Cuerpos de números y el teorema de las S-unidades

Raúl Segurado Herrera

Universidad Autónoma de Madrid

Julio de 2024

Anillo de enteros de un cuerpo de números

Anillo de enteros de un cuerpo de números

Definición

Un *cuerpo de números* K es una extensión finita $K/\mathbb{Q}$.

Anillo de enteros de un cuerpo de números

Definición

Un *cuerpo de números* K es una extensión finita $K/\mathbb{Q}$.

Anillo de enteros algebraicos:

$$\overline{\mathbb{Z}} = \{\alpha \in \mathbb{C} : f(\alpha) = 0 \text{ para algún } f \in \mathbb{Z}[x] \text{ mónico}\}.$$

Definición

El *anillo de enteros de* K es

$$\mathcal{O}_K = K \cap \overline{\mathbb{Z}}.$$

Anillo de enteros de un cuerpo de números

Definición

Un *cuerpo de números* K es una extensión finita $K/\mathbb{Q}$.

Anillo de enteros algebraicos:

$$\overline{\mathbb{Z}} = \{\alpha \in \mathbb{C} : f(\alpha) = 0 \text{ para algún } f \in \mathbb{Z}[x] \text{ mónico}\}.$$

Definición

El *anillo de enteros de* K es

$$\mathcal{O}_K = K \cap \overline{\mathbb{Z}}.$$

¿Cuál es la estructura de $\mathcal{O}_K^*$?

Teorema de las Unidades de Dirichlet

$[K : \mathbb{Q}] = n = r_1 + 2r_2$:

- $r_1 = \#$ inmersiones $K \to \mathbb{R}$.
- $r_2 = \#$ pares de inmersiones conjugadas $K \to \mathbb{C}$.

Teorema (Unidades de Dirichlet)

K cuerpo de números:

$$\mathcal{O}_K^* \cong W_K \times \mathbb{Z}^r, \quad r = r_1 + r_2 - 1,$$

con W_K el grupo de raíces de la unidad contenidas K.

Unidades de Dirichlet: idea de la demostración

Consideramos el hiperplano

$$H^r := \left\{ v = (v_1, \ldots, v_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : \sum_{i=1}^{r_1+r_2} v_i = 0 \right\}.$$

Existe un homomorfismo

$$l^{\#} : \mathcal{O}_K^* \to H^r$$

que cumple:

- $\ker l^{\#} = W_K$.
- $\operatorname{Im} l^{\#}$ es un retículo de H^r.

Ejemplo: cuerpos cuadráticos

$K_d = \mathbb{Q}(\sqrt{d})$, d libre de cuadrados.

Ejemplo: cuerpos cuadráticos

$K_d = \mathbb{Q}(\sqrt{d})$, d libre de cuadrados.

$$\mathrm{id} : \sqrt{d} \mapsto \sqrt{d}, \quad \sigma : \sqrt{d} \mapsto -\sqrt{d}$$

Ejemplo: cuerpos cuadráticos

$K_d = \mathbb{Q}(\sqrt{d})$, d libre de cuadrados.

$$\mathrm{id} : \sqrt{d} \mapsto \sqrt{d}, \quad \sigma : \sqrt{d} \mapsto -\sqrt{d}$$

- Si $d < 0$: $r_1 = 0, r_2 = 1$ y $\mathcal{O}_{K_d}^* = W_{K_d}$.

Ejemplo: cuerpos cuadráticos

$K_d = \mathbb{Q}(\sqrt{d})$, d libre de cuadrados.

$$\mathrm{id} : \sqrt{d} \mapsto \sqrt{d}, \quad \sigma : \sqrt{d} \mapsto -\sqrt{d}$$

- Si $d < 0$: $r_1 = 0, r_2 = 1$ y $\mathcal{O}_{K_d}^* = W_{K_d}$.
- Si $d > 0$: $r_1 = 2, r_2 = 0$ y $\mathcal{O}_{K_d}^* \cong W_{K_d} \times \mathbb{Z}$.

Ejemplo: cuerpos cuadráticos

$K_d = \mathbb{Q}(\sqrt{d})$, d libre de cuadrados.

$$\mathrm{id} : \sqrt{d} \mapsto \sqrt{d}, \quad \sigma : \sqrt{d} \mapsto -\sqrt{d}$$

- Si $d < 0$: $r_1 = 0, r_2 = 1$ y $\mathcal{O}_{K_d}^* = W_{K_d}$.
- Si $d > 0$: $r_1 = 2, r_2 = 0$ y $\mathcal{O}_{K_d}^* \cong W_{K_d} \times \mathbb{Z}$.

  De hecho, si $\mathcal{O}_{K_d} = \mathbb{Z}[\sqrt{d}]$, entonces las unidades vienen de la *ecuación de Pell*:

$$a^2 - db^2 = \pm 1.$$

Ejemplo: cuerpos cuadráticos

$K_d = \mathbb{Q}(\sqrt{d})$, d libre de cuadrados.

$$\mathrm{id} : \sqrt{d} \mapsto \sqrt{d}, \quad \sigma : \sqrt{d} \mapsto -\sqrt{d}$$

- Si $d < 0$: $r_1 = 0, r_2 = 1$ y $\mathcal{O}_{K_d}^* = W_{K_d}$.
- Si $d > 0$: $r_1 = 2, r_2 = 0$ y $\mathcal{O}_{K_d}^* \cong W_{K_d} \times \mathbb{Z}$.

  De hecho, si $\mathcal{O}_{K_d} = \mathbb{Z}[\sqrt{d}]$, entonces las unidades vienen de la *ecuación de Pell*:

  $$a^2 - db^2 = \pm 1.$$

  ¡Siempre que $d \not\equiv 1\,(4)$!

S-enteros y S-unidades en $\mathbb{Q}$

$S = \{p_1, p_2, \ldots, p_k\}$ colección finita de primos.

S-enteros y S-unidades en $\mathbb{Q}$

$S = \{p_1, p_2, \ldots, p_k\}$ colección finita de primos.

Definición

Sea $a/b \in \mathbb{Q}$ fracción irreducible:

- a/b es S-*entero* si b factoriza con los primos de S.
- a/b es S-*unidad* si a, b factorizan con los primos de S.

El anillo de S-enteros y el grupo de S-unidades son

$$\mathcal{O}_S = \mathbb{Z}[(p_1 p_2 \ldots p_k)^{-1}], \quad \mathcal{O}_S^* = \{\pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} : \alpha_j \in \mathbb{Z}\}.$$

S-enteros y S-unidades en $\mathbb{Q}$

$S = \{p_1, p_2, \ldots, p_k\}$ colección finita de primos.

Definición

Sea $a/b \in \mathbb{Q}$ fracción irreducible:

- a/b es *S-entero* si b factoriza con los primos de S.
- a/b es *S-unidad* si a, b factorizan con los primos de S.

El anillo de S-enteros y el grupo de S-unidades son

$$\mathcal{O}_S = \mathbb{Z}[(p_1 p_2 \ldots p_k)^{-1}], \quad \mathcal{O}_S^* = \{\pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} : \alpha_j \in \mathbb{Z}\}.$$

¿Cómo generalizamos esta idea en cuerpos de números?

S-enteros y S-unidades en K

Problema: no tenemos factorización única en $\mathcal{O}_K$.

S-enteros y S-unidades en K

Problema: no tenemos factorización única en $\mathcal{O}_K$.

Idea: utilizar la factorización única en ideales primos.

S-enteros y S-unidades en K

Problema: no tenemos factorización única en $\mathcal{O}_K$.

Idea: utilizar la factorización única en ideales primos.

Tomamos $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k : \mathfrak{p}_j \in \mathrm{Spec}(\mathcal{O}_K) \text{ no nulos}\}$.

S-enteros y S-unidades en K

Problema: no tenemos factorización única en $\mathcal{O}_K$.

Idea: utilizar la factorización única en ideales primos.

Tomamos $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k : \mathfrak{p}_j \in \mathrm{Spec}(\mathcal{O}_K) \text{ no nulos}\}$.

Definición

Sea $\alpha \in K$, escribimos $\alpha = x/y$ para $x, y \in \mathcal{O}_K$ (de hecho, podemos suponer $y \in \mathbb{Z}^+$):

- α es *S-entero* si, en la factorización de $(\alpha) = (x)(y)^{-1}$, las potencias negativas son de ideales primos de S.
- α es *S-unidad* si, en la factorización de $(\alpha) = (x)(y)^{-1}$, todas las potencias son de ideales primos de S.

Teorema de las S-unidades

Teorema de las S-unidades

Teorema (S-unidades)

La ecuación $x + y = 1$ tiene un número finito de soluciones con $x, y \in \mathcal{O}_S^*$.

Teorema de las S-unidades

Teorema (S-unidades)

La ecuación $x + y = 1$ tiene un número finito de soluciones con $x, y \in \mathcal{O}_S^*$.

Algunas observaciones:

- Válido para todo cuerpo de números K, y todo conjunto finito de ideales primos S.
- La prueba que veremos es no efectiva, no obtendremos una cota para el número de soluciones, solo su finitud.

Una aplicación a las ecuaciones diofánticas

Teorema

Sea $P \in \mathbb{Z}[x, y]$ homogéneo con algún factor irreducible de grado ≥ 3, entonces para $c \in \mathbb{Z}\backslash\{0\}$ la ecuación $P(x, y) = c$ tiene un número finito de soluciones enteras.

Una aplicación a las ecuaciones diofánticas

Teorema

Sea $P \in \mathbb{Z}[x, y]$ homogéneo con algún factor irreducible de grado ≥ 3, entonces para $c \in \mathbb{Z}\backslash\{0\}$ la ecuación $P(x, y) = c$ tiene un número finito de soluciones enteras.

Ejemplo

Para $n, d, c \in \mathbb{Z}^+$, sea $P(x, y) = x^n - dy^n$.

Una aplicación a las ecuaciones diofánticas

Teorema

Sea $P \in \mathbb{Z}[x, y]$ homogéneo con algún factor irreducible de grado ≥ 3, entonces para $c \in \mathbb{Z}\backslash\{0\}$ la ecuación $P(x, y) = c$ tiene un número finito de soluciones enteras.

Ejemplo

Para $n, d, c \in \mathbb{Z}^+$, sea $P(x, y) = x^n - dy^n$.

- Si $n \geq 3$, la ecuación

$$x^n - dy^n = c$$

tiene un número finito de soluciones enteras.

Una aplicación a las ecuaciones diofánticas

Teorema

Sea $P \in \mathbb{Z}[x, y]$ homogéneo con algún factor irreducible de grado ≥ 3, entonces para $c \in \mathbb{Z}\backslash\{0\}$ la ecuación $P(x, y) = c$ tiene un número finito de soluciones enteras.

Ejemplo

Para $n, d, c \in \mathbb{Z}^+$, sea $P(x, y) = x^n - dy^n$.

- Si $n \geq 3$, la ecuación

$$x^n - dy^n = c$$

  tiene un número finito de soluciones enteras.
- Si $n = 1$, hay infinitas soluciones.

Una aplicación a las ecuaciones diofánticas

Teorema

Sea $P \in \mathbb{Z}[x, y]$ homogéneo con algún factor irreducible de grado ≥ 3, entonces para $c \in \mathbb{Z}\backslash\{0\}$ la ecuación $P(x, y) = c$ tiene un número finito de soluciones enteras.

Ejemplo

Para $n, d, c \in \mathbb{Z}^+$, sea $P(x, y) = x^n - dy^n$.

- Si $n \geq 3$, la ecuación

$$x^n - dy^n = c$$

  tiene un número finito de soluciones enteras.
- Si $n = 1$, hay infinitas soluciones.
- Si $n = 2$ y d no es un cuadrado, recuperamos (más o menos) la ecuación de Pell, ¡con infinitas soluciones!

S-unidades: idea de la demostración (1)

S-unidades: idea de la demostración (1)

Concepto clave: alturas.

S-unidades: idea de la demostración (1)

Concepto clave: alturas.

Consideramos el grupo $\Gamma = \mathcal{O}_S^* \times \mathcal{O}_S^*$ y el isomorfismo

$$\varphi : \Gamma/\Gamma_{\mathsf{tor}} \to \mathbb{Z}^r,$$

esto nos permite definir una norma en $\mathbb{Z}^r$:

$$\|\vec{n}\| := h(\varphi^{-1}(\vec{n}))$$

S-unidades: idea de la demostración (1)

Concepto clave: alturas.

Consideramos el grupo $\Gamma = \mathcal{O}_S^* \times \mathcal{O}_S^*$ y el isomorfismo

$$\varphi : \Gamma/\Gamma_{\text{tor}} \to \mathbb{Z}^r,$$

esto nos permite definir una norma en $\mathbb{Z}^r$:

$$\|\vec{n}\| := h(\varphi^{-1}(\vec{n}))$$

Idea: pasar las soluciones por φ, acotar sus normas y aplicar:

Teorema (Northcott)

Para $M \in \mathbb{R}^+$, el conjunto $\{\vec{n} \in \mathbb{Z}^r : \|\vec{n}\| \leq M\}$ es finito.

S-unidades: idea de la demostración (2)

Necesitamos un resultado de acotación:

S-unidades: idea de la demostración (2)

Necesitamos un resultado de acotación:

Teorema (Resultado fundamental)

Si $\vec{u}, \vec{v} \in \mathbb{Z}^r$ son vectores correspondientes a soluciones de la ecuación del teorema de las S-unidades, existe una constante c_0 tal que

$$\|\vec{u}\| \leq \frac{1}{4}c_0 + \frac{2}{n-1}\|\vec{v} - 2n\vec{u}\|, \text{ para todo } n \in \mathbb{Z}_{>1}.$$

S-unidades: idea de la demostración (2)

Necesitamos un resultado de acotación:

Teorema (Resultado fundamental)

Si $\vec{u}, \vec{v} \in \mathbb{Z}^r$ son vectores correspondientes a soluciones de la ecuación del teorema de las S-unidades, existe una constante c_0 tal que

$$\|\vec{u}\| \leq \frac{1}{4}c_0 + \frac{2}{n-1}\|\vec{v} - 2n\vec{u}\|, \text{ para todo } n \in \mathbb{Z}_{>1}.$$

Consecuencia: pocos vectores solución en direcciones parecidas.

S-unidades: idea de la demostración (2)

Necesitamos un resultado de acotación:

Teorema (Resultado fundamental)

Si $\vec{u}, \vec{v} \in \mathbb{Z}^r$ son vectores correspondientes a soluciones de la ecuación del teorema de las S-unidades, existe una constante c_0 tal que

$$\|\vec{u}\| \leq \frac{1}{4}c_0 + \frac{2}{n-1}\|\vec{v} - 2n\vec{u}\|, \text{ para todo } n \in \mathbb{Z}_{>1}.$$

Consecuencia: pocos vectores solución en direcciones parecidas.

Concluimos fijando una cantidad suficientemente grande de direcciones; separamos el espacio en *conos*.

Principales referencias

- Beukers, F., & Schlickewei, H. (1996). *The equation $x + y = 1$ in finitely generated groups*. Acta Arithmetica, 78(2), 189-199.
- Chamizo. F. (2022). *Teoría combinatoria y analítica de números curso* $2022/23$ (Sec. 3.3). Universidad Autónoma de Madrid.
- Conrad, K. (2010). *Ostrowski for number fields*. Expository papers on Algebraic Number Theory.
- Ono, T. (2012). *An introduction to algebraic number theory*. Springer Science.
- Zannier, U. (2009). *Lecture notes on Diophantine analysis* (Vol. 8). Edizioni della Normale, Pisa.