Introducción a los Números Algebraicos

Clase 3: Enteros algebraicos II

Gonzalo Tornaría

20 de marzo, 2007

2.3 Discriminante

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

Definición 2.3.1. Si $\{\alpha_1, \dots, \alpha_n\} \subseteq K$ definimos el *discriminante* de dicha n-upla como

$$\Delta(\alpha_1, \dots, \alpha_n) := \det(\sigma_i(\alpha_j))^2.$$

Notar que el orden de los σ_i y de los α_j solamente altera el signo del determinante, que está al cuadrado, de modo que la definición es independiente del orden.

Veamos que el discriminante está relacionado con la traza.

Proposición 2.3.2.

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(T(\alpha_i\alpha_j)).$$

Demostración. Pues

$$(\sigma_j(\alpha_i))(\sigma_i(\alpha_j)) = (\sigma_1(\alpha_i\alpha_j)) + \dots + (\sigma_n(\alpha_i\alpha_j)) = (T(\alpha_i\alpha_j)),$$

y tomando determinante de ambos lados se sigue la proposición. □

Corolario 2.3.3. $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$. *Además, si todos los α_i son enteros algebraicos, entonces $\Delta(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.*

Proposición 2.3.4. $\Delta(\alpha_1, \dots, \alpha_n) = 0$ *si y sólo si $\alpha_1, \dots, \alpha_n$ son linealmente dependientes sobre $\mathbb{Q}$.*

Demostración. Si α_i son linealmente dependientes, también lo serán las columnas de la matriz $(\sigma_i(\alpha_j))$, y por lo tanto el discriminate será 0. Recíprocamente, si $\Delta(\alpha_1, \dots, \alpha_n) = 0$ las columnas de la matriz $(T(\alpha_i\alpha_j))$ serán linealmente dependientes sobre $\mathbb{Q}$. Digamos que $a_1T(\alpha_1\alpha_j)+a_2T(\alpha_2\alpha_j)+\dots+a_nT(\alpha_n\alpha_j) = 0$ para todo j, con $a_i \in \mathbb{Q}$. Entonces podemos considerar $\alpha = a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n$; se sigue que $T(\alpha\alpha_i) = 0$ para todo i. Suponiendo que $\{\alpha_1, \dots, \alpha_n\}$ es base de $K/\mathbb{Q}$, tendríamos que $T(\alpha\beta) = 0$ para todo $\beta \in K$, pero $\alpha \neq 0$, lo cual es una contradicción (e.g. tomar $\beta = \alpha^{-1}$). □

Proposición 2.3.5. *Sean $\{\alpha_1, \dots, \alpha_n\}$ y $\{\beta_1, \dots, \beta_n\}$ dos bases de $K/\mathbb{Q}$, y supongamos que $\alpha_i = \sum_j a_{i,j}\beta_j$ con $a_{i,j} \in \mathbb{Q}$. Entonces*

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(a_{i,j})^2\, \Delta(\beta_1, \dots, \beta_n).$$

Demostración. Puesto que $a_{i,j} \in \mathbb{Q}$, se sigue que $(\sigma_i(\alpha_k)) = (a_{i,j})(\sigma_j(\beta_k))$, □

En el caso particular en que $K = \mathbb{Q}[\alpha]$, sabemos que una base de K está dada por $\{1, \alpha, \dots, \alpha^{n-1}\}$, y denotaremos $\Delta(\alpha) := \Delta(1, \alpha, \dots, \alpha^{n-1}) \neq 0$.

Proposición 2.3.6. *Sea $K = \mathbb{Q}[\alpha]$ y $f = \mathrm{Irr}_{\mathbb{Q}}(\alpha)$. Entonces*

$$\Delta(\alpha) = \pm N(f'(\alpha))$$

donde el signo es + sii $n \equiv 0, 1 \pmod 4$.

Demostración. La matriz $(\sigma_i(\alpha^j)) = (\sigma_i(\alpha)^j)$ es de tipo de Vandermonde; luego su determinante es

$$\prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha)).$$

Se sigue que $\Delta(\alpha) = \pm\prod_{i\neq j}(\sigma_i(\alpha) - \sigma_j(\alpha))$. Como $f(X) = \prod_i(X - \sigma_i(\alpha))$, tenemos que

$$f'(\sigma_j(\alpha)) = \prod_{i\neq j}(\sigma_j(\alpha) - \sigma_i(\alpha)),$$

y el resultado sigue tomando normas pues $N(f'(\alpha)) = \prod_j f'(\sigma_j(\alpha))$. □

2.4 Bases enteras

Sea K un cuerpo de números de grado n sobre $\mathbb{Q}$. El objetivo de esta sección es describir la estructura aditiva de $\mathcal{O}_K$. Concretamente, veremos que $\mathcal{O}_K$ es un grupo abeliano libre de rango n.

Definición 2.4.1. Una *base entera* de $\mathcal{O}_K$ es un conjunto $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}_K$ tal que cualquier $\alpha \in \mathcal{O}_K$ puede escribirse de manera única como

$$a_1\alpha_1 + \cdots + a_n\alpha_n, \quad a_i \in \mathbb{Z}.$$

Es fácil ver que existen bases de $K/\mathbb{Q}$ con todos sus elementos enteros. En efecto, dado $\alpha \in K$ existe un entero $m \in \mathbb{Z}$ tal que $m\alpha \in \mathcal{O}_K$ (ejercicio 24).

Proposición 2.4.2. *Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de $K/\mathbb{Q}$ con todos sus elementos enteros y $|\Delta(\alpha_1, \ldots, \alpha_n)|$ minimal. Entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de $\mathcal{O}_K$.*

Demostración. Sea $\alpha \in \mathcal{O}_K$ y escribamos $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ con $a_i \in \mathbb{Q}$. Tenemos que mostrar que los $a_i \in \mathbb{Z}$. Supongamos que no; sin perdida de generalidad $a_1 \notin \mathbb{Z}$. Entonces $a_1 = m + r$, con $m \in \mathbb{Z}$ y $r \in (0,1)$. Sea $\alpha_1' = \alpha - m\alpha_1 = \theta\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n \in \mathcal{O}_K$. Entonces $\{\alpha_1', \ldots, \alpha_n\}$ es otra base de $K/\mathbb{Q}$ con todos sus elementos enteros, y la matriz de cambio de base tiene determinante θ. Se sigue que $\Delta(\alpha_1', \ldots, \alpha_n) = \theta^2\,\Delta(\alpha_1, \ldots, \alpha_n)$, y como $\theta < 1$ esto contradice la minimalidad de $|\Delta(\alpha_1, \ldots, \alpha_n)|$. □

Corolario 2.4.3. *Existen bases enteras de $\mathcal{O}_K$. Lo que es lo mismo, $\mathcal{O}_K$ es un grupo abeliano libre de rango n.*

Corolario 2.4.4. *$\mathcal{O}_K$ es noetheriano (sus ideales son finitamente generados).*

Demostración. Como $\mathbb{Z}$ es noetheriano, y $\mathcal{O}_K$ es finitamente generado como $\mathbb{Z}$-módulo, el *teorema de la base de Hilbert* muestra que $\mathcal{O}_K$ es noetheriano. □

Demostración alternativa. Sea $A \neq \{0\}$ un ideal de $\mathcal{O}_K$. Observemos primero que A contiene una base de $K/\mathbb{Q}$. En efecto, sea $\alpha \in A$ no nulo y sea $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de $\mathcal{O}_K$. Entonces $\{\alpha\alpha_1, \ldots, \alpha\alpha_n\}$ es una base de $K/\mathbb{Q}$ contenida en A. Generalizando la proposición (con la misma demostración) al caso de A, concluimos igualmente que A es un grupo abeliano libre de rango n, en particular es finitamente generado. □

Proposición 2.4.5. *Sean $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$, dos bases enteras de $\mathcal{O}_K$. Entonces $\Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\beta_1, \ldots, \beta_n)$.*

Demostración. Sea M la matriz de cambio de base, de modo que

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(M)^2\,\Delta(\beta_1, \ldots, \beta_n).$$

Pero M tiene coeficientes en $\mathbb{Z}$ y su inversa también. Luego, $\det M = \pm 1$. □

Por la proposición, el discriminante de una base entera es un invariante de $\mathcal{O}_K$, que denotaremos $\Delta(\mathcal{O}_K)$, o incluso $\Delta(K)$.

Ejemplo 2.4.6. Sea $K = \mathbb{Q}[\sqrt{m}]$, con m libre de cuadrados. Entonces

$$\Delta(\mathcal{O}_K) = \begin{cases} \Delta(\sqrt{m}) = 4m & \text{si } m \equiv 2, 3 \pmod 4; \\ \Delta\left(\frac{1+\sqrt{m}}{2}\right) = m & \text{si } m \equiv 1 \pmod 4. \end{cases}$$

En efecto, conocemos una base entera de $\mathcal{O}_K$ (ejercicio 14).

Este ejemplo es consistente con el *criterio de Stickelberger*: para cualquier cuerpo de números $\Delta(\mathcal{O}_K) \equiv 0, 1 \pmod 4$ (ejercicio 23).

Proposición 2.4.7. *Sean $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. Entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base entera de $\mathcal{O}_K$ si y sólo si $\Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\mathcal{O}_K)$.*

Demostración. Escribiendo $\alpha_1, \ldots, \alpha_n$ en una base entera de $\mathcal{O}_K$ vemos que la matriz que resulta es invertible sobre $\mathbb{Z}$ sii los discriminantes coinciden. □

En vista de la Proposición 2.0.2 podemos preguntarnos si es cierto que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ para algún $\alpha \in \mathcal{O}_K$. Más adelante veremos ejemplos en los que esto no es cierto. Lo que puede probarse es

Proposición 2.4.8. *Sea $\alpha \in \mathcal{O}_K$ de grado n. Entonces hay una base entera*

$$\left\{1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\right\},$$

donde $d_i \in \mathbb{Z}$ y $d_1 \mid d_2 \mid \cdots \mid d_{n-n}$, los f_i son polinomios mónicos de grado i con coeficientes en $\mathbb{Z}$. Los d_i están determinados (son los divisores elementales *del grupo finito $\mathcal{O}_K/\mathbb{Z}[\alpha]$).* □

Ejemplo 2.4.9. Ya vimos que si $\alpha = \sqrt{m}$ con m libre de cuadrados, tenemos una base entera $\{1, \alpha\}$ cuando $m \equiv 2, 3 \pmod 4$ y $\left\{1, \frac{1+\alpha}{2}\right\}$ cuando $m \equiv 1 \pmod 4$.

Ejemplo 2.4.10. Sea $\alpha = \sqrt[3]{m}$, con m libre de cubos, y consideremos el *cuerpo cúbico puro* $K = \mathbb{Q}[\sqrt[3]{m}]$. Podemos escribir $m = hk^2$ donde h y k son libres de cuadrados y relativamente primos entre sí ($k = 1$ cuando m es libre de cuadrados). Entonces una base entera de $\mathcal{O}_K$ está dada por

$$\left\{1, \alpha, \frac{\alpha^2}{k}\right\} \qquad \text{si } m \not\equiv \pm 1 \pmod 9,$$
$$\left\{1, \alpha, \frac{\alpha^2 \pm k^2\alpha + k^2}{3k}\right\} \qquad \text{si } m \equiv \pm 1 \pmod 9,$$

2.5 Dominios de Dedekind

Definición 2.5.1. Un dominio integral R con cuerpo de fracciones K se dice *integralmente cerrado* (en K) si para todo $\alpha \in K$ tal que α es raíz de un polinomio mónico con coeficientes en R se tiene que $\alpha \in R$.

Proposición 2.5.2. *Sea K un cuerpo de números y sea $\mathcal{O}_K$ su anillo de enteros. Entonces $\mathcal{O}_K$ es integralmente cerrado en K.*

Demostración. Sea $\alpha \in K$ raíz de un polinomio mónico con coeficientes en $\mathcal{O}_K$. Se muestra que α es un entero algebraico (ejercicio 25), y por lo tanto $\alpha \in \mathcal{O}_K$. $\square$

Ejemplo 2.5.3. Sea $K = \mathbb{Q}[\sqrt{-3}]$. El anillo $\mathbb{Z}[\sqrt{-3}]$ *no* es integralmente cerrado en K. En efecto $\frac{1+\sqrt{-3}}{2} \notin \mathbb{Z}[\sqrt{-3}]$ pero es un entero algebraico.

De aquí en más *ideal* significará ideal distinto de cero.

Definición 2.5.4. Un dominio integral es un *dominio de Dedekind* si

1. es noetheriano;
2. es integralmente cerrado en su cuerpo de fracciones; y
3. todo ideal primo es maximal.

Ya vimos que el anillo de enteros $\mathcal{O}_K$ de un cuerpo de números es noetheriano e integralmente cerrado. A continuación veremos que también cumple la última condición, por lo que $\mathcal{O}_K$ es un dominio de Dedekind.

Lema 2.5.5. *Si A es un ideal de $\mathcal{O}_K$, entonces $A \cap \mathbb{Z} \neq \{0\}$.*

Demostración. Sea $\alpha \in A$ con $\alpha \neq 0$, y sea $f = \operatorname{Irr}_{\mathbb{Q}}(\alpha)$. Entonces $f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, de donde $a_0 \in \mathbb{Z}$. $\square$

Proposición 2.5.6. *Si A es un ideal de $\mathcal{O}_K$, entonces $\mathcal{O}_K/A$ es finito.*

Demostración. Sea $a \in A \cap \mathbb{Z}$ con $a \neq 0$. El grupo abeliano $\mathcal{O}_K/A$ es finitamente generado, y es anulado por la multiplicación por a. Se sigue que $\mathcal{O}_K/A$ es un grupo finito. $\square$

Observar que, como $\mathcal{O}_K/A$ es finito, se sigue que hay una cantidad finita de ideales de $\mathcal{O}_K$ que contienen a A; esta es otra manera de probar que $\mathcal{O}_K$ es noetheriano.

Lema 2.5.7. *Sea R un dominio integral finito. Entonces R es un cuerpo.*

Demostración. Sea a un elemento no nulo de R. Como R es un dominio integral, multiplicación por a es una función inyectiva; como R es finito se sigue que también es sobreyectiva. La preimagen de 1 es a^{-1}. $\square$

Proposición 2.5.8. *El anillo de enteros $\mathcal{O}_K$ de un cuerpo de números es un dominio de Dedekind.*

Demostración. Falta probar que todo ideal primo es maximal. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$. Entonces $\mathcal{O}_K/\mathfrak{p}$ es un dominio integral finito. Pero todo dominio integral finito es un cuerpo, así que $\mathfrak{p}$ es maximal. $\square$

Definición 2.5.9. Un *ideal fraccional* de $\mathcal{O}_K$ es un $\mathcal{O}_K$-submódulo de K distinto de cero que sea finitamente generado como $\mathcal{O}_K$-módulo.

Para evitar confusiones llamaremos *ideal entero* a un ideal en el sentido clásico. Como un ideal fraccional es finitamente generado, es posible eliminar denominadores, resultando que cualquier ideal fraccional de $\mathcal{O}_K$ se puede escribir como $\frac{1}{a}I$ con $a \in \mathbb{Z}$ e I un ideal entero.

Veremos que los ideales fraccionales de un dominio de Dedekind forman un grupo abeliano con la multiplicación (con identidad $\mathcal{O}_K$).