Introducción a los Números Algebraicos
Clase 5: Factorización única II

Gonzalo Tornaría

27 de marzo, 2007

3.3 Teorema Chino de los Restos

Podemos definir el máximo comun divisor $\operatorname{mcd}(I, J)$ y el mínimo común múltiplo $\operatorname{mcm}(I, J)$ de dos ideales usando su factorización en primos. El $\operatorname{mcd}(I, J)$ será el ideal más pequeño conteniendo I y J, y el $\operatorname{mcm}(I, J)$ será el ideal más grande contenido en ambos. Es decir

$$\operatorname{mcd}(I, J) = I + J,$$
$$\operatorname{mcm}(I, J) = I \cap J.$$

Decimos que I y J son coprimos si no tienen factores primos en común, es decir si $\operatorname{mcd}(I, J) = R$.

Lema 3.3.1. *Si I y J son ideales de R coprimos, entonces existen $x \in I$ e $y \in J$ tales que $x + y = 1$.*

Demostración. Inmediato, pues $I + J = \operatorname{mcd}(I, J) = R$. □

Teorema 3.3.2. *Sea $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$ un ideal de R. Entonces el mapa natural $\phi : R \to (R/\mathfrak{p}_1^{n_1}) \times \cdots \times (R/\mathfrak{p}_s^{n_s})$ induce un isomorfismo*

$$R/I \cong (R/\mathfrak{p}_1^{n_1}) \times \cdots \times (R/\mathfrak{p}_s^{n_s})$$

Demostración. Veamos primero que ϕ es sobreyectivo: en primer lugar observemos que cada proyección $R \to R/\mathfrak{p}_i^{n_i}$ es sobreyectiva. Como $\mathfrak{p}_i^{n_i}$ es coprimo con $J := I\mathfrak{p}_i^{-n_i}$ podemos encontrar $x \in \mathfrak{p}_i^{n_i}$ e $y \in J$ tales que $x + y = 1$. Entonces $\phi(y) = 0 \times \cdots 0 \times 1_i \times 0 \times \cdots \times 0$ (pues $y \in J \subseteq \mathfrak{p}_j^{n_j}$ para $j \neq i$, y también $y \equiv 1 \pmod{\mathfrak{p}_i^{n_i}}$). Luego ϕ es sobreyectiva.

Por otra parte $\ker \phi = \bigcap_i \mathfrak{p}_i^{n_i} = \prod_i \mathfrak{p}_i^{n_i} = I$. □

Corolario 3.3.3. *Sean $I_1, \ldots, I_s$ ideales de R coprimos dos a dos y sean $\alpha_1, \ldots, \alpha_s$ elementos de R. Entonces existe $\alpha \in R$ tal que*

$$\alpha \equiv \alpha_i \pmod{I_i}$$

para todo i.

Demostración. Es la sobreyectividad de ϕ. □

Corolario 3.3.4. *Sea I un ideal en un dominio de Dedekind R, y sea $\alpha \in I$ con $\alpha \neq 0$. Entonces existe $\beta \in I$ tal que $I = (\alpha, \beta)$.*

Demostración. Alcanza encontrar $\beta \in R$ tal que $I = \operatorname{mcd}((\alpha), (\beta))$.

Sea $\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$ la descomposición en factores primos de I, donde los $\mathfrak{p}_i$ son distintos. Entonces (α) es divisible entre todos los $\mathfrak{p}_i^{n_i}$. Sean $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ los otros primos que dividen a (α).

Necesitamos construir β tal que $\mathfrak{q}_i \nmid (\beta)$ y $\mathfrak{p}_i^{n_i} \parallel (\beta)$. Esto puede conseguirse usando el *Teorema Chino de los Restos*: sea $\beta_i \in \mathfrak{p}_i^{n_i} - \mathfrak{p}_i^{n_i+1}$, y sea β que satisfaga las congruencias:

$$\beta \equiv \beta_i \pmod{\mathfrak{p}_i^{n_i+1}}$$
$$\beta \equiv 1 \pmod{\mathfrak{q}_i}$$

□

3.4 Norma de ideales

Volvemos ahora al caso del anillo de enteros $\mathcal{O}_K$ en un cuerpo de números K de grado n sobre $\mathbb{Q}$.

Definición 3.4.1. La *norma* de un ideal I de $\mathcal{O}_K$ es $N(I) := \#(\mathcal{O}_K/I)$.

La norma es finita por la Proposición 2.5.6. Muchos de los resultados que trataremos pueden generalizarse a otros dominios de Dedekind siempre y cuando cumplan la misma propiedad. Esencialmente ésto nos restringe a cuerpos de números y cuerpos de funciones de curvas sobre cuerpos finitos.

Teorema 3.4.2. *Si I y J son ideales de $\mathcal{O}_K$, entonces*

$$N(IJ) = N(I)N(J).$$

Además, para $\alpha \in \mathcal{O}_K$ *tenemos*

$$N((\alpha)) = |N_K(\alpha)|\,.$$

En particular, si $a \in \mathbb{Z}$*,*

$$N((a)) = |a|^n\,.$$

Demostración. Asumamos primero que I y J son coprimos; por el Teorema Chino de los Restos

$$R/IJ \cong (R/I) \times (R/J),$$

por lo tanto $N(IJ) = N(I)N(J)$. En virtud de ésto y por la factorización única en ideales primos, nos alcanzará probar que $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$. Para esto consideramos la cadena de ideales

$$\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p} \supset \cdots \supset \mathfrak{p}^n.$$

Necesitamos probar que $N(\mathfrak{p}) = \#(\mathfrak{p}^k/\mathfrak{p}^{k+1})$. Pero para cualquier $\alpha \in \mathfrak{p}^k - \mathfrak{p}^{k+1}$ tenemos un mapa

$$R \to \mathfrak{p}^k/\mathfrak{p}^{k+1},$$

dado por multiplicación por α. Este mapa es sobreyectivo pues se tiene que $(\alpha) + \mathfrak{p}^{k+1} = \mathfrak{p}^k$ (es el máximo común divisor, y $\mathfrak{p}^k \parallel (\alpha)$.) Por otra parte, el núcleo será $\left\{\beta \in R \;:\; \alpha\beta \in \mathfrak{p}^{k+1}\right\} = \mathfrak{p}$ (pues $\mathfrak{p}$ es primo y $\mathfrak{p}^k \parallel (\alpha)$.)

Supongamos ahora que $a \in \mathbb{Z}$. Sabemos que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango n. Entonces $\mathcal{O}_K/(a) \cong (\mathbb{Z}/a)^n$ que tiene orden a^n, luego $N((a)) = a^n$.

Finalmente, consideremos $\alpha \in \mathcal{O}_K$. Supondremos que K es una extensión normal de $\mathbb{Q}$, de modo que $\sigma(\alpha) \in \mathcal{O}_K$ para los n automorfismos σ de $\mathcal{O}_K$. Notemos que

$$N((\sigma(\alpha))) = N((\alpha)),$$

pues $\sigma : \mathcal{O}_K/\alpha \to \mathcal{O}_K/\sigma(\alpha)$ es un isomorfismo. Pero entonces

$$N((\alpha))^n = \prod_{\sigma} N((\sigma(\alpha))) = N((n)) = |n|^n\,,$$

donde $n = N_K(\alpha)$; se sigue que $N((\alpha)) = |n|$ pues ambos son positivos. $\square$