideales maximales  $\mathfrak{m} \subset A$ . Topológicamente,  $X$  está dotado de la topología cofinita: los únicos conjuntos cerrados propios son colecciones finitas de ideales maximales.

Para entender los puntos cerrados de  $X$ , pasamos a la cerradura algebraica  $\bar{K}$ . Sea  $X_{\bar{K}} = \text{Spec}(\bar{K}[x, y]/\langle f \rangle)$ . Al aplicar la correspondencia de órbitas bajo el grupo absoluto de Galois  $G_K = \text{Gal}(\bar{K}/K)$  deducida anteriormente:

- Los puntos cerrados de  $X_{\bar{K}}$  están en biyección con los puntos afines clásicos de la curva elíptica sobre  $\bar{K}$ , es decir, el conjunto  $E(\bar{K}) \setminus \{O\}$  (donde  $O$  es el punto en el infinito).
- Un ideal maximal  $\mathfrak{m} \in X$  tiene como campo residual una extensión finita  $L := A/\mathfrak{m}$  sobre  $K$ . Su preimagen bajo el morfismo  $X_{\bar{K}} \rightarrow X$  (que es continuo por la Proposición 2.4) corresponde a una única órbita de  $G_K$  actuando sobre  $E(\bar{K})$ .
- La longitud de esta órbita es el grado de la extensión  $[L : K]$ .
  1. Si  $\mathfrak{m}$  corresponde a una órbita de longitud 1, entonces  $L = K$ . Estos son los puntos racionales  $E(K)$ .
  2. Si  $\mathfrak{m}$  corresponde a una órbita de longitud  $d > 1$ , representa un conjunto de  $d$  puntos conjugados en  $E(\bar{K})$  que no pueden separarse mediante ecuaciones con coeficientes en  $K$ .

Consideremos el esquema aritmético-geométrico  $X = \text{Spec}(\mathbb{Q}[x, y]/\langle f \rangle)$ . Su topología consta del punto genérico  $\eta$  y una infinidad numerable de puntos cerrados (ideales maximales).

Utilizando la descripción de Galois con  $G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ , clasificamos los puntos cerrados según su grado topológico  $[L : \mathbb{Q}]$ :

1. **Puntos de Grado 1 (Órbitas triviales):** Corresponden a los ideales maximales de la forma  $\mathfrak{m} = \langle \bar{x} - x_0, \bar{y} - y_0 \rangle$  donde  $(x_0, y_0) \in \mathbb{Q}^2$  satisface  $f(x_0, y_0) = 0$ . Estos puntos forman el conjunto afín de puntos racionales  $E(\mathbb{Q})_{\text{afín}}$ . Por el Teorema de Mordell, sabemos que la

estructura del grupo proyectivo es finitamente generada:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

Topológicamente, si el rango  $r > 0$ , hay una infinidad de puntos de grado 1. Si  $r = 0$ , solo hay un número finito de puntos cerrados de grado 1 (correspondientes a la torsión afín).

2. **Puntos de Grado 2 (Órbitas cuadráticas):** Ideales maximales cuyo campo residual es una extensión cuadrática  $\mathbb{Q}(\sqrt{D})$ . Corresponden a pares de puntos conjugados de la forma  $(x_0 \pm y_0\sqrt{D}, z_0 \pm w_0\sqrt{D}) \in E(\bar{\mathbb{Q}})$ . La topología de Zariski no puede separar este par de puntos conjugados; para el esquema  $X$ , constituyen un único indivisible punto topológico.
3. **Puntos provenientes de la torsión algebraica (Grado arbitrario):** Si consideramos los puntos de torsión  $E[n] \subset E(\bar{\mathbb{Q}})$ , las coordenadas de estos puntos son raíces de los polinomios de división  $\psi_n(x) \in \mathbb{Q}[x]$ . Un factor irreducible de  $\psi_n(x)$  de grado  $d$  sobre  $\mathbb{Q}$  generará un ideal maximal en  $X$  cuyo campo residual tiene grado  $d$  (o  $2d$ , dependiendo de la coordenada  $y$ ). Este único punto topológico en  $X$  codifica toda la órbita de Galois de ese punto de torsión específico.

### 3.4. Los numeros Duales

Sea  $k$  un campo, definimos los numeros duales como  $k[\varepsilon] := k[x]/(x^2)$ .

**Proposición 3.5** Sea  $k$  un campo y consideremos el homomorfismo de anillos  $\varphi: k \rightarrow k[x]/\langle x^2 \rangle$  definido por la composición de la inclusión natural  $k \hookrightarrow k[x]$  y la proyección canónica  $k[x] \rightarrow k[x]/\langle x^2 \rangle$ . Entonces, la función continua inducida en los espectros,

$$\varphi^*: \text{Spec}(k[x]/\langle x^2 \rangle) \rightarrow \text{Spec}(k), \quad \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}),$$

es un homeomorfismo.

*Demostración.* Procedemos determinando explícitamente los conjuntos subyacentes de ambos espacios topológicos:

1. Dado que  $k$  es un campo, sus únicos ideales son  $\langle 0 \rangle$  y  $k$ . El único ideal primo es el ideal nulo. Por lo tanto, el espacio topológico consta de un único punto:

$$\text{Spec}(k) = \{\langle 0 \rangle\}.$$

2. Por los teoremas de isomorfismo de anillos, existe una correspondencia biyectiva que preserva contenciones entre los ideales de  $k[x]/\langle x^2 \rangle$  y los ideales de  $k[x]$  que contienen a  $\langle x^2 \rangle$ . Esta correspondencia se restringe a ideales primos. Sea  $\mathfrak{q} \subset k[x]$  un ideal primo tal que  $\langle x^2 \rangle \subseteq \mathfrak{q}$ . Al ser  $\mathfrak{q}$  primo, es en particular un ideal radical, lo que implica que:

$$\sqrt{\langle x^2 \rangle} \subseteq \sqrt{\mathfrak{q}} = \mathfrak{q}.$$

Dado que  $\sqrt{\langle x^2 \rangle} = \langle x \rangle$ , se tiene la contención  $\langle x \rangle \subseteq \mathfrak{q}$ . Como  $k$  es un campo, el anillo de polinomios  $k[x]$  es un dominio de ideales principales y  $\langle x \rangle$  es un ideal maximal. En consecuencia, la única posibilidad es  $\mathfrak{q} = \langle x \rangle$ . Por lo tanto, el anillo cociente  $k[x]/\langle x^2 \rangle$  posee un único ideal primo, generado por la clase de equivalencia  $\bar{x} = x + \langle x^2 \rangle$ :

$$\text{Spec}(k[x]/\langle x^2 \rangle) = \{\langle \bar{x} \rangle\}.$$

Evaluamos ahora el morfismo inducido  $\varphi^*$  en el único punto del dominio. El homomorfismo

$\varphi$  envía cualquier  $a \in k$  a la clase  $a + \langle x^2 \rangle$ . La preimagen del ideal  $\langle \bar{x} \rangle$  bajo  $\varphi$  es:

$$\varphi^*(\langle \bar{x} \rangle) = \varphi^{-1}(\langle \bar{x} \rangle) = \{a \in k \mid \varphi(a) \in \langle \bar{x} \rangle\}.$$

En  $k[x]/\langle x^2 \rangle$ , un elemento  $a + \langle x^2 \rangle$  pertenece al ideal  $\langle \bar{x} \rangle$  si y solo si es un múltiplo de  $\bar{x}$ . Como  $a \in k$  es una constante, esto ocurre si y solo si  $a = 0$ . Por lo tanto:

$$\varphi^*(\langle \bar{x} \rangle) = \{0\} = \langle 0 \rangle.$$

Concluimos que  $\varphi^*$  es una función biyectiva entre dos espacios topológicos que constan de un solo punto. Todo espacio de un solo punto tiene como únicos subconjuntos abiertos (y cerrados) al conjunto vacío y al espacio total. Como la preimagen y la imagen directa de estos subconjuntos bajo una biyección preservan esta estructura trivial,  $\varphi^*$  es continua, abierta y cerrada, siendo consecuentemente un homeomorfismo. ■

## 4. La categoría de variedades afines.

**Proposición 4.1** Sea  $X = \text{Spec}R$  entonces  $\{D(f)\}_{f \in R}$  forma una base para  $X$ .

*Demostración.* Sea  $U \subseteq X$  un abierto entonces  $C := X - U$  es un cerrado, entonces  $C = V(J)$  para algun ideal  $J \trianglelefteq R$ . Consideremos  $S \subseteq R$  un generador de  $J$ , es decir  $J = \langle S \rangle$ . Obteniendo:

$$C = V(J) = V\left(\sum_{s \in S} \langle s \rangle\right) = \bigcap_{s \in S} V(\langle s \rangle),$$

aplicando el complemento

$$U = \bigcup_{s \in S} D(s).$$

■

Para construir la gavilla de las funciones regulares para  $X = \text{Spec}R$ , recordando la interpretación de cada elemento  $f \in R$  como una función para  $X$ . En un abierto  $D(f)$ , la función  $f$  no se anula (es decir,  $f \notin \mathfrak{p}$ ). Por lo tanto, debería ser invertible.

- El anillo natural de funciones en el abierto  $D(f)$  es la localización  $R_f$ .

Para cualquier abierto  $U \subseteq X$ , definimos  $\mathcal{O}_X(U)$  como el anillo de funciones  $s : U \rightarrow \prod_{\mathfrak{p} \in U} R_{\mathfrak{p}}$  tales que:

1. Para cada  $\mathfrak{p} \in U$ ,  $s(\mathfrak{p}) \in R_{\mathfrak{p}}$ .
2. Para cada  $\mathfrak{p} \in U$ , existe un entorno abierto  $V \subseteq U$  con  $\mathfrak{p} \in V$ , y elementos  $a, g \in R$  tales que para todo  $\mathfrak{q} \in V$ ,  $g \notin \mathfrak{q}$  y  $s(\mathfrak{q}) = \frac{a}{g} \in R_{\mathfrak{q}}$ .

**Proposición 4.2** Las siguientes afirmaciones son válidas:

1. Para todo  $\mathfrak{p} \in X$ , el tallo (stalk) es el anillo local  $\mathcal{O}_{X, \mathfrak{p}} \cong R_{\mathfrak{p}}$ .
2. Para todo  $f \in R$ ,  $\mathcal{O}_X(D(f)) \cong R_f$ . En particular, las funciones globales son  $\mathcal{O}_X(X) \cong R$ .

**Proposición 4.3** El funtor

$$\mathcal{O}_X : \text{Open}(X) \longrightarrow \mathbf{Rng}, U \mapsto \mathcal{O}_X(U).$$

es una gavilla.

■ **Ejemplo 4.1** Consideremos  $k$  un campo y su álgebra de números duales  $k[\varepsilon] \cong k[x]/\langle x^2 \rangle$ . Denotemos los esquemas afines  $X = \text{Spec}(k)$  y  $Y = \text{Spec}(k[\varepsilon])$ . Topológicamente, ambos espacios constan de un único punto y son homeomorfos:

$$X = \{\langle 0 \rangle\}, \quad Y = \{\langle \varepsilon \rangle\}.$$

Dado que tienen la misma estructura topológica (los únicos abiertos son el vacío y el espacio total), evaluamos las gavillas estructurales  $\mathcal{O}_X$  y  $\mathcal{O}_Y$  en su sección global para compararlas. Aplicando la Proposición 4.2, obtenemos los isomorfismos de anillos:

$$\mathcal{O}_X(X) \cong k$$

$$\mathcal{O}_Y(Y) \cong k[\varepsilon]$$

Para determinar si  $\mathcal{O}_X$  y  $\mathcal{O}_Y$  son equivalentes, analizamos la estructura algebraica de sus secciones globales. El anillo  $k$  es un campo, lo que implica que su único elemento nilpotente es el cero. Por otro lado, por la construcción del álgebra de números duales, existe un elemento  $\varepsilon \in k[\varepsilon]$  que cumple:

$$\varepsilon \neq 0 \quad \text{y} \quad \varepsilon^2 = 0.$$

Es decir,  $k[\varepsilon]$  posee elementos nilpotentes no nulos. En consecuencia, no existe un isomorfismo de anillos entre ellos:

$$\mathcal{O}_X(X) \not\cong \mathcal{O}_Y(Y).$$

Al asignar anillos no isomorfos al mismo abierto topológico, se concluye que las gavillas  $\mathcal{O}_X$  y  $\mathcal{O}_Y$  son distintas. El esquema  $Y$  retiene la información algebraica de las derivadas (funciones nilpotentes) que la topología de Zariski por sí sola no puede detectar. ■

Esto dice que para capturar la geometría completa se requiere:

1. El anillo de funciones  $R$ .
2. El espacio topológico  $\text{Spec}(R)$ .
3. La gavilla estructural  $\mathcal{O}_X$  donde sus tallos son anillo locales.

**Definición 4.1 — Espacio Anillado..** Un espacio anillado  $(X, \mathcal{O}_X)$  es un espacio topológico junto con una gavilla de anillos.

**Definición 4.2 — Espacio localmente anillado..** Un espacio localmente anillado es un espacio anillado donde cada tallo  $\mathcal{O}_{X,p}$  es un anillo local (es decir, tiene un único ideal maximal  $\mathfrak{m}_p$ ).

El ejemplo prototipo de espacio localmente anillado es  $(\text{Spec}(R), \mathcal{O}_{\text{Spec}(R)})$ .

**Definición 4.3 — Morfismo de espacios anillados..** Un morfismo de espacios localmente anillados es un par  $(f, f^\#) : (X, \mathcal{O}_X) \rightarrow (Y, \mathcal{O}_Y)$  donde:

- $f : X \rightarrow Y$  es continua.
- $f^\# : \mathcal{O}_Y \rightarrow f_*\mathcal{O}_X$  es un morfismo de gavillas.
- El homomorfismo inducido en los tallos  $f_p^\# : \mathcal{O}_{Y,f(p)} \rightarrow \mathcal{O}_{X,p}$  preserva el ideal maxi-

$$\text{mal: } (f_p^\#)^{-1}(\mathfrak{m}_p) = \mathfrak{m}_{f(p)}.$$

**Definición 4.4 — Esquemas.** Un Esquema Afín es un espacio localmente anillado que es isomorfo a  $(\text{Spec}(R), \mathcal{O}_{\text{Spec}(R)})$  para algún anillo conmutativo  $R$ .

Un esquema es un espacio localmente anillado que localmente posee una cubierta de abiertos donde cada abierto es un esquema afín.

Denotemos **Scheme** a la categoría de esquemas y morfismos de espacios anillados. Existe un funtor contravariante entre **Rng**<sub>1</sub> la categoría de anillos conmutativos con 1 y la subcategoría de esquemas afines.

Sea  $\phi : R \rightarrow S$  un homomorfismo de anillos. Entonces por proposición 2.4, entonces  $f : \text{Spec}(S) \rightarrow \text{Spec}(R)$  es continua. El morfismo  $\phi$  induce naturalmente mapas de localización  $R_{\phi^{-1}(p)} \rightarrow S_p$ , que a nivel global conforman un morfismo de gavillas  $f^\# : \mathcal{O}_{\text{Spec}(R)} \rightarrow f_* \mathcal{O}_{\text{Spec}(S)}$ .

**Teorema 4.4 — Equivalencia anillos y esquemas afines.** El funtor  $R \mapsto (\text{Spec}(R), \mathcal{O}_{\text{Spec}(R)})$  induce una equivalencia (dualidad) de categorías:

$$\text{Hom}_{\text{LocRingSp}}(\text{Spec}(S), \text{Spec}(R)) \cong \text{Hom}_{\text{Rings}}(R, S)$$

Todo morfismo entre dos esquemas afines proviene únicamente de un homomorfismo de sus anillos globales.

## A. Algunos lemas técnicos.

**Teorema A.1 — Nullstellensatz Débil.** Existe una biyección canónica entre los puntos  $p = (a_1, \dots, a_n) \in \mathbb{A}_k^n$  y los ideales maximales de  $k[x_1, \dots, x_n]$ , dada por  $p \mapsto \mathfrak{m}_p = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ .

**Teorema A.2** Sea  $(\phi, \psi)$  una conexión de Galois antitonas entre conjuntos parcialmente ordenados  $P$  y  $Q$ . Entonces:

1.  $\psi\phi : P \rightarrow P$  y  $\phi\psi : Q \rightarrow Q$  son operadores de clausura.
2.  $\phi(\text{Cl}_{\psi\phi}(P)) = \text{Cl}_{\phi\psi}(Q)$  y  $\psi(\text{Cl}_{\phi\psi}(Q)) = \text{Cl}_{\psi\phi}(P)$ .
3. Las restricciones inducen un anti-isomorfismo de conjuntos parcialmente ordenados

$$\text{Cl}_{\psi\phi}(P) \cong \text{Cl}_{\phi\psi}(Q).$$

Si  $P$  y  $Q$  son retículas, este es un anti-isomorfismo de retículas.

**Proposición A.3 — Lema de Zariski vía TNN.** Sea  $K$  un campo que es una  $k$ -álgebra de tipo finito. Entonces  $K$  es una extensión algebraica de  $k$ .