

ENTEROS ALGEBRAICOS

ALAN REYES-FIGUEROA
TEORÍA DE NÚMEROS

(AULA 25) 21.OCTUBRE.2021

Enteros Algebraicos

En esta sección, haremos una pequeña introducción a la teoría algebraica de números. Introducimos algunos conceptos básicos (sin ahondar demasiado), pero que nos permitirán apreciar algunas de las técnicas usadas en esta área.

Números Algebraicos:

Definición

Un número complejo $z \in \mathbb{C}$ es un **número algebraico** si existe un polinomio no nulo $f(x) \in \mathbb{Q}[x]$ tal que $f(z) = 0$.

Obs!: Todo número algebraico z satisface un único polinomio mónico e irreducible $g(x) = 0$, sobre \mathbb{Q} (su polinomio minimal), y todo polinomio $f \in \mathbb{Q}[x]$ tal que $f(z) = 0$ es divisible por $g(x)$. El **grado** de z es el grado de su polinomio minimal $g(x)$.

Definición

Un número algebraico $z \in \mathbb{C}$ es un **entero algebraico** si satisface una ecuación polinomial $f(x) = x^n + b_1x^{n-1} + \dots + b_2x^2 + b_1x + b_0 \in \mathbb{Z}[x]$, con coeficientes enteros.

Enteros Algebraicos

Ejemplo: Todo número racional $r \in \mathbb{Q}$ es algebraico, pues satisface el polinomio $f(x) = x - r \in \mathbb{Q}[x]$.

De entre todos los racionales, los únicos enteros algebraicos son los números enteros $0, \pm 1, \pm 2, \dots$

Algunas propiedades:

- Si α, β son números algebraicos, también lo son $\alpha + \beta$, $\alpha - \beta$ y $\alpha\beta$, $-\alpha$, $\frac{1}{\alpha}$ (cuando $\alpha \neq 0$).
- De hecho, los números algebraicos forman un cuerpo, llamado el **cuerpo de número algebraicos** $\mathcal{A} \subset \mathbb{C}$.
- Los enteros algebraicos forman un anillo, el **anillo de enteros algebraicos** A , contenido dentro de \mathcal{A} .

Definición

Un **cuerpo de números** K es cualquier cuerpo contenido en \mathbb{C} . El **anillo de enteros** de K , denotado \mathcal{O}_K , es la intersección $K \cap A$.

Enteros Algebraicos

Ejemplos:

- $\mathbb{Z} = \mathbb{Q} \cap A = \mathcal{O}_{\mathbb{Q}}$.
- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} = \mathbb{Q}(i) \cap A = \mathcal{O}_{\mathbb{Q}(i)}$.

Ya vimos que A es un cuerpo.

Definición

Un **cuerpo de números algebraicos** es cualquier cuerpo contenido en A .

La forma más común de construir cuerpos algebraicos de números es mediante extensiones de \mathbb{Q} . Esto es, dado un número algebraicos $\xi \notin \mathbb{Q}$, consideramos la **extensión** de \mathbb{Q} por ξ

$\mathbb{Q}(\xi)$ = el menor cuerpo contenido en A que contiene a \mathbb{Q} y a ξ .

Para dar una expresión más adecuada para $\mathbb{Q}(\xi)$, nos limitamos a extensiones finitas, esto es, donde $\deg(\xi) = n$ (ξ satisface un polinomio de grado n en $\mathbb{Q}[x]$).

Enteros Algebraicos

Teorema

Si $\xi \in \mathcal{A}$ es un número algebraico de grado n , entonces todo número en $\mathbb{Q}(\xi)$ se escribe en forma única como una combinación lineal

$$a_0 + a_1\xi + a_2\xi^2 + \dots + a_{n-1}\xi^{n-1}, \quad a_i \in \mathbb{Q}.$$

Así, $\mathbb{Q}(\xi) \cong \mathbb{Q}^n$ como \mathbb{Q} -espacio vectorial, y $\{1, \xi, \xi^2, \dots, \xi^{n-1}\}$ es base de $\mathbb{Q}(\xi)$.

Ejemplo 1: Consideramos el número $\sqrt{3} \in \mathbb{C}$. $\sqrt{3}$ es un número algebraico, pues satisface $x^2 - 3 = 0$. Además, $\deg(\sqrt{3}) = 2$.

Entonces, $\mathbb{Q}(\sqrt{3})$ es una extensión algebraica de \mathbb{Q} , de grado 2, de modo que

$$\mathbb{Q}(\sqrt{3}) = \{a_0 + a_1\sqrt{3} : a_0, a_1 \in \mathbb{Q}\} = \mathbb{Q} + \mathbb{Q}\sqrt{3}.$$

La suma en $\mathbb{Q}(\sqrt{3})$ es la suma usual por componentes (se suman las partes reales, y se suman las partes imaginarias). El producto en $\mathbb{Q}(\sqrt{3})$ funciona según la regla

$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

Enteros Algebraicos

Ejemplo 2: Consideramos el número $\xi = \sqrt[3]{2} \in \mathbb{R}$. ξ es un número algebraico, pues satisface $x^3 - 2 = 0$. Además, $\deg(\xi) = 3$.

Entonces, $\mathbb{Q}(\xi) = (\sqrt[3]{2})$ es una extensión algebraica de \mathbb{Q} , de grado 3, y

$$\mathbb{Q}(\xi) = \{a_0 + a_1\xi + a_2\xi^2 : a_0, a_1, a_2 \in \mathbb{Q}\} \cong \mathbb{Q} + \xi\mathbb{Q} + \xi^2\mathbb{Q}.$$

La suma en $\mathbb{Q}(\xi)$ es la suma usual por componentes

$$(a + b\xi + c\xi^2) + (d + e\xi + f\xi^2) = (a + d) + (b + e)\xi + (c + f)\xi^2.$$

El producto en $\mathbb{Q}(\xi)$ funciona según la reglas

$$1 \cdot \xi = \xi, \quad 1 \cdot \xi^2 = \xi^2, \quad \xi \cdot \xi = \xi^2, \quad \xi \cdot \xi^2 = \xi^3 = 2, \quad \xi^2 \cdot \xi^2 = \xi^4 = 2\xi.$$

En particular

$$(a + b\xi + c\xi^2)(d + e\xi + f\xi^2) = (ad + 2bf + 2ce) + (ae + bd + 2cf)\xi + (af + be + cd)\xi^2.$$

Cuerpos Cuadráticos

Cuerpos cuadráticos:

Definición

Un cuerpo cuadrático (o extensión cuadrática), es una extensión de la forma $\mathbb{Q}(\xi)$, donde ξ satisface un polinomio de grado 2 sobre \mathbb{Q} . Esto es $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2$.

Obs!

- Sabemos que $\mathbb{Q}(\xi) = \{a + b\xi : a, b \in \mathbb{Q}\}$.
- Si $\deg(\xi) = 2$, recordemos que ξ debe ser de la forma

$$\xi = \frac{a + b\sqrt{m}}{c}, \quad \text{con } a, b, c, m \in \mathbb{Z}, c \neq 0, m \neq 0, 1, m \text{ libre de cuadrados.}$$

En particular,

$$\mathbb{Q}(\xi) = \mathbb{Q}\left(\frac{a + b\sqrt{m}}{c}\right) = \mathbb{Q}(a + b\sqrt{m}) = \mathbb{Q}(b\sqrt{m}) = \mathbb{Q}(\sqrt{m}).$$

- Si $m \neq n$, entonces $\mathbb{Q}(m) \neq \mathbb{Q}(n)$.

Cuerpos Cuadráticos

Tenemos una definición de norma en campos cuadráticos, muy importante para el desarrollo aritmético.

Definición

La **norma** $N(\alpha)$ de un número $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ se define como

$$N(\alpha) = \alpha\bar{\alpha} = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2m \in \mathbb{Q}.$$

Propiedades

Sean $\alpha, \beta, \gamma \in \mathbb{Q}(\sqrt{m})$. Entonces

- $N(\alpha\beta) = N(\alpha)N(\beta)$.
- $N(\alpha) = 0 \implies \alpha = 0$.
- Si $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ es un entero, entonces $N(\gamma) \in \mathbb{Z}$ es un entero racional.
- $N(\gamma) = \pm 1 \iff \gamma$ es una unidad en $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.

Cuerpos Cuadráticos

Prueba: (1.) $N(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = (\alpha\bar{\alpha})(\beta\bar{\beta}) = N(\alpha)N(\beta)$.

(2.) Sea $\alpha \in \mathbb{Q}(\sqrt{m})$. Entonces $N(\alpha) = 0 \iff \alpha\bar{\alpha} = 0 \iff \alpha = 0 \text{ ó } \bar{\alpha} = 0$. En cualquier caso, esto es equivalente a $\alpha = 0$.

(3.) A continuación, si $\gamma \in \mathbb{Q}(\sqrt{m})$ es un número entero algebraico, éste tiene grado 1 ó 2. Si tiene grado 1, entonces γ es un número entero racional en \mathbb{Z} , portanto $N(\gamma) = \gamma\bar{\gamma} = \gamma^2 \in \mathbb{Z}$ de modo que $N(\gamma)$ es un número entero racional. Si γ es de grado 2, entonces el polinomio mínimo de γ es

$$x^2 - (\gamma + \bar{\gamma})x + \gamma\bar{\gamma} = 0,$$

y este posee coeficientes en \mathbb{Z} . De ahí que nuevamente $N(\gamma) = \gamma\bar{\gamma} \in \mathbb{Z}$.

(4.) Finalmente, si $N(\gamma) = \pm 1$ y γ es un número entero, entonces $\gamma\bar{\gamma} = \pm 1$, $\gamma \mid 1$, de modo que γ es una unidad. Para demostrar la recíproca, suponga que γ es una unidad. Entonces existe ε entero, tal que $\gamma\varepsilon = 1$. Esto implica $N(\gamma)N(\varepsilon) = N(1) = 1$, de modo que $N(\gamma) = \pm 1$, ya que $N(\gamma)$ y $N(\varepsilon)$ son números enteros racionales en \mathbb{Z} .

Cuerpos Cuadráticos

Primos en cuerpos cuadráticos:

Definición

Un entero algebraico α , no unidad, en un cuerpo cuadrático $\mathbb{Q}(\sqrt{m})$ es llamado un **primo** si sólo es divisible por sus asociados, o por unidades del cuerpo.

Teorema

Si la norma de un entero $\alpha \in \mathbb{Q}(\sqrt{m})$ es $\pm p$, con p primo, entonces α es un primo en $\mathbb{Q}(\sqrt{m})$.

Prueba: Suponga $\alpha = \beta\gamma$, con β, γ enteros en $\mathbb{Q}(\sqrt{m})$. Como la norma es multiplicativa, entonces $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma) = \pm p$. ahora, como $N(\beta), N(\gamma) \in \mathbb{Z}$, entonces alguno de ellos debe ser ± 1 , de modo que β ó γ es una unidad en $\mathbb{Q}(\sqrt{m})$. Esto muestra que α es primo. \square

Teorema

Todo entero en $\mathbb{Q}(\sqrt{m})$ no o ó unidad, se factora como producto de primos. \square

Cuerpos Cuadráticos

Obs!

- Aunque el teorema anterior garantiza la factoración en primos, ésta no necesariamente es única.

Por ejemplo, tenemos que en $\mathbb{Q}(\sqrt{-5})$ vale $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$.

- Recordemos que cuando vale la propiedad de factoración única, $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ se llama un dominio de factoración única (UFD).
 - todo cuerpo es UFD.
 - todo dominio Euclideo es UFD.
 - todo PID es UFD.
- **Teorema:** Los cuerpos $\mathbb{Q}(\sqrt{m})$, con $m = -1, -2, -3, -7, 2, 3$ son Euclideos, portanto $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ es UFD.
- El Teorema de STARK-HEEGNER establece que si $m < 0$, entonces $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ es UFD $m \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.

Cuerpos Cuadráticos

Una propiedad importante que caracteriza la forma de los anillos de enteros asociados a cuerpos cuadráticos es la siguiente:

Teorema (Anillos de Enteros Cuadráticos)

Sea $m \in \mathbb{Z}$ libre de cuadrados, $m \neq 0, 1$. Entonces el anillo de enteros, asociado a cuerpo cuadrático $\mathbb{Q}(\sqrt{m})$ es

$$\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\omega], \text{ con } \omega = \begin{cases} \frac{1 + \sqrt{m}}{2}, & \text{si } m \equiv 1 \pmod{4}; \\ \sqrt{m}, & \text{caso contrario. } \square \end{cases}$$

Ejemplos:

- Para $m = -1$, el anillo $\mathcal{O}_{\mathbb{Q}(i)}$ es igual a $\mathbb{Z}[i]$, **enteros Gaussianos**.
- Para $m = -3$, el anillo $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ es igual a $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, **enteros de Eisenstein**.