Introducción a los Números Algebraicos

Clase 2: Enteros algebraicos

Gonzalo Tornaría

15 de marzo, 2007

2 Enteros algebraicos

Definición 2.0.1. Un *cuerpo de números* es un subcuerpo de $\mathbb{C}$ de grado finito sobre $\mathbb{Q}$.

Proposición 2.0.2. *Si K es un cuerpo de números, existe $\alpha \in \mathbb{C}$ tal que $K = \mathbb{Q}[\alpha]$. Además, α es algebraico de grado $n = [K : \mathbb{Q}]$, y*

$$\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$$

es una base de $K/\mathbb{Q}$.

Demostración. Álgebra 2. □

Ejemplo 2.0.3. $\mathbb{Q}[e^{\frac{2\pi i}{m}}]$, el *$m$-ésimo cuerpo ciclotómico*. El grado es $\varphi(m)$ (ejercicio 11).

Ejemplo 2.0.4. $\mathbb{Q}[\sqrt{m}]$, con $m \in \mathbb{Z}$ no un cuadrado perfecto, es un *cuerpo cuadrático*. Todos los cuerpos de grado 2 son de esta forma (ejercicio 12). Una base es $\{1, \sqrt{m}\}$. Puede suponerse m libre de cuadrados.

Cuando $m > 0$, tenemos $\mathbb{Q}[\sqrt{m}] \subseteq \mathbb{R}$, se dice cuerpo cuadrático *real*, mientras que si $m < 0$ tenemos $\mathbb{Q}[\sqrt{m}] \not\subseteq \mathbb{R}$, se dice cuerpo cuadrático *imaginario*.

Notar que $\mathbb{Q}[i]$ es un cuerpo cuadrático imaginario y el cuarto cuerpo ciclotómico. Otro cuerpo cuadrático imaginario es $\mathbb{Q}[\sqrt{-3}]$, que también es un cuerpo ciclotómico (cuál?).

Definición 2.0.5. Un *entero algebraico* es un $\alpha \in \mathbb{C}$ que sea raíz de un polimomio *mónico* con coeficentes en $\mathbb{Z}$.

Recordemos que si α es algebraico sobre $\mathbb{Q}$ entonces existe un único polinomio mónico irreducible sobre $\mathbb{Q}$ con α como raíz, que denotaremos $\mathrm{Irr}_{\mathbb{Q}}(\alpha)$.

Teorema 2.0.6. *Sea α un entero algebraico. Entonces $\mathrm{Irr}_{\mathbb{Q}}(\alpha)$ tiene coeficientes en $\mathbb{Z}$.*

Demostración. Supongamos que $f(\alpha) = 0$, donde f es mónico con coeficientes en $\mathbb{Z}$, entonces $= g \cdot \mathrm{Irr}_{\mathbb{Q}}$, por propiedad del polinomio minimal. El resultado se sigue del siguiente Lema. □

Lema 2.0.7 (de Gauss)**.** *Sea $f \in \mathbb{Z}[X]$ mónico. Si $f = g \cdot h$ con g, h mónicos y coeficientes en $\mathbb{Q}$, entonces f y g tienen coeficientes en $\mathbb{Z}$.*

Demostración. Existen enteros positivos m y n minimales tales que $mg, nh \in \mathbb{Z}[X]$. Supongamos que $p \mid mn$; entonces $mnf = (mg)(mh)$, y reduciendo módulo p concluimos que

$$0 \equiv (mg)(mh) \pmod{p}.$$

Pero $(\mathbb{Z}/p)[X]$ es un dominio integral (pues $\mathbb{Z}/p$ lo es), y se sigue que $p \mid mg$ ó $p \mid nh$, contradiciendo la minimalidad de m y n. □

Corolario 2.0.8. *Los enteros de $\mathbb{Q}$ son exactamente los elementos de $\mathbb{Z}$ (también llamados* enteros racionales*).*

Corolario 2.0.9. *Sea $m \in \mathbb{Z}$ libre de cuadrados. Los enteros de $\mathbb{Q}[\sqrt{m}]$ son*

$$\begin{cases} \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \ : \ a, b \in \mathbb{Z}\} & \text{si } m \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{\frac{a+b\sqrt{m}}{2} \ : \ a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\} & \text{si } m \equiv 1 \pmod 4 \end{cases}$$

(ver ejercicio 14).

Notar que en ambos casos los enteros forman un anillo. Vamos a probar que esto es cierto para cualquier cuerpo de números. Necesitaremos otra caracterización (muy importante) de los enteros algebraicos:

Teorema 2.0.10. *Son equivalentes, para $\alpha \in \mathbb{C}$:*

1. *α es un entero algebraico;*

2. $\mathbb{Z}[\alpha]$ *es finitamente generado (como grupo abeliano);*

3. $\alpha \in R$ *para algún anillo finitamente generado.*

4. $\alpha A \subseteq A$ *para algún subgrupo aditivo* $A \neq \{0\}$ *de* $\mathbb{C}$ *finitamente generado.*

Demostración.

$(1 \to 2)$ Si $f(\alpha) = \alpha^n + g(\alpha) = 0$, con g de grado menor que n, entonces $\alpha^n = -g(\alpha)$ y se sigue que $\mathbb{Z}[\alpha]$ está generado por $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

$(2 \to 3 \to 4)$ trivial.

$(4 \to 1)$ Sea $\{a_1, \ldots, a_n\}$ un conjunto generador de A. Como $\alpha A \subseteq A$, tenemos que

$$\begin{pmatrix} \alpha a_1 \\ \alpha a_2 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix},$$

donde M es una matriz con coeficientes en $\mathbb{Z}$. Como $A \neq \{0\}$, algún $a_i \neq 0$ y se sigue que α es un valor propio de M. Luego el polinomio característico de M es un polinomio mónico con coeficientes en $\mathbb{Z}$ con α como raíz.

□

Corolario 2.0.11. *Si* α *y* β *son enteros algebraicos, entonces* $\alpha + \beta$ *y* $\alpha\beta$ *también lo son.*

Demostración. Como $\mathbb{Z}[\alpha]$ y $\mathbb{Z}[\beta]$ son finitamente generados, entonces $\mathbb{Z}[\alpha, \beta]$ también lo será. En efecto, si $\{a_1, \ldots, a_n\}$ y $\{b_1, \ldots, b_m\}$ son generadores de $\mathbb{Z}[\alpha]$ y de $\mathbb{Z}[\beta]$, respectivamente, entonces $\{a_i b_j \ : \ i = 1, \ldots, n, \ j = 1, \ldots, m\}$ será un generador de $\mathbb{Z}[\alpha, \beta]$. *Notar que aquí se usa que* $\alpha\beta = \beta\alpha$*!!* Como $\alpha + \beta \in \mathbb{Z}[\alpha, \beta]$ se sigue que $\alpha + \beta$ es un entero algebraico, y lo mismo para $\alpha\beta$. □

Notar que es esencial utilizar la propiedad conmutativa. Por ejemplo, usando definiciones similares para matrices, podemos decir que $\alpha = \left(\begin{smallmatrix} 0 & 2 \\ -1/2 & 0 \end{smallmatrix}\right)$ y $\beta = \left(\begin{smallmatrix} 0 & -1/2 \\ 2 & 0 \end{smallmatrix}\right)$ son matrices enteras: ambas son raíz de $X^2 + 1$, y tanto $\mathbb{Z}[\alpha]$ como $\mathbb{Z}[\beta]$ son finitamente generados. Sin embargo $\alpha + \beta = \left(\begin{smallmatrix} 0 & 3/2 \\ 3/2 & 0 \end{smallmatrix}\right)$ no es entera, y lo mismo para $\alpha\beta$ (verificar y comparar con ejercicio 15 que trata el caso de álgebras de cuaterniones).

Corolario 2.0.12. *El conjunto de enteros algebraicos de un cuerpo de números* K *es un anillo, que llamamos* anillo de enteros de K *y denotamos por* $\mathcal{O}_K$.

2.1 Monomorfismos en $\mathbb{C}$

Sea K un cuerpo de números de grado n sobre $\mathbb{Q}$. Recordemos que existen exactamente n monomorfismos o inmersiones distintas de K en $\mathbb{C}$.

En efecto, si $K = \mathbb{Q}[\alpha]$ entonces α tiene grado n y por lo tanto n conjugados $\{\alpha = \alpha_1, \ldots, \alpha_n\}$ (las n raíces, necesariamente distintas, de $\mathrm{Irr}_{\mathbb{Q}}(\alpha)$ en $\mathbb{C}$).

Los n monomorfismos de K en $\mathbb{C}$ están dados por

$$\begin{aligned} \sigma_i : K &\to \mathbb{C} \\ \alpha &\mapsto \alpha_i \end{aligned}$$

para $i = 1, \ldots, n$.

Ejemplo 2.1.1. Para el cuerpo cuadrático $\mathbb{Q}[\sqrt{m}]$, los dos monomorfismos están dadas por:

$$\begin{aligned} a + b\sqrt{m} &\overset{\mathrm{id}}{\longmapsto} a + b\sqrt{m} \\ &\longmapsto a - b\sqrt{m} \end{aligned}$$

Ambos son *automorfismos* de K.

Ejemplo 2.1.2. Para el cuerpo ciclotómico $\mathbb{Q}[\omega]$, con $\omega = e^{\frac{2\pi i}{m}}$, los $\varphi(m)$ monomorfismos están dadas por:

$$\omega \longmapsto \omega^k$$

para $1 \leq k < m$, con $(k, m) = 1$. De nuevo son todos automorfismos.

Ejemplo 2.1.3. El cuerpo cúbico $\mathbb{Q}[\sqrt[3]{2}]$ tiene tres monomorfismos

$$\begin{aligned} \sqrt[3]{2} &\overset{\mathrm{id}}{\longmapsto} \sqrt[3]{2} \\ &\longmapsto \omega\sqrt[3]{2} \\ &\longmapsto \omega^2\sqrt[3]{2} \end{aligned}$$

donde $\omega = e^{\frac{2\pi i}{3}}$ es una raíz cúbica de 1. Notar que en este ejemplo solamente el monomorfismo trivial es un automorfismo.

Cuando para un cuerpo de números todos los monomorfismos son automorfismos, como en los dos primeros ejemplos, decimos que el cuerpo de números es *normal*.

2.2 Traza y Norma

Sea K un cuerpo de números de grado n sobre $\mathbb{Q}$, y sean $\sigma_1 \ldots, \sigma_n$ sus monomorfismos en $\mathbb{C}$. Si $\alpha \in K$ definimos

$$T(\alpha) = T_K(\alpha) := \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha),$$
$$N(\alpha) = N_K(\alpha) := \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha),$$

su *traza* y su *norma* desde K, respectivamente. Notar que $T(\alpha + \beta) = T(\alpha) + T(\beta)$ y que $N(\alpha\beta) = N(\alpha)N(\beta)$.

Alternativamente, supongamos que $\alpha \in K$ tiene grado d sobre $\mathbb{Q}$, es decir que α tiene d conjugados $\{\alpha = \alpha_1, \ldots, \alpha_d\}$. Podemos definir

$$t(\alpha) := \alpha_1 + \alpha_2 + \cdots + \alpha_n,$$
$$n(\alpha) := \alpha_1\alpha_2\cdots\alpha_n.$$

Proposición 2.2.1.

$$T_K(\alpha) = \frac{n}{d} \cdot t(\alpha);$$
$$N_K(\alpha) = n(\alpha)^{\frac{n}{d}}.$$

Demostración. Cada uno de los d monomorfismos de $\mathbb{Q}[\alpha]$ en $\mathbb{C}$ tiene $\frac{n}{d}$ extensiones a K, es decir que en $\{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$ aparece cada conjugado de α exactamente $\frac{n}{d}$ veces. □

Corolario 2.2.2. $T(\alpha), N(\alpha) \in \mathbb{Q}$

Demostración. $t(\alpha)$ y $n(\alpha)$ son coeficientes de $\mathrm{Irr}_{\mathbb{Q}}(\alpha)$, y $\frac{n}{d} \in \mathbb{Z}$. □

Corolario 2.2.3. *Si α es entero, entonces $T(\alpha), N(\alpha) \in \mathbb{Z}$.*

Demostración. Ídem □

Ejemplo 2.2.4. Si $K = \mathbb{Q}[\sqrt{m}]$, entonces

$$T(a + b\sqrt{m}) = 2a, \qquad N(a + b\sqrt{m}) = a^2 - mb^2.$$