# Encontrando Ideales Maximales

Luis Manuel Reyes de la Luz

Julio 2026

**Resumen**

Notas de un curso de Curvas Elípticas.

## Índice

1. Introducción 1

2. Framework 1

3. Acción de Galois 4

## Notación

## 1. Introducción

El objetivo es responder la siguiente pregunta

**Cuestión 1.1** Si $A$ es una $k$-álgebra finitamente generada. ¿Como encuentro todos los puntos de $\mathrm{Spec}(A)$?

## 2. Framework

Consideremos $R$ un anillo conmutativo con 1. Denotamos $X = \mathrm{Spec}(R)$ como su espectro de ideales primos, y se tiene la función que define los cerrados de Zariski

$$V : \mathrm{Id}(X) \longrightarrow \mathrm{Sub}(X),\ I \mapsto V(I) := \{\mathfrak{p} \in X \mid I \subseteq \mathfrak{p}\}$$

Algunos resultados básicos son

**Proposición 2.1 — Lema de Zariski.** *Sea $K$ un campo que es una $k$-álgebra de tipo finito. Entonces $K$ es una extensión algebraica de $k$.*

**Proposición 2.2 — Teorema de Krull.** *Para todo ideal no trivial $I \triangleleft R$, existe un ideal maximal $\mathfrak{m}$ tal que*

$$I \subseteq \mathfrak{m}$$

Esto implica que $V(I) = \emptyset$ si y sólo si $I = R$. Denotemos $\mathrm{mSpec}(X) \subseteq \mathrm{Spec}(X)$ como el subconjunto de ideales maximales de un anillo $R$ (donde $X = \mathrm{Spec}(R)$).

**Corolario 2.3** *El radical de Jacobson de $R$, denotado por $J(R)$ (definido como el conjunto de elementos $x \in R$ tales que $1 - xy$ es una unidad para todo $y \in R$), cumple que:*

$$J(R) = \bigcap_{\mathfrak{m} \in m\mathrm{Spec}(X)} \mathfrak{m}$$

*Demostración.* Sea $x \in \bigcap_{\mathfrak{m} \in \mathrm{mSpec}(X)} \mathfrak{m}$. Supongamos por contradicción que existe $y \in R$ tal que $1 - xy$ no es una unidad. Entonces, el ideal generado por $(1 - xy)$ es propio, es decir, $(1 - xy) \neq R$. Por el Teorema de Krull 2.2, existe un ideal maximal $\mathfrak{m}_0$ tal que $(1 - xy) \subseteq \mathfrak{m}_0$. Como $x \in \mathfrak{m}_0$ por hipótesis, entonces $xy \in \mathfrak{m}_0$. Esto implica que $1 = (1 - xy) + xy \in \mathfrak{m}_0$, lo cual es una contradicción porque ningún ideal maximal contiene al 1. Por lo tanto, $x \in J(R)$.

Inversamente, sea $x \in J(R)$ y supongamos que existe un ideal maximal $\mathfrak{m}$ tal que $x \notin \mathfrak{m}$. Como $\mathfrak{m}$ es maximal, el ideal generado por $\mathfrak{m}$ y $x$ es todo el anillo $R$. Así, existen $m \in \mathfrak{m}$ e $y \in R$ tales que $m + xy = 1$, lo que implica que $1 - xy = m \in \mathfrak{m}$. Pero como $x \in J(R)$, $1 - xy$ debe ser una unidad, lo cual es absurdo porque $\mathfrak{m}$ es un ideal propio y no puede contener unidades. Por tanto, $x$ debe pertenecer a todos los ideales maximales. ∎

**Definición 2.1 — Anillo de Jacobson.** Un anillo $R$ se llama **anillo de Jacobson** si para todo ideal primo $\mathfrak{p} \triangleleft R$, la intersección de todos los ideales maximales en el dominio cociente $R/\mathfrak{p}$ es el ideal nulo $(0)$.

**Proposición 2.4** *Sea $k$ un campo. Toda $k$-álgebra finitamente generada es un anillo de Jacobson.*

*Demostración.* Para demostrar que una $k$-álgebra finitamente generada $A$ es un anillo de Jacobson, basta con verificar la definición equivalente: para cualquier ideal primo $\mathfrak{p} \subset A$, la intersección de todos los ideales maximales en el dominio cociente $B = A/\mathfrak{p}$ es estrictamente $(0)$. Esto es equivalente a demostrar que, para cualquier elemento no nulo $f \in B$, existe al menos un ideal maximal $\mathfrak{m} \subset B$ tal que $f \notin \mathfrak{m}$.

Sea $f \in B$ con $f \neq 0$. Consideremos la localización del anillo $B$ en $f$, denotada como $B_f = B[1/f]$. Dado que $B$ es una $k$-álgebra finitamente generada, $B_f$ también lo es (se obtiene añadiendo un nuevo generador $x$ y la relación $xf - 1 = 0$). Como $B$ es un dominio y $f \neq 0$, $B_f$ es un anillo no trivial, por lo que el Teorema de Krull 2.2 garantiza la existencia de al menos un ideal maximal $\mathfrak{n} \subset B_f$.

El cociente $L = B_f/\mathfrak{n}$ es un campo que hereda la estructura de $k$-álgebra finitamente generada. Por el Lema de Zariski 2.1, cualquier campo que sea una $k$-álgebra finitamente generada es una extensión algebraica finita de $k$. Por lo tanto, $L$ es un $k$-espacio vectorial de dimensión finita.

Consideremos ahora el homomorfismo natural de composición $\varphi \colon B \to B_f \to L$. Definimos $\mathfrak{m} = \ker(\varphi)$, que equivale a la contracción $\mathfrak{n} \cap B$. Por el Primer Teorema de Isomorfía, el anillo cociente $B/\mathfrak{m}$ es isomorfo a un subanillo del campo $L$.

Al ser un subanillo de un campo, $B/\mathfrak{m}$ es un dominio de integridad. Además, como es un subespacio vectorial de $L$ (que tiene dimensión finita sobre $k$), $B/\mathfrak{m}$ es también un $k$-espacio vectorial de dimensión finita. Es un hecho algebraico conocido que todo dominio de integridad de dimensión finita sobre un campo es necesariamente un campo. En consecuencia, $\mathfrak{m}$ es un ideal maximal de $B$.

Finalmente, notemos que la imagen de $f$ bajo la localización $B \to B_f$ es invertible, por lo que su imagen bajo $\varphi$ en $L$ no puede ser cero (el cero no es invertible en un campo). Esto significa que $f \notin \ker(\varphi)$, es decir, $f \notin \mathfrak{m}$.

Hemos encontrado un ideal maximal $\mathfrak{m}$ en $B$ que no contiene a $f$. Como esto se cumple para todo $f \neq 0$, deducimos que la intersección de todos los ideales maximales en $B = A/\mathfrak{p}$ es $(0)$, concluyendo así que $A$ es un anillo de Jacobson. ■

**Corolario 2.5** *Si $R$ es un anillo de Jacobson, para todo ideal primo $\mathfrak{p}$ se cumple que*

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \in mSpec(X) \\ \mathfrak{p} \subseteq \mathfrak{m}}} \mathfrak{m}$$

*Demostración.* La contención $\subseteq$ es inmediata por la definición de intersección de conjuntos.

Para la contención $\supseteq$, tomemos un elemento $x \notin \mathfrak{p}$. En el dominio cociente $R/\mathfrak{p}$, la clase $\overline{x}$ es no nula. Dado que $R$ es un anillo de Jacobson, la intersección de todos los ideales maximales de $R/\mathfrak{p}$ es estrictamente $(0)$. Por consiguiente, debe existir algún ideal maximal $\overline{\mathfrak{m}} \subset R/\mathfrak{p}$ tal que $\overline{x} \notin \overline{\mathfrak{m}}$.

Por el teorema de correspondencia, al retraer $\overline{\mathfrak{m}}$ a través de la proyección canónica $R \to R/\mathfrak{p}$, obtenemos un ideal maximal $\mathfrak{m} \subset R$ que contiene a $\mathfrak{p}$ pero no contiene a $x$. Por contrapositiva, esto demuestra que si un elemento está en la intersección de todos los maximales que contienen a $\mathfrak{p}$, necesariamente debe estar en $\mathfrak{p}$. ■

Esto nos dice que, geométricamente, podemos conocer todos los puntos del espacio $\mathrm{Spec}(X)$ conociendo únicamente sus ideales maximales, los cuales representan los *puntos cerrados* de la variedad.

El caso principal de nuestro interés aplica directamente este principio. Consideremos un campo $k$. Como probamos anteriormente, toda $k$-álgebra de tipo finito $A$ es un anillo de Jacobson, por lo que su geometría está completamente determinada por sus ideales maximales. Estructuralmente, sabemos que esta álgebra $A$ siempre se puede expresar de la forma

$$A \cong \frac{k[x_1, \ldots, x_n]}{I}$$

en donde $x_1, \ldots, x_n$ representan un conjunto finito de variables e $I \triangleleft k[x_1, \ldots, x_n]$ es un ideal. Más aún, gracias al Teorema de la Base de Hilbert, como $k$ es un campo, el anillo de polinomios $k[x_1, \ldots, x_n]$ es noetheriano, lo que nos garantiza que el ideal $I$ siempre estará generado por un número finito de polinomios. Existe un resultado fundamental dentro de la geometría algebraica que establece lo siguiente:

**Teorema 2.6 — Teorema de los ceros de Hilbert débil.** *Sea $k = \overline{k}$ un campo algebraicamente cerrado. Entonces, todo ideal maximal $\mathfrak{m} \triangleleft k[x_1, \ldots, x_n]$ es de la forma*

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

*para algún punto $(a_1, \ldots, a_n) \in k^n$.*

En particular, consideremos una $k$-álgebra finitamente generada $A$ sobre un campo alge-

braicamente cerrado $k$. Si tomamos un epimorfismo

$$g\colon k[x_1,\dots,x_n] \longrightarrow A,$$

el teorema de correspondencia de ideales nos asegura que la imagen inversa $g^{-1}$ induce una biyección natural:

$$\mathrm{mSpec}(A) \cong \{\mathfrak{m} \in \mathrm{mSpec}(k[x_1,\dots,x_n]) \mid \ker g \subseteq \mathfrak{m}\} = V(\ker g) \cap \mathrm{mSpec}(k[x_1,\dots,x_n]).$$

Denotando $\overline{x_i} := g(x_i)$ para cada $i = 1,\dots,n$, el Teorema de los ceros débil 2.6 nos permite escribir cualquier ideal maximal $\mathfrak{m} \triangleleft A$ de la forma

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

donde el punto $(a_1,\dots,a_n) \in k^n$ necesariamente anula a todos los polinomios contenidos en $\ker g$.

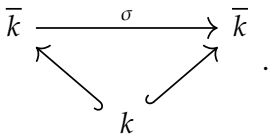
Este razonamiento establece una biyección que sirve como puente fundamental entre la geometría algebraica clásica y la geometría de esquemas:

$$\mathrm{mSpec}(A) \cong \{(a_1,\dots,a_n) \in k^n \mid f(a_1,\dots,a_n) = 0,\ \forall f \in \ker g\}. \tag{1}$$

Con esto, obtenemos una respuesta directa a la pregunta 1.1 sobre cómo describir los puntos de un espacio de manera cuantitativa cuando trabajamos sobre un campo algebraicamente cerrado.

## 3. Acción de Galois

Para responder la pregunta 1.1 en el caso general en donde $k$ no es algebraicamente cerrado, consideraremos la acción de Galois. Fijamos $\overline{k}$ una cerradura separable de $k$, y sea $G_K := \mathrm{Gal}(\overline{k}/k)$ su grupo absoluto de Galois. Para cada elemento $\sigma \in G_K$ consiste en un homomorfismo de $k$-algebras



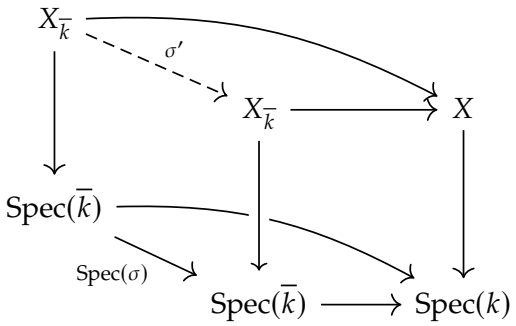

Si $X$ es un esquema sobre $k$, es decir existe un morfismo de esquemas

$$X \longrightarrow \mathrm{Spec}(k)$$

definimos $X_{\overline{k}} := X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$, es decir esta definido por el cuadrado cartesiano

$$\begin{array}{ccc} X_{\overline{k}} & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\overline{k}) & \longrightarrow & \mathrm{Spec}(k) \end{array}.$$

Entonces $X_{\overline{k}}$ tiene una acción natural de $G_k$ definido como sigue; dado $\sigma \in G_k$, $\sigma' \in \mathrm{Aut}_k(X_{\overline{k}})$ es definido mediante la propiedad universal del pullback




Cuando $X = \mathrm{Spec}(A)$ entonces $X_{\overline{k}} = \mathrm{Spec}(A \otimes_k \overline{k})$, obteniendo que $\sigma' := \mathrm{Id}_A \otimes \sigma$.

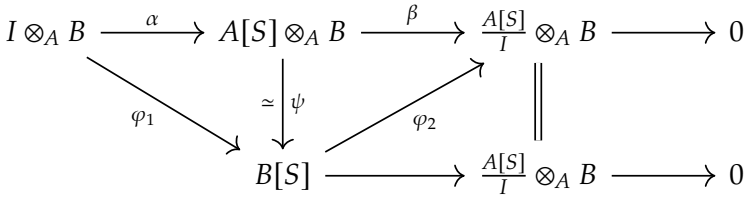
**Lema 3.1** *Sean $S$ un conjunto, $f : A \to B$ un homomorfismo de anillos, $I \trianglelefteq A[S]$ un ideal e $I' := I^e$ su ideal extensión, entonces existe un homomorfismo canónico*

$$A[S]/I \otimes_A B \cong B[S]/I'$$

*Demostración.* Consideremos la sucesión exacta de $A$-módulos

$$I \longrightarrow A[S] \longrightarrow A[S]/I \longrightarrow 0.$$

Aplicamos el funtor $- \otimes_A B$, el cual es exacto a la derecha, obteniendo la fila superior exacta en el siguiente diagrama conmutativo:




Notemos que la flecha vertical central $\psi$ es el isomorfismo canónico que envía $a(s) \otimes b \mapsto f(a(s))b$. Para cada elemento $\sum i_j(s) \otimes b_j \in I \otimes_A B$, por la conmutatividad del diagrama tenemos

$$\varphi_1\left(\sum i_j(s) \otimes b_j\right) = \sum f(i_j(s))b_j \in I'.$$

Dado que el ideal extensión $I'$ es generado precisamente por la imagen de $I$ en $B[S]$, concluimos que $\mathrm{Im}(\varphi_1) = I'$.

Por otro lado, debido a que la fila superior es exacta en $A[S] \otimes_A B$, sabemos que $\ker \beta = \mathrm{Im}(\alpha)$. Como el diagrama es conmutativo, tenemos que $\varphi_2 \circ \psi = \beta$.

Evaluando el núcleo de $\varphi_2$, un elemento $p(s) \in B[S]$ pertenece a $\ker \varphi_2$ si y solo si $\varphi_2(p(s)) = 0$. Como $\psi$ es biyectiva, existe un único $x \in A[S] \otimes_A B$ tal que $\psi(x) = p(s)$. Entonces:

$$\varphi_2(\psi(x)) = 0 \iff \beta(x) = 0 \iff x \in \ker \beta = \mathrm{Im}(\alpha).$$

Si $x \in \mathrm{Im}(\alpha)$, entonces $p(s) = \psi(x) \in \psi(\mathrm{Im}(\alpha))$. Pero por la conmutatividad del triángulo izquierdo, $\psi(\mathrm{Im}(\alpha)) = \mathrm{Im}(\varphi_1)$. Por lo tanto, deducimos que:

$$\ker \varphi_2 = \mathrm{Im}(\varphi_1) = I'.$$

Finalmente, como $\varphi_2$ es suprayectiva (pues $\beta$ lo es y $\psi$ es isomorfismo), por el Primer Teorema

de Isomorfía obtenemos el isomorfismo canónico

$$B[S]/I' \cong A[S]/I \otimes_A B.$$

■

Con lo anterior, podemos establecer el resultado principal de este trabajo. Consideremos $S = \{x_1, \cdots, x_n\}$ un conjunto finito de variables y definamos

$$A := \frac{k[S]}{I}$$

una $k$-algebra del tipo finito, $X = \mathrm{Spec}(A)$ entonces $X_{\overline{k}} \cong \mathrm{Spec}\left(\overline{k}[S]/I'\right)$ y este esquema sobre $\overline{k}$ en sus puntos maximales tienen la descripción dada por (1). Denotemos

$$\rho\colon k[S]/I \longrightarrow \overline{k}[S]/I'$$

el morfismo canónico.

**Teorema 3.2 — Correspondencia de puntos cerrados.** *Sea $\overline{\mathfrak{m}} \in m\mathrm{Spec}(A \otimes_k \overline{k})$ y $\mathfrak{m} = \overline{m}$ su contracción, son equivalentes:*

1. *Dos ideales maximales $\overline{\mathfrak{m}}_1, \overline{\mathfrak{m}}_2$ en la variedad geométrica sobre $\overline{k}$ se contraen al mismo ideal maximal $\mathfrak{m}$ en $A$.*
2. *Existe un elemento $\sigma \in G_k$ tal que $\sigma(\overline{\mathfrak{m}}_1) = \overline{\mathfrak{m}}_2$.*

*Además:*

$$\mathfrak{m} = \left(\bigcap_{\sigma \in G_k} \sigma(\overline{\mathfrak{m}})\right) \cap A$$

*Demostración.* Fijemos la notación. Sea $A = k[S]/I \cong k[x_1, \ldots, x_n]/I$ y consideremos el morfismo canónico (inyección) $\rho\colon A \to A_{\overline{k}}$, donde $A_{\overline{k}} = \overline{k}[S]/I'$. La contracción de un ideal $\overline{J} \subset A_{\overline{k}}$ a $A$ denota simplemente a la preimagen $\rho^{-1}(\overline{J}) = \overline{J} \cap A$.

Dado que $\overline{k}$ es algebraicamente cerrado, el Teorema de los ceros de Hilbert débil (Teorema 2.6) y la ecuación (1) establecen una biyección entre $\mathrm{mSpec}(A_{\overline{k}})$ y el conjunto de puntos $V(I') \subseteq \overline{k}^n$.

Todo ideal maximal $\overline{\mathfrak{m}} \in \mathrm{mSpec}(A_{\overline{k}})$ es el núcleo del morfismo de evaluación en un punto $\alpha = (\alpha_1, \ldots, \alpha_n) \in \overline{k}^n$ que anula a $I'$. Es decir, la composición:

$$ev_\alpha\colon A \xrightarrow{\rho} A_{\overline{k}} \longrightarrow \overline{k}$$

donde $ev_\alpha(\bar{x}_i) = \alpha_i$. Observemos que la contracción $\mathfrak{m} = \rho^{-1}(\overline{\mathfrak{m}})$ es exactamente $\ker(ev_\alpha|_A)$.

La acción del grupo de Galois $G_k$ sobre $\mathrm{mSpec}(A_{\overline{k}})$ corresponde a la acción coordenada a coordenada sobre los puntos de $\overline{k}^n$: si $\sigma \in G_k$, entonces $\sigma(\overline{\mathfrak{m}})$ es el ideal maximal asociado al punto $\sigma(\alpha) = (\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$.

2 $\implies$ 1. Supongamos que existe $\sigma \in G_k$ tal que $\sigma(\overline{\mathfrak{m}}_1) = \overline{\mathfrak{m}}_2$. Sean $\alpha, \beta \in \overline{k}^n$ los puntos correspondientes a $\overline{\mathfrak{m}}_1$ y $\overline{\mathfrak{m}}_2$ respectivamente, por lo que $\beta = \sigma(\alpha)$.

Sea $f \in A \subset A_{\overline{k}}$. Dado que los coeficientes de $f$ residen en $k$ y $\sigma$ fija a $k$, la acción de Galois conmuta con la evaluación del polinomio:

$$f(\beta) = f(\sigma(\alpha)) = \sigma(f(\alpha))$$

Por lo tanto, $f \in \rho^{-1}(\overline{\mathfrak{m}}_2)$ si y solo si $f(\beta) = 0$. Como $\sigma$ es un automorfismo, esto ocurre si y solo si $f(\alpha) = 0$, lo que equivale a $f \in \rho^{-1}(\overline{\mathfrak{m}}_1)$.En consecuencia, $\overline{\mathfrak{m}}_1 \cap A = \overline{\mathfrak{m}}_2 \cap A = \mathfrak{m}$.

$1 \implies 2$. Supongamos que $\overline{\mathfrak{m}}_1 \cap A = \overline{\mathfrak{m}}_2 \cap A = \mathfrak{m}$. Por definición de contracción, $\mathfrak{m}$ es un ideal primo en $A$. Afirmamos que de hecho $\mathfrak{m} \in \mathrm{mSpec}(A)$.

Sean $\alpha, \beta \in \overline{k}^n$ los puntos que definen a $\overline{\mathfrak{m}}_1$ y $\overline{\mathfrak{m}}_2$. Las evaluaciones $ev_\alpha$ y $ev_\beta$ inducen inyecciones del dominio cociente $A/\mathfrak{m}$:

$$\varphi_\alpha \colon A/\mathfrak{m} \hookrightarrow \overline{k} \quad \text{y} \quad \varphi_\beta \colon A/\mathfrak{m} \hookrightarrow \overline{k}$$

Dado que $A/\mathfrak{m}$ es isomorfo a una sub-$k$-álgebra de $\overline{k}$, es un dominio entero de tipo finito sobre $k$. Como está contenido en un campo, el Lema de Zariski (Proposición 2.1) garantiza que $A/\mathfrak{m}$ es en realidad un campo y una extensión algebraica finita de $k$. Esto prueba que $\mathfrak{m}$ es maximal.

Al ser $\overline{k}$ la cerradura separable de $k$, la extensión $\overline{k}/k$ es normal (es una extensión de Galois). En la teoría de campos, dos encajes cualesquiera $\varphi_\alpha, \varphi_\beta$ de una extensión finita $K = A/\mathfrak{m}$ en su cerradura normal $\overline{k}$ difieren por un automorfismo de Galois de la clausura.Es decir, existe $\sigma \in G_k = \mathrm{Gal}(\overline{k}/k)$ tal que:

$$\varphi_\beta = \sigma \circ \varphi_\alpha$$

Al evaluar en los generadores $\bar{x}_i$ de $A/\mathfrak{m}$, obtenemos $\beta_i = \sigma(\alpha_i)$ para todo $i = 1, \ldots, n$. Geoméricamente, $\beta = \sigma(\alpha)$, y a nivel de ideales esto significa exactamente que $\overline{\mathfrak{m}}_2 = \sigma(\overline{\mathfrak{m}}_1)$.

Resta probar la igualdad. Por definición del morfismo de contracción, las operaciones de intersección y preimagen conmutan:

$$\left( \bigcap_{\sigma \in G_k} \sigma(\overline{\mathfrak{m}}) \right) \cap A = \rho^{-1} \left( \bigcap_{\sigma \in G_k} \sigma(\overline{\mathfrak{m}}) \right) = \bigcap_{\sigma \in G_k} \rho^{-1}(\sigma(\overline{\mathfrak{m}}))$$

Por la implicación $2 \implies 1$ ya demostrada, la contracción de cualquier conjugado de Galois coincide con la contracción original. Es decir, para todo $\sigma \in G_k$, se tiene que $\rho^{-1}(\sigma(\overline{\mathfrak{m}})) = \mathfrak{m}$.

Sustituyendo esto en la intersección, obtenemos:

$$\bigcap_{\sigma \in G_k} \mathfrak{m} = \mathfrak{m}$$

■

■ **Ejemplo 3.1** Consideremos la curva plana sobre el campo finito de tres elementos, $k = \mathbb{F}_3$, dada por el anillo cociente:

$$A = \mathbb{F}_3[x, y]/(y^2 - x^3 + 1).$$

Nuestro objetivo es determinar puntos cerrados (ideales maximales) de $\mathrm{Spec}(A)$ examinando las órbitas bajo la acción del grupo absoluto de Galois $G_{\mathbb{F}_3} = \mathrm{Gal}(\overline{\mathbb{F}}_3/\mathbb{F}_3)$.

De acuerdo con la correspondencia de puntos cerrados 3.2, los ideales maximales de $A$ están en correspondencia biyectiva con las órbitas de $G_{\mathbb{F}_3}$ sobre los puntos de la curva geométrica en $\overline{\mathbb{F}}_3^2$:

$$X(\overline{\mathbb{F}}_3) = \{(\alpha, \beta) \in \overline{\mathbb{F}}_3^2 \mid \beta^2 - \alpha^3 + 1 = 0\}.$$

El grupo $G_{\mathbb{F}_3}$ está generado topológicamente por el automorfismo de Frobenius $F(\alpha) = \alpha^3$.

La órbita de un punto $(\alpha, \beta)$ es finita y está formada por los puntos:

$$O_{(\alpha,\beta)} = \{(\alpha, \beta), (\alpha^3, \beta^3), (\alpha^9, \beta^9), \dots\}.$$

El cardinal de esta órbita, digamos $d$, corresponde al grado de la extensión residual $[\mathbb{F}_3(\alpha, \beta) : \mathbb{F}_3]$, y el ideal maximal en $A$ asociado a esta órbita se obtiene como:

$$\mathfrak{m} = \left( \bigcap_{i=0}^{d-1} (x - \alpha^{3^i}, y - \beta^{3^i}) \right) \cap A.$$

Analicemos algunos puntos de bajo grado:

**1. Puntos $\mathbb{F}_3$-racionales (Grado 1):**

Buscamos soluciones con $\alpha, \beta \in \mathbb{F}_3 = \{0, 1, 2\}$. Evaluando la ecuación $y^2 = x^3 - 1$ sobre $\mathbb{F}_3$:

- Si $x = 0$, entonces $y^2 = -1 = 2$. No hay cuadrados en $\mathbb{F}_3$ iguales a 2.
- Si $x = 1$, entonces $y^2 = 1^3 - 1 = 0 \implies y = 0$. Obtenemos el punto $(1, 0)$.
- Si $x = 2$, entonces $y^2 = 2^3 - 1 = 8 - 1 = 7 \equiv 1 \pmod 3 \implies y \in \{1, 2\}$. Obtenemos los puntos $(2, 1)$ y $(2, 2)$.

Estos tres puntos tienen grado 1 (órbitas de tamaño 1 bajo Frobenius). Sus ideales maximales correspondientes en $A$ son directamente:

$$\mathfrak{m}_1 = (\bar{x} - 1, \bar{y}), \quad \mathfrak{m}_2 = (\bar{x} - 2, \bar{y} - 1), \quad \mathfrak{m}_3 = (\bar{x} - 2, \bar{y} - 2).$$

**2. Puntos de grado 2:**

Buscamos soluciones en la única extensión cuadrática $\mathbb{F}_{3^2}$, que podemos construir como $\mathbb{F}_3[i]/(i^2 + 1)$ (ya que $-1$ no es residuo cuadrático en $\mathbb{F}_3$). Así, los elementos de $\mathbb{F}_9$ son de la forma $a + bi$ con $a, b \in \mathbb{F}_3$.

Retomemos el caso donde $x = 0$. Habíamos visto que $y^2 = 2 \equiv -1$. En $\mathbb{F}_9$, las soluciones son $y = i$ e $y = -i = 2i$. Por tanto, tenemos los puntos en $\overline{\mathbb{F}}_3^2$:

$$P_1 = (0, i) \quad \text{y} \quad P_2 = (0, -i).$$

Aplicando el Frobenius $F(z) = z^3$, vemos que $F(0, i) = (0, i^3) = (0, -i) = P_2$. La órbita es $\{(0, i), (0, -i)\}$.

El ideal maximal correspondiente en la $k$-álgebra es la contracción a $A$ de la intersección en $\overline{\mathbb{F}}_3[x, y]/(y^2 - x^3 + 1)$:

$$\begin{aligned} \mathfrak{m}_4 &= \big((x, y - i) \cap (x, y + i)\big) \cap A \\ &= (x, (y - i)(y + i)) \cap A \\ &= (x, y^2 + 1) \cap A. \end{aligned}$$

Este ideal maximal $\mathfrak{m}_4 = (\bar{x}, \bar{y}^2 + 1)$ tiene cuerpo residual isomorfo a $\mathbb{F}_9$. Geométricamente, aunque en el espectro maximal de $A$ vemos un solo punto cerrado, el cambio de base a $\overline{\mathbb{F}}_3$ revela que este se desdobla en dos puntos distintos conjugados. ▪

▪ **Ejemplo 3.2** Consideremos el plano afín sobre los racionales, con anillo de coordenadas $R = \mathbb{Q}[x, y]$. Sea la curva plana afín definida por el polinomio de grado cuatro (una cuártica):

$$f(x, y) = y^2 - x^4 + 2.$$

Es sencillo verificar que $f(x,y)$ es irreducible en $\mathbb{Q}[x,y]$, por lo que genera un ideal primo $\mathfrak{p} = (y^2 - x^4 + 2)$. En el esquema $\mathrm{Spec}(\mathbb{Q}[x,y])$, este ideal primo $\mathfrak{p}$ no es maximal (la dimensión de Krull del cociente es 1) y representa el **punto genérico** de nuestra curva cuártica.

Como $\mathbb{Q}$ es un campo, la $\mathbb{Q}$-álgebra finitamente generada $R$ es un anillo de Jacobson (Proposición 2.4). Por el Corolario 2.5, el punto genérico $\mathfrak{p}$ debe poder recuperarse como la intersección de todos los ideales maximales de $R$ que lo contienen.

Construyamos explícitamente una familia infinita de tales ideales maximales y demostremos que su intersección es exactamente $\mathfrak{p}$. Para cada entero $a \in \mathbb{Z}$, definimos el ideal:

$$\mathfrak{m}_a = (x - a, y^2 - x^4 + 2) = (x - a, y^2 - a^4 + 2).$$

**Afirmación 1: $\mathfrak{m}_a$ es un ideal maximal para todo $a \in \mathbb{Z}$.**
Notemos que el isomorfismo de evaluación en $x = a$ nos da $R/\mathfrak{m}_a \cong \mathbb{Q}[y]/(y^2 - a^4 + 2)$. Para que este cociente sea un campo, basta con que el polinomio $y^2 - a^4 + 2$ sea irreducible sobre $\mathbb{Q}$, lo cual ocurre si y solo si $a^4 - 2$ no es un cuadrado perfecto en $\mathbb{Q}$. Si existiera $k \in \mathbb{Q}$ tal que $k^2 = a^4 - 2$, al ser $a \in \mathbb{Z}$, $k$ también debe ser entero. Factorizando tendríamos $(a^2 - k)(a^2 + k) = 2$. Los únicos divisores de 2 son $\pm 1, \pm 2$, lo que obligaría a que $2a^2 = \pm 3$, lo cual no tiene solución en los enteros. Por lo tanto, $a^4 - 2$ nunca es un cuadrado en $\mathbb{Q}$, la extensión residual tiene grado 2 (isomorfa a $\mathbb{Q}(\sqrt{a^4 - 2})$), y $\mathfrak{m}_a$ es maximal.

Geométricamente (y conectando con el teorema de la correspondencia), $\mathfrak{m}_a$ es la contracción a $\mathbb{Q}[x,y]$ de la órbita de Galois formada por el par de puntos conjugados $(a, \sqrt{a^4 - 2})$ y $(a, -\sqrt{a^4 - 2})$ en $\overline{\mathbb{Q}}^2$.

**Afirmación 2: $\mathfrak{p} = \bigcap_{a \in \mathbb{Z}} \mathfrak{m}_a$.**
Claramente, como $f(x,y) \in \mathfrak{m}_a$ para todo $a$, se tiene la contención $\mathfrak{p} \subseteq \bigcap_{a \in \mathbb{Z}} \mathfrak{m}_a$.

Para ver la contención inversa, sea $g(x,y) \in \bigcap_{a \in \mathbb{Z}} \mathfrak{m}_a$. Queremos demostrar que $g \in \mathfrak{p}$. Podemos ver a $g(x,y)$ como un elemento del anillo de polinomios $(\mathbb{Q}[x])[y]$. Usando el algoritmo de la división para polinomios mónicos en la variable $y$, dividimos $g(x,y)$ entre $f(x,y) = y^2 - x^4 + 2$:

$$g(x,y) = q(x,y)f(x,y) + r(x,y),$$

donde el residuo $r(x,y)$ tiene grado menor estricto que 2 respecto a $y$. Por tanto, el residuo tiene la forma:

$$r(x,y) = c(x)y + d(x) \quad \text{con } c(x), d(x) \in \mathbb{Q}[x].$$

Dado que $g(x,y) \in \mathfrak{m}_a = (x - a, f(x,y))$ y trivialmente $q(x,y)f(x,y) \in \mathfrak{m}_a$, deducimos que el residuo también pertenece al ideal:

$$c(x)y + d(x) \in (x - a, y^2 - a^4 + 2).$$

Al evaluar módulo $(x - a)$, pasamos a $\mathbb{Q}[y]/(y^2 - a^4 + 2)$, lo que implica que el polinomio en una variable $c(a)y + d(a)$ debe ser un múltiplo de $y^2 - a^4 + 2$ en $\mathbb{Q}[y]$.

Pero el grado de $c(a)y + d(a)$ respecto a $y$ es a lo más 1, mientras que el de $y^2 - a^4 + 2$ es 2. La única forma en que esto sea un múltiplo es que sea el polinomio cero:

$$c(a) = 0 \quad \text{y} \quad d(a) = 0.$$

Como esto debe cumplirse para **todos** los infinitos enteros $a \in \mathbb{Z}$, los polinomios $c(x)$ y $d(x) \in \mathbb{Q}[x]$ tienen infinitas raíces, por lo que deben ser el polinomio nulo: $c(x) = 0$ y $d(x) = 0$.

Por lo tanto, $r(x,y) = 0$, lo que implica $g(x,y) = q(x,y)f(x,y) \in (f(x,y)) = \mathfrak{p}$.

Esto concluye la prueba de que el punto genérico $\mathfrak{p}$ está unívocamente determinado algebraicamente por la familia de puntos cerrados (ideales maximales) que yacen sobre él. ∎

## Referencias