Notas de Geometría Algebraica
Teorema de Luroth

Luis Manuel Reyes de la Luz

Mayo 2026

Resumen

Primer tema del parcial 4.

Índice

1. Acerca de funciones Racionales. 1

2. Teorema de Luroth. 4

3. Ejemplos y aplicaciones. 11

A. Algunos lemas técnicos. 17

Notación

1. Acerca de funciones Racionales.

En esta sección consideramos X una variedad afin, es decir un conjunto algebraico irreducicble. Para cada $p \in X$ el anillo de germenes es definido como

$$\mathcal{O}_{X,p} := \varinjlim_{p \in U} \mathcal{O}_X(U),$$

este viene incluido con un morfismo sobreyectivo

$$\mathrm{ev}_p : \mathcal{O}_{X,p} \longrightarrow K,\ [f] \mapsto f(p)$$

cuyo kernel es

$$\mathfrak{m}_p := \{[f] \in \mathcal{O}_{X,p} \mid\ f(p) = 0\}.$$

Ademas decimos que una función regular $\phi : X \longrightarrow Y$ es dominante si

$$\overline{\phi(X)} = Y.$$

Lo anterior es equivalente a pedir que su morfismo en la categoría de k-álgebras $\phi^* : K[Y] \longrightarrow K[X]$ es inyectivo.

Definición 1.1 — Funciones Racionales. El cuerpo de funciones racionales $K(X)$ se define como el colímite de este sistema dirigido en la categoría de k-álgebras:

$$K(X) = \varinjlim_{U \in \mathcal{T}_X} \mathcal{O}_X(U)$$

Como X es una variedad, es decir X es irreducible entonces $K[X]$ es un dominio entero y usando el Lema A.1 tenemos que

$$Fracc(K[X]) = K(X).$$

Recordemos que existe una transformación natural

$$\alpha \colon O_X(-) \Rightarrow Fun(-, K),$$

Entonces, un elemento $\alpha \in K(X)$ es, por definición de colímite, una clase de equivalencia $[(U, f)]$. Esto garantiza que para cualquier representante, existe un abierto de Zariski U donde la función (mediante la transformación natural), vive como una función racional $f : U \to k$, $f = P/Q$, $P, Q \in k[X]$, $Q(p) \neq 0$. Para cualquier punto $p \in U$, el valor de la función racional en ese punto se define simplemente como $\phi(p) := f(p)$. Si elegimos otro representante (V, g) para el mismo elemento α, la relación de equivalencia en el colímite impone que f y g deben coincidir en un abierto denso contenido en $U \cap V$.

Ahora para definir los morfismos racionales entre variedades tenemos lo siguiente. Fijemos X, Y variedades algebraicas, y consideremos el funtor

$$\mathcal{F}_{X,Y} \colon \tau_X^{op} \longrightarrow K\textbf{-Alg},\ U \mapsto \mathrm{Hom}_{\mathbf{Var}}(U, Y)$$

donde $\mathrm{Hom}_{\mathbf{Var}}(U, Y)$ es el conjunto de morfismos regulares $f \colon U \to Y$. Entonces el conjunto de morfismos racionales desde X hacia Y se define como

$$Rat(X, Y) := \varinjlim_{U \neq \emptyset} \mathcal{F}_{X,Y}$$

Recordemos que una función regular en un abierto $U \subseteq X$ es definido como sigue; Una función $f : U \to k$ es regular si para cada punto $p \in U$, existe un entorno abierto $V_p \subseteq U$ que contiene a p y polinomios $P, Q \in k[X]$ tales que:

1. $Q(x) \neq 0$ para todo $x \in V_p$.
2. $f(x) = \frac{P(x)}{Q(x)}$ para todo $x \in V_p$.

Entonces una función racional $\phi \colon X \to Y$ se entiende como una clase de funciones donde tiene ϕ está representada por un morfismo regular $\phi_U : U \to Y$ definido en algún abierto denso $U \subseteq X$. Dado que el codominio está inmerso en $\mathbb{A}^m$, el morfismo ϕ_U está determinado por sus m funciones coordenadas:

$$\phi_U(x) = (f_1(x), f_2(x), \ldots, f_m(x)),\ f_i \in K(X),\ \mathrm{dom}\, f_i \subseteq U.$$

Definición 1.2 — Domiancia. Un mapa racional $\phi : X \dashrightarrow Y$ es dominante si para algún representante (U, ϕ_U), la imagen $\phi_U(U)$ es densa en Y (es decir, $\overline{\phi_U(U)} = Y$).

Proposición 1.1 *Si $\phi : X \dashrightarrow Y$ es dominante, induce un homomorfismo inyectivo de k-álgebras en los cuerpos de funciones:*

$$\phi^* : K(Y) \hookrightarrow K(X), \quad f \mapsto f \circ \phi$$

Consideremos $\mathbf{Proj}_K$ la categoria de variedades proyectivas y morfismos racionales dominantes, construimos el funtor

$$\mathcal{F} : \mathbf{Proj}_K \longrightarrow K\text{-}\mathbf{Alg}^{grad}, \ X \mapsto K(X)$$

este funtor captura la siguiente información

1. $K(X)$ es un campo, $K(X)/K$ es una extensión de grado trascendente finito.

Teorema 1.2 *Existe una equivalencia entre las categorías de variedades proyectivas y extensiones de campos finitamente generado.*

Demostración. Dado L/K una extensión de campos finitamente generada, existen elementos $x_1, \ldots, x_n \in L$ tales que $L = K(x_1, \ldots, x_n)$ (es decir, L es el campo de fracciones más pequeño que contiene a K y a los elementos x_i). Dentro del campo L, consideramos el subanillo generado por estos mismos elementos sobre K:

$$A = K[x_1, \ldots, x_n] \subseteq L$$

Este subanillo A sí es, por definición, un K-álgebra finitamente generada. Además, al ser un subanillo de un cuerpo (L), A carece de divisores de cero, por lo que es un dominio de integridad.Consideramos el epimorfismo natural de evaluación desde el anillo de polinomios:

$$\pi : K[T_1, \ldots, T_n] \longrightarrow A$$

$$T_i \longmapsto x_i$$

Sea $I = \ker(\pi)$. Como A es un dominio de integridad, I es un ideal primo.Geométricamente, este ideal primo I define una variedad afín irreducible $U = V(I) \subseteq \mathbb{A}^n_K$.Por construcción, el anillo de coordenadas afines de esta variedad es $K[U] \cong K[T_1, \ldots, T_n]/I \cong A$.

Calculamos ahora el cuerpo de funciones racionales de nuestra variedad afín U. Por definición, es el campo de fracciones de su anillo de coordenadas:

$$K(U) = \mathrm{Frac}(K[U]) \cong \mathrm{Frac}(A) = \mathrm{Frac}(K[x_1, \ldots, x_n])$$

Pero al inicio establecimos que L es exactamente el campo generado por los x_i, lo que algebraicamente significa que L es el campo de fracciones de A. Por lo tanto:

$$K(U) \cong L$$

Consideramos el encaje estándar del espacio afín en el espacio proyectivo $\mathbb{A}^n_K \hookrightarrow \mathbb{P}^n_K$, dado por $(a_1, \ldots, a_n) \mapsto [1 : a_1 : \cdots : a_n]$.Identificamos a U con su imagen bajo este encaje y definimos X como la clausura de Zariski de U en $\mathbb{P}^n_K$:

$$X = \overline{U} \subseteq \mathbb{P}^n_K$$

Por propiedades básicas de la topología de Zariski, U es un subconjunto abierto denso de la variedad proyectiva X.Como el cuerpo de funciones racionales se define como el colímite sobre

abiertos densos, X y U comparten exactamente el mismo cuerpo de funciones:

$$K(X) \cong K(U) \cong L$$

Queda así construida la variedad proyectiva X. ■

Corolario 1.3 *$\phi : X \dashrightarrow Y$ es un isomorfismo biracional si y solo si $\phi^* : K(Y) \xrightarrow{\sim} K(X)$ es un isomorfismo de cuerpos.*

2. Teorema de Luroth.

Definición 2.1 — Variedades racionales. Una variedad proyectiva X es racional si es biracionalmente equivalente a $\mathfrak{P}^d$. Ademas decimos que X es *unirracional* si existe un mapa racional dominante $\mathbb{P}^d \dashrightarrow X$.

■ **Ejemplo 2.1** Consideremos la curva afín plana $C \subset \mathbb{A}^2$ definida sobre un campo algebraicamente cerrado por el polinomio:

$$f(x, y) = y^2 - x^3 - x^2 = 0$$

Para demostrar que esta curva es una variedad racional, necesitamos encontrar una equivalencia birracional con $\mathbb{A}^1$. Podemos hacer esto proyectando desde la singularidad (el nodo) que se encuentra en el origen $(0, 0)$.

Trazamos rectas por el origen: Consideremos el haz de rectas que pasan por el origen, dadas por la ecuación $y = tx$, donde t es el parámetro (la pendiente).Sustituimos en la curva:

$$(tx)^2 = x^3 + x^2$$

$$t^2x^2 = x^2(x + 1)$$

Despejamos para $x \neq 0$:

$$t^2 = x + 1 \implies x = t^2 - 1$$

Encontramos y:

$$y = t(t^2 - 1) = t^3 - t$$

Así, hemos construido una aplicación racional $\phi : \mathbb{A}^1 \dashrightarrow C$ dada por:

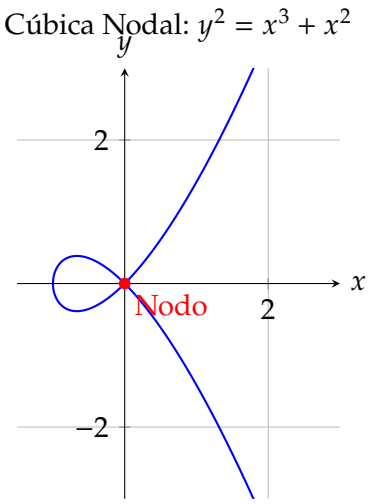
$$\phi(t) = (t^2 - 1, t^3 - t)$$

Esta aplicación tiene una inversa racional $\psi : C \dashrightarrow \mathbb{A}^1$ dada simplemente por la pendiente de la recta:

$$\psi(x, y) = \frac{y}{x}$$

Esta inversa está definida en todos los puntos de la curva excepto en el nodo $(0, 0)$.

■



■ **Ejemplo 2.2** Consideremos la superficie afín $V \subset \mathbb{A}^3$ definida sobre un campo algebraicamente cerrado por el polinomio:

$$x^2 - y^2 z = 0$$

Para demostrar que esta superficie es racional, construimos una aplicación racional $\phi : \mathbb{A}^2 \dashrightarrow V$. Tomando los parámetros (u, v) en $\mathbb{A}^2$, definimos:

$$\phi(u, v) = (uv, u, v^2)$$

Es inmediato verificar que la imagen satisface la ecuación de la superficie:

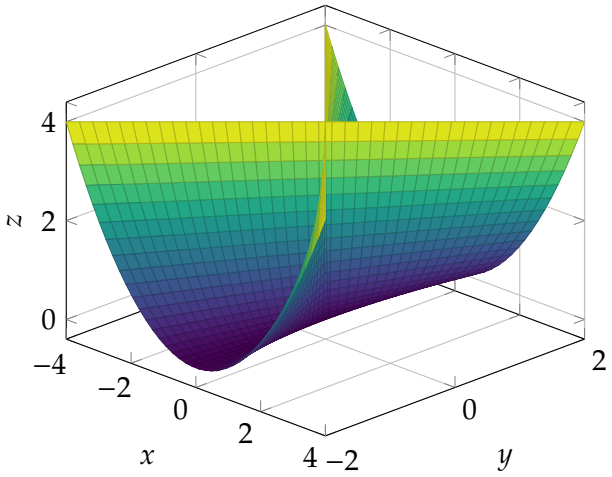
$$(uv)^2 = u^2 v^2 \implies x^2 = y^2 z$$

La aplicación racional inversa $\psi : V \dashrightarrow \mathbb{A}^2$ recupera los parámetros originales a partir de las coordenadas del espacio:

$$\psi(x, y, z) = \left(y, \frac{x}{y} \right)$$

Esta inversa está bien definida en todos los puntos de la superficie excepto en el eje z (donde $y = 0$ y $x = 0$). Geométricamente, este eje constituye el lugar geométrico singular (el "mango"de la sombrilla, donde la superficie se cruza a sí misma). Esto demuestra formalmente que el campo de funciones racionales de V es isomorfo a $k(u, v)$, y por lo tanto, la superficie es racional. ■

Sombrilla de Whitney: $x^2 = y^2 z$



Geométricamente, una variedad X sobre un campo k es uniracional si existe una aplicación racional dominante $\mathbb{P}^n_k \dashrightarrow X$. En términos algebraicos, esto significa que el campo de funciones $k(X)$ se puede encajar (inyectar) en una extensión puramente trascendente del campo base: $k \subset k(X) \subset k(t_1, \ldots, t_n)$.

Cuestión 2.1 — Problema de Luroth. ¿Es una variedad uniracional una variedad racional?

▪ **Ejemplo 2.3** Consideremos la variedad proyectiva $X \subset \mathbb{P}^4_{\mathbb{C}}$ dada por la ecuación:

$$x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3 = 0$$

Definimos el subespacio lineal $L_0 \cong \mathbb{P}^1$ mediante el sistema de ecuaciones lineales:

$$x_0 + x_1 = 0, \quad x_2 + x_3 = 0, \quad x_4 = 0$$

Una parametrización de L_0 en términos de coordenadas $(u : v) \in \mathbb{P}^1$ es $(u : -u : v : -v : 0)$. Sustituyendo esto en la ecuación de X:

$$F(u, -u, v, -v, 0) = u^3 + (-u)^3 + v^3 + (-v)^3 + 0^3 = u^3 - u^3 + v^3 - v^3 = 0$$

Dado que la identidad se sostiene para todo $(u : v)$, la recta L_0 está contenida íntegramente en X.

Para construir la proyección desde L_0, aplicamos un automorfismo lineal de $\mathbb{P}^4$ para aislar las ecuaciones de la recta. Definimos nuevas coordenadas:

$$y_0 = x_0 + x_1, \quad z_0 = x_0 - x_1$$

$$y_1 = x_2 + x_3, \quad z_1 = x_2 - x_3$$

$$y_2 = x_4$$

La relación inversa para las dos primeras variables es $x_0 = \frac{1}{2}(y_0 + z_0)$ y $x_1 = \frac{1}{2}(y_0 - z_0)$. Evaluando la suma de sus cubos:

$$x_0^3 + x_1^3 = \frac{1}{8}\left((y_0 + z_0)^3 + (y_0 - z_0)^3\right) = \frac{1}{4}(y_0^3 + 3y_0 z_0^2)$$

Aplicando el mismo desarrollo a x_2, x_3, la ecuación de X en el nuevo sistema de coordenadas es:

$$y_0^3 + 3y_0z_0^2 + y_1^3 + 3y_1z_1^2 + 4y_2^3 = 0$$

La recta L_0 ahora está dada por el ideal $I = (y_0, y_1, y_2)$.

Consideremos la proyección racional $\pi : \mathbb{P}^4 \dashrightarrow \mathbb{P}^2$ con centro en L_0, dada por:

$$\pi(y_0 : y_1 : y_2 : z_0 : z_1) = (y_0 : y_1 : y_2)$$

Para un punto genérico $y = (y_0 : y_1 : y_2) \in \mathbb{P}^2$, la fibra $\pi^{-1}(y)$ en $\mathbb{P}^4$ es un plano afín $\Pi_y \cong \mathbb{P}^2$ que contiene a L_0. Podemos parametrizar los puntos de este plano usando coordenadas proyectivas internas $(z_0 : z_1 : w)$, donde las coordenadas en $\mathbb{P}^4$ se recuperan como $(wy_0 : wy_1 : wy_2 : z_0 : z_1)$.

Sustituimos esta parametrización del plano Π_y en la ecuación de X:

$$(wy_0)^3 + 3(wy_0)z_0^2 + (wy_1)^3 + 3(wy_1)z_1^2 + 4(wy_2)^3 = 0$$

Factorizamos w:

$$w\left[3y_0z_0^2 + 3y_1z_1^2 + w^2(y_0^3 + y_1^3 + 4y_2^3)\right] = 0$$

El factor $w = 0$ corresponde a la recta base L_0. El factor residual define una cónica C_y en el plano Π_y:

$$C_y : \quad 3y_0z_0^2 + 3y_1z_1^2 + w^2(y_0^3 + y_1^3 + 4y_2^3) = 0$$

Esto demuestra que X es birracional a un haz de cónicas sobre $\mathbb{P}^2$.

Para parametrizar el haz de cónicas mediante funciones racionales, la cónica genérica C_y (vista como una curva sobre el campo de funciones de la base $K = \mathbb{C}(y_1/y_0, y_2/y_0)$) debe tener un punto K-racional.La ecuación de la cónica es de la forma $Az_0^2 + Bz_1^2 + Cw^2 = 0$. Estableciendo $z_1 = 0$, buscamos una solución para $3y_0z_0^2 + (y_0^3 + y_1^3 + 4y_2^3)w^2 = 0$.Haciendo $w = 1$, requerimos que exista un elemento β tal que:

$$3y_0\beta^2 + (y_0^3 + y_1^3 + 4y_2^3) = 0$$

Esta condición define una superficie algebraica $S \subset \mathbb{P}^3$ con coordenadas $(y_0 : y_1 : y_2 : \beta)$. Como el polinomio es homogéneo de grado 3, S es una superficie cúbica suave.

Notemos el campo de funciones $\mathbb{C}(S)$ es una extensión puramente trascendente de grado 2, $\mathbb{C}(S) \cong \mathbb{C}(s_1, s_2)$.

Consideremos la proyección natural $\rho : S \to \mathbb{P}^2$ dada por:

$$\rho(y_0 : y_1 : y_2 : \beta) = (y_0 : y_1 : y_2)$$

Dado un punto genérico $(y_0 : y_1 : y_2) \in \mathbb{P}^2$, la ecuación cuadrática $3y_0\beta^2 = -(y_0^3 + y_1^3 + 4y_2^3)$ tiene exactamente dos soluciones distintas para β. Por lo tanto, el morfismo ρ tiene grado 2.Al realizar el cambio de base del haz de cónicas a través de ρ, obtenemos el producto fibrado $X_S = X \times_{\mathbb{P}^2} S$.Sobre el campo de funciones $\mathbb{C}(S)$, la cónica genérica ahora posee un punto racional explícito $P = (\beta, 0, 1)$. Proyectando desde este punto racional P, la cónica se vuelve isomorfa a $\mathbb{P}^1_{\mathbb{C}(S)}$, parametrizada por un nuevo generador trascendente t.Algebraicamente, esto significa que la variedad X_S es birracionalmente equivalente a $S \times \mathbb{P}^1$. Dado que S es racional (birracional a $\mathbb{P}^2$), tenemos una equivalencia birracional completa:

$$\Psi : \mathbb{P}^3 \cong \mathbb{P}^2 \times \mathbb{P}^1 \dashrightarrow X_S$$

Esta aplicación Ψ tiene grado 1.

Finalmente, la aplicación racional dominante buscada $\Phi : \mathbb{P}^3 \dashrightarrow X$ se define como la composición de Ψ con la proyección canónica $p_1 : X_S \to X$:

$$\Phi = p_1 \circ \Psi$$

Dado que p_1 es el pullback geométrico inducido por ρ, hereda el grado de ρ.Como $\deg(\Psi) = 1$ y $\deg(p_1) = \deg(\rho) = 2$, se concluye formalmente que la aplicación dominante $\Phi : \mathbb{P}^3 \dashrightarrow X$ tiene exactamente grado 2. ∎

Sean t un elemento trascendente sobre el campo k y $u \in k(t)$ dado por la función racional $u = \frac{p(t)}{q(t)}$.

Lema 2.2 *El elemento t es algebraico sobre $k(u)$. Específicamente, t es raíz del polinomio $f(X) = p(X) - uq(X) \in k(u)[X]$. El grado de la extensión $[k(t) : k(u)]$ es exactamente $n = \deg p$.*

Demostración. Consideremos el polinomio en la variable X con coeficientes en el campo $k(u)$:

$$f(X) = p(X) - uq(X) \in k(u)[X]$$

Evaluando este polinomio en $X = t$, obtenemos:

$$f(t) = p(t) - uq(t) = p(t) - \frac{p(t)}{q(t)}q(t) = 0$$

Obteniendo que t es efectivamente raíz de $f(X)$, lo que demuestra que t es algebraico sobre $k(u)$.

Analicemos el grado de $f(X)$ como polinomio en X. El coeficiente de X^m en $f(X)$ es de la forma $a_m - ub_m$, donde a_m y b_m son los coeficientes de X^m en $p(X)$ y $q(X)$ respectivamente.Dado que t es trascendente sobre k, $u = p(t)/q(t)$ no pertenece a k. Como $u \notin k$, el coeficiente principal $a_m - ub_m$ nunca puede anularse (pues $a_m, b_m \in k$).En consecuencia, no hay cancelación de términos de mayor grado, y el grado de $f(X)$ es exactamente:

$$\deg_X f(X) = \max(\deg p, \deg q)$$

Por la hipótesis de que $n = \deg p \geq \deg q$, concluimos que $\deg_X f(X) = n$.

Para demostrar que el grado de la extensión $[k(t) : k(u)]$ es exactamente n, es necesario y suficiente probar que $f(X)$ es irreducible en $k(u)[X]$, lo cual lo convierte en el polinomio mínimo de t sobre $k(u)$.

Para hacer esto, observemos que el anillo de polinomios $k[u, X]$ es isomorfo a $k[X][u]$. Visto en $k[X][u]$, podemos reescribir nuestra expresión como un polinomio en la variable u con coeficientes en el dominio de factorización única $k[X]$:

$$F(u) = -q(X)u + p(X)$$

Este es un polinomio de grado 1 en la variable u. Un polinomio lineal $A \cdot u + B$ sobre un dominio de factorización única es irreducible si y solo si sus coeficientes A y B son coprimos.Por hipótesis, $p(X)$ y $q(X)$ son polinomios coprimos en $k[X]$. Es decir:

$$\gcd(-q(X), p(X)) = 1$$

Por lo tanto, el polinomio $F(u)$ es primitivo como elemento de $k[X][u]$, y al ser de grado 1 en u, es irreducible en $k[X, u]$.

Ahora aplicamos el Lema de Gauss A.2. Dado que $k[u]$ es un dominio de factorización única y $k(u)$ es su campo de fracciones, un polinomio en $k[u][X]$ es irreducible en $k(u)[X]$ si y solo si es irreducible en $k[u, X]$ (y primitivo respecto a $k[u]$). Como hemos demostrado que $p(X) - uq(X)$ es irreducible en $k[u, X]$, se sigue directamente que $f(X)$ es irreducible en $k(u)[X]$. ■

Teorema 2.3 — Teorema de Luroth. *Sea k un campo y t una variable trascendente. Si L es una extensión de cuerpos tal que $k \subsetneq L \subseteq k(t)$, entonces existe $u \in L$ tal que $L = k(u)$.*

Demostración. Dado que $k \subsetneq L \subseteq k(t)$, existe al menos un elemento $v \in L \setminus k$. Como $v \in k(t)$, podemos escribirlo como una función racional $v = \frac{p_1(t)}{q_1(t)}$ con $p_1, q_1 \in k[X]$ coprimos y $\max(\deg p_1, \deg q_1) \geq 1$. Por el Lema 2.2, sabemos que $[k(t) : k(v)] = \max(\deg p_1, \deg q_1) < \infty$.

Como $k(v) \subseteq L \subseteq k(t)$, la extensión torre nos dice que L también es una extensión finita sobre $k(v)$, y más importante, $k(t)$ es una extensión finita sobre L. Sea este grado:

$$d = [k(t) : L]$$

Como la extensión $k(t)/L$ es finita, t es algebraico sobre L. Sea $m(X) \in L[X]$ el polinomio mínimo mónico de t sobre L. Por definición, el grado de este polinomio es:

$$\deg_X m(X) = d$$

Escribamos explícitamente a $m(X)$:

$$m(X) = X^d + c_{d-1}X^{d-1} + \cdots + c_1X + c_0$$

donde $c_i \in L$. Como t es trascendente sobre k, su polinomio mínimo no puede tener todos sus coeficientes en k. Por lo tanto, existe al menos un índice j tal que $c_j \in L \setminus k$.Elijamos a este coeficiente como nuestro candidato a generador:

$$u = c_j$$

Como $u \in L \subseteq k(t)$, podemos escribir $u = \frac{p(t)}{q(t)}$ donde $p(X), q(X) \in k[X]$ son polinomios coprimos. Sea:

$$n = \max(\deg p, \deg q)$$

Nuevamente, por el Lema 2.2, sabemos exactamente que:

$$[k(t) : k(u)] = n$$

Dado que $k(u) \subseteq L \subseteq k(t)$, por multiplicatividad de grados tenemos:

$$n = d \cdot [L : k(u)]$$

Nuestra meta a partir de aquí es demostrar que $n = d$, lo cual forzará a que $[L : k(u)] = 1$ y, por lo tanto, $L = k(u)$.

Consideremos el polinomio que anula a t sobre $k(u)$:

$$f(X) = p(X) - uq(X) \in k(u)[X]$$

Sabemos que $f(t) = 0$. Como $u \in L$, entonces $f(X) \in L[X]$. Al ser $m(X)$ el polinomio mínimo de t sobre L, $m(X)$ divide a $f(X)$ en $L[X]$. Esto ya implica que $d \leq n$.

Para probar la igualdad, pasemos al anillo bivariado $k[t, X]$. Cada coeficiente $c_i \in L$ de $m(X)$ es una función racional $c_i(t) = \frac{a_i(t)}{b_i(t)}$ (en forma reducida). Sea $b(t) \in k[t]$ el mínimo común múltiplo de todos los denominadores $b_i(t)$. Definimos:

$$M(t, X) = b(t)m(X) \in k[t, X]$$

Al multiplicar por el mínimo común múltiplo, nos aseguramos de que el máximo común divisor de los coeficientes de $M(t, X)$ (visto como polinomio en X con coeficientes en $k[t]$) sea 1. Por lo tanto, $M(t, X)$ es un polinomio primitivo en $k[t][X]$.

Analicemos el grado de $M(t, X)$ respecto a la variable t. El coeficiente del término X^j en $M(t, X)$ es $b(t)c_j(t) = b(t)\frac{p(t)}{q(t)}$. Como $M(t, X) \in k[t, X]$, el polinomio $q(t)$ debe dividir a $b(t)p(t)$. Al ser $\gcd(p, q) = 1$, $q(t)$ debe dividir a $b(t)$, luego $b(t) = q(t)h(t)$ para algún $h \in k[t]$.

1. El coeficiente principal de X^d en M es $b(t)$, por lo que $\deg_t M \geq \deg b \geq \deg q$.
2. El coeficiente de X^j en M es $h(t)p(t)$, por lo que $\deg_t M \geq \deg(hp) \geq \deg p$.Por lo tanto, concluimos rigurosamente que:

$$\deg_t M(t, X) \geq \max(\deg p, \deg q) = n$$

Definamos ahora un análogo limpio de denominadores para $f(X)$:

$$F(t, X) = p(X)q(t) - p(t)q(X) \in k[t, X]$$

Notemos que $F(t, t) = p(t)q(t) - p(t)q(t) = 0$. Además, los grados máximos por variable están acotados por la construcción de p y q:

$$\deg_t F(t, X) \leq n \quad \text{y} \quad \deg_X F(t, X) \leq n$$

Como $m(X)$ divide a $f(X)$ en $L[X]$, y $f(X) = \frac{F(t,X)}{q(t)}$, entonces $m(X)$ divide a $F(t, X)$ en el campo de fracciones $k(t)[X]$.Dado que $M(t, X) = b(t)m(X)$, M y m difieren solo por una unidad en $k(t)$, por lo que $M(t, X)$ también divide a $F(t, X)$ en $k(t)[X]$.

Apliquemos el lema A.3, como $M(t, X)$ es primitivo en $k[t][X]$ y divide a $F(t, X)$ en $k(t)[X]$, debe dividir a $F(t, X)$ directamente en el anillo $k[t, X]$. Es decir, existe $Q(t, X) \in k[t, X]$ tal que:

$$F(t, X) = M(t, X)Q(t, X)$$

Igualando los grados respecto a la variable t en la factorización obtenemos:

$$\deg_t F = \deg_t M + \deg_t Q$$

Sabemos que $\deg_t F \leq n$ y que $\deg_t M \geq n$. La única forma de que esta ecuación se sostenga en los números naturales es que se den las igualdades:

$$\deg_t F = n, \quad \deg_t M = n, \quad \text{y} \quad \deg_t Q = 0$$

Que $\deg_t Q = 0$ significa que el factor Q no depende de t, es decir, $Q(t, X) = Q(X) \in k[X]$.

Ahora sustituimos $Q(X)$ en la factorización original:

$$F(t, X) = M(t, X)Q(X)$$

Si observamos esta igualdad como polinomios en la variable t, el polinomio $Q(X)$ debe ser un divisor común de todos los coeficientes de $F(t, X)$.

Desarrollando $F(t, X) = p(X)q(t) - q(X)p(t)$, vemos que sus coeficientes en t son combinaciones lineales de $p(X)$ y $q(X)$. Como elegimos $p(X)$ y $q(X)$ para que fueran coprimos en $k[X]$, su máximo común divisor es 1.

En consecuencia, $Q(X)$ tiene que dividir a 1, lo que implica que $Q(X)$ es simplemente una constante no nula $c \in k$.

Si Q es constante, $\deg_X Q = 0$. Igualando ahora los grados respecto a X:

$$\deg_X F = \deg_X M + \deg_X Q$$

Como $F(t, X)$ es antisimétrico ($F(t, X) = -F(X, t)$), su grado respecto a X es igual a su grado respecto a t, el cual es n.

Por otro lado, el grado de $M(t, X)$ respecto a X es exactamente el grado del polinomio mínimo $m(X)$, que es d.Sustituyendo los valores:

$$n = d + 0 \implies n = d$$

■

3. Ejemplos y aplicaciones.

Supongamos que, tenemos una curva racional afín dada por:

$$x = \frac{p_1(t)}{q_1(t)}, \quad y = \frac{p_2(t)}{q_2(t)}$$

donde los polinomios son coprimos en cada fracción.

Geométricamente, afirmar que una curva afín irreducible $C \subset \mathbb{A}^2$ es parametrizable por funciones racionales equivale a postular la existencia de una aplicación racional dominante $\mathbb{A}^1 \dashrightarrow C$. Usando la equivalencia de categorias 1.2, este morfismo induce un encaje inyectivo entre sus campos de funciones, estableciendo la contención $k(C) \hookrightarrow k(t)$. A priori, esta inmersión únicamente clasifica a C como una curva uniracional.

Es precisamente en este escenario donde el Teorema de Lüroth 2.3 ejerce su papel: nos asegura que cualquier subextensión de $k(t)$ que trascienda estrictamente al campo base k es forzosamente una extensión puramente trascendente. Dado que C tiene dimensión 1, su campo de funciones $k(C)$ no se reduce a k, por lo que se concluye de manera ineludible que $k(C) \cong k(s)$ para algún parámetro generador $s \in k(t)$.

Consecuentemente, el teorema nos garantiza que no solo existe una parametrización, sino que siempre es posible elegir un parámetro algebraicamente óptimo que defina una parametrización propia (birracional), garantizando una correspondencia uno a uno en casi todos los puntos y la existencia de una inversa racional $s = h(x, y)$.

Queremos encontrar el ideal de la curva $I_C = \ker(\phi) \subset k[x, y]$.

Proposición 3.1 *Consideremos el ideal J en el anillo polinomial grande $k[t, x, y, w]$ definido por las ecuaciones de los numeradores y la inversión de los denominadores:*

$$J = \langle q_1(t)x - p_1(t),\ q_2(t)y - p_2(t),\ 1 - w \cdot q_1(t)q_2(t) \rangle$$

Entonces, el ideal de la curva C se recupera mediante eliminación clásica:

$$I_C = J \cap k[x, y]$$

Demostración. Sea $f(x, y) \in J \cap k[x, y]$. Al pertenecer al ideal $J \subset R$, existen polinomios $A, B, C \in k[t, x, y, w]$ tales que podemos expresar f como la combinación lineal:

$$f(x, y) = A \cdot (q_1(t)x - p_1(t)) + B \cdot (q_2(t)y - p_2(t)) + C \cdot (1 - wq_1(t)q_2(t))$$

Consideremos el homomorfismo de evaluación $\varphi : k[t, x, y, w] \to k(t)$ definido por las siguientes sustituciones en el campo de fracciones:

$$x \mapsto \frac{p_1(t)}{q_1(t)}, \quad y \mapsto \frac{p_2(t)}{q_2(t)}, \quad w \mapsto \frac{1}{q_1(t)q_2(t)}, \quad t \mapsto t$$

Aplicando este homomorfismo a los generadores de J, observamos que todos se anulan:$q_1(t)\left(\frac{p_1(t)}{q_1(t)}\right) - p_1(t) = 0q_2(t)\left(\frac{p_2(t)}{q_2(t)}\right) - p_2(t) = 01 - \left(\frac{1}{q_1(t)q_2(t)}\right) q_1(t)q_2(t) = 1 - 1 = 0$Por lo tanto, al aplicar φ a toda la expresión de $f(x, y)$, obtenemos:

$$f\left(\frac{p_1(t)}{q_1(t)}, \frac{p_2(t)}{q_2(t)}\right) = \varphi(A) \cdot 0 + \varphi(B) \cdot 0 + \varphi(C) \cdot 0 = 0$$

Dado que f se anula al evaluarse en la parametrización de la curva, concluimos formalmente que $f \in I_C$.

Sea $f(x, y) \in I_C$. Por definición, sabemos que:

$$f\left(\frac{p_1(t)}{q_1(t)}, \frac{p_2(t)}{q_2(t)}\right) = 0 \quad \text{en } k(t)$$

Ahora, operando en el anillo de polinomios con coeficientes en el campo $k(t)[x, y]$, podemos realizar una expansión de Taylor polinomial de $f(x, y)$ centrada en el punto de evaluación $\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)$. Al saber que la evaluación en ese punto es 0, la expansión nos garantiza que $f(x, y)$ pertenece al ideal generado por las diferencias:

$$f(x, y) \in \left\langle x - \frac{p_1(t)}{q_1(t)},\ y - \frac{p_2(t)}{q_2(t)} \right\rangle_{k(t)[x,y]}$$

Esto significa que existen funciones racionales $H_1(t, x, y)$ y $H_2(t, x, y)$ con denominadores que dependen únicamente de $q_1(t)$ y $q_2(t)$ tales que:

$$f(x, y) = H_1 \cdot \left(x - \frac{p_1}{q_1}\right) + H_2 \cdot \left(y - \frac{p_2}{q_2}\right)$$

$$f(x, y) = \frac{H_1}{q_1} \cdot (q_1x - p_1) + \frac{H_2}{q_2} \cdot (q_2y - p_2)$$

Para llevar esta ecuación de $k(t)[x, y]$ al anillo polinomial $k[t, x, y]$, multiplicamos ambos lados por una potencia suficientemente alta N del producto $q_1(t)q_2(t)$ para limpiar todos los denominadores de $\frac{H_1}{q_1}$ y $\frac{H_2}{q_2}$. Obtenemos:

$$(q_1q_2)^N f(x, y) = \tilde{A}(t, x, y) \cdot (q_1x - p_1) + \tilde{B}(t, x, y) \cdot (q_2y - p_2)$$

donde $\tilde{A}, \tilde{B} \in k[t, x, y]$. En este punto interviene la variable w. En el anillo $k[t, x, y, w]$, consideramos la identidad algebraica:

$$1 - (wq_1q_2)^N = (1 - wq_1q_2) \sum_{k=0}^{N-1} (wq_1q_2)^k$$

Lo cual implica que existe un polinomio $D \in k[t, x, y, w]$ tal que:

$$1 = (wq_1q_2)^N + D \cdot (1 - wq_1q_2)$$

Multiplicamos el polinomio $f(x, y)$ por 1 utilizando esta última identidad:

$$f(x, y) = f(x, y) \left[(wq_1q_2)^N + D \cdot (1 - wq_1q_2) \right]$$

$$f(x, y) = w^N \left[(q_1q_2)^N f(x, y) \right] + f(x, y)D \cdot (1 - wq_1q_2)$$

Sustituimos la expresión libre de denominadores de $(q_1q_2)^N f(x, y)$ que obtuvimos anteriormente:

$$f(x, y) = w^N \left[\tilde{A} \cdot (q_1x - p_1) + \tilde{B} \cdot (q_2y - p_2) \right] + fD \cdot (1 - wq_1q_2)$$

$$f(x, y) = (w^N\tilde{A}) \cdot (q_1x - p_1) + (w^N\tilde{B}) \cdot (q_2y - p_2) + (fD) \cdot (1 - wq_1q_2)$$

Dado que cada uno de los términos de la suma es un múltiplo en $k[t, x, y, w]$ de uno de los tres generadores del ideal J, hemos demostrado que:

$$f(x, y) \in J$$

Como el polinomio f original dependía exclusivamente de x e y, se sigue trivialmente que $f \in J \cap k[x, y]$.Al demostrar ambas inclusiones, queda rigurosamente establecido que $I_C = J \cap k[x, y]$. ■

■ **Ejemplo 3.1** Consideremos la parametrización racional estándar de la circunferencia unitaria sobre $k = \mathbb{Q}$. Sabemos geométricamente que su ecuación implícita es $x^2 + y^2 - 1 = 0$, pero asumamos que solo conocemos su forma paramétrica proyectando desde el punto $(-1, 0)$:

$$x(t) = \frac{1 - t^2}{1 + t^2}, \quad y(t) = \frac{2t}{1 + t^2}$$

Identificamos inmediatamente los polinomios numeradores y denominadores de nuestra parametrización:

1. $p_1(t) = 1 - t^2$
2. $q_1(t) = 1 + t^2$
3. $p_2(t) = 2t$
4. $q_2(t) = 1 + t^2$

Trabajamos en el anillo de polinomios extendido $\mathbb{Q}[w, t, x, y]$. Aplicando directamente la proposición, construimos los tres generadores del ideal J.El primer generador limpia el denominador de x:

$$g_1 = q_1(t)x - p_1(t) = (1 + t^2)x - (1 - t^2) = x + xt^2 - 1 + t^2 = t^2(x + 1) + x - 1$$

El segundo generador limpia el denominador de y:

$$g_2 = q_2(t)y - p_2(t) = (1+t^2)y - 2t = yt^2 - 2t + y$$

El tercer generador introduce la variable w para forzar la inversión del producto de los denominadores $q_1(t)q_2(t)$, asegurando que no estamos evaluando en las raíces $t = \pm i$ donde la parametrización no está definida:

$$g_3 = 1 - w \cdot q_1(t)q_2(t) = 1 - w(1+t^2)(1+t^2) = 1 - w(1+2t^2+t^4)$$

Por lo tanto, el ideal es:

$$J = \langle (1+t^2)x - (1-t^2),\ (1+t^2)y - 2t,\ 1 - w(1+t^2)^2 \rangle \subset \mathbb{Q}[w,t,x,y]$$

Para eliminar las variables w y t, imponemos un orden monomial de eliminación (como el orden lexicográfico) donde las variables a eliminar sean estrictamente "mayores"que las variables de la curva: $w > t > x > y$.

Al calcular la Base de Gröbner reducida G del ideal J bajo este orden, el Teorema de Eliminación asegura que los polinomios en G que solo dependen de x e y forman una Base de Gröbner para I_C.

En este caso particular, si realizamos las reducciones (o multiplicamos apropiadamente combinaciones de g_1 y g_2), uno de los elementos resultantes en la base será exactamente el polinomio implícito, libre de t y w:

$$x^2 + y^2 - 1 \in I_C$$

Dado que este polinomio es irreducible, genera un ideal primo de dimensión 1, por lo que $I_C = \langle x^2 + y^2 - 1 \rangle$. ∎

Geométricamente, una parametrización racional $\phi : \mathbb{P}^1 \dashrightarrow C$ dada por $(x(t), y(t))$ recorre la curva C. Sin embargo, nadie garantiza a priori que la recorra una sola vez. Podría estar envolviendo la curva múltiples veces.

Definición 3.1 — Grado algebraico de una aplicación biracional. Sea $K = k(x(t), y(t))$ el campo de funciones de la curva. La aplicación ϕ induce una extensión de campos $K \subseteq k(t)$. El grado topológico del morfismo ϕ es exactamente el grado de la extensión de campos:

$$d = [k(t) : K]$$

1. Si $d = 1$, la parametrización es fiel (birracional) y la curva se traza una vez.
2. Si $d > 1$, la parametrización es impropia.

Lüroth no solo dice que $K \cong k(s)$, sino que nos da el mecanismo para encontrar ese s. Afirma que, sin importar qué tan enredada esté la parametrización original $x(t), y(t)$, siempre existe una función racional $s = h(t) \in k(t)$ tal que:

$$K = k(h(t))$$

Y por lo tanto, existen nuevas funciones racionales $\tilde{x}, \tilde{y}$ tales que:

$$x(t) = \tilde{x}(h(t)), \quad y(t) = \tilde{y}(h(t))$$

donde la nueva parametrización $s \mapsto (\tilde{x}(s), \tilde{y}(s))$ es estrictamente de grado 1.

Técnicamente, el generador $h(t)$ se puede calcular directamente gracias a la estructura de la prueba de Lüroth (específicamente usando el polinomio $F(t, X)$ de la prueba del teorema 2.3), mediante el cálculo del máximo común divisor en el anillo bivariado.

Proposición 3.2 — Cálculo de la Reparametrización. *Sean $x(t) = \frac{p_1(t)}{q_1(t)}$ y $y(t) = \frac{p_2(t)}{q_2(t)}$. Consideremos los polinomios en $k(t)[Z]$:*

$$N_1(t, Z) = p_1(Z)q_1(t) - p_1(t)q_1(Z)$$

$$N_2(t, Z) = p_2(Z)q_2(t) - p_2(t)q_2(Z)$$

El polinomio mínimo de t sobre el campo $K = k(x(t), y(t))$ es un divisor del $\gcd(N_1, N_2)$ evaluado en el campo racional. Los coeficientes de este máximo común divisor (que no sean constantes en k) son generadores de Lüroth $h(t)$.

■ **Ejemplo 3.2** Consideremos

$$x(t) = \frac{1 - t^4}{1 + t^4}, \quad y(t) = \frac{2t^2}{1 + t^4}$$

Factorizamos. Para $x(t)$:

$$N_1(t, Z) = p_1(Z)q_1(t) - p_1(t)q_1(Z)$$

$$N_1(t, Z) = (1 - Z^4)(1 + t^4) - (1 - t^4)(1 + Z^4)$$

Expandiendo y simplificando:

$$N_1(t, Z) = (1 + t^4 - Z^4 - t^4Z^4) - (1 + Z^4 - t^4 - t^4Z^4)$$

$$N_1(t, Z) = 2t^4 - 2Z^4 = -2(Z^4 - t^4)$$

Podemos factorizar esta diferencia de cuadrados en la variable Z:

$$N_1(t, Z) = -2(Z^2 - t^2)(Z^2 + t^2)$$

Para $y(t)$:

$$N_2(t, Z) = p_2(Z)q_2(t) - p_2(t)q_2(Z)$$

$$N_2(t, Z) = (2Z^2)(1 + t^4) - (2t^2)(1 + Z^4)$$

Expandiendo:

$$N_2(t, Z) = 2Z^2 + 2Z^2t^4 - 2t^2 - 2t^2Z^4$$

Agrupamos inteligentemente para factorizar:

$$N_2(t, Z) = 2(Z^2 - t^2) + 2t^2Z^2(t^2 - Z^2)$$

$$N_2(t, Z) = 2(Z^2 - t^2) - 2t^2Z^2(Z^2 - t^2)$$

$$N_2(t, Z) = 2(Z^2 - t^2)(1 - t^2Z^2)$$

Ahora debemos calcular el máximo común divisor de N_1 y N_2 en el anillo de polinomios $k(t)[Z]$. Observando nuestras factorizaciones:

1. $N_1(t, Z) = -2 \cdot (Z^2 - t^2) \cdot (Z^2 + t^2)$

2. $N_2(t, Z) = 2 \cdot (Z^2 - t^2) \cdot (1 - t^2 Z^2)$

Es evidente que el factor común de mayor grado respecto a Z es $Z^2 - t^2$. (El factor $Z^2 + t^2$ no divide a $1 - t^2 Z^2$).

Por lo tanto, el $\gcd(N_1, N_2)$ mónico es:

$$G(t, Z) = Z^2 - t^2$$

La proposición establece que los coeficientes de este polinomio gcd respecto a la variable Z que no sean constantes en el campo base k nos darán el generador de Lüroth $h(t)$.Escribiendo $G(t, Z)$ explícitamente como polinomio en Z:

$$G(t, Z) = 1 \cdot Z^2 + 0 \cdot Z + (-t^2) \cdot Z^0$$

El coeficiente independiente es $-t^2$. Por lo tanto, salvo constantes multiplicativas o aditivas, nuestro parámetro de Lüroth, que genera la subextensión exacta del campo de funciones, es:

$$s = h(t) = t^2$$

■

■ **Ejemplo 3.3 — Curva de Ocho de Gerono.** La curva de Ocho de Gerono se define como:

$$x(\theta) = -\cos(2\theta)$$

$$y(\theta) = -\sin(2\theta)\cos(2\theta)$$

Aplicamos el cambio racional $t = \tan\left(\frac{\theta}{2}\right)$, obtenemos:

$$x(s) = \frac{-s^4 + 6s^2 - 1}{s^4 + 2s^2 + 1}, \quad y(s) = -\left(\frac{4s - 4s^3}{s^4 + 2s^2 + 1}\right)\left(\frac{s^4 - 6s^2 + 1}{s^4 + 2s^2 + 1}\right) = \frac{4s^7 - 28s^5 + 28s^3 - 4s}{(s^2 + 1)^4}$$

Aplicando la proposición 3.2 tebemos

$$N_1(s, Z) = -8(Z^2 - s^2)(s^2 Z^2 - 1) = -8(Z - s)(Z + s)(sZ - 1)(sZ + 1)$$

Para $N_2(s, Z)$, en lugar de expandir polinomios de grado 8, usamos la teoría de raíces. Sabemos que el $\gcd(N_1, N_2)$ está formado por aquellas raíces Z de N_1 que también cumplen $y(Z) = y(s)$. Evaluamos las cuatro raíces de N_1:

1. $Z = s \implies y(s) = y(s)$ (Raíz válida).
2. $Z = -s \implies y(-s) = -y(s) \neq y(s)$ (Descartada, pues el numerador de $y(s)$ es impar).
3. $Z = 1/s \implies y(1/s) = -y(s) \neq y(s)$ (Descartada tras evaluar).
4. $Z = -1/s \implies y(-1/s) = -y(1/s) = -(-y(s)) = y(s)$ (Raíz válida).

Por lo tanto, las únicas raíces comunes son $Z = s$ y $Z = -1/s$. El máximo común divisor es el polinomio que las contiene:

$$G(s, Z) = (Z - s)\left(Z + \frac{1}{s}\right) = Z^2 + \left(\frac{1 - s^2}{s}\right) Z - 1$$

Tomamos este coeficiente (y para mayor familiaridad estética, lo invertimos y multiplicamos

por 2, lo cual es válido pues genera el mismo subcampo):

$$u = \frac{2s}{1-s^2}$$

Hacemos la sustitución $(x(s), y(s))$:

$$x(u) = \frac{u^2-1}{u^2+1}, \quad y(u) = \frac{2u(u^2-1)}{(u^2+1)^2}$$

Esta parametrización en la variable u tiene grado topológico 1. Traza la Curva en Ocho de Gerono una única vez.

Ahora que contamos con una parametrización propia, podemos deducir la ecuación implícita de la curva mediante la eliminación del parámetro. Queremos encontrar el ideal de la curva $I_C = \ker(\phi) \subset k[x, y]$.

Por la proposición 3.2, consideramos el ideal J en el anillo polinomial grande $k[u, x, y, w]$ definido por las ecuaciones de los numeradores y la inversión de los denominadores:

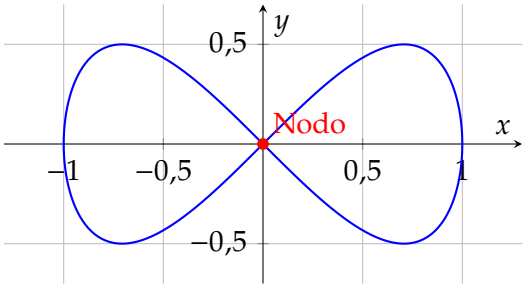
$$J = \left\langle (u^2+1)x - (u^2-1),\ (u^2+1)^2 y - 2u(u^2-1),\ 1 - w(u^2+1)^3 \right\rangle$$

Entonces, el ideal de la curva C se recupera mediante eliminación clásica: $I_C = J \cap k[x, y]$. Si calculamos la base de Gröbner para este ideal con un orden lexicográfico tal que $w > u > x > y$, las variables auxiliares desaparecen. Obtenemos la ecuación implícita original de la Lemniscata de Gerono:

$$I_C = \langle x^4 - x^2 + y^2 \rangle$$

■

Curva de Ocho de Gerono: $x^4 - x^2 + y^2 = 0$



La siguiente gran implicación es puramente de geometría birracional y se conecta directamente con la teoría de curvas algebraicas proyectivas suaves. El Teorema de Lüroth es algebraicamente equivalente al siguiente enunciado geométrico:

> **Teorema 3.3** *Si una curva algebraica C admite un morfismo racional dominante desde $\mathbb{P}^1$, entonces C es birracional a $\mathbb{P}^1$.*

Esto parece intuitivo en dimensión 1, pero la justificación técnica profunda proviene de la fórmula de Riemann-Hurwitz, donde la extensión de campos de Lüroth se revela como un corsé topológico.

A. Algunos lemas técnicos.

Lema A.1 *Sea R un anillo conmutativo con identidad y sea $\{S_i\}_{i\in I}$ una familia dirigida de subconjuntos multiplicativos de R. (Es decir, I es un conjunto parcialmente ordenado y para todo $i, j \in I$, existe $k \in I$ tal que $S_i \subseteq S_k$ y $S_j \subseteq S_k$).Sea $S = \bigcup_{i\in I} S_i$ el supremo de esta familia de subconjuntos multiplicativos.Entonces, existe un isomorfismo canónico de R-álgebras:*

$$\varinjlim_{i\in I} S_i^{-1}R \cong S^{-1}R$$

Lema A.2 — Lema de Gauss. *Sea R un dominio de factorización única y K su campo de fracciones. Sea $f(X) \in R[X]$ un polinomio no constante. Entonces, $f(X)$ es irreducible en $R[X]$ si y solo si es irreducible en $K[X]$ y es un polinomio primitivo.*

Lema A.3 — Lema de Gauss versión 2. *Si un polinomio primitivo $f(X) \in R[X]$ se puede factorizar en $K[X]$ como el producto de dos polinomios no constantes $f(X) = G(X)H(X)$ con $G, H \in K[X]$, entonces existen polinomios $g(X), h(X) \in R[X]$ tales que $f(X) = g(X)h(X)$, donde g y h son múltiplos escalares (por elementos de K) de G y H respectivamente.*