Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Héctor Pastén
Ayudante: José Cuevas Barrientos
Curso: Teoría de Números
Sigla: MAT2225
Fecha: 3 de noviembre de 2023

Ecuaciones en el espacio proyectivo

1. El espacio proyectivo

Definición 1.1: Sea k un cuerpo, y sea $n \in \mathbb{N}$ un natural fijado. En el espacio vectorial k^{n+1} removemos el origen $\vec{0}$, y aquí denotamos que dos vectores $\boldsymbol{u}, \boldsymbol{v}$ son linealmente equivalentes $\boldsymbol{u} \sim \boldsymbol{v}$ si existe $\lambda \in k^\times$ tal que $\boldsymbol{u} = \lambda \boldsymbol{v}$. El ***espacio proyectivo*** $\mathbb{P}^n(k)$ se define como las clases de equivalencia $(k^{n+1} \setminus \{\vec{0}\})/\sim$. Los elementos de $\mathbb{P}^n(k)$ se denotan $[a_0 : a_1 : \cdots : a_n]$, donde los $a_i \in k$ son no todos nulos.

Dado un polinomio $f(x_1, \ldots, x_n) \in k[\boldsymbol{x}]$, el conjunto de sus soluciones usuales se denota

$$\mathbf{V}(f) := \{(a_1, \ldots, a_n) \in k^n : f(\boldsymbol{a}) = 0\} \subseteq \mathbb{A}^n(k).$$

El grado (total) de un monomio $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ es $\alpha_1 + \alpha_2 + \cdots + \alpha_n$. Un polinomio $f(\boldsymbol{x}) \in k[\boldsymbol{x}]$ se dice ***homogéneo*** si todos sus monomios tienen el mismo grado total. Si $f(x_0, \ldots, x_n) \in k[\boldsymbol{x}]$ es un polinomio homogéneo, entonces las soluciones proyectivas de $f(\boldsymbol{x}) = 0$ se denota $\mathbf{V}_+(f)$ y es un subconjunto de $\mathbb{P}^n(k)$.

Nótese que todo polinomio homogéneo posee una solución ***trivial*** dada por $(0, 0, \ldots, 0)$; esta nunca es una solución proyectiva.

Ejemplo: Considere $k = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$. El polinomio $f(x, y) = x + 2y$ es homogéneo de grado 1, y las soluciones afines de $x + 2y = 0$ son

$$\mathbf{V}(x + 2y) = \{(0, 0), \quad (2, 4), \quad (4, 3), \quad (1, 2), \quad (3, 1)\} \subseteq \mathbb{A}^2(k).$$

Si ahora miramos el conjunto $\mathbf{V}_+(f) \subseteq \mathbb{P}^1(k)$, entonces el punto $(0, 0)$ no aparece y notamos que, por ejemplo $[2 : 4] = 4 \cdot [3 : 1] = [12 : 4]$, y así, en realidad, $\mathbf{V}_+(f) = \{[1 : 2]\} \subseteq \mathbb{P}^1(k)$ corresponde a un solo punto.

1. *a*) Demuestre que un polinomio irreducible en una variable $f(x) \in k[x]$ posee a lo más una solución.
   b) Sea $f(x, y) \in k[x, y]$ un polinomio homogéneo irreducible no nulo. Demuestre que a menos que $f(x, y) = ax$ o $f(x, y) = ay$ para algún $a \in k^\times$, entonces $[0 : 1]$ y $[1 : 0]$ no son soluciones de $f(x, y)$.
   c) Con lo anterior, concluya que $\mathbf{V}_+(f)$ es o bien vacío, o bien consiste de un solo punto.

Definición 1.2: Considere un polinomio $f(x_0, \ldots, x_{n-1}) \in k[\boldsymbol{x}]$ en n variables. Su ***homogenización*** (respecto a z) es el polinomio en $n + 1$ variables:

$$g(\boldsymbol{x}, z) := z^{\deg f} \cdot f\left(\frac{x_0}{z}, \ldots, \frac{x_{n-1}}{z}\right).$$

Si, por el contrario, tenemos un polinomio homogéneo $h(\boldsymbol{x}, z) \in k[\boldsymbol{x}, z]$ en $n+1$ variables, el polinomio $h(\boldsymbol{x}, 1)$ se dice su ***deshomogenización*** (respecto a z).

Por ejemplo, dado el polinomio $f(x, y) = x^3 - 3xy + 6y$, su homogenización es $x^3 - 3xyz + 6z^2$.

2. (Prueba de sanidad)
   a) Verifique que la homogenización de un polinomio efectivamente es un polinomio homogéneo.

b) Sea $f(\boldsymbol{x}) \in k[\boldsymbol{x}]$ un polinomio y sea $g(\boldsymbol{x}, y)$ su homogenización. Verifique que hay una inclusión canónica de $\mathbf{V}(f)$ las soluciones afines de f en $\mathbf{V}_+(g)$ las soluciones proyectivas de g dada por

$$(a_1, a_2, \ldots, a_n) \longmapsto [a_1 : a_2 : \cdots : a_n : 1].$$

Este proceso se le llama ***clausura proyectiva***. Los puntos que están en $\mathbf{V}_+(g) \setminus \mathbf{V}(f)$ le llamaremos el ***resto de la homogenización***.[1]

c) Considere la ecuación de Weierstrass

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x + a_6.$$

Verifique que hay solo un punto en el resto de su homogenización.

d) Sea $f(\boldsymbol{x}) \in k[\boldsymbol{x}]$ un polinomio. Demuestre que si lo homogenizamos (añadiendo z) y luego lo deshomogenizamos (respecto a z), entonces volvemos al mismo f.
No obstante, dé un ejemplo de un polinomio homogéneo $h(\boldsymbol{x}, z) \in k[\boldsymbol{x}, z]$ tal que si lo deshomogenizamos (respecto a z) y luego lo homogenizamos (respecto a z), no volvemos al mismo h original.

3. Considere un polinomio $f(x, y) \in k[x, y]$ no constante, y su conjunto de soluciones $\mathbf{V}(f) \subseteq \mathbb{A}^2(k)$ que, intuitivamente representa un conjunto de curvas. Demuestre que, si k es algebraicamente cerrado (e.g., $k = \mathbb{C}$), el resto de la homogenización no es ni vacío, ni infinito. Demuestre, no obstante, que puede tener cualquier cardinalidad.

2. Ejemplos relacionados al Último Teorema de Fermat

Los siguientes dos ejemplos están sacados del primer capítulo de Edwards [**1,** págs. 6-10].

4. Sea (a, b, c) una terna pitagórica (i.e., $a^2 + b^2 = c^2$). Demuestre que existen $d, u, v \in \mathbb{Z}$ con u, v coprimos tales que

$$a = d(u^2 - v^2), \quad b = 2duv, \quad c = d(u^2 + v^2).$$

Pista: Nótese que el d es el máximo común divisor de a, b, c en conjunto, así que redúzcase al caso en que a, b, c son coprimos. Así, pruebe que exactamente uno de ellos es par y, además, que c no puede serlo. Prosiga por un argumento del tipo «producto de dos coprimos es un cuadrado syss ambos factores son cuadrados»; para ello deberá cancelar un factor común de dos inducido por la paridad de uno de los términos. □

5. Demuestre que la ecuación diofántica $x^4 - y^4 = z^2$ no posee soluciones no triviales, y por tanto, que el Último Teorema de Fermat se satisface para el exponente 4.

Pista: El argumento es por «descenso infinito», es decir, construya maneras en las que emplear la pregunta anterior para ir refinando los números involucrados y llegue a una contradicción de tamaños. □

El caso de exponente $n = 4$ es una de las pocas demostraciones que Fermat sí dio a una de sus afirmaciones; si bien Fermat jamás fue un publicador metódico, por sus argumentos podemos reconocer que no era «charlatán» sino que tenía la intuición apropiada en varios casos. La abundancia de conjeturas por parte de Fermat se debe a una injusticia de nosotros como matemáticos: estas estaban principalmente en apuntes o cartas privadas de Fermat, y ciertamente él no buscaba fama de ningun tipo al querer desafiar a matemáticos con sus cuestiones.

Los casos $n = 3$ y $n = 5$ son bastante más laboriosos, pero se pueden lograr trabajando en una extensión de $\mathbb{Z}$ apropiada. Para $n = 3$ necesitamos jugar con los *enteros de Eisenstein* dados por $\mathbb{Z}[\zeta_3]$, donde ζ_3 es una raíz cúbica primitiva de la unidad, vale decir, es raíz de $x^2 + x + 1$ (cfr. [**1,** págs. 40-42, 52-54]) y para $n = 5$ trabajamos con $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ (cfr. [**1,** págs. 65-73]).

[1] ¡Ésta es terminología no estándar!

3. Dos problemas bonus

6. **Teorema de Chevalley-Warning:** Considere $k = \mathbb{F}_p$ y sea $f(x_0, \ldots, x_n) \in k[\boldsymbol{x}]$ un polinomio homogéneo de grado d. Si $d < n + 1$, entonces $\mathbf{V}_+(f)$ no es vacío (es decir, $f(\boldsymbol{x})$ posee una solución no trivial).

   Se dice que un cuerpo es C_1 si satisface las condiciones anteriores. Uno puede demostrar en un cuerpo C_1 que toda cónica no degenerada (i.e., todo conjunto de soluciones afín $\mathbf{V}_+(f) \subseteq \mathbb{P}^2(k)$, donde f es homogéneo, irreducible y de grado 2) es isomorfa a $\mathbb{P}^1(k)$. Esto puede fallar en general, por ejemplo, basta tomar la cónica

$$\{[x : y : z] : x^2 + y^2 + z^2 = 0\} \subseteq \mathbb{P}^2(\mathbb{R})$$

   y notar que no tiene puntos $\mathbb{R}$-racionales para concluir que no puede ser isomorfa a $\mathbb{P}^1(\mathbb{R})$.

7. **Contar puntos de altura acotada en $\mathbb{P}^1(\mathbb{Q})$:** Dado $B \geq 0$ real, demuestre que la cantidad de puntos $[x : y] \in \mathbb{P}^1(\mathbb{Q})$ de altura acotada $H([x : y]) \leq B$ es

$$\frac{6}{\pi^2} B^2 + O(B \log B).$$

   Pista: Uno puede observar que esto equivale a contar pares de coprimos y, mediante una fórmula recursiva, reducirse a calcular asintóticamente

$$\sum_{i=1}^{n} \phi(n),$$

   donde ésto representa la función ϕ de Euler. Empleando inversión de Möbius podemos reescribirlo en términos de la función μ de Möbius y, finalmente, reconocer este problema de la ayudantía «O grande, o chica» del 25 de agosto. □

4. Comentarios adicionales

¿Por qué interesarse en el espacio proyectivo? Digamos que elegimos $k = \mathbb{R}$, entonces el lector podría considerar que es mucho más natural tomar ecuaciones en $\mathbb{R}^n$; pero éste último, no es un espacio compacto, lo que produce problemas. En topología, éste problema «se resuelve» añadiéndole un punto a $\mathbb{R}^n$ y así cerrando el espacio en una esfera $\mathbb{S}^n$.

Algebraicamente, esta operación no es siempre la más óptima, pero el lector debería pensar que el espacio proyectivo representa el análogo del proceso anterior, y surge naturalmente en la tarea de «compactificar a k^n». Una vez obtenido este objeto, las ventajas de «ser compacto» salen rápidamente a relucir: quizá una de las más famosas es el *teorema de Bézout* que dice que la cantidad de intersecciones de curvas en el plano proyectivo es la apropiada (véase Wikipedia, por ejemplo, para un enunciado más preciso). Este resultado es el comienzo de la *geometría enumerativa*, una disciplina que difícilmente puede decir algo acerca de «objetos no compactos».

Geometría algebraica y teoría de números. Las conexiones entre geometría algebraica y teoría de números son bastante ricas, aquí vamos a esbozar el por qué un teorista de números podría interesarse en ésta disciplina.

- *Curvas elípticas:* Su definición es meramente geométrica. Varias de las propiedades básicas de las curvas elípticas, originalmente descubiertas y estudiadas sobre $\mathbb{C}$, se extienden a lo que se conoce como *variedades abelianas* y el enfoque más moderno permite extender los teoremas sobre $\mathbb{C}$ hacia otros cuerpos de coeficientes como $\mathbb{F}_p$.
- *Teorema(s) de Faltings:* Al estudiar aproximaciones diofánticas de Thue-Roth vimos cómo se traducen en la finitud de soluciones (racionales) de polinomios irreducibles en dos variables de grado ≥ 3. La geometría algebraica permite una generalización de tal polinomio a lo que se conoce como «una curva de género ≥ 2» y era una conjetura de Mordell el que, al igual que en el caso anterior, tal curva debería tener finitos puntos (racionales).

Esta conjetura fue probada por Gerd Faltings, pero en el camino Faltings también probó otro enunciado con gran contenido aritmético: que toda variedad abeliana sobre $\mathbb{Q}$ satisface la conjetura de Tate. No obstante, enunciar apropiadamente éste teorema (y explicar sus repercusiones aritméticas) es algo que escapa a los contenidos del curso.

- *Alturas:* Aquí estamos tecnicamente haciendo trampa, ya que también fue parte de las investigaciones de Faltings. El mundo de las alturas (que vosotros ya conoceís sobre $\mathbb{Q}$) permite una extensión natural a las variedades sobre $\mathbb{Q}$, y por tanto permiten hacerse preguntas del tipo: ¿los teoremas de aproximación son ciertos sobre variedades? O cualquier enunciado sobre alturas en $\mathbb{Q}$ admite su análogo para alturas en variedades; varias veces demostrándose de igual manera su validez.

  El ejemplo del problema 7 de contar puntos de altura acotada es del libro Lang **[5,** págs. 71-75**]**, y es un caso particular del *teorema de Schanuel*.
- *El Último Teorema de Fermat:* Es archiconocido el que ésta conjetura fue resuelta por Wiles (¡y muchas otras personas!) en 1994, y que sus métodos fueron una mezcla de ténicas aritmético-geométricas. No obstante, la geometría no otorga solo el lenguaje para una reformulación del Último Teorema de Fermat, sino que es un protagonista en la prueba; por ejemplificar, conceptos como cohomología de Galois, teoría de deformaciones e intersección completa son parte escencial de la demostración.

¿Acercamientos a la geometría? Mi personal recomendación es comenzar por los libros de Smith *et al.* **[7]** y Kempf **[3].** Otra acotación es que, si no se siente atado a trabajar en total generalidad, entonces le adelantamos que la geometría algebraica *compleja* está bastante desarrollada y es, en varios aspectos, más accesible que la geometría general; para ello recomendamos comenzar con cualquier libro de análisis complejo (e.g., Lang **[6]** o Kodaira **[4]**) y luego ir aventurándose a los aspectos más específicamente geométricos.

La geometría algebraica ha pasado por varias transformaciones y, en realidad, en un punto ya no habla de conjuntos de soluciones en espacios proyectivos; aquí necesitamos introducir la palabra *esquema* que es el bloque fundamental de la geometría algebraica después de los 60's (y es precisamente el lenguaje que emplea Hartshorne **[2]** desde el capítulo 2 en adelante). Un esquema es como un conjunto de soluciones, pero que posiblemente sobre un anillo y que tiene «decodificado sus ecuaciones de definición»; esto da la ventaja de admitir una operación fundamental llamada *cambio de base*. Un ejemplo comparable es tomar una ecuación con coeficientes en $\mathbb{Z}$, esto determina un esquema, pero también podemos ver sus soluciones en $\mathbb{Q}$ y, también sus soluciones módulo p (o en $\mathbb{F}_p$); estos son todos ejemplos de cambio de base.

Referencias y lecturas adicionales

1. Edwards, H. M. *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory. Graduate Texts in Mathematics* **50** (Springer-Verlag, 1977).
2. Hartshorne, R. *Algebraic Geometry. Graduate Texts in Mathematics* **52** (Springer-Verlag New York, 1977).
3. Kempf, G. R. *Algebraic Varieties.* (Cambridge University Press, 1993).
4. Kodaira, K. *Complex Analysis. Cambridge Studies in Advanced Mathematics* **107** (Cambridge University Press, 2007).
5. Lang, S. *Fundamentals of Diophantine Geometry.* (Springer-Verlag, 1983).
6. Lang, S. *Complex Analysis.* (Springer-Verlag, 1999).
7. Smith, K. E., Kahanpää, L., Kekäläinen, P. y Traves, W. *An Invitation to Algebraic Geometry.* (Springer-Verlag New York, 2000).

Correo electrónico: josecuevasbtos@uc.cl