Introducción a los Números Algebraicos

Clase 14: Clases de ideales

Gonzalo Tornaría

3 de mayo, 2007

7 El grupo de clases de ideales

7.1 Introducción

Sea K un cuerpo de números cualquiera (no necesariamente normal). Definimos una relación de equivalencia $\sim$ en el conjunto de ideales (enteros, no nulos) de $\mathcal{O}_K$, de la siguiente manera: si I y J son ideales de $\mathcal{O}_K$, entonces

$$I \sim J \qquad \Longleftrightarrow \qquad \alpha I = \beta J \text{ con } \alpha, \beta \in \mathcal{O}_K - \{0\}.$$

En el ejercicio 10 se prueba que es una relación de equivalencia, y que las clases forman un grupo abeliano dado que se cumple el siguiente

Lema 7.1.1. *Sea I un ideal de $\mathcal{O}_K$, entonces existe J tal que IJ es principal*

Demostración. Sabemos que I tiene inverso, que es un ideal fraccional, digamos $I^{-1} = \frac{1}{a}J$ con J entero, entonces $IJ = (a)$. □

Al *grupo de clases de ideales* de $\mathcal{O}_K$ lo denotaremos $C(\mathcal{O}_K)$.

Observación 7.1.2. Todo ideal fraccional de K es "equivalente" a uno entero, de modo que $C(\mathcal{O}_K) = I(K)/P(K)$, donde $I(K)$ es el grupo de ideales fraccionales de K (3.1.2), y $P(K)$ es el subgrupo de los ideales principales.

Por otra parte, hay un homomorfismo natural sobreyectivo $K^\times \to P(K)$ cuyo núcleo es $\mathcal{O}_K^\times$. Obtenemos, entonces, la sucesión exacta

$$1 \to \mathcal{O}_K^\times \to K^\times \to I(K) \to C(\mathcal{O}_K) \to 1$$

En éste y el próximo capítulo los objetos de estudio serán $C(\mathcal{O}_K)$ y $\mathcal{O}_K^\times$, respectivamente, conúcleo y núcleo del homomorfismo $K^\times \to I(K)$. De alguna manera, dado que tenemos factorización única en $I(K)$, es decir que $I(K)$ es un grupo libre, entender éstos objetos permite completar la información sobre la estructura multiplicativa de $K^\times$.

Por una parte la estructura de $\mathcal{O}_K^\times$ influye en la definición de elementos asociados en $K^\times$. Por otra, de alguna manera $C(\mathcal{O}_K)$ es una obstrucción para factorización única en $K^\times$ (por ejemplo $C(\mathcal{O}_K)$ trivial es equivalente a factorización única en $K^\times$).

En el presente capítulo mostraremos que $C(\mathcal{O}_K)$ es un grupo abeliano *finito*, cuantificando así la falta de factorización única.

En el siguiente capítulo mostraremos que $\mathcal{O}_K^\times$ es un grupo abeliano finitamente generado, dando una formula explícita para su rango.

7.2 Finitud del grupo de clases

Teorema 7.2.1. *Sea K un cuerpo de números. Entonces existe $\lambda = \lambda(K)$ tal que todo ideal I de $\mathcal{O}_K$ contiene un $\alpha \neq 0$ tal que*

$$|N(\alpha)| \leq \lambda \cdot N(I).$$

Corolario 7.2.2. *Toda clase de ideales contiene un J entero con $N(J) \leq \lambda$.*

Demostración. Sea $\alpha \in I$ como en el teorema. Entonces $J = \alpha I^{-1}$ es entero (como $\alpha \in I$ entonces $I \mid \alpha$), y $N(J) = \frac{|N(\alpha)|}{N(I)} \leq \lambda$. □

Corolario 7.2.3. *$C(\mathcal{O}_K)$ es finito.*

Demostración. Basta ver que hay un número finito de ideales enteros J con $N(J) \leq \lambda$. Por factorización única, basta ver que hay un número finito de ideales primos en $\mathcal{O}_K$ de norma acotada, pero los ideales primos de $\mathcal{O}_K$ están arriba de primos racionales, que estarán acotados, y por lo tanto serán finitos, etc. □

Demostración del Teorema. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base entera de $\mathcal{O}_K$ y sean $\sigma_1, \ldots, \sigma_n$ los monomorfismos de K en $\mathbb{C}$. Consideremos

$$\lambda := \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |\sigma_i \alpha_j| \right).$$

Ahora, dado un ideal I, sea m el único entero positivo tal que $m^n \leq N(I) < (m+1)^n$. Los elementos

$$\sum_{j=1}^{n} m_j \alpha_j \qquad \text{con } 0 \leq m_j \leq m,$$

son $(m+1)^n$ elementos de $\mathcal{O}_K$, luego necesariamente habrá dos en la misma clase módulo I. Tomando la diferencia, encontramos

$$\alpha = \sum_{j=1}^{n} m_j \alpha_j \qquad \text{con } |m_j| \leq m,$$

cuya norma satisface

$$\begin{aligned} |N(\alpha)| = \prod_i |\sigma_i \alpha| &= \prod_i \left(\left| \sum_j m_j \sigma_i \alpha_j \right| \right) \\ &\leq \prod_i \left(m \sum_j |\sigma_i \alpha_j| \right) \leq m^n \lambda \leq N(I)\lambda, \end{aligned}$$

como queríamos probar. □

Ejemplo 7.2.4. Sea $K = \mathbb{Q}[\sqrt{2}]$, una base entera de $\mathcal{O}_K$ es $\{1, \sqrt{2}\}$, y $\lambda = (1+\sqrt{2})^2$ está entre 5 y 6. Luego, todo ideal es equivalente a uno con norma a lo sumo 5, o sea que tenemos que considerar los ideales primos arriba de 2, 3, y 5. El primero ramifica, y $(\sqrt{2})$ es un ideal primo de norma 2. En cambio, (3) y (5) son inertes en $\mathcal{O}_K$, con norma 9 y 25 respectivamente. Como $(\sqrt{2})$ es principal, se sigue que $C(\mathcal{O}_K)$ es trivial, y $\mathcal{O}_K$ es un dominio de ideales principales.

Ejemplo 7.2.5. Sea $K = \mathbb{Q}[\sqrt{-5}]$, una base entera de $\mathcal{O}_K$ es $\{1, \sqrt{-5}\}$, y $\lambda = (1+\sqrt{5})^2$ está entre 10 y 11. Todo ideal es equivalente a uno con norma a lo sumo 10. Arriba de 2 tenemos $(2, 1+\sqrt{-5})$ (ramifica), arriba de 3 tenemos $(3, 1+\sqrt{-5})$ y $(3, 1-\sqrt{-5})$, arriba de 5 tenemos $(\sqrt{-5})$, y arriba de 7 tenemos $(7, 3+\sqrt{-5})$ y $(7, 3-\sqrt{-5})$ (todos resultado de factorizar X^2+5 módulo p).

Ahora, $(2, 1+\sqrt{-5})$ tiene norma 2, y por lo tanto no es principal, pues en $\mathcal{O}_K$ no hay elementos de norma 2 ($N(a+b\sqrt{-5}) = a^2+5b^2$). Del mismo modo se ve que los ideales arriba de 3 y de 7 no son principales. Pero

$(2, 1+\sqrt{-5}) \cdot (3, 1 \pm \sqrt{-5}) = (1+\sqrt{-5})$ y una cuenta similar para los primos arriba de 7 muestra que todos estos ideales no principales son equivalentes entre sí (observar que $(2, 1+\sqrt{-5})$ tiene orden 2 en $C(\mathcal{O}_K)$). Se sigue que $C(\mathcal{O}_K) \cong \mathbb{Z}/2$.