EL NIVEL DE UN CUERPO

¿O CUÁNDO -1 ES SUMA DE CUADRADOS?

JOSÉ CUEVAS BARRIENTOS

RESUMEN. En ésta presentación exponemos un invariante de los cuerpos, denominado el *nivel* y veremos que los valores que toma corresponden exactamente a las potencias de 2. Ésto también se vincula con identidades de sumas de cuadrados.

1. Los teoremas de Pfister

Definición 1.1: Se le llama el *nivel* (alemán, *Stufe*) de un cuerpo k, denotado $s(k)$, al mínimo n tal que existen $a_1, \ldots, a_n \in k$ tales que

$$a_1^2 + \cdots + a_n^2 = -1.$$

Se define $s(k) = \infty$ si no existe tal n (en cuyo caso, k es llamado un *cuerpo formalmente real* [**2,** Teo. 1.8, pág. 4]).

Ejemplo:
- $s(\mathbb{Q}) = s(\mathbb{R}) = \infty$.
- $s(k) = 1$ syss $\sqrt{-1} \in k$. En particular, $s(\mathbb{Q}(\sqrt{-1})) = s(\mathbb{C}) = 1$.
- $s(\mathbb{F}_p) = 1$ syss $p = 2$ o $p \equiv 1 \pmod 4$ por ley de reciprocidad cuadrática. En caso contrario, $s(\mathbb{F}_p) = 2$ (ejercicio).
- $s(\mathbb{Q}(\sqrt{-2})) = 2$ pues $-2 + 1 = -1$.
- $s(\mathbb{Q}(\sqrt{-3}))$ y $s(\mathbb{Q}(\sqrt{-11})) \leq 3$ pues $-3 + 1 + 1 = -11 + 9 + 1 = -1$. ¿Se alcanzará igualdad?

Algo útil será notar que si $s(k) = n$, entonces eso equivale a ver que

$$x_1^2 + \cdots + x_{n+1}^2 = 0$$

es la primera ecuación que tiene solución no trivial.

Recordemos la famosa identidad:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2, \tag{1}$$

conocida desde la Antigua Grecia. Ésto nos dice que las sumas de dos cuadrados forman una especie de grupo multiplicativo (hay que eliminar al 0 para que se cumpla). Parte de nuestra travesía consiste en estudiar para qué sumas de n cuadrados hay leyes multiplicativas de dicho estilo:

Date: 30 de septiembre de 2022.

Teorema 1.2: Sea k un cuerpo arbitrario y sea $n = 2^m$. Entonces existen identidades de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \tag{2}$$

donde:

$$z_j = \sum_{i=1}^{n} t_{ij} y_j, \qquad t_{ij} \in k(x_1, \ldots, x_n).$$

DEMOSTRACIÓN: Lo haremos por inducción sobre m. El caso base $m = 1$ corresponde a (1). Supongamos que aplica para m, y por tanto la identidad (2) es válida para $n = 2^m$. Denotando $T := [t_{ij}]_{ij}$, entonces se reescribe como

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = T \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Empleando productos internos podemos reescribir la identidad como

$$\begin{aligned}(x_1^2 + \cdots + x_n^2)(y_1, \ldots, y_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} &= (z_1, \ldots, z_n) \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \\ &= (y_1, \ldots, y_n) t^t t \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.\end{aligned}$$

Reordenando los términos equivale a que

$$\begin{aligned}(y_1, \ldots, y_n)\big((x_1^2 + \cdots + x_n^2) I_n - T^t T\big) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0, \\ (x_1^2 + \cdots + x_n^2) I_n = T^t T.\end{aligned}$$

Ahora, queremos ver que éste es el caso para $m+1$ y, por ende, para $2n$. Sea

$$\big((x_1, \ldots, x_n), (x_{n+1}, \ldots, x_{2n})\big) = (\boldsymbol{X}_1, \boldsymbol{X}_n).$$

Por hipótesis inductiva existen T_1, T_2 tales que:

$$\begin{aligned}(x_1^2 + \cdots + x_n^2) I_n = \boldsymbol{X}_1 \boldsymbol{X}_1^t I_n = T_1 T_1^t = T_1^t T_1, \\ (x_{n+1}^2 + \cdots + x_{2n}^2) I_n = \boldsymbol{X}_2 \boldsymbol{X}_2^t I_n = T_2 T_2^t = T_2^t T_2.\end{aligned}$$

Queremos encontrar un T que funcione para ambas matrices en simultáneo. Sea $T := \left(\begin{smallmatrix} T_1 & T_2 \\ T_2 & M \end{smallmatrix}\right)$, entonces se tiene que

$$\begin{aligned}T^t T &= \begin{bmatrix} T_1^t T_1 + T_2^t T_2 & T_1^t T_2 + T_2^t M \\ T_2^t T_1 + M^t T_2 & T_2^t T_2 + M^t X \end{bmatrix} \\ &= \begin{bmatrix} (x_1^2 + \cdots + x_{2n}^2) I_n & A \\ B & C \end{bmatrix}.\end{aligned}$$

Y queremos elegir a M de modo que $A = B = 0$ y $C = (x_1^2 + \cdots + x_{2n}^2)I_n$. Para forzar las primeras dos condiciones elegimos $M = -(T_2^t)^{-1}T_1^{-1}T_2$ (¿por qué?), pero milagrosamente también satisface la tercera condición:

$$\begin{aligned} C = T_2^t T_2 + M^t M &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + T_2^t T_1 T_2^{-1}(T_2^t)^{-1}T_1^t T_2 \\ &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + (x_{n+1}^2 + \cdots + x_{2n}^2)^{-1}T_2^t T_1 T_1^t T_2 \\ &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + (x_1^2 + \cdots + x_n^2)I_n. \end{aligned}$$

Ésto completa la demostración. □

Varios corolarios:

Corolario 1.3: Sea $\operatorname{car} k \neq 2$ y sea $f(x_1, \ldots, x_m) \in k(x_1, \ldots, x_m)$ una suma de n cuadrados. Sean $a_1, \ldots, a_m \in k$ tales que $f(a_1, \ldots, a_m)$ está bien definido (el denominador no es cero), entonces $f(a_1, \ldots, a_m)$ es una suma de n cuadrados.

Corolario 1.4: Sea k un cuerpo arbitrario. Denotemos por $G_n(k)$ a los elementos no nulos que se pueden escribir con n cuadrados, donde n es una potencia de 2. Entonces $G_n(k)$ es un grupo con la multiplicación.

Demostración: Ésto sale del teorema 1.2. Para los inversos:

$$\beta := \sum_{i=1}^{n} a_i^2 \in G_n(k) \implies \beta^{-1} = \frac{\beta}{\beta^2} = \sum_{i=1}^{n} \left(\frac{a_i}{\beta}\right)^2 \in G_n(k). \qquad \square$$

Lema 1.5 (Cassels): Sea $f(x) \in k[x] \subseteq k(x)$. Si $f(x)$ es una suma de n cuadrados en $k(x)$, entonces también es una suma de n cuadrados en $k[x]$.

Demostración: Veamos un par de casos aislados:

(a) Si $n = 1$, entonces es trivial.
(b) Si $\operatorname{car} k = 2$, entonces como $a^2 + b^2 = (a + b)^2$ se nota que se reduce al caso $n = 1$.
(c) Si $\operatorname{car} k \neq 2$ y $s(k) < n$, entonces digamos que $-1 = b_1^2 + \cdots + b_{n-1}^2$ con $b_i \in k$. Luego, nótese que

$$\begin{aligned} f(x) &= \left(\frac{f+1}{2}\right)^2 - \left(\frac{f-1}{2}\right)^2 \\ &= \left(\frac{f+1}{2}\right)^2 + \left(b_1 \cdot \frac{f-1}{2}\right)^2 + \cdots + \left(b_{n-1} \cdot \frac{f-1}{2}\right)^2. \end{aligned}$$

Si ninguno de los casos previos se da, entonces sea

$$f(x) = (p_1/q_1)^2 + \cdots + (p_n/q_n)^2 \in k(x),$$

luego, limpiando denominadores tenemos la ecuación

$$f \cdot h^2 = g_1^2 + \cdots + g_n^2, \qquad g_1, \ldots, g_n, h \in k[x], h \neq 0.$$

Es decir, la ecuación $f \cdot Z^2 = Y_1^2 + \cdots + Y_n^2$ tiene alguna solución no trivial $Z \neq 0$ en $k[x]$, queremos ver que posee alguna solución no trivial en k y para ello, elegiremos $(\zeta, \eta_1, \ldots, \eta_n)$ una solución con $\deg \zeta$ minimal.

Por contradicción supongamos que $\deg \zeta > 0$. Por algoritmo de la división (sobre $k[x]$) sea $\eta_j = \lambda_j \zeta + \gamma_j$ para todo j, donde γ_j es o bien nulo, o bien $\deg \gamma_j < \deg \zeta$. Nótese que, por minimalidad de ζ, existe algún j tal que $\gamma_j \neq 0$. Definamos

$$\alpha := \sum_{i=1}^n \lambda_i^2 - f, \qquad \beta := \sum_{i=1}^n \lambda_i \eta_i - f\zeta,$$
$$\bar{\zeta} := \alpha\zeta - 2\beta, \qquad \bar{\eta}_j := \alpha\eta_j - 2\beta\lambda_j.$$

Es claro que ambos son polinomios en $k[x]$.

(I) $\underline{(\bar{\zeta}, \bar{\eta}_1, \ldots, \bar{\eta}_n) \text{ es solución:}}$ Ésto es un cálculo. Puede reducirse a probar que $\sum_{j=1}^n \bar{\eta}_j^2 = f\bar{\zeta}^2$, ésto nos queda como

$$\sum_{j=1}^n (\alpha^2\eta_j^2 - 4\alpha\beta\eta_j\lambda_j + 4\beta^2\lambda_j^2) = (\alpha^2\zeta^2 - 4\alpha\beta\zeta + 4\beta^2)f.$$

Reordenando términos, factorizando el 4β común y expandiendo la definición de α, β se reduce a probar que

$$4\beta \cdot \left(\left(\sum_{i=1}^n \lambda_i\eta_i - f\zeta \right) \sum_{j=1}^n \lambda_j^2 - \left(\sum_{i=1}^n \lambda_i^2 - f \right) \sum_{j=1}^n \eta_j\lambda_j \right.$$
$$\left. - \left(\sum_{j=1}^n \lambda_j\eta_j - f\zeta \right) f + \left(\sum_{i=1}^n \lambda_i^2 - f \right) f\zeta \right) = 0.$$

(II) $\underline{\bar{\zeta} \neq 0:}$ Comenzamos por definir $\Lambda_j := \gamma_j/\zeta = \eta_j/\zeta - \lambda_j \in k(x)$. Luego tenemos que

$$\bar{\zeta} = \left(\sum_{j=1}^n \left(\frac{\eta_j^2}{\zeta^2} - \frac{2\eta_j\Lambda_j}{\zeta} + \Lambda_j^2 \right) - f \right) \zeta - 2 \left(\sum_{j=1}^n \left(\frac{\eta_j}{\zeta} - \Lambda_j \right) \eta_j - f\zeta \right)$$
$$= (\Lambda_1^2 + \cdots + \Lambda_n^2)\zeta = \frac{1}{\zeta} \sum_{j=1}^n \gamma_j^2.$$

Como $s(k) \geq n$, mirando el mayor coeficiente de γ_j^2 concluimos que la suma es no nula.

(III) $\underline{\deg(\bar{\zeta}) < \deg \zeta:}$ Por la última igualdad tenemos que $\zeta \cdot \bar{\zeta} = \sum_{j=1}^n \gamma_j^2$, de modo que $\deg \zeta + \deg \bar{\zeta} = 2 \operatorname{máx}_j(\gamma_j) < 2 \deg \zeta$ (puesto que $\deg \gamma_j < \deg \zeta$ para todo j), de modo que $\deg(\bar{\zeta}) < \deg \zeta$.

Ésto contradice la minimalidad del grado de ζ lo que es absurdo. □

Corolario 1.6: Sea $\operatorname{car} k \neq 2$ y sea $d \in k$. El polinomio $x^2 + d \in k[x]$ es una suma de n cuadrados en $k(x)$ (y por lema de Cassels en $k[x]$) syss -1 o d son sumas de $n-1$ cuadrados en k.

DEMOSTRACIÓN: $\Longleftarrow$ es claro. Veamos $\Longrightarrow$: Sea $x^2 + d = p_1(x)^2 + \cdots + p_n(x)^2$ con $p_i(x) \in k[x]$ de grado ≤ 1. Luego $p_i = a_i x + b_i$ y tenemos

$$x^2 + d = (a_1 x + b_1)^2 + \cdots + (a_n x + b_n)^2,$$

nótese que si $\operatorname{car} k \neq 2$, entonces para algún j se cumple que la ecuación $C = \pm(a_j C + b_j)$ posee solución (separar por casos si $a_j = 1$ o no). Luego podemos reordenar los términos de modo que $C = \pm p_n(C)$ y evaluando en $x = C$ se obtiene

$$\cancel{C^2} + d = (a_1 C + b_1)^2 + \cdots + (a_{n-1} C + b_{n-1})^2 + \cancel{C^2},$$

con lo que comprobamos que d se escribe como suma de $n-1$ cuadrados. □

Corolario 1.7: Considere $\mathbb{R}(x_1, \ldots, x_n)$, aquí $x_1^2 + \cdots + x_n^2$ no es una suma de $n-1$ cuadrados.

PISTA: Aplicar inducción y definir $k := \mathbb{R}(x_1, \ldots, x_n)$ de modo que $k(x_{n+1}) = \mathbb{R}(x_1, \ldots, x_{n+1})$. □

Teorema 1.8: Sea k un cuerpo no formalmente real. Entonces $s(k)$ es una potencia de 2. Recíprocamente, dada la potencia 2^m existe un cuerpo k tal que $s(k) = 2^m$.

DEMOSTRACIÓN:

(I) Los niveles son potencias de 2: Nótese que siempre existe m tal que

$$n := 2^m \leq s(k) < 2^{m+1} = 2n.$$

Así pues, sea $a_1^2 + \cdots + a_n^2 + a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1 = 0$ para algunos $a_i \in k$ (posiblemente nulos). Sean

$$A := a_1^2 + \cdots + a_n^2, \qquad B := a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1,$$

Como $s(k) \geq n$ entonces podemos elegir los a_i's de modo que $A \neq 0 \neq B$ y la condición se traduce en que $A + B = 0$, o equivalentemente, $A = -B$. Por definición $A, B \in G_n(k)$, de modo que $A/B = -1 \in G_n(k)$, por ser grupo multiplicativo, luego -1 se escribe como una suma de n cuadrados y $s(k) \leq n$. Por antisimetría del $\leq$, $s(k) = n$ como se quería probar.

(II) Las potencias de 2 son niveles: El caso $n = 1$ es conocido (e.g., $s(\mathbb{C}) = 1$). Sea $n = 2^m > 1$ y sean $k := \mathbb{R}(x_1, \ldots, x_{n+1})$ y $L := k(\gamma)$, donde los x_i's son indeterminadas (elementos trascendentes algebraicamente independientes) y γ es raíz del polinomio:

$$\gamma^2 + x_1^2 + \cdots + x_{n+1}^2 = 0,$$

dividiendo por γ^2 se concluye que $s(L) \leq n+1$ y por ende $s(L) \leq n$ puesto que tiene que ser una potencia de 2.

Si $s(L) < n$, entonces existen $t_1, \ldots, t_n \in L$ tales que

$$t_1^2 + \cdots + t_n^2 = 0.$$

Como L/k es una extensión de grado 2, entonces cada $t_i = \alpha_i\gamma + \beta_i$. Luego, la igualdad superior se reescribe como

$$\left(\gamma^2 \cdot \sum_{i=1}^{n} \alpha_i^2 + \sum_{i=1}^{n} \beta_i^2\right) + 2\gamma \sum_{i=1}^{n} \alpha_i\beta_i = 0.$$

Como k es formalmente real, entonces algún α_i es no nulo, y análogamente se puede ver que algún β_i es no nulo. Enfocándonos en el primer paréntesis, nos queda que

$$-\gamma^2 = x_1^2 + \cdots + x_{n+1}^2 = \frac{\sum_{i=1}^{n} \beta_i^2}{\sum_{i=1}^{n} \alpha_i^2} \in G_n(k),$$

puesto que $G_n(k)$ es un grupo bajo multiplicación. Pero ésto contradice el corolario anterior. En conclusión, se cumple que $n = s(L)$ como se quería probar. □

Ahora también podemos probar un recíproco del teorema 1.2:

Teorema 1.9: Sea n un número que no es potencia de 2. Entonces existe un cuerpo k en donde no se satisface una identidad de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2,$$

donde:

$$z_j = \sum_{i=1}^{n} t_{ij}y_j, \qquad t_{ij} \in k(x_1, \ldots, x_n).$$

Demostración: Sea m tal que $2^{m-1} < n < 2^m$ y sea k un cuerpo tal que $s(k) = 2^m$. Luego podemos elegir $a_i \in k$ tales que

$$a_1^2 + \cdots + a_n^2 + a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1 = 0,$$

puesto que $2n > s(k)$ y definir $A := a_1^2 + \cdots + a_n^2$ y $B := a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1$ notando que son no nulos. Si existiese una identidad de ese estilo, entonces se comprobaría que $G_n(k)$ es un grupo con la multiplicación y así $-1 = A/B \in G_n(k)$, pero ésto es absurdo puesto que $n < s(k)$. □

2. Comentarios adicionales

Recuerde la fórmula (2) con la que empezamos. En el teorema 1.2 dejamos que los z_j's sean polinomiales en los x_i's, pero la identidad (1) es de hecho lineal en los x_i's y sin término libre, de modo que es, de hecho, bilineal en sus coordenadas. Podemos hacernos la pregunta de para qué n's hay identidades de ese estilo y notaremos que éstos deben ser también potencias

de 2, pero podrían ser menos y, de hecho, sólo existen dichas identidades para $n \in \{1, 2, 4, 8\}$. Ésto se conoce como el *problema de Hurwitz* y la resolvió en 1898. Una curiosidad es que el problema de Hurwitz está intrínsecamente relacionada a las $\mathbb{R}$-álgebras de división finitamente generadas:

Dimensión	$\mathbb{R}$-álgebra	Nombres	
1	$\mathbb{R}$	Reales	—
2	$\mathbb{C}$	Complejos	—
4	$\mathbb{H}$	Cuaterniones	Hamilton, 1843
8	$\mathbb{O}$	Octoniones	Degan-Cayley, 1844-1845

Otra curiosidad es que empleando el corolario 1.7 podemos probar que el cuerpo $\mathbb{R}(x_1, x_2, x_3, \dots)$, el cual es formalmente real, posee una cualidad bien peculiar: el conjunto de sus elementos totalmente positivos[1] no es diofántico,[2] contrario a lo que sucedía con $\mathbb{Q}$, debido a que $x_1 + \cdots + x_n^2$ requiere al menos n sumandos.

Por último, cabe destacar que todos nuestros ejemplos de cuerpos de nivel alto estaban relacionados con los cuerpos de fracciones polinomiales o, dicho de otra manera, poseían altos grados de trascendencia. Es una pregunta abierta el verificar que éste sea el caso en general.

Los dos ejemplos que no alcanzaban igualdad pueden admitir como solución:

$$\left(\frac{1+\sqrt{-3}}{2}\right)^2 + \left(\frac{1-\sqrt{-3}}{2}\right)^2 = \left(\frac{3+\sqrt{-11}}{2}\right)^2 + \left(\frac{3-\sqrt{-11}}{2}\right)^2 = -1.$$

Referencias

1. Jacobson, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
2. Prestel, A. *Lectures on Formally Real Fields* (American Mathematical Society, 1975).
3. Rajwade, A. R. *Squares* (Cambridge University Press, 1993).

Email address: josecuevasbtos@uc.cl

[1] Un elemento de un cuerpo formalmente real R se dice *totalmente positivo* si es positivo en todo ordenamiento admisible con las propiedades de anillo sobre R. En particular, uno puede probar que los elementos totalmente positivos son exactamente aquellos que son sumas de cuadrados (cf. [**2,** Cor. 1.9, pág. 4]).

[2] Un conjunto $X \subseteq A^n$, donde A es un anillo, se dice *diofántico* si corresponde a las soluciones de varios polinomios, donde algunas variables pueden estar ligadas por un cuantificador existencial.