El diablo de los números

Sección a cargo de

Javier Fresán

La aritmética de las ecuaciones con muchas variables

por

Diego Izquierdo

Consideremos un entero $n \geq 0$ y un polinomio $f(X_0, \ldots, X_n) \in \mathbb{Z}[X_0, \ldots, X_n]$ con coeficientes enteros. ¿Es posible determinar si la ecuación $f(x_0, \ldots, x_n) = 0$ tiene soluciones enteras? Si esta pregunta remonta a la Antigüedad (más precisamente a Diofanto de Alejandría) y destaca por su sencillez, hemos tenido que esperar hasta los años 60 para tener una respuesta convincente. Es en aquel entonces cuando Davis, Putnam, Robinson y Matijasevic demuestran que la pregunta es indecidible. Dicho de otra manera, no existe ningún algoritmo que permita determinar de forma general si nuestra ecuación $f(x_0, \ldots, x_n) = 0$ tiene soluciones enteras.

Sorprendentemente, el problema se vuelve aún más complicado cuando se sustituyen los números enteros por los números racionales. Incluso a día de hoy, seguimos sin saber si existe o no un algoritmo que permita decidir si la ecuación $f(x_0, \ldots, x_n) = 0$ tiene soluciones racionales. Por supuesto, se puede generalizar el problema a un cuerpo K cualquiera en lugar del de los números racionales, y entonces la dificultad dependerá de las propiedades aritméticas de K.

Intuitivamente, es natural pensar que, cuantas más variables tenga el polinomio f y cuanto menor sea su grado, más posibilidades hay de que la ecuación $f = 0$ tenga soluciones en el cuerpo K. El objetivo de este artículo es presentar algunos resultados importantes así como algunas preguntas abiertas interesantes en esta dirección. Se trata de una rama de la teoría de números que ha sido muy fructífera en las últimas décadas, que ha permitido mezclar técnicas variadas, ya sean algebraicas, analíticas o geométricas, y que sigue siendo muy activa.

1. Cuerpos C_i. Definición y primeros ejemplos

Como acabamos de explicar, queremos formalizar la idea intuitiva de que, dado un cuerpo K, las ecuaciones polinomiales con muchas variables y con grado pequeño sobre el cuerpo K tienen tendencia a tener soluciones. El punto de partida es la definición siguiente, que remonta a Artin y Lang [24]:

Definición 1.1. Sean K un cuerpo e i un entero no negativo. Decimos que K tiene *la propiedad* C_i si para todo $n > 0$, para todo $d > 0$ y para todo polinomio homogéneo $f \in K[X_0, \ldots, X_n]$ de grado d tales que $d^i \leq n$, la ecuación $f(\mathbf{x}) = 0$ tiene una solución no nula $\mathbf{x} \in K^{n+1} \setminus \{(0, \ldots, 0)\}$.

A modo de ejemplo, demostremos que los cuerpos que tienen la propiedad C_0 son exactamente los cuerpos algebraicamente cerrados. Para verlo, observemos que, a cada polinomio $g \in K[X]$ de grado $d > 0$ sobre un cuerpo K, se puede asociar el polinomio homogéneo $f(X_0, X_1) = X_0^d g(X_1/X_0)$. En particular, si K tiene la propiedad C_0, la ecuación $f = 0$ tiene al menos una solución no nula (x_0, x_1) en el cuerpo K. El cociente x_1/x_0 (en el que x_0 no es nulo porque, si no, x_1 también lo sería) es entonces una raíz de g en K, lo que demuestra que K es algebraicamente cerrado. La recíproca es prácticamente evidente y la dejamos como ejercicio.

Si los cuerpos con la propiedad C_0 son, en cierto modo, los cuerpos que tienen las propiedades aritméticas más sencillas, los cuerpos C_i con $i \geq 1$ son aritméticamente más interesantes y más complicados de estudiar. En las secciones siguientes, vamos a dar algunos ejemplos importantes.

Pero antes, observemos que existen también cuerpos que no tienen la propiedad C_i para ningún i. Es el caso, por ejemplo, del cuerpo de los números reales, puesto que la ecuación $x_0^2 + \cdots + x_n^2 = 0$ no tiene soluciones reales no nulas para ningún $n \geq 0$. Por supuesto, los subcuerpos de $\mathbb{R}$ (como el cuerpo de los números racionales) tampoco tienen la propiedad C_i para ningún i.

1.1. Cuerpos finitos

Consideremos un cuerpo finito $\mathbb{F}$ con q elementos e intentemos ver si $\mathbb{F}$ tiene la propiedad C_i para algún $i \geq 1$. Para hacernos una idea, miremos un caso particularmente sencillo: supongamos que $\mathbb{F}$ no es de característica 2 e intentemos encontrar un entero n, de preferencia pequeño, tal que la ecuación $f = 0$ tenga automáticamente soluciones no nulas para cualquier polinomio homogéneo $f \in \mathbb{F}[X_0, \ldots, X_n]$ de grado 2.

Dado que f es de grado 2, podemos identificar f con una forma cuadrática sobre el $\mathbb{F}$-espacio vectorial $\mathbb{F}^{n+1}$. Dicha forma cuadrática se diagonaliza en alguna base de $\mathbb{F}^{n+1}$, y, por tanto, podemos encontrar un automorfismo φ de $\mathbb{F}^{n+1}$ y elementos $a_0, \ldots, a_n \in \mathbb{F}$ tales que

$$f(\varphi(X_0, \ldots, X_n)) = a_0 X_0^2 + \cdots + a_n X_n^2.$$

Conviene entonces distinguir dos casos:

(i) Si $a_{i_0} = 0$ para algún $i_0 \in \{0, \ldots, n\}$, entonces la n-upla $(0, \ldots, 0, 1, 0, \ldots, 0)$ donde el 1 está en la i_0-ésima posición es solución de $f(\varphi(x_0, \ldots, x_n)) = 0$ y, por tanto, $\varphi(0, \ldots, 0, 1, 0, \ldots, 0)$ es una solución no nula de la ecuación $f = 0$.

(ii) Supongamos ahora que $a_i \neq 0$ para todo i. Como $\mathbb{F}$ no es de característica 2, es sencillo comprobar que exactamente la mitad de los elementos de $\mathbb{F}^\times := \mathbb{F} \setminus \{0\}$ son cuadrados, lo cual contando el 0 hace un total de

$$\#\{x^2 \mid x \in \mathbb{F}\} = \frac{q+1}{2}$$

cuadrados en $\mathbb{F}$. Por tanto,

$$\#\{a_0x_0^2 \mid x_0 \in \mathbb{F}\} = \#\{-a_1x_1^2 - a_2 \mid x_1 \in \mathbb{F}\} = \frac{q+1}{2},$$

de modo que

$$\#\{a_0x_0^2 \mid x_0 \in \mathbb{F}\} + \#\{-a_1x_1^2 - a_2 \mid x_1 \in \mathbb{F}\} = q + 1 > \#\mathbb{F}.$$

Deducimos que los conjuntos $\{a_0x_0^2 \mid x_0 \in \mathbb{F}\}$ y $\{-a_1x_1^2 - a_2 \mid x_1 \in \mathbb{F}\}$ se intersecan, lo que demuestra que existen x_0 y x_1 en $\mathbb{F}$ tales que $a_0x_0^2 = -a_1x_1^2 - a_2$, o, lo que es lo mismo,

$$f(x_0, x_1, 1, 0, \ldots, 0) = 0.$$

Por supuesto, este último argumento solo funciona si f tiene grado 2 y $n \geq 2$, lo que sugiere que el cuerpo $\mathbb{F}$ tiene la propiedad C_1. Dicho resultado fue establecido por Chevalley y Warning en el año 1935:

Teorema 1.2 (Chevalley [10], Warning [30]). *Los cuerpos finitos tienen la propiedad C_1.*

La demostración es elemental, así que vamos a explicarla brevemente aquí. Démonos un cuerpo finito $\mathbb{F}$ con q elementos, dos enteros positivos n y d tales que $n \geq d$, y un polinomio homogéneo $f \in \mathbb{F}[X_0, \ldots, X_n]$ de grado d. Sea s el número de soluciones de la ecuación $f = 0$ en el cuerpo $\mathbb{F}$. Como el grupo $\mathbb{F}^\times$ tiene orden $q-1$, el teorema de Lagrange nos dice que, dado $\mathbf{x} \in \mathbb{F}^{n+1}$, se tiene la igualdad

$$f(\mathbf{x})^{q-1} = \begin{cases} 0 & \text{si } f(\mathbf{x}) = 0, \\ 1 & \text{si no.} \end{cases}$$

Por tanto, si introducimos la función $g = 1 - f^{q-1}$, las igualdades

$$s = \sum_{\mathbf{x} \in \mathbb{F}^{n+1}} \left(1 - f(\mathbf{x})^{q-1}\right) = \sum_{\mathbf{x} \in \mathbb{F}^{n+1}} g(\mathbf{x}) \tag{1}$$

son ciertas en el cuerpo $\mathbb{F}$.

El resto de la demostración consiste en calcular esta suma. Como g es un polinomio de grado $\leq d(q-1)$, podemos escribir

$$g = \sum_{\substack{\mathbf{i}=(i_0,\ldots,i_n) \in \mathbb{Z}_{\geq 0}^{n+1} \\ i_0 + \cdots + i_n \leq d(q-1)}} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}},$$

con la convención $0^0 = 1$. Por tanto, sustituyendo en la ecuación (1), obtenemos

$$\begin{aligned} s &= \sum_{\mathbf{x} \in \mathbb{F}^{n+1}} \sum_{\substack{\mathbf{i}=(i_0,\ldots,i_n) \in \mathbb{Z}_{\geq 0}^{n+1} \\ i_0 + \cdots + i_n \leq d(q-1)}} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} = \sum_{\substack{\mathbf{i}=(i_0,\ldots,i_n) \in \mathbb{Z}_{\geq 0}^{n+1} \\ i_0 + \cdots + i_n \leq d(q-1)}} a_{\mathbf{i}} \left(\sum_{\mathbf{x} \in \mathbb{F}^{n+1}} \mathbf{x}^{\mathbf{i}} \right) \\ &= \sum_{\substack{\mathbf{i}=(i_0,\ldots,i_n) \in \mathbb{Z}_{\geq 0}^{n+1} \\ i_0 + \cdots + i_n \leq d(q-1)}} a_{\mathbf{i}} \left(\sum_{x \in \mathbb{F}} x^{i_0} \right) \cdots \left(\sum_{x \in \mathbb{F}} x^{i_n} \right). \end{aligned} \tag{2}$$

Para terminar el cálculo, usamos un sencillo lema sobre los cuerpos finitos:

Lema 1.3. *Dados un cuerpo finito $\mathbb{F}$ con q elementos y un entero $j \geq 0$, se tiene:*

$$\sum_{x \in \mathbb{F}} x^j = \begin{cases} -1 & \text{si } j \text{ es múltiplo de } q-1 \text{ y } j \neq 0, \\ 0 & \text{si no.} \end{cases}$$

En cada término de la suma (2) tenemos $i_0 + \cdots + i_n \leq d(q-1) < (n+1)(q-1)$, así que alguna de las coordenadas de $\mathbf{i}$ tiene que ser (estrictamente) inferior a $q-1$. Del lema que acabamos de enunciar se deduce que cada término de la suma (2) es nulo y, por tanto, que $s = 0$.

Llegado este punto, hay que tener un poco de cuidado: todas las igualdades que hemos escrito son igualdades en el cuerpo $\mathbb{F}$. En particular, la igualdad $s = 0$ es válida únicamente en $\mathbb{F}$ (y no en $\mathbb{Z}$), lo que significa que la característica p de $\mathbb{F}$ divide a s. Pero $(0, \ldots, 0)$ es siempre solución de la ecuación $f = 0$, por lo que $s \geq 1$. Se deduce que $s \geq p$, y, por tanto, la ecuación $f = 0$ tiene soluciones en el cuerpo $\mathbb{F}$ distintas de la solución trivial $(0, \ldots, 0)$. Es justamente lo que queríamos demostrar.

1.2. Cuerpos de fracciones racionales

En el párrafo anterior, hemos visto que los cuerpos finitos tienen la propiedad C_1. Es natural preguntarse si, a partir de un cuerpo K con alguna de las propiedades C_i, se pueden construir otros cuerpos que tengan también algunas de las propiedades C_i. Un resultado importante en esta dirección es el teorema de Tsen-Lang-Nagata:

Teorema 1.4 (Tsen-Lang-Nagata [26]). *Sean $i \geq 0$ un entero y K un cuerpo con la propiedad C_i. Entonces el cuerpo de fracciones racionales $K(T)$ en una variable y con coeficientes en K tiene la propiedad C_{i+1}.*

Por ejemplo, dado un entero $n \geq 1$, los cuerpos $\mathbb{C}(T_1, \ldots, T_n)$ y $\mathbb{F}(T_1, \ldots, T_{n-1})$, donde $\mathbb{F}$ es un cuerpo finito, tienen la propiedad C_n.

La demostración del teorema de Tsen-Lang-Nagata es elemental, pero bastante larga y técnica, así que vamos a explicar aquí únicamente el caso particularmente sencillo en el que $K = \mathbb{C}$. En otras palabras, como sabemos que $\mathbb{C}$ tiene la propiedad C_0, al ser un cuerpo algebraicamente cerrado, vamos a demostrar que el cuerpo de fracciones racionales $\mathbb{C}(T)$ tiene la propiedad C_1. Para ello, consideremos un polinomio homogéneo $f(X_0, \ldots, X_n)$ con coeficientes en el cuerpo $\mathbb{C}(T)$ y de grado $d \leq n$. Queremos encontrar fracciones racionales $x_0(T), \ldots, x_n(T)$ no todas nulas tales que

$$f(x_0(T), \ldots, x_n(T)) = 0. \tag{3}$$

Eliminando los denominadores, podemos suponer que los coeficientes de f están en el anillo de polinomios $\mathbb{C}[T]$ y que las soluciones que buscamos $x_0(T), \ldots, x_n(T)$ son polinomios. En particular, podemos escribir

$$\begin{cases} x_0(T) = x_{00} + x_{01}T + \cdots + x_{0\delta}T^\delta, \\ \vdots \\ x_n(T) = x_{n0} + x_{n1}T + \cdots + x_{n\delta}T^\delta, \end{cases}$$

para un cierto $\delta > 0$ y ciertos números complejos x_{ij}. Sustituyendo en la ecuación (3) y observando que dicha ecuación equivale a la anulación de todos los coeficientes del polinomio $f(x_0(T), \ldots, x_n(T))$, vemos que queremos demostrar que un sistema de ecuaciones polinomiales complejas y homogéneas en las variables x_{ij} tiene soluciones no nulas. El sistema tiene $(n+1)(\delta+1)$ variables, y si llamamos d_0 al máximo grado de un coeficiente de f, vemos que el sistema tiene $\delta d + d_0$ ecuaciones. En particular, como $d \leq n$, si escogemos δ suficientemente grande, el sistema tendrá más variables que ecuaciones y, por tanto, tendrá soluciones complejas no nulas, como queríamos demostrar.

1.3. Cuerpos de series de Laurent

Dado un cuerpo K, el *cuerpo de series de Laurent* $K((T))$ sobre K es el cuerpo cuyos elementos son las series formales con coeficientes en K de la forma

$$\sum_{n \geq -n_0} a_n T^n$$

para algún $n_0 \geq 0$. Es el cuerpo de fracciones del *anillo de series formales* $K[[T]]$, cuyos elementos son series de la forma

$$\sum_{n \geq 0} a_n T^n.$$

Como para los cuerpos de fracciones racionales, disponemos del teorema siguiente, que fue establecido por Greenberg en 1966 y que permite trasladar la propiedad C_i para el cuerpo K al cuerpo $K((T))$:

Teorema 1.5 (Greenberg [18]). *Sean $i \geq 0$ un entero y K un cuerpo. Si K tiene la propiedad C_i, entonces el cuerpo de series de Laurent $K((T))$ con coeficientes en K tiene la propiedad C_{i+1}.*

Sorprendentemente, la demostración de este teorema resulta ser mucho más delicada que la del teorema de Tsen-Lang-Nagata. Para dar una idea de dónde viene el resultado y de la dificultad de su demostración, miremos un caso sencillo, cuando el cuerpo K es finito. En ese caso, sabemos que K tiene la propiedad C_1, así que queremos establecer la propiedad C_2 para el cuerpo $K((T))$.

Dados dos enteros positivos n y d tales que $n \geq d^2$, así como un polinomio homogéneo $f \in K((T))[X_0, \ldots, X_n]$ de grado d y con coeficientes en $K((T))$, queremos demostrar que la ecuación $f = 0$ tiene soluciones no nulas en $K((T))$. Eliminando denominadores, podemos suponer que f tiene coeficientes en el anillo de series formales $R := K[[T]]$, y nuestro objetivo consiste entonces en encontrar series formales $x_0(T), \ldots, x_n(T)$ en el anillo R tales que $f(x_0(T), \ldots, x_n(T)) = 0$.

Para resolver este problema, es natural querer proceder por inducción:

- En el primer paso, intentamos encontrar elementos $x_0^{(0)}, \ldots, x_n^{(0)} \in K$ tales que el término constante de la serie $f(x_0^{(0)}, \ldots, x_n^{(0)}) \in K[[T]]$ sea nulo;

- en el segundo paso, intentamos encontrar elementos $x_0^{(1)}, \dots, x_n^{(1)} \in K$ tales que el coeficiente de T en la serie $f(x_0^{(0)} + x_0^{(1)}T, \dots, x_n^{(0)} + x_n^{(1)}T) \in K[[T]]$ sea nulo;
- en el tercer paso, habrá que buscar elementos $x_0^{(2)}, \dots, x_n^{(2)} \in K$ tales que el coeficiente de T^2 en la serie $f(x_0^{(0)} + x_0^{(1)}T + x_0^{(2)}T^2, \dots, x_n^{(0)} + x_n^{(1)}T + x_n^{(2)}T^2)$ sea nulo;
- y así sucesivamente.

Si conseguimos llevar a cabo esta inducción, entonces obtendremos la igualdad deseada $f(x_0(T), \dots, x_n(T)) = 0$ si tomamos

$$\begin{cases} x_0(T) = \sum_{i \geq 0} x_0^{(i)} T^i, \\ \vdots \\ x_n(T) = \sum_{i \geq 0} x_n^{(i)} T^i. \end{cases}$$

Analicemos los primeros pasos de dicha inducción. Para hallar $x_0^{(0)}, \dots, x_n^{(0)}$, tenemos que encontrar soluciones de una ecuación homogénea de grado d en $n+1$ variables con coeficientes en el cuerpo K. Y eso lo podemos hacer puesto que $n \geq d^2 \geq d$ y que K tiene la propiedad C_1.

Ahora, para hallar los términos $x_0^{(1)}, \dots, x_n^{(1)}$ con las propiedades deseadas, conviene escribir el desarrollo de Taylor de f:

$$\begin{aligned} &f(x_0^{(0)} + x_0^{(1)}T, \dots, x_n^{(0)} + x_n^{(1)}T) \\ &\quad = f(x_0^{(0)}, \dots, x_n^{(0)}) + \left(\sum_{i=0}^{n} x_i^{(1)} \frac{\partial f}{\partial X_i}(x_0^{(0)}, \dots, x_n^{(0)}) \right) T + \text{términos de grado} \geq 2. \end{aligned}$$

Para que el coeficiente de T en la serie $f(x_0^{(0)} + x_0^{(1)}T, \dots, x_n^{(0)} + x_n^{(1)}T)$ sea nulo, debemos por tanto hallar $x_0^{(1)}, \dots, x_n^{(1)}$ tales que el elemento

$$\sum_{i=0}^{n} x_i^{(1)} \frac{\partial f}{\partial X_i}(x_0^{(0)}, \dots, x_n^{(0)})$$

sea igual al coeficiente de T en la serie $-f(x_0^{(0)}, \dots, x_n^{(0)}) \in K[[T]]$. Esto lo podemos hacer en general, a condición de que exista algún $i \in \{0, \dots, n\}$ tal que

$$\frac{\partial f}{\partial X_i}(x_0^{(0)}, \dots, x_n^{(0)}) \neq 0.$$

Repitiendo este proceso, que es idéntico al método de aproximación de Newton que se usa habitualmente en análisis, uno puede llevar a cabo la inducción deseada siempre y cuando se cumpla la condición anterior. El problema es que no hay ninguna razón para que esa condición sea cierta.

Para evitar este problema, en lugar de proceder por inducción buscando los coeficientes de las series $x_0(T), \dots, x_n(T)$ uno tras otro, vamos a encontrar directamente, para cada $m \geq 0$, polinomios $p_0^{(m)}(T), \dots, p_n^{(m)}(T)$ tales que todos los términos de la serie $f(p_0^{(m)}(T), \dots, p_n^{(m)}(T))$ sean de grado $\geq m$. Para ello, usamos la propiedad C_1 del cuerpo K, así como el teorema de Tsen-Lang-Nagata.

En efecto, recordemos que los coeficientes del polinomio $f(X_0, \dots, X_n)$ son series formales contenidas en el anillo $K[[T]]$. Podemos, por tanto, considerar el polinomio $f_m(X_0, \dots, X_n)$ obtenido a partir de f truncando sus coeficientes hasta el grado $m-1$ (es decir, guardando únicamente aquellos términos de los coeficientes de f que son de grado $\leq m-1$). Así, los coeficientes del polinomio f_m viven en el anillo $K[T]$. Aplicando el teorema de Tsen-Lang-Nagata, que nos dice que $K(T)$ tiene la propiedad C_2, así como la desigualdad $d^2 \leq n$, deducimos que existen polinomios $p_0^{(m)}(T), \dots, p_n^{(m)}(T)$ tales que $f_m(p_0^{(m)}(T), \dots, p_n^{(m)}(T)) = 0$. Como consecuencia, los términos de la serie $f(p_0^{(m)}(T), \dots, p_n^{(m)}(T))$ son todos de grado $\geq m$.

El problema que tenemos ahora es que, a priori, no hay ninguna relación entre los polinomios $p_0^{(m-1)}(T), \dots, p_n^{(m-1)}(T)$ y los polinomios $p_0^{(m)}(T), \dots, p_n^{(m)}(T)$, de modo que, dado un entero $i \in \{0, \dots, n\}$, no está claro cómo construir una serie $x_i(T) \in K[[T]]$ a partir de la sucesión de polinomios $(p_i^{(m)}(T))_{m \geq 0}$. Para superar este obstáculo, recurrimos a un argumento topológico. En efecto, podemos dotar al anillo de series formales $K[[T]]$ de la distancia T-ádica, definida por la fórmula

$$d(x(T), y(T)) = e^{-v_T(x(T)-y(T))}, \tag{4}$$

donde, dada una serie $z(T) \in K[[T]]$, se tiene $v_T(z(T)) = n$ si

$$z(T) = z_n T^n + z_{n+1} T^{n+1} + z_{n+2} T^{n+2} + \cdots$$

con $z_n \neq 0$. Dicho de otra manera, cuanto mayor es el orden de anulación en 0 de la serie $x(T) - y(T)$, más cerca están $x(T)$ e $y(T)$ respecto a la distancia T-ádica. De este modo, se puede dotar al anillo $K[[T]]$ de una topología.

Ahora bien, es fácil comprobar que la finitud del cuerpo K implica la compacidad del anillo $K[[T]]$. Por lo tanto, la sucesión $(p_0^{(m)}(T), \dots, p_n^{(m)}(T))_{m \geq 0}$ de elementos de $K[[T]]^{n+1}$ debe tener un valor de adherencia $(x_0(T), \dots, x_n(T)) \in K[[T]]^{n+1}$. Pero hemos visto que, para cada $m \geq 0$, los términos de la serie $f(p_0^{(m)}(T), \dots, p_n^{(m)}(T))$ son todos de grado $\geq m$. Se deduce que

$$d\left(f(p_0^{(m)}(T), \dots, p_n^{(m)}(T)), 0\right) \leq e^{-m},$$

y, por tanto,

$$\lim_{m \to \infty} f(p_0^{(m)}(T), \dots, p_n^{(m)}(T)) = 0.$$

De ahí se obtiene que

$$f(x_0(T), \dots, x_n(T)) = 0.$$

A priori, las series $x_0(T), \dots, x_n(T)$ podrían ser todas nulas, pero, retomando los argumentos anteriores con más cuidado, podemos asegurarnos de que eso no ocurra. Es exactamente lo que queríamos demostrar.

La estrategia anterior falla si no suponemos que el cuerpo K es finito, puesto que en tal caso el anillo $K[[T]]$ no es compacto. Hay, por tanto, que encontrar otro argumento para construir las series $x_0(T), \dots, x_n(T)$ a partir de los polinomios $p_0^{(m)}(T), \dots, p_n^{(m)}(T)$. Aquí reside la principal dificultad del teorema de Greenberg. La clave es el siguiente enunciado, que es muy delicado de demostrar:

Teorema 1.6 (Greenberg [18]). *Sean K un cuerpo y $R = K[[T]]$ el anillo de series formales con coeficientes en K. Dado un polinomio homogéneo $f \in R[X_0, \dots, X_n]$ con coeficientes en R, la ecuación $f = 0$ tiene soluciones no nulas en el cuerpo de series de Laurent $K((T))$ si y solo si, para cada $m \geq 1$, existen polinomios $p_0(T), \dots, p_n(T) \in K[T]$ no todos múltiplos de T tales que los m primeros coeficientes de la serie $f(x_0(T), \dots, x_n(T))$ son nulos.*

2. Cuerpos C_i y cohomología

Hemos visto que los cuerpos que tienen la propiedad C_0 son los cuerpos algebraicamente cerrados. En esta sección, nos gustaría indagar si hay resultados similares para los cuerpos con la propiedad C_i para algún $i \geq 1$.

Para ello, será útil disponer de un poco de vocabulario de la teoría de cuerpos. Así, dados dos cuerpos K y L, decimos que L es una *extensión* de K si L contiene a K. En tal caso, L es naturalmente un K-espacio vectorial. Cuando su dimensión es finita, decimos que L es una *extensión finita* de K.

2.1. Cuerpos C_1 y álgebras de división

Empecemos por el caso $i = 1$. Dado un cuerpo K cualquiera, conviene entender cómo construir polinomios homogéneos $f \in K[X_0, \dots, X_n]$ de grado $\leq n$ tales que la ecuación $f = 0$ no tenga soluciones no nulas. Podremos entonces deducir que dicha construcción siempre falla al suponer que K tiene la propiedad C_1.

Para construir polinomios con las propiedades deseadas, es natural considerar la función determinante

$$\det \colon \mathrm{Mat}_n(K) \to K,$$

puesto que det es una función polinomial en los coeficientes de las matrices, y además sabemos exactamente cuándo se anula: dada una matriz M, su determinante es nulo si y solo si M no es invertible.

Ahora tomemos una K-álgebra (no necesariamente conmutativa) A de dimensión finita r, es decir, un anillo A dotado de una estructura compatible de K-espacio vectorial de dimensión r. Cada elemento $a \in A$ induce una aplicación K-lineal

$$\begin{aligned} m_a \colon A &\to A, \\ b &\mapsto ab \end{aligned}$$

y por tanto podemos definir la función

$$\begin{aligned} N \colon A &\to K \\ a &\mapsto \det(m_a). \end{aligned}$$

Se tiene entonces que $N(a) \neq 0$ si y solo si m_a es invertible, lo cual equivale a que a sea invertible en el anillo A. En particular, si suponemos a partir de ahora que todo elemento no nulo de A es invertible —decimos que A es un *cuerpo no conmutativo* o un *anillo de división*—, se tiene entonces:

$$\text{para todo } a \in A, \quad N(a) = 0 \iff a = 0.$$

Además, si fijamos una base $\omega_1, \ldots, \omega_r$ de A como K-espacio vectorial, se puede comprobar fácilmente que N es una función polinomial homogénea de grado r en las coordenadas en dicha base. En otras palabras, la función

$$\begin{aligned} N' \colon K^r &\to K \\ (x_1, \ldots, x_r) &\mapsto N(x_1\omega_1 + \cdots + x_r\omega_r) \end{aligned}$$

es un polinomio homogéneo de grado r con coeficientes en K tal que la ecuación $N' = 0$ no tiene soluciones no nulas. De este modo, ya casi hemos construido un polinomio con las propiedades que queríamos. Pero tenemos un pequeño problema: el grado de N' es demasiado grande respecto al número de variables.

Para intentar entender cómo resolver esta dificultad, tomemos un ejemplo concreto. Dados dos elementos no nulos $a, b \in K$, introduzcamos el *álgebra de cuaterniones* $H_{a,b}$, definida como la K-álgebra (no conmutativa) de dimensión 4 con base $(1, i, j, k)$, en la cual la multiplicación viene dada por

$$i^2 = a, \quad j^2 = b, \quad k = ij = -ji.$$

Por ejemplo, $H_{1,1}$ se identifica con el álgebra de matrices $\mathrm{Mat}_2(K)$ mediante la correspondencia

$$1 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad k \longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

y, cuando $K = \mathbb{R}$, el álgebra $H_{-1,-1}$ coincide con el álgebra de cuaterniones de Hamilton.

Para las álgebras de cuaterniones, resulta sencillo calcular las funciones N y N':

$$N'(x,y,z,t) = N(x+yi+zj+tk) = \begin{vmatrix} x & ay & bz & -abt \\ y & x & bt & -bz \\ z & -at & x & ay \\ t & -z & y & x \end{vmatrix} = (x^2 - ay^2 - bz^2 + abt^2)^2,$$

de modo que $N' = f^2$, donde f es el polinomio $X^2 - aY^2 - bZ^2 + abT^2$. En particular, las ecuaciones $N' = 0$ y $f = 0$ tienen las mismas soluciones, y, por tanto, si suponemos que $H_{a,b}$ es un anillo de división, entonces la ecuación $f = 0$ no puede tener soluciones no nulas. Pero esto no puede ocurrir si K tiene la propiedad C_1, puesto que f tiene 4 variables y grado 2. De ahí se deduce que, sobre los cuerpos con la propiedad C_1, las álgebras de cuaterniones no pueden ser nunca anillos de división.

Lo mismo ocurre en general: dada cualquier K-álgebra de división no conmutativa A de dimensión finita r, siempre existen un polinomio f y un entero $m > 1$ tales que $N' = f^m$. En particular, la única solución de la ecuación $f = 0$ es la solución nula. Pero esto no puede ocurrir si K tiene la propiedad C_1, puesto que

$$\deg f < \deg N' = \#\{\text{variables de } f\}.$$

De ahí deducimos la importante propiedad siguiente:

Teorema 2.1. *Si K es un cuerpo con la propiedad C_1, entonces toda K-álgebra de división de dimensión finita es conmutativa.*

Nótese que este resultado se aplica, por ejemplo, a todos los cuerpos finitos (en cuyo caso el teorema se atribuye a Wedderburn), así como a $\mathbb{C}(T)$ y a $\mathbb{C}((T))$.

2.2. Cohomología de Galois

Para entender un poco mejor el sentido del teorema 2.1, es conveniente saber clasificar las álgebras de división sobre un cuerpo K. Para ello introducimos ahora la noción un poco técnica de cohomología de Galois.

Fijemos un cuerpo K cualquiera y sea $\overline{K}$ una clausura separable de K. En el caso en el que K es de característica 0 o un cuerpo finito, $\overline{K}$ es también una clausura algebraica de K. Una idea fundamental en teoría de cuerpos es que hay un diccionario entre las propiedades del cuerpo K y las de un grupo topológico compacto llamado el *grupo de Galois absoluto* de K. Se trata del grupo $\mathrm{Gal}(\overline{K}/K)$ de automorfismos de $\overline{K}$ que fijan K, dotado de la topología en la que una base de entornos abiertos de la identidad viene dada por los subgrupos

$$G_L := \{\text{automorfismos de } \overline{K} \text{ que fijan } L\}$$

cuando L describe las extensiones finitas de K contenidas en $\overline{K}$.

Ahora que tenemos el grupo topológico $\mathrm{Gal}(\overline{K}/K)$, podemos usar todas las herramientas que queramos de la teoría de grupos para estudiarlo. En particular, se puede estudiar su cohomología e intentar extraer de ahí todas las informaciones que uno quiera. Es lo que se llama la *cohomología de Galois de K*.

En lo que sigue, nos vamos a concentrar en la cohomología del grupo $\mathrm{Gal}(\overline{K}/K)$ con coeficientes en grupos abelianos, que admite una descripción explícita en términos de espacios de funciones. Más precisamente, démonos un grupo abeliano M (dotado de la topología discreta) y un entero $n \geq 0$, y consideremos el grupo abeliano Z^n compuesto por las funciones continuas

$$f\colon \mathrm{Gal}(\overline{K}/K)^n \to M$$

que satisfacen la ecuación funcional

$$\begin{aligned} f(g_2, \ldots, g_{n+1}) \\ + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) \\ + (-1)^{n+1} f(g_1, \ldots, g_n) = 0 \end{aligned}$$

para todo $g_1, \ldots, g_{n+1} \in \mathrm{Gal}(\overline{K}/K)$. Este grupo, llamado el *grupo de los n-cociclos*, contiene como subgrupo al conjunto B^n de funciones

$$h\colon \mathrm{Gal}(\overline{K}/K)^n \to M$$

de la forma

$$\begin{aligned} h(g_1, \ldots, g_n) = {} & h_0(g_2, \ldots, g_n) \\ & + \sum_{i=1}^{n-1} (-1)^i h_0(g_1, \ldots, g_{i-1}, g_i g_{i+1}, \ldots, g_n) \\ & + (-1)^n h_0(g_1, \ldots, g_{n-1}) \end{aligned}$$

para alguna función continua $h_0\colon \mathrm{Gal}(\overline{K}/K)^{n-1} \to M$. Los elementos de B^n se llaman los *n-cobordes*. El *n-ésimo grupo de cohomología de K con coeficientes en M* es entonces el cociente del grupo de los n-cociclos por los n-cobordes:

$$H^n(K, M) := Z^n/B^n.$$

Esta definición es técnica y no es necesario retenerla con precisión para leer el resto del artículo. Conviene simplemente entender que los grupos $H^n(K, M)$ están definidos de una manera muy explícita, que disponemos de múltiples métodos prácticos para calcularlos, y que solo dependen del grupo de Galois $\mathrm{Gal}(\overline{K}/K)$ (y no de las propiedades aritméticas internas del cuerpo K).

Podemos ahora formular el teorema de álgebra abstracta que permite clasificar las álgebras de división sobre cuerpos que contienen todas las raíces de la unidad:

Teorema 2.2. *Sea K un cuerpo que contiene r raíces r-ésimas de la unidad para todo $r \geq 1$, y sea $AD(K)$ el conjunto de todas las K-álgebras de división de dimensión finita. Para cada $n \geq 1$ y para cada extensión finita L de K, existe una aplicación inyectiva $i_{L,n}\colon H^2(L, \mathbb{Z}/n\mathbb{Z}) \to AD(K)$ de modo que la imagen del elemento neutro* 0 *sea el álgebra de división L y que*

$$AD(K) = \coprod_L \bigcup_{n \geq 1} i_{L,n}\left(H^2(L, \mathbb{Z}/n\mathbb{Z})\right).$$

Con las hipótesis y la terminología de este teorema, decir que toda álgebra de división de dimensión finita sobre K es conmutativa es lo mismo que decir que

$$AD(K) = \{L \mid L \text{ es una extensión finita de } K\} = \coprod_L \bigcup_{n \geq 1} i_{L,n}(0).$$

Por el teorema 2.2, esto equivale a la anulación $H^2(L, \mathbb{Z}/n\mathbb{Z}) = 0$ para todo entero $n \geq 1$ y toda extensión finita L de K. Pero todo grupo abeliano finito es suma directa de grupos cíclicos, y, por lo tanto, todas las afirmaciones anteriores equivalen también a la anulación $H^2(L, M) = 0$ para todo grupo abeliano finito M y toda extensión finita L de K.

Cuando un cuerpo K tiene esta propiedad, decimos que K tiene dimensión cohomológica inferior o igual a 2. Más generalmente, se define la dimensión cohomológica de un cuerpo del siguiente modo:

Definición 2.3. Sea K un cuerpo. La *dimensión cohomológica* $\mathrm{cd}(K)$ de K es el menor entero $r \geq 0$ tal que $H^{r+1}(L, M) = 0$ para todo grupo abeliano finito M y toda extensión finita L de K. Al igual que los grupos de cohomología de K, la dimensión cohomológica solo depende del grupo de Galois $\mathrm{Gal}(\overline{K}/K)$ y no de las propiedades aritméticas internas del cuerpo K.

Pese a que el teorema 2.2 solo es válido bajo la hipótesis de que el cuerpo K contiene todas las raíces de la unidad, se puede interpretar de forma totalmente general la no existencia de álgebras de división no conmutativas sobre un cuerpo cualquiera K en términos de dimensión cohomológica. En efecto:

Teorema 2.4. *Sea K un cuerpo cualquiera. Toda K-álgebra de división de dimensión finita es conmutativa si y solo si* $\mathrm{cd}(K) \leq 1$. *Por el teorema 2.1, esto es cierto, en particular, si K tiene la propiedad C_1.*

Este último resultado es especialmente interesante, ya que demuestra que una propiedad puramente diofántica del cuerpo K como es la propiedad C_1 impone una estructura algebraica particular sobre el grupo de Galois $\mathrm{Gal}(\overline{K}/K)$.

Ahora, ¿qué ocurre con la propiedad C_i para $i \geq 2$? Pues bien, resulta que la dimensión cohomológica y las propiedades C_i se comportan de forma muy similar:

- La dimensión cohomológica de un cuerpo algebraicamente cerrado es 0;
- la dimensión cohomológica de un cuerpo finito es 1;
- si un cuerpo K tiene dimensión cohomológica r, entonces los cuerpos $K(T)$ y $K((T))$ tienen dimensión cohomológica $r + 1$.

Parece claro que hay un paralelismo entre estas propiedades de la dimensión cohomológica y los resultados que hemos enunciado en la sección 1 sobre las propiedades C_i. Por esa razón, Serre formuló la siguiente conjetura en 1962:

Conjetura 2.5 (Serre [27]). *Sea $i \geq 0$ un entero. Si K tiene la propriedad C_i, entonces* $\mathrm{cd}(K) \leq i$.

Por el teorema 2.4, la conjetura es cierta para $i = 1$. Un teorema complicado de Suslin [28] establece la conjetura para $i = 2$. El caso $i \geq 3$ sigue estando totalmente abierto, aunque existen resultados parciales (véase, por ejemplo, [23]).

Observación 2.6. En la sección siguiente, introduciremos los cuerpos p-ádicos y veremos que son contraejemplos al enunciado recíproco de la conjetura de Serre en el caso $i = 2$. En 1965, Ax [4] demostró que hay contraejemplos incluso para $i = 1$.

3. Cuerpos p-ádicos y cuerpos de números

El punto de partida de la teoría de números es el estudio del anillo de enteros $\mathbb{Z}$ y del cuerpo de números racionales $\mathbb{Q}$, pero rápidamente uno se da cuenta de que conviene entender también otros cuerpos un poco más grandes que $\mathbb{Q}$, como el cuerpo $\mathbb{Q}(i) := \{x + yi \mid x, y \in \mathbb{Q}\}$ o el cuerpo $\mathbb{Q}(\sqrt[3]{2}) = \{x + y\sqrt[3]{2} + z\sqrt[3]{4} \mid x, y, z \in \mathbb{Q}\}$. Por ejemplo, si quisiésemos hallar las soluciones racionales de la ecuación $x^3 = y^2 + 1$, convendría trabajar en el cuerpo $\mathbb{Q}(i)$ para poder factorizar el lado derecho de la

ecuación y escribir $x^3 = (y+i)(y-i)$. Los cuerpos $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt[3]{2})$ son ambos *cuerpos de números*, es decir, extensiones finitas de $\mathbb{Q}$ contenidas en $\mathbb{C}$.

A finales del siglo XIX y principios del XX, con el fin de estudiar el cuerpo $\mathbb{Q}$ o, más generalmente, los cuerpos de números, Hensel introdujo el lenguaje de los cuerpos p-ádicos. La idea puede resumirse de la manera siguiente. Como $\mathbb{Q}$ está contenido en $\mathbb{R}$, se pueden usar propiedades del cuerpo de los números reales para resolver problemas sobre los números racionales. En vista de que $\mathbb{R}$ es la compleción de $\mathbb{Q}$ respecto a la distancia usual, es entonces natural preguntarse si el cuerpo $\mathbb{Q}$ posee otras distancias (que se comporten bien con respecto de su estructura de cuerpo). Y, si así fuera, ¿qué ocurriría si se sustituyera la distancia usual por alguna de esas otras distancias?

Pues bien, resulta que cada número primo p define una distancia p-ádica sobre $\mathbb{Q}$ por medio de la fórmula

$$d_p(x, y) = e^{-v_p(x-y)},$$

donde la valuación p-ádica $v_p(z)$ de un número racional z es el exponente de p cuando se escribe z como producto de potencias de números primos distintos. De este modo, cuanto mayor es la valuación p-ádica de $x - y$, más cerca están x e y. El *cuerpo de números p-ádicos* $\mathbb{Q}_p$ es la compleción de $\mathbb{Q}$ respecto a la distancia d_p. Se pueden entonces usar las propiedades algebraicas, pero también analíticas, del cuerpo $\mathbb{Q}_p$ para entender los números racionales.

Llegado este punto, conviene hacer un paralelismo entre los cuerpos de números p-ádicos y los cuerpos de series de Laurent que introdujimos en la sección 1.3. Para cada número primo p, el cuerpo $\mathbb{Q}_p$ se obtiene por compleción de $\mathbb{Q}$ respecto de la distancia p-ádica d_p, del mismo modo que, para cada cuerpo K, el cuerpo de series de Laurent $K((T))$ se obtiene por compleción de $K(T)$ respecto de la distancia T-ádica definida por la ecuación (4). Como las dos construcciones son muy similares, cabe esperar que el cuerpo p-ádico $\mathbb{Q}_p$ tenga propiedades parecidas a las de los cuerpos de series de Laurent. En particular, satisface una propiedad muy similar al teorema 1.6:

Teorema 3.1. *Dado un número primo p, si $f \in \mathbb{Z}[X_0, \ldots, X_n]$ es un polinomio homogéneo, la ecuación $f = 0$ tiene soluciones no nulas en el cuerpo $\mathbb{Q}_p$ si y solo si, para todo $r \geq 1$, la congruencia*

$$f(x_0, \ldots, x_n) \equiv 0 \mod p^r$$

tiene soluciones $x_0, \ldots, x_r \in \mathbb{Z}$ tales que no todos los x_j son divisibles por p.

Este resultado se demuestra usando el mismo argumento de compacidad que nos permitió establecer el teorema 1.6 en el caso de un cuerpo K finito.

De forma más general, en lugar de considerar el cuerpo de números racionales, podemos partir de un cuerpo de números K cualquiera y completarlo respecto a distancias que sean compatibles con su estructura de cuerpo. Se obtienen así extensiones de K que pueden ser de tres tipos:

- Un cuerpo isomorfo a los números reales;
- un cuerpo isomorfo a los números complejos;

- un *cuerpo p-ádico*, es decir, una extensión finita de algún $\mathbb{Q}_p$.

En toda esta sección, vamos a estudiar las propiedades C_i para los cuerpos p-ádicos y para los cuerpos de números.

3.1. La conjetura de Artin para los cuerpos p-ádicos

Empecemos estudiando los cuerpos p-ádicos. Es fácil ver que la congruencia

$$x^2 + y^2 + z^2 \equiv 0 \mod 4$$

no tiene soluciones en las que x, y, z no sean todos pares. Por lo tanto, usando el teorema 3.1, deducimos que la ecuación

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

no tiene soluciones no nulas en el cuerpo $\mathbb{Q}_2$. En particular, $\mathbb{Q}_2$ no tiene la propiedad C_1.

Consideremos ahora un primo impar p. En tal caso, existe un entero a que no es un cuadrado módulo p. Démonos tres enteros x, y, z tales que

$$x^2 - ay^2 + pz^2 \equiv 0 \mod p^2. \tag{5}$$

En particular, tenemos que $x^2 \equiv ay^2 \mod p$. Pero a no es un cuadrado módulo p, así que y debe ser múltiplo de p. La congruencia (5) implica entonces que x y z también deben serlo, lo que demuestra que dicha congruencia no tiene soluciones en las que x, y, z no sean todos divisibles por p. Por el teorema 3.1, la ecuación

$$x^2 - ay^2 + pz^2 = 0$$

no tiene soluciones no nulas en el cuerpo $\mathbb{Q}_p$. En particular, $\mathbb{Q}_p$ no tiene la propiedad C_1.

De forma más general, se puede demostrar por métodos análogos que este resultado se extiende a todos los cuerpos p-ádicos.

¿Qué pasa ahora con las propiedades C_i para $i \geq 2$? De forma relativamente sencilla (aunque no elemental), se puede demostrar que los cuerpos p-ádicos tienen dimensión cohomológica 2. Por esa razón, Artin conjeturó a comienzos de los años 50 que los cuerpos p-ádicos tendrían la propiedad C_2 (véase [3]).

De hecho, algunos resultados parecían corroborar la conjetura. Hasse había demostrado anteriormente en 1924 que, sobre los cuerpos p-ádicos, las ecuaciones homogéneas de grado 2 con al menos $2^2 + 1 = 5$ variables siempre tienen soluciones no nulas [19]. Y, posteriormente, los trabajos de Demjanov y Lewis en los años 50 permitieron establecer que, sobre los cuerpos p-ádicos, las ecuaciones homogéneas de grado 3 con al menos $3^2 + 1 = 10$ variables también tienen soluciones no nulas [13, 25]. Habría que esperar hasta el año 1966 para que Terjanian consiguiera dar un contraejemplo de grado 4 a la conjetura de Artin:

Teorema 3.2 (Terjanian [29]). *El cuerpo $\mathbb{Q}_2$ no tiene la propiedad C_2, ya que existe una ecuación homogénea de grado 4 en 18 variables sin soluciones no nulas en $\mathbb{Q}_2$.*

La demostración de este resultado es elemental ya que se basa en sencillos argumentos de aritmética modular. En efecto, supongamos dado un polinomio homogéneo $h(X,Y,Z) \in \mathbb{Z}[X,Y,Z]$ de grado 4 tal que, para toda terna $(x,y,z) \in \mathbb{Z}^3$ de enteros no todos pares, se tiene

$$h(x,y,z) \equiv 1 \mod 4. \tag{6}$$

Como h es homogéneo de grado 4, se tiene además la congruencia

$$h(x,y,z) \equiv 0 \mod 4$$

para tres enteros pares x,y,z cualesquiera, y, por tanto, el polinomio

$$g(X_1,\ldots,X_9) = h(X_1,X_2,X_3) + h(X_4,X_5,X_6) + h(X_7,X_8,X_9)$$

satisface la propiedad siguiente: para todo $(x_1,\ldots,x_9) \in \mathbb{Z}^9$, se tiene

$$g(x_1,\ldots,x_9) \equiv 0 \mod 4 \iff x_1,\ldots,x_9 \text{ son todos pares.}$$

Consideremos ahora el polinomio

$$f(X_1,\ldots,X_{18}) = g(X_1,\ldots,X_9) + 4g(X_{10},\ldots,X_{18})$$

y fijemos dieciocho enteros $x_1,\ldots,x_{18}$ tales que

$$f(x_1,\ldots,x_{18}) \equiv 0 \mod 16.$$

Entonces $g(x_1,\ldots,x_9) \equiv 0 \mod 4$, por lo que $x_1,\ldots,x_9$ son todos pares. Como h tiene grado 4, deducimos que $g(x_1,\ldots,x_9)$ es divisible por 16, lo que implica que 4 divide a $g(x_{10},\ldots,x_{18})$. De ahí obtenemos que, al igual que $x_1,\ldots,x_9$, los enteros $x_{10},\ldots,x_{18}$ son todos pares. Por el teorema 3.1, deducimos que la ecuación $f=0$ no tiene soluciones no nulas en $\mathbb{Q}_2$. Pero f tiene 18 variables y grado 4, así que para terminar la demostración del teorema de Terjanian nos basta con hallar un polinomio homogéneo h de grado 4 que satisfaga la congruencia (6), por ejemplo:

$$h(X,Y,Z) = X^4 + Y^4 + Z^4 - (X^2YZ + XY^2Z + XYZ^2 + X^2Y^2 + Y^2Z^2 + X^2Z^2).$$

En realidad, se puede ir mucho más lejos. Poco después de que Terjanian enunciase el teorema 3.2 en 1966, Browkin [7] demostró que ningún cuerpo p-ádico tiene la propiedad C_2. Es más, unos quince años más tarde, en los años 80, Alemu por un lado y Arkhipov-Karatsuba por otro establecieron el resultado siguiente, cuya demostración es bastante más delicada:

Teorema 3.3 (Alemu [1], Arkhipov-Karatsuba [2]). *Dados un número primo p y un entero no negativo i, ningún cuerpo p-ádico tiene la propiedad C_i.*

De este resultado se deduce fácilmente que todos los cuerpos de números son contraejemplos a todas las propiedades C_i. Como ya explicamos anteriormente, este resultado es evidente para aquellos cuerpos de números que son isomorfos a un subcuerpo de los números reales (como $\mathbb{Q}$ o $\mathbb{Q}(\sqrt[3]{2})$), pero no para los demás (como $\mathbb{Q}(i)$). Nótese que estos últimos cuerpos de números que no se pueden ver como subcuerpos de $\mathbb{R}$ tienen siempre dimensión cohomológica 2.

En el resto de esta sección, nos dedicaremos a la búsqueda de sustitutos a las propiedades C_i que sí sean ciertos para los cuerpos p-ádicos y los cuerpos de números.

3.2. El teorema de Ax-Kochen

Empecemos por los cuerpos p-ádicos. Aunque hemos visto que dichos cuerpos no satisfacen la propiedad C_2 como había conjeturado Artin, Ax y Kochen consiguieron demostrar en 1965 con métodos de lógica matemática un teorema espectacular:

Teorema 3.4 (Ax-Kochen [5]). *Dado un entero $d \geq 1$, existe un entero $m(d)$ tal que, para todo número primo $p \geq m(d)$, para todo $n \geq d^2$ y para todo polinomio homogéneo $f \in \mathbb{Q}_p[X_0, \ldots, X_n]$ de grado d, existen elementos $x_0, \ldots, x_n \in \mathbb{Q}_p$ no todos nulos tales que $f(x_0, \ldots, x_n) = 0$.*

En otras palabras, para cada $d \geq 1$, los cuerpos $\mathbb{Q}_p$ satisfacen «la propiedad C_2 en grado d» para p suficientemente grande. En 1978, Brown [8] demostró además que, en el teorema 3.4, se puede tomar

$$m(d) = 2^{2^{2^{2^{11^{d^{4d}}}}}}.$$

Expliquemos ahora brevemente cómo Ax y Kochen demuestran el teorema 3.4.

La idea general es muy bonita. Hemos visto anteriormente que, dado un número primo p, el cuerpo de números p-ádicos $\mathbb{Q}_p$ y el cuerpo de series de Laurent $\mathbb{F}_p((T))$ (donde $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$) tienden a comportarse de manera similar. Como sabemos que $\mathbb{F}_p((T))$ tiene la propiedad C_2 por el teorema de Greenberg, la idea consiste en ver cómo pasar de $\mathbb{F}_p((T))$ a $\mathbb{Q}_p$. El precio a pagar para poder hacerlo es restringirse a aquellos primos p que son suficientemente grandes.

Más precisamente, para trabajar con todos los cuerpos $\mathbb{Q}_p$ al mismo tiempo, como requiere el teorema de Ax-Kochen, es natural introducir el producto $\prod_p \mathbb{Q}_p$. El problema es que este producto no es un cuerpo. Por esa razón, es necesario sustituir el producto anterior por cocientes adecuados que sí sean cuerpos, los llamados *ultraproductos*.

De la misma manera, considerando cocientes del producto $\prod_p \mathbb{F}_p((T))$, se obtienen ultraproductos asociados a los cuerpos $\mathbb{F}_p((T))$. El punto clave en la demostración de Ax-Kochen, que usa de forma crucial la teoría de modelos, consiste en observar que los ultraproductos asociados a los cuerpos p-ádicos y los ultraproductos asociados a los cuerpos de series de Laurent $\mathbb{F}_p((T))$ comparten suficientes propiedades algebraicas para que sean *elementalmente equivalentes*. Esto significa que, dado un enunciado lógico P de primer orden, los ultraproductos asociados a los cuerpos p-ádicos satisfacen P si y solo si los ultraproductos asociados a los cuerpos de series de Laurent $\mathbb{F}_p((T))$ también lo satisfacen.

Abandonando el lenguaje de los ultraproductos y volviendo a los cuerpos p-ádicos y a las series de Laurent, se deduce que, dado un enunciado lógico P de primer orden, existe un entero n tal que $\mathbb{Q}_p$ satisface P para todo $p \geq n$ si y solo si existe un entero m tal que $\mathbb{F}_p((T))$ satisface P para todo $p \geq m$. El teorema de Ax-Kochen

se obtiene entonces aplicando este resultado al enunciado P siguiente:

$$\forall\, (a_{i_0,\dots,i_{d^2}})_{\substack{i_0\geq 0,\dots,i_{d^2}\geq 0\\ i_0+\cdots+i_{d^2}=d}},\ \exists\, x_0,\dots,x_{d^2},$$

$$\left(\sum_{\substack{i_0\geq 0,\dots,i_{d^2}\geq 0\\ i_0+\cdots+i_{d^2}=d}} a_{i_0,\dots,i_{d^2}} x_0^{i_0}\cdots x_{d^2}^{i_{d^2}} = 0\right)\ \wedge\ ((x_0=1)\ \vee\ \cdots\ \vee\ (x_{d^2}=1))\,,$$

y observando que, para todo primo p, el cuerpo $\mathbb{F}_p((T))$ tiene la propiedad C_2 y, por tanto, satisface P. (Nótese que, en el enunciado P, la condición

$$(x_0=1)\ \vee\ \cdots\ \vee\ (x_{d^2}=1)$$

equivale a imponer que los x_i no sean todos nulos, puesto que la ecuación

$$\sum_{\substack{i_0\geq 0,\dots,i_{d^2}\geq 0\\ i_0+\cdots+i_{d^2}=d}} a_{i_0,\dots,i_{d^2}} x_0^{i_0}\cdots x_{d^2}^{i_{d^2}} = 0$$

es homogénea en las variables x_i.)

Observación 3.5. Hace poco, Denef ha establecido una conjetura de Colliot-Thélène que implica el teorema de Ax-Kochen por métodos puramente geométricos, evitando así todo argumento de lógica matemática [15, 14].

3.3. El principio de Hasse

Pasemos ahora al cuerpo de los números racionales $\mathbb{Q}$. Nuestro objetivo consiste en hallar versiones débiles de las propiedades C_i para que $\mathbb{Q}$ las satisfaga.

Para intentar alcanzar esta meta, conviene recordar la razón por la cual $\mathbb{Q}$ no satisface ninguna de las propiedades C_i: el cuerpo $\mathbb{Q}$ está contenido en $\mathbb{R}$ y, para todo n, la única solución real de la ecuación $x_0^2+\cdots+x_n^2=0$ es la solución nula. Este argumento se basa en una observación muy sencilla: para ver que una ecuación no tiene soluciones racionales, basta con demostrar que no tiene soluciones reales.

Por supuesto, la afirmación anterior sigue siendo válida si se sustituyen los números reales por los números p-ádicos para algún primo p. Así, para que una ecuación tenga soluciones racionales, es necesario que tenga soluciones en el cuerpo $\mathbb{R}$ y en todos los cuerpos $\mathbb{Q}_p$.

Esta observación puede darnos una idea para introducir una versión más débil de las propiedades C_i cuando trabajamos con el cuerpo de los números racionales: en vez de pedir que toda ecuación homogénea $f(x_0,\dots,x_n)=0$ de grado d con n «grande» comparado con d tenga soluciones racionales no nulas, podemos restringirnos a aquellas ecuaciones que tengan soluciones no nulas en $\mathbb{R}$ y en cada $\mathbb{Q}_p$. Por esta razón, introducimos la definición siguiente:

Definición 3.6. Sea $\mathcal{E}$ una familia de ecuaciones polinomiales homogéneas con coeficientes racionales. Decimos que $\mathcal{E}$ satisface el *principio de Hasse* si la implicación siguiente es cierta: si una ecuación en $\mathcal{E}$ tiene soluciones no nulas en $\mathbb{R}$ y en cada $\mathbb{Q}_p$, entonces también tiene soluciones racionales no nulas.

En otras palabras, recordando el teorema 3.1, si una familia de ecuaciones homogéneas $\mathcal{E}$ satisface el principio de Hasse, entonces una ecuación $f(x_0,\dots,x_n)=0$ en $\mathcal{E}$ tiene soluciones racionales no nulas si y solo si tiene soluciones reales no nulas y, para todo primo p y todo entero $r\geq 1$, la congruencia $f(x_0,\dots,x_n)\equiv 0 \mod p^r$ tiene soluciones en las que p no divide a todos los x_i.

Dados dos enteros $d,n\geq 1$, introduzcamos el conjunto $\mathcal{E}_{d,n}$ cuyos elementos son las ecuaciones polinomiales homogéneas de grado d con coeficientes racionales en $n+1$ variables. Uno puede entonces debilitar las propiedades C_i para el cuerpo $\mathbb{Q}$ preguntando si, para todo n y todo d tales que n es en cierto sentido «grande» comparado con d, la familia $\mathcal{E}_{d,n}$ satisface el principio de Hasse.

En grado 1, es muy fácil comprobar que la familia $\mathcal{E}_{1,n}$ satisface el principio de Hasse para todo $n\geq 1$. El primer resultado importante no trivial en esta dirección es el célebre teorema de Hasse-Minkowski, que remonta a los años 20 del siglo pasado y que trata el caso de las ecuaciones de grado 2:

Teorema 3.7 (Hasse-Minkowski). *La familia $\mathcal{E}_{2,n}$ satisface el principio de Hasse para todo $n\geq 1$. En otras palabras, si una ecuación polinomial homogénea de grado 2 tiene soluciones en $\mathbb{R}$ y en todos los $\mathbb{Q}_p$, entonces tiene soluciones racionales no nulas.*

A partir del grado 3, las cosas se complican. En efecto, para todo $d\geq 3$ existen contraejemplos al principio de Hasse en grado d. Es el caso, por ejemplo, de la ecuación cuártica

$$\prod_{\epsilon,\eta\in\{1,-1\}}\left(x_1+\epsilon x_2\sqrt{13}+\eta x_3\sqrt{17}+\epsilon\eta x_4\sqrt{221}\right)=-t^4 \tag{7}$$

estudiada por Hasse en 1934 y que demuestra que la familia $\mathcal{E}_{4,4}$ no satisface el principio de Hasse.

Si observamos detenidamente el ejemplo anterior, nos damos cuenta de que presenta características geométricas algo desagradables, ya que la ecuación (7) define una variedad proyectiva compleja singular. En términos concretos, esto significa que la ecuación (7) y sus derivadas parciales respecto de las cinco variables x_1,x_2,x_3,x_4 y t tienen al menos una solución compleja no nula en común. De acuerdo con el siguiente teorema, que demostró Birch en 1962 usando técnicas de teoría analítica de números (en particular estimaciones de sumas exponenciales y el método del círculo de Hardy-Littlewood), todo funciona mucho mejor si solo consideramos ecuaciones que definen variedades proyectivas complejas no singulares:

Teorema 3.8 (Birch [6]). *Sean d y n dos enteros tales que $n\geq (d-1)2^d-1$. La subfamilia $\mathcal{E}'_{d,n}$ de $\mathcal{E}_{d,n}$ formada por aquellas ecuaciones que definen variedades proyectivas complejas no singulares satisface el principio de Hasse.*

Si bien este teorema demuestra que las ecuaciones de grado pequeño en comparación con el número de variables tienen tendencia a satisfacer el principio de Hasse, la desigualdad impuesta $n\geq (d-1)2^d-1$ es mucho peor que la desigualdad $n\geq d^i$ que aparece en la propiedad C_i. El teorema que sigue, demostrado por Browning, Le Boudec y Sawin en 2020, trata sobre la familia $\mathcal{E}'_{d,n}$ cuando $d\leq n$. Como hemos

visto con el contraejemplo de Hasse (7), no se puede esperar demostrar que dicha familia satisfaga el principio de Hasse. De ahí que Browning, Le Boudec y Sawin solamente demuestren este resultado en un sentido estadístico:

Teorema 3.9 (Browning, Le Boudec y Sawin [9]). *Sean n y d dos enteros tales que $n \geq d$ y $(n,d) \neq (3,3)$. El 100 % de las ecuaciones de la familia $\mathcal{E}'_{d,n}$ satisface el principio de Hasse.*

Expliquemos qué significa la expresión «100 % de las ecuaciones de la familia $\mathcal{E}'_{d,n}$». Para ello, observemos que, dado un polinomio f y un número racional λ, la ecuación $f = 0$ satisface el principio de Hasse si y solo si la ecuación $\lambda f = 0$ también lo satisface. Por lo tanto, como para toda ecuación $f = 0$ existe un racional λ tal que el polinomio λf tiene coeficientes enteros primos entre sí, estudiar la familia $\mathcal{E}'_{d,n}$ es lo mismo que estudiar la subfamilia $\mathcal{F}'_{d,n} \subseteq \mathcal{E}'_{d,n}$ que contiene solo las ecuaciones cuyos coeficientes son enteros y primos entre sí. Dada una ecuación $E \in \mathcal{F}'_{d,n}$, se define la *altura* $H(E) \in \mathbb{R}_{\geq 0}$ de E como la norma euclídea del vector formado por los coeficientes de E. Con esta definición, dado un número real $B > 0$, el conjunto

$$\mathcal{F}'_{d,n}(B) := \{E \in \mathcal{F}'_{d,n} \mid H(E) \leq B\}$$

es finito. Es, por tanto, natural definir la *proporción* $\rho_{d,n}$ de ecuaciones que satisfacen el principio de Hasse en la familia $\mathcal{E}_{d,n}$ como el límite

$$\rho_{d,n} := \lim_{B \to +\infty} \frac{\#\{E \in \mathcal{F}'_{d,n}(B) \mid E \text{ satisface el principio de Hasse}\}}{\#\mathcal{F}'_{d,n}(B)}.$$

El teorema 3.9 dice entonces que, para $n \geq d$ con $(n,d) \neq (3,3)$, la proporción $\rho_{d,n}$ es igual a 1. Se conjetura que el resultado es también cierto para $(n,d) = (3,3)$, pero este caso sigue abierto por ahora.

Todos los resultados anteriores se inscriben en una importante conjetura que fue formulada por Colliot-Thélène en 1990 y que sigue abierta. Como vamos a ver, la conjetura no cubre únicamente el caso del cuerpo de los números racionales, sino que también se aplica a todos los cuerpos de números.

Conjetura 3.10 (Colliot-Thélène). *Sea K un cuerpo de números. Dados dos enteros n y d tales que $n \geq d$ y $(n,d) \neq (3,3)$, las ecuaciones polinomiales homogéneas de grado d con coeficientes en K en $n+1$ variables que definen una variedad proyectiva compleja no singular satisfacen el principio de Hasse. En otras palabras, dada una ecuación que satisface las condiciones anteriores, si tiene soluciones no nulas en todos los cuerpos que se pueden obtener por compleción a partir de K, entonces tiene soluciones no nulas en K.*

El enunciado análogo es falso para $(n,d) = (3,3)$. Por ejemplo, la ecuación cúbica

$$5x^3 + 9y^3 + 10z^3 + 12t^3 = 0$$

estudiada por Cassels y Guy en 1966 tiene soluciones no nulas en $\mathbb{R}$ y en todos los $\mathbb{Q}_p$, pero no en $\mathbb{Q}$, pese a que la variedad proyectiva compleja definida por la ecuación no es singular. Aún así, se puede también formular una conjetura en este caso, sustituyendo el principio de Hasse por una noción más fina y mucho menos elemental, la llamada *obstrucción de Brauer-Manin*.

3.4. Cero-ciclos de grado 1

La conjetura de Colliot-Thélène del párrafo anterior trata sobre las ecuaciones homogéneas de grado menor que el número de variables, así que es, en cierto modo, un sustituto a la propiedad C_1 para los cuerpos de números. Pero dichos cuerpos, cuando no se pueden ver como subcuerpos de $\mathbb{R}$, tienen dimensión cohomológica 2, así que sería también natural hallar un sustituto para la propiedad C_2. Kato y Kuzumaki propusieron una forma de hacerlo en el año 1986. Para explicar su idea, conviene introducir la definición siguiente, que permite debilitar la noción de «solución de una ecuación algebraica»:

Definición 3.11. Sea $f = 0$ una ecuación polinomial homogénea con coeficientes en un cuerpo K. Decimos que la ecuación tiene un *cero-ciclo de grado* 1 si existen extensiones finitas $K_1, \ldots, K_r$ de K tales que:

(i) Las dimensiones de $K_1, \ldots, K_r$ como K-espacios vectoriales son primas entre sí;

(ii) la ecuación $f = 0$ tiene soluciones no nulas en cada uno de los K_i.

En particular, si una ecuación $f = 0$ tiene una solución no nula en el cuerpo K, entonces tiene un cero-ciclo de grado 1. Kato y Kuzumaki conjeturan que, para aquellos cuerpos de números que no se pueden ver como subcuerpos de $\mathbb{R}$, se debería poder sustituir la existencia de soluciones por la existencia de cero-ciclos de grado 1 en la propiedad C_2:

Conjetura 3.12 (Kato-Kuzumaki [22]). *Sean K un cuerpo de números que no es isomorfo a un subcuerpo de $\mathbb{R}$ y $f(X_0, \ldots, X_n) \in K[X_0, \ldots, X_n]$ un polinomio homogéneo de grado d con $n \geq d^2$. Entonces la ecuación $f = 0$ tiene un cero-ciclo de grado* 1.

Esta conjetura sigue totalmente abierta a día de hoy. El lector interesado podrá consultar [32], [20] y [21] para algunos desarrollos recientes.

4. Cuerpos C_i y geometría

Vamos a terminar este artículo indagando en los vínculos entre las propiedades C_i de Artin y Lang y la geometría. Para ello, partimos de una pregunta muy natural: sabemos que, sobre un cuerpo con la propiedad C_i, las ecuaciones homogéneas con muchas variables y pequeño grado tienen soluciones no nulas, pero ¿qué ocurre si consideramos sistemas de ecuaciones? Más precisamente, dado un sistema de ecuaciones polinomiales homogéneas

$$\begin{cases} f_1(x_0, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_0, \ldots, x_n) = 0, \end{cases} \tag{8}$$

sobre un cuerpo C_i, ¿tiene automáticamente soluciones no nulas cuando los grados de $f_1, \ldots, f_m$ son pequeños en comparación con n?

Esta pregunta es más complicada de lo que pueda parecer a primera vista. Se conjetura el resultado siguiente:

Conjetura 4.1. *Sean i un entero no negativo y K un cuerpo con la propiedad C_i. Démonos m polinomios homogéneos $f_1, \dots, f_m \in K[X_0, \dots, X_n]$ y sean $d_1, \dots, d_m$ sus grados respectivos. Si $d_1^i + \cdots + d_m^i \leq n$, entonces el sistema* (8) *tiene al menos una solución no nula en el cuerpo K.*

Se sabe que esta conjetura es cierta en el caso $d_1 = \cdots = d_m$, gracias a un teorema de Artin-Lang-Nagata [26], o cuando, para todo $d > 1$, existe una ecuación polinomial homogénea con coeficientes en K, de grado d y con d^i variables que no tiene soluciones no nulas (Lang [24]). Esta segunda condición se comprueba en muchas situaciones, por ejemplo si K es el cuerpo de fracciones racionales $k(X_1, \dots, X_r)$ para algún $r \geq 0$ y algún cuerpo k finito o algebraicamente cerrado. Pese a ello, la conjetura 4.1 sigue totalmente abierta a día de hoy. Esto nos lleva, naturalmente, a buscar otras formas de generalizar las propiedades C_i a los sistemas de ecuaciones.

Como ya hicimos en la sección 3, si el cuerpo K sobre el que trabajamos es un subcuerpo de los números complejos, el sistema de ecuaciones (8) define una variedad proyectiva compleja, y entonces podríamos preguntarnos qué propiedades geométricas de dicha variedad garantizarían que el sistema tuviese automáticamente soluciones en nuestro cuerpo K. A primera vista, no está claro cómo generalizar esta idea a todo cuerpo. Afortunadamente, uno dispone del lenguaje de la geometría algebraica, que permite ver en toda generalidad, sea cual sea el cuerpo K, el sistema de ecuaciones (8) como un objeto geométrico, una «variedad» sobre K. Así, al igual que las variedades complejas, este objeto puede tener diversas propiedades geométricas: por ejemplo, puede ser singular o no, puede ser conexo o no...

Dado un polinomio homogéneo $f \in K[X_0, \dots, X_n]$ de grado $\leq n$, la ecuación $f = 0$ define una variedad sobre K que tiene propiedades geométricas muy fuertes. Es lo que se llama una *variedad racionalmente conexa*. No quiero entrar aquí en la definición precisa y técnica de esta noción (que uno puede encontrar, por ejemplo, en el artículo [31]), pero para dar una vaga idea, el lector se puede imaginar que una variedad es racionalmente conexa si por dos puntos cualesquiera pasa una recta contenida en la variedad.

Es entonces razonable formular la conjetura siguiente:

Conjetura 4.2. *Sean $f_1, \dots, f_m \in K[X_0, \dots, X_n]$ polinomios homogéneos con coeficientes en un cuerpo K con la propiedad C_1. Si el sistema* (8) *define una variedad racionalmente conexa no singular, entonces tiene soluciones no nulas en K.*

Esta conjetura es particularmente interesante, puesto que establece un vínculo fuerte entre dos mundos totalmente distintos: por un lado, el de las propiedades diofánticas de los cuerpos y por otro el de la geometría de las variedades algebraicas. Aunque a día de hoy la conjetura sigue totalmente abierta, sí hay algunos casos que han sido resueltos:

- El caso en el que la variedad es de dimensión ≤ 2 (Colliot-Thélène [11]);
- el caso en que el cuerpo estudiado K es un cuerpo finito (Esnault [16]);
- el caso en que K es $\mathbb{C}(T)$ o $\mathbb{C}((T))$ (Graber, Harris, Starr y de Jong, [17, 12]).

Sería, por supuesto, muy interesante hallar también vínculos entre la geometría y las propiedades C_i para $i \geq 2$, pero por ahora no está nada claro qué noción geométrica podría sustituir a la de «variedad racionalmente conexa».

Agradecimientos. Me gustaría dar las gracias a Javier Fresán por haberme propuesto escribir este artículo y por todas sus sugerencias que han permitido mejorarlo sustancialmente.

Referencias

[1] Y. Alemu, On zeros of forms over local fields, *Acta Arith.* **45** (1985), no. 2, 163–171.

[2] G. I. Arkhipov y A. A. Karatsuba, On local representation of zero by a form, *Izv. Akad. Nauk SSSR Ser. Mat.* **45** (1981), no. 5, 948–961, en ruso; traducido al inglés en *Math. USSR-Izv.* **19** (1982), no. 2, 231–240.

[3] E. Artin, *The collected papers of Emil Artin*, editado por S. Lang y J. Tate, Addison-Wesley, Reading, MA, y London, 1965.

[4] J. Ax, Proof of some conjectures on cohomological dimension, *Proc. Amer. Math. Soc.* **16** (1965), 1214–1221.

[5] J. Ax y S. Kochen, Diophantine problems over local fields. I, *Amer. J. Math.* **87** (1965), 605–630.

[6] B. J. Birch, Forms in many variables, *Proc. Roy. Soc. London Ser. A* **265** (1961/62), 245–263.

[7] J. Browkin, On forms over p-adic fields, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **14** (1966), 489–492.

[8] S. S. Brown, Bounds on transfer principles for algebraically closed and complete discretely valued fields, *Mem. Amer. Math. Soc.* **15** (1978), no. 204.

[9] T. Browning, P. Le Boudec y W. Sawin, The Hasse principle for random Fano hypersurfaces, *prepublicación*, `https://arxiv.org/abs/2006.02356`.

[10] C. Chevalley, Démonstration d'une hypothèse de M. Artin, *Abh. Math. Sem. Univ. Hamburg* **11** (1935), no. 1, 73–75.

[11] J.-L. Colliot-Thélène, Arithmétique des variétés rationnelles et problèmes birationnels, *Proceedings of the International Congress of Mathematicians* (Berkeley, Calif., 1986), Vol. 1, 641–653, Amer. Math. Soc., Providence, RI, 1987.

[12] A. J. de Jong y J. Starr, Every rationally connected variety over the function field of a curve has a rational point, *Amer. J. Math.* **125** (2003), no. 3, 567–580.

[13] V. B. Demjanov, On cubic forms in discretely normed fields, *Doklady Akad. Nauk SSSR (N.S.)* **74** (1950), 889–891.

[14] J. Denef, Geometric proofs of theorems of Ax-Kochen and Eršov, *Amer. J. Math.* **138** (2016), no. 1, 181–199.

[15] J. Denef, Proof of a conjecture of Colliot-Thélène and a diophantine excision theorem, *Algebra Number Theory* **13** (2019), no. 9, 1983–1996.

[16] H. Esnault, Varieties over a finite field with trivial Chow group of 0-cycles have a rational point, *Invent. Math.* **151** (2003), no. 1, 187–191.

[17] T. Graber, J. Harris y J. Starr, Families of rationally connected varieties, *J. Amer. Math. Soc.* **16** (2003), no. 1, 57–67.

[18] M. J. Greenberg, Rational points in Henselian discrete valuation rings, *Inst. Hautes Études Sci. Publ. Math.* **31** (1966), 59–64.

[19] H. Hasse, Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, *J. Reine Angew. Math.* **153** (1924), 113–130.

[20] D. Izquierdo, On a conjecture of Kato and Kuzumaki, *Algebra Number Theory* **12** (2018), no. 2, 429–454.

[21] D. Izquierdo y G. Lucchini Arteche, Homogeneous spaces, algebraic K-theory and cohomological dimension of fields, *J. Eur. Math. Soc. (JEMS)*, aceptado, `https://arxiv.org/abs/1812.04668`.

[22] K. Kato y T. Kuzumaki, The dimension of fields and algebraic K-theory, *J. Number Theory* **24** (1986), no. 2, 229–244.

[23] D. Krashen y E. Matzri, Diophantine and cohomological dimensions, *Proc. Amer. Math. Soc.* **143** (2015), no. 7, 2779–2788.

[24] S. Lang, On quasi algebraic closure, *Ann. of Math.* **55** (1952), 373–390.

[25] D. J. Lewis, Cubic homogeneous polynomials over p-adic number fields, *Ann. of Math.* **56** (1952), 473–478.

[26] M. Nagata, Note on a paper of Lang concerning quasi algebraic closure, *Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math.* **30** (1957), 237–241.

[27] J.-P. Serre, *Galois cohomology*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1997.

[28] A. Suslin y S. Joukhovitski, Norm varieties, *J. Pure Appl. Algebra* **206** (2006), no. 1-2, 245–276.

[29] G. Terjanian, Un contre-exemple à une conjecture d'Artin, *C. R. Acad. Sci. Paris Sér. A-B* **262** (1966), A612.

[30] E. Warning, Bemerkung zur vorstehenden Arbeit von Herrn Chevalley, *Abh. Math. Sem. Univ. Hamburg* **11** (1935), 76–83.

[31] O. Wittenberg, La connexité rationnelle en arithmétique, *Variétés rationnellement connexes: aspects géométriques et arithmétiques*, 61–114, Panor. Synthèses **31**, Soc. Math. France, Paris, 2010.

[32] O. Wittenberg, Sur une conjecture de Kato et Kuzumaki concernant les hypersurfaces de Fano, *Duke Math. J.* **164** (2015), no. 11, 2185–2211.

Diego Izquierdo, CMLS, École polytechnique, F-91128 Palaiseau Cedex, Francia
Correo electrónico: `diego.izquierdo@polytechnique.edu`
Página web: `https://perso.pages.math.cnrs.fr/users/diego.izquierdo/`