



Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Ricardo Menares
Curso: Teoría de Números
Fecha: 7 de noviembre de 2025

Ayudante: José Cuevas Barrientos
Sigla: MAT2814

Curvas y cónicas

1. EJERCICIOS

A lo largo de esta ayudantía, k denotará un cuerpo.

1. Encuentre los «puntos al infinito» de las siguientes curvas afines:
 - a) $3x - 7y + 5 = 0$.
 - b) $x^2 + xy - 2y^2 + x - 5y + 7 = 0$.
 - c) $x^3 + x^2y - 3xy^2 - 3y^3 + 2x^2 - 2y + 5 = 0$.
2. Para las siguientes curvas encuentre la tangente al punto P (o, de no existir, declare si P es singular):
 - a) $y^2 = x^3 - x$ en $P = (1, 0)$.
 - b) $X^2 + Y^2 = Z^2$ en $P = [3 : 4 : 5]$.
 - c) $x^2 + y^4 + 2xy + 2x + 2y + 1$ en $P = (-1, 0)$.
3. Sea C' la cónica proyectiva dada por la ecuación:

$$aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0. \quad (1)$$

- a) Pruebe que C' es suave si el determinante

$$\delta := \det \begin{bmatrix} 2a & b & d \\ b & 2c & e \\ d & e & 2f \end{bmatrix}.$$

es no nulo.

- b) Pruebe que si C' es suave y tiene un punto (racional) $[x_0 : y_0 : z_0] \in C(k)$, entonces $C' \cong \mathbb{P}^1(k)$.
•• PISTA: Hay una biyección entre $\mathbb{P}^1(k) = k \cup \{\infty\}$ y las pendientes de rectas racionales. □
4. Describa *todos* los puntos \mathbb{Q} -racionales de $x^2 + y^2 = 2$ parándose en $(1, 1)$.
 5. Definamos el círculo afín $C(k) := \{(x, y) \in k : x^2 + y^2 = 1\}$. Para dos puntos en $C(k)$ definamos

$$(x_1, y_1) \boxplus (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1).$$

Pruebe que $(C(k), \boxplus)$ determina un grupo abeliano.

6. a) Pruebe que si $\text{car } k \neq 2$ y existe $\sqrt{-1} \in k$, entonces $(C(k), \boxplus) \cong (k^\times, \cdot)$.
b) Pruebe que $C(\mathbb{Q})_{\text{tors}} = \{(\pm 1, 0), (0, \pm 1)\}$.

PISTA: Hay una contención que es clara. Para la recíproca, sería útil poder calcular la torsión mediante el inciso anterior, por lo cual conviene preguntarse qué es k_{tors}^\times . □

A. COHOMOLOGÍA DE GALOIS Y COMENTARIOS ADICIONALES

El ejercicio 6 puede mejorarse así:

7. Sea L/K una extensión cíclica (i.e., una extensión de Galois finita cuyo grupo es cíclico).
 - a) Sea $\sigma \in \text{Gal}(L/K)$ un generador, pruebe que la sucesión

$$1 \longrightarrow K^\times \hookrightarrow L^\times \xrightarrow{1-\sigma} L^\times \xrightarrow{\text{Nm}_{L/K}} K^\times$$

es exacta (aquí « $1 - \sigma$ » denota el homomorfismo $\beta \mapsto \beta/\sigma(\beta)$).

- b) Pruebe que $\ker \text{Nm}_{L/K} \cong L^\times / K^\times$.

8. Sea K un cuerpo de $\text{car } K \neq 2$ y suponga que el polinomio $x^2 + 1$ es irreducible en K . Pruebe que $(C(K), \boxplus) \cong (K(\sqrt{-1})^\times / K^\times, \cdot)$.

Estructuras como el círculo $C(K)$ que son variedades algebraicas con una estructura de grupo definida por ecuaciones algebraicas, se llaman *grupos algebraicos*, y son de suma importancia en general. Otros ejemplos de grupos algebraicos son el grupo multiplicativo (K^\times, \cdot) y las curvas elípticas.

REFERENCIAS

1. SILVERMAN, J. H. y TATE, J. *Rational points on elliptic curves* doi:[10 . 1007 / 978 - 1 - 4757 - 4252 - 7](https://doi.org/10.1007/978-1-4757-4252-7) (Springer-Verlag, New York, 1992).

Correo electrónico: josecuezasbtos@uc.cl