Suma de Cuadrados en un Cuerpo

Ignacio Ibarra Duhalde

1. Nivel y número de Pitágoras

Sea R un anillo conmutativo unitario. Denotamos por $char(R)$ la característica de R, por[1] $R^\times$ el grupo multiplicativo de R y por[2] $R^{\times 2} \leq R^\times$ el subgrupo de cuadrados no nulos en R. Veamos algunos ejemplos con anillos conocidos.

Ejemplo 1.1. Calculamos $\mathbf{R}^\times$ y $\mathbf{R}^{\times 2}$ para distintos anillos $\mathbf{R}$.

- $\mathbf{Z}^\times = \{1, -1\}$ y $\mathbf{Z}^{\times 2} = \{1\}$
- $\mathbf{R}^\times = \mathbf{R} \setminus \{0\}$ y $\mathbf{R}^{\times 2} = \{x^2 | x \in \mathbf{R}^\times\} = (0, +\infty)$
- $\mathbf{C}^\times = \mathbf{C} \setminus \{0\}$ y $\mathbf{C}^{\times 2} = \{x^2 | x \in \mathbf{C}^\times\} = \mathbf{C}^\times$ pues $\mathbf{C}$ es algebraicamente cerrado.
- $\left(\frac{\mathbf{Z}}{8\mathbf{Z}}\right)^\times = \{1, 3, 5, 7\}$ y $\left(\frac{\mathbf{Z}}{8\mathbf{Z}}\right)^{\times 2} = \{1\}$. Aquí tenemos un caso donde el polinomio $x^2 - 1$ con coeficientes en el anillo $\frac{\mathbf{Z}}{8\mathbf{Z}}$ tiene más de dos soluciones, pues $1^2 = 3^2 = 5^2 = 7^2 = 1$. En $\frac{\mathbf{Z}}{12\mathbf{Z}}$ ocurre algo similar.
- $\left(\frac{\mathbf{Z}}{9\mathbf{Z}}\right)^\times = \{1, 2, 4, 5, 7, 8\}$ y $\left(\frac{\mathbf{Z}}{9\mathbf{Z}}\right)^{\times 2} = \{1, 4, 7\}$. Aquí tenemos un caso donde el polinomio $x^2 - 1$ con coeficientes en el anillo $\frac{\mathbf{Z}}{8\mathbf{Z}}$ tiene exactamente dos soluciones, pues $1^2 = 8^2 = 1$ (note que $8 = -1$)
- Sea $\mathbf{F}$ un cuerpo finito. Entonces $\mathbf{F}^\times = \mathbf{F} \setminus \{0\} = \langle a \rangle$ con a no nulo de orden $|\mathbf{F}|$. Note que $\varphi : \mathbf{F}^\times \to \mathbf{F}^\times : x \mapsto x^2$ es homomorfismo de grupos. Luego $\mathbf{F}^{\times 2} = Im(\varphi) \cong \mathbf{F}^\times / ker(\varphi)$. Si $char(\mathbf{F}) = 2$, se sigue que φ es inyectiva y por ende un isomorfismo, luego $\mathbf{F}^\times = \mathbf{F}^{\times 2}$. Si $char(\mathbf{F}) \neq 2$, entonces $\mathbf{F}^{\times 2} \cong \mathbf{F}^\times / \{1, -1\}$ y así $|\mathbf{F}^{\times 2}| = \frac{|\mathbf{F}|-1}{2}$. Por ejemplo $\mathbf{F_7}^\times = \{1, 2, 3, 4, 5, 6\}$ y $\mathbf{F_7}^{\times 2} = \{1, 2, 4\} \cong \frac{\mathbf{Z}}{3\mathbf{Z}}$. Para $\mathbf{F_9} \cong \frac{\mathbf{F_3}[x]}{(x^2-x-1)} = \{\overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2}\}$, se tiene que $\mathbf{F_9}^{\times 2} \cong \left(\frac{\mathbf{F_3}[x]}{(x^2-x-1)}\right)^{\times 2} = \{\overline{1}, \overline{2}, \overline{x+1}, \overline{2x+2}\} \cong \frac{\mathbf{Z}}{4\mathbf{Z}}$.
- $\mathbf{Z}[\mathbf{i}]^\times = \{1, -1, i, -i\}$ y $\mathbf{Z}[\mathbf{i}]^{\times 2} = \{1, -1\}$.
- Sea $\mathbf{K}$ un cuerpo, entonces $\mathbf{K}[\mathbf{x}]^\times = \{p(x) | p \text{ constante no nula}\} \cong K^\times$ y $\mathbf{K}[\mathbf{x}]^{\times 2} \cong \mathbf{K}^{\times 2}$. Si cambiamos $\mathbf{K}$ por un anillo conmutativo unitario A, entonces la descripción de $\mathbf{K}[\mathbf{x}]^\times$ es más complicada [véase Atiyah-Macdonald, algebra conmutativa p.12 ejercicio 2(i)]

[1] $R^\times := U(R)$ el grupo de unidades o elementos invertibles de R.
[2] $R^{\times 2} := \{r^2 | r \in R^\times\}$, es decir, la imagen del homomorfismo de grupos $\mathbf{R}^\times \to \mathbf{R}^\times : r \mapsto r^2$.

Las definiciones anteriores no tienen sentido si R no es un anillo conmutativo, ya que existen anillos donde un elemento tiene neutro multiplicativo por un lado, pero no por el otro.

Para $n \in \mathbf{N}$ denotamos por $\sum_n R^2$ el conjunto de elementos de R que pueden ser escritos como suma de n cuadrados en R y $\sum R^2 := \bigcup_{n\in\mathbf{N}} \sum_n R^2$. Definimos el **nivel** y el **número de pitágoras** de R, denotados $s(R)$ y $p(R)$, respectivamente, como

$$s(R) = \text{ínf}\left\{ n \in \mathbf{N} \;\middle|\; -1 \in \sum_n R^2 \right\} \quad y \quad p(R) = \text{ínf}\left\{ n \in \mathbf{N} \;\middle|\; \sum R^2 = \sum_n R^2 \right\}$$

En caso de que no exista tal natural, decimos que $s(R) = p(R) = \infty$ y así los ínfimos toman valores en $\mathbf{N} \cup \{\infty\}$. Si $\mathbf{F}$ es un cuerpo finito, el **Lema** 2.1 implica que

$$p(\mathbf{F}) = \begin{cases} 1 & \text{si } char(\mathbf{F}) = 2, \\ 2 & \text{si } char(\mathbf{F}) \neq 2. \end{cases}$$

En particular si $char(\mathbf{F}) = 2$, tenemos $s(\mathbf{F}) = p(\mathbf{F}) = 1$. Estaremos especialmente interesados cuando $R = \mathbf{K}$ sea un cuerpo. Los dos lemas siguientes serán útiles para calcular $p(\mathbf{R}(x))$, el número de pitágoras del cuerpo de funciones racionales en una variable con coeficientes en $\mathbf{R}$. Recordamos que $f(x) \in \mathbf{R}[x]$ es no negativo si $f(x) \geq 0$ para todo $x \in \mathbf{R}$.

Con estos lemas, podemos probar que $p(\mathbf{R}(x)) = 2$. En efecto, consideremos $\sum_{i=1}^n (\frac{a_i}{b_i})^2 \in \mathbf{R}(x)$. Tenemos $\displaystyle\sum_{i=1}^n (\frac{a_i}{b_i})^2 = \frac{\sum_{i=1}^n c_i a_i^2}{(\prod_{i=1}^n b_i)^2}$, donde $c_i = \prod_{j\neq i}^n b_j^2$. Note tanto numerador como denominador son polinomios no negativos en $\mathbf{R}[x]$, luego $\sum_{i=1}^n (\frac{a_i}{b_i})^2 = \frac{A}{B^2}$ con $A = \sum_{i=1}^n c_i a_i^2$ y $B = \prod_{i=1}^n b_i$. El **lema** 2.2 implica que $A^2 = C^2 + D^2$ para ciertos $C, D \in \mathbf{R}[x]$. Entonces $\sum_{i=1}^n (\frac{a_i}{b_i})^2 = \frac{C^2+D^2}{B^2} = (\frac{C}{B})^2 + (\frac{D}{B})^2$ es una suma de dos cuadrados en $\mathbf{R}(x)$.

Note que -1 no es un cuadrado en $\mathbf{R}$ ni en $\mathbf{F_3}$, pero sí es un cuadrado en $\frac{\mathbf{R}[x]}{(x^2+1)} \cong \mathbf{C}$ y en $\frac{\mathbf{F_3}[x]}{(x^2-x-1)} \cong \mathbf{F_9}$. También note que $-1 = 2 = 1^2 + 1^2$ en $\mathbf{F_3}$. Aquí vemos que en ciertos cuerpos, podemos expresar -1 como un cuadrado o como suma de cuadrados (esto luego lo formalizaremos como el nivel de un anillo). Por otro lado, note que en los cuerpos $\mathbf{F_2}, \mathbf{F_3}, \mathbf{F_4}, \mathbf{F_5}, \mathbf{F_7}, \mathbf{F_9}, \mathbf{F_{11}}$,etc; todo elemento puede escribirse como suma de dos cuadrados (y en particular, cualquier suma finita de cuadrados en tales cuerpos siempre es una suma de dos cuadrados. Esto lo formalizaremos con el número de pitágoras de un anillo). Comencemos con un resultado básico pero interesante de los cuerpos finitos.

2. Resultados conocidos

Lema 2.1. *En un cuerpo finito, todo elemento es suma de dos cuadrados.*

Demostración. *Evidentemente* $0 = 0^2 + 0^2$*, así que nos interesamos por lo elementos no nulos. Sea* $\mathbf{F}$ *un cuerpo finito y* $char(\mathbf{F}) = p$*. Consideremos el homomorfismo de grupos abelianos* $\varphi : \mathbf{F}^\times \to \mathbf{F}^\times : x \mapsto x^2$*. Si* $p = 2$ *se sigue que* φ *es inyectiva y como* $\mathbf{F}$ *es finito, entonces es una biyección. Luego todo elemento no nulo es un cuadrado en* $\mathbf{F}$*. Si* $p \neq 2$*, entonces* $ker(\varphi) = \{1, -1\}$ *y* $\mathbf{F}^\times / ker(\varphi) \cong Im(\varphi)$ *con lo cual* $|Im(\varphi)| = \frac{|\mathbf{F}|-1}{2}$*. Note que* $A := Im(\varphi) \cup \{0\}$ *es el conjunto de todos los cuadrados de* $\mathbf{F}$ *y tiene cardinalidad* $|Im(\varphi)| + 1 = \frac{|\mathbf{F}|+1}{2}$*. Fijemos un elemento* $x \in \mathbf{F}^\times$*. Entonces el conjunto* $B := \{x - a | a \in A\}$ *tiene la misma cardinalidad que* A *(pues* $A \to B : a \mapsto x - a$ *es biyectiva). Tenemos que* $|A| + |B| = |\mathbf{F}| + 1 > |\mathbf{F}|$

y como A, B son subconjuntos de $\mathbf{F}$ ocurre que $A \cap B \neq \emptyset$. Luego existen $a, a' \in A$ tales que $a = x - a'$ y por ende $x = a + a'$ es una suma de dos cuadrados en $\mathbf{F}$. ■

Lema 2.2. *Sea $f(x) \in \mathbf{R}[x]$ no negativo. Si $a \in \mathbf{R}$ es una raíz de multiplicidad m de $f(x)$, entonces m es par.*

Demostración. *Tenemos $f(x) = (x-a)^m g(x)$ donde $g(x) \in \mathbf{R}[x]$ y $g(a) \neq 0$. Si $g(a) > 0$, la continuidad de g vista como funcion $\mathbf{R} \to \mathbf{R}$ implica que para $\epsilon = \frac{g(a)}{2} > 0$, existe $\delta > 0$ tal que $|x-a| < \delta \implies |g(x) - g(a)| < \frac{g(a)}{2}$, con lo cual $|x-a| < \delta \implies \frac{g(a)}{2} < g(x) < \frac{3g(a)}{2}$. Dicho de otro modo, para $\epsilon = \frac{g(a)}{2} > 0$, existe $\delta > 0$ tal que $|x-a| < \delta \Rightarrow g(x) \in (\epsilon, 3\epsilon)$. Esto significa que para valores x muy cercanos a a, el signo de $g(x)$ es positivo. En otras palabras, para $x \in (a-\delta, a+\delta)$ se tiene que $g(x) > 0$. El caso $g(a) < 0$ se hace igual, considerando $\epsilon = -\frac{g(a)}{2}$, y aquí obtenemos que para valores x cercanos a a, se tiene que $g(x)$ es negativo. Supongamos que m es impar y sin pérdida de generalidad, podemos suponer que existe un entorno $(a-\delta, a+\delta)$ de a tal que para todo $x \in (a-\delta, a+\delta)$ se tiene que $g(x) > 0$. Si $a - \delta < x < a$ entonces $f(x) = (x-a)^m g(x)$ es negativo, contradicción. Luego m es par.* ■

Lema 2.3. *Sea $f(x) \in \mathbf{R}[x]$ no negativo. Entonces $f(x)$ es una suma de dos cuadrados en $\mathbf{R}[x]$.*

Demostración. *Si $f(x)$ es el polinomio cero el resultado es obvio. Si $f(x)$ es una constante no nula, ésta debe ser positiva y el resultado es obvio. Supongamos que $f(x)$ es un polinomio no constante (de grado ≥ 1) y escribimos $f(x) = c\prod p_i(x)$ donde $c > 0$ y los $p_i(x) \in \mathbf{R}[x]$ son polinomios mónicos irreducibles. Notemos que el grado cada cada p_i es a lo más 2. Fijemos un $p_i \in \mathbf{R}[x] \subseteq \mathbf{C}[x]$, entonces $p_i(x) = (x-a_1)\cdots(x-a_k)$ para ciertos $a_k \in \mathbf{C}$. En particular si $\alpha \in \mathbf{C}$ es una raíz de p_i, también lo es su conjugado $\overline{\alpha} \in \mathbf{C}$. Entonces podemos reescribir*

$$\begin{aligned} p_i(x) &= (x-\alpha)(x-\overline{\alpha})(x-\beta)(x-\overline{\beta})\cdots \\ &= (x^2 - (\alpha+\overline{\alpha}) + |\alpha|^2)\cdot(x^2 - (\beta+\overline{\beta}) + |\beta|^2)\cdots \\ &= \underbrace{(x^2 - 2\Re(\alpha) + |\alpha|^2)}_{\in \mathbf{R}[x]} \cdot \underbrace{(x^2 - 2\Re(\beta) + |\beta|^2)}_{\in \mathbf{R}[x]}\cdots \end{aligned}$$

Si p_i tiene grado par, entonces es un producto de cuadráticas en $\mathbf{R}[x]$ y si es de grado impar es un producto de cuadráticas en $\mathbf{R}[x]$ y un factor lineal en $\mathbf{R}[x]$. Note que las cuadráticas pueden ser irreducibles o no en $\mathbf{R}[x]$. Por lo tanto podemos escribir $f(x) = c\prod_i (x-\alpha_i)^{m_i} \prod_j (x^2 + a_j x + b_j)^{n_j}$ en $\mathbf{R}[x]$, donde las cuadráticas son irreducibles. Note que

$$x^2 + a_j x + b_j = (x - \tfrac{a_j}{2})^2 + b_j - (\tfrac{a_j}{2})^2 = (x-\tfrac{a_j}{2})^2 + b_j - \tfrac{a_j^2}{4} = (x-\tfrac{a_j}{2})^2 + \left(\sqrt{b_j - \tfrac{a_j^2}{4}}\right)^2,$$

ya que el discriminante de la cuadrática es negativo. Luego $x^2 + a_j x + b_j = A_j^2 + B_j^2$ en $\mathbf{R}[X]$. Usando reiteradas veces la ***identidad de Brahmagupta-Fibonacci:*** $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$,

obtenemos que $\prod_j (x^2+a_jx+b_j)^{n_j}$ *es una suma de dos cuadrados en* $\mathbf{R}[x]$*, digamos* $\prod_j (x^2+a_jx+b_j)^{n_j} = A^2 + B^2$ *con* $A(x), B(x) \in \mathbf{R}[x]$*. Se sigue que*

$$f(x) = c\prod_i (x-\alpha_i)^{m_i}(A^2+B^2) = \prod_i (x-\alpha_i)^{m_i}[(\sqrt{c}A)^2 + (\sqrt{c}B)^2] = \prod_i (x-\alpha_i)^{m_i}(\tilde{A}^2+\tilde{B}^2)$$

Por otro lado, el ***lema*** *2.2 implica que cada* m_i *es par, digamos* $m_i = 2k_i$*. Tenemos que*

$$\prod_i (x-\alpha_i)^{m_i} = \prod_i (x-\alpha_i)^{2k_i} = \left(\prod_i (x-\alpha_i)^{k_i}\right)^2 = C^2$$

Finalmente, $f(x) = C^2(\tilde{A}^2+\tilde{B}^2) = (C\tilde{A})^2 + (C\tilde{B})^2$ *es una suma de cuadrados en* $\mathbf{R}[x]$*.* ■