Introducción a los Números Algebraicos
Clase 6: Factorización única III

Gonzalo Tornaría

22 de marzo, 2007

3.5 Factorización de primos

Vimos ejemplos de primos en $\mathbb{Z}$ que no son irreducibles en extensiones. Por ejemplo, en $\mathbb{Z}[i]$ tenemos $5 = (2+i)(2-i)$. En $\mathbb{Z}[\sqrt{-5}]$, si bien 2 y 3 son irreducibles, no son ideales primos: $(2) = (2, 1+\sqrt{-5})^2$ y $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. Este fenómeno se llama *descomposición*. Decimos que 3 descompone en el producto de dos ideales primos en $\mathbb{Z}[\sqrt{-5}]$ y que 2 *ramifica* en $\mathbb{Z}[\sqrt{-5}]$.

Notemos que, por 2.5.5, si I es un ideal de $\mathcal{O}_K$ (en K de grado n sobre $\mathbb{Q}$) entonces $I \mid (a)$ con $a \in \mathbb{Z}$. Pero $a = p_1^{n_1} \cdots p_s^{n_s}$, de modo que:

1. si I es primo, entonces $I \mid p_i$ para algún primo racional $p_i \in \mathbb{Z}$, de modo que todos los ideales primos de $\mathcal{O}_K$ aparecen en la descomposición de los primos racionales. Observar también que si $I \mid p_i$ entonces $N(I) \mid p_i^n$.

2. En general, conocer la factorización de cada p_i es suficiente para conocer la factorización de I.

Cuando $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$, por lo dicho $\mathfrak{p} \mid p$ para algún primo racional $p \in \mathbb{Z}$. En tal caso decimos que $\mathfrak{p}$ *está arriba* de p. Notemos que $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$.

Si p es un primo racional, los primos arriba de p serán los ideales primos que aparecen en la factorización de (p). Los exponentes con los que ocurren se llaman *índices de ramificación*. Es decir que si $\mathfrak{p}$ está arriba de p entonces el índice de ramificación, denotado $e(\mathfrak{p}|p)$, es el entero $e \geq 1$ tal que $\mathfrak{p}^e \parallel (p)$. Cuando $e(\mathfrak{p}|p) > 1$ decimos que $\mathfrak{p}$ *es ramificado sobre* p. Si alguno de los

factores $\mathfrak{p}$ ramifica sobre p, decimos que p ramifica en $\mathcal{O}_K$. Dicho de otro modo, p ramifica en $\mathcal{O}_K$ sii (p) no es libre de cuadrados como ideal de $\mathcal{O}_K$.

Ejemplo 3.5.1. En $\mathbb{Z}[i]$ tenemos que $(2) = (1-i)^2$. Es decir que $(1-i)$ es ramificado sobre 2 (su índice de ramificación es 2), o sea que 2 ramifica en $\mathbb{Z}[i]$.

Ejemplo 3.5.2. En $\mathbb{Z}[\alpha]$ con $\alpha^3 = \alpha + 1$, tenemos (ejercicio 28) la factorización $(23) = (23, \alpha - 10)^2 (23, \alpha - 3)$. Es decir que 23 ramifica en $\mathbb{Z}[\alpha]$ y, más concretamente, $(23, \alpha - 10)$ es ramificado sobre 23 (con índice de ramificación 2) pero $(23, \alpha - 3)$ no lo es.

Proposición 3.5.3. *Sea p un primo racional, cuya descomposición en $\mathcal{O}_K$ es $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. Entonces $e_1 + \cdots + e_g \leq n$. Más aún, si escribimos $N(\mathfrak{p}_i) = p^{f_i}$, entonces $e_1 f_1 + \ldots e_g f_g = n$.*

Demostración. Observemos primero que, como $\mathfrak{p}_i \mid (p)$ entonces necesariamente $N(\mathfrak{p}_i) \mid N((p)) = p^n$, de modo que $N(\mathfrak{p}_i) = p^{f_i}$ con $1 \leq f_i \leq n$. Para probar la igualdad alcanza con tomar normas en la descomposición de (p), y la desigualdad es simple consecuencia pues $f_i \geq 1$ para todo i. □

El número f_i que aparece en la proposición se llama *grado de inercia* de $\mathfrak{p}_i$ sobre p (o simplemente *grado* de $\mathfrak{p}_i$), y también se lo denota $f(\mathfrak{p}_i|p)$. Otra manera de definirlo es la siguiente: sea $\mathfrak{p}$ un ideal primo sobre p. Como $\mathfrak{p} \cap \mathbb{Z} = (p)$, la inclusión $\mathbb{Z} \to \mathcal{O}_K$ induce un monomorfismo $\mathbb{Z}/(p) \to \mathcal{O}_K/\mathfrak{p}$. Éstos últimos se llaman *cuerpos residuales* correspondientes a (p) y a $\mathfrak{p}$ respectivamente. Sabemos que son cuerpos finitos, de modo que tenemos una extensión de cuerpos. El grado de inercia es el grado de dicha extensión.

Ejemplo 3.5.4. Sea p un primo racional, y consideremos el ideal $(1-\omega)$ en $\mathbb{Z}[\omega]$, donde $\omega = e^{\frac{2\pi i}{p}}$. Veremos que es primo. En efecto, sabemos que $(1-\omega)^n = (p)$, donde $n = p-1$ es el grado de $\mathbb{Q}[\omega]$ sobre $\mathbb{Q}$. Por la proposición concluimos que $(1-\omega)$ es primo pues no es posible que (p) se descomponga más (su índice de ramificación es n y su grado de inercia es 1). Alternativamente, $N((1-\omega)) = p$ es primo, así que $(1-\omega)$ tendrá que ser primo.

Ejemplo 3.5.5. En el ejercicio 27 se muestra que, en $\mathbb{Z}[\alpha]$ con $\alpha = \sqrt[3]{2}$, tenemos que $(5) = (5, \alpha+2)(5, \alpha^2 + 3\alpha - 1)$ donde el segundo factor tiene grado de inercia 2, luego el primer factor tiene grado de inercia 1.

En éste último ejemplo los grados de inercia de los primos sobre 5 no son iguales, mientras que en el ejemplo 3.5.2 los índices de ramificación de los primos sobre 23 no son iguales. Veremos que esto no puede suceder en extensiones normales.

Supongamos entonces que K es una extensión normal de $\mathbb{Q}$. Es claro que el grupo de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$ permuta los ideales primos sobre un primo racional p dado. En efecto, si $\mathfrak{p} \cap \mathbb{Z} = (p)$ entonces $\sigma(\mathfrak{p}) \cap \mathbb{Z} = \sigma((p)) = (p)$ para todo $\sigma \in G$; además $\mathfrak{p}$ primo implica que $\sigma(\mathfrak{p})$ es primo.

Proposición 3.5.6. *Sean $\mathfrak{p}$ y $\mathfrak{p}'$ dos ideales primos de $\mathcal{O}_K$ sobre el mismo primo racional p. Entonces existe $\sigma \in G$ tal que $\sigma(\mathfrak{p}) = \mathfrak{p}'$. Dicho de otro modo, la acción de G en los ideales primos sobre p es transitiva.*

Demostración. Supongamos que $\sigma(\mathfrak{p}) \neq \mathfrak{p}'$ para todo $\sigma \in G$. Por el Teorema Chino de los Restos, existe $\alpha \in \mathcal{O}_K$ tal que

$$\begin{aligned} \alpha &\equiv 0 \pmod{\mathfrak{p}'}; \\ \alpha &\equiv 1 \pmod{\sigma(\mathfrak{p})} \qquad \text{para todo } \sigma \in G. \end{aligned}$$

Pero entonces, como $\alpha \in \mathfrak{p}'$ tenemos que $N_K(\alpha) \in \mathbb{Z} \cap \mathfrak{p}' = (p)$. Por otra parte, como $\alpha \notin \sigma(\mathfrak{p})$ para todo σ tenemos que $\sigma(\alpha) \notin \mathfrak{p}$ para todo σ, y se sigue (pues $\mathfrak{p}$ es primo) que $N_K(\alpha) \notin \mathfrak{p}$, lo cual es absurdo. □

Corolario 3.5.7. *Si K es normal sobre $\mathbb{Q}$, y si $\mathfrak{p}$ y $\mathfrak{p}'$ son dos ideales primos de $\mathcal{O}_K$ sobre el mismo primo racional p, entonces $e(\mathfrak{p}|p) = e(\mathfrak{p}'|p)$ y $f(\mathfrak{p}|p) = f(\mathfrak{p}'|p)$.*

Demostración. La primer parte se ve usando factorización única. Para la segunda parte, se ve que hay un isomorfismo $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}'$ (dado por un automorfismo en G). □

3.6 Un método de factorización

Supongamos que $K = \mathbb{Q}[\alpha]$ es un cuerpo de números y $\mathcal{O}_K = \mathbb{Z}[\alpha]$ es su anillo de enteros (esto no siempre es posible, ver ejercicio 31). En este caso, es posible dar un método sencillo para factorizar primos:

Teorema 3.6.1. *Supongamos que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ y sea $F(X) = \mathrm{Irr}_{\mathbb{Q}}(\alpha)$ su polinomio minimal (mónico con coeficientes en $\mathbb{Z}$). Sea p un primo racional, y supongamos que*

$$\widetilde{F}(X) = \widetilde{F_1}(X)^{e_1} \cdots \widetilde{F_g}^{e_g}$$

es la factorización de $\widetilde{F}(X)$ en $\mathbb{Z}/(p)[X]$, con $F_i(X) \in \mathbb{Z}[X]$ mónico. Entonces

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

donde $\mathfrak{p}_i = (p, F_i(\alpha))$ es un ideal primo de grado $f_i = \mathrm{gr}\,\widetilde{F}_i(X)$.

Ejemplo 3.6.2. Sea $F(X) = X^3 + 10X + 1$. Para $p = 2, 3, 5, 7, 11, 23$ tenemos que $F(X)$ tiene una única raíz módulo p, y por lo tanto $(p) = \mathfrak{p}\mathfrak{p}'$ donde uno de los factores tiene grado 1 y el otro tiene grado 2. En el caso de $p = 13, 17, 19$, vemos que $F(X)$ no tiene raices módulo p, y por lo tanto $(p) = \mathfrak{p}$ es inerte (de grado 3). Para $p = 29$, vemos que $F(X)$ tiene tres raíces distintas módulo p, y se sigue que $(p) = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$.

Demostración. Tenemos un isomorfismo $\mathbb{Z}[X]/(F(X)) \to \mathcal{O}_K$ dado por $X \mapsto \alpha$. Éste induce un isomorfismo

$$(\mathbb{Z}/(p))[X]/(\widetilde{F}(X)) = \mathbb{Z}[X]/(p, F(X)) \cong \mathcal{O}_K/(p).$$

Entonces los ideales de $\mathcal{O}_K$ sobre p corresponden con ideales en $\mathcal{O}_K/(p)$, que a su vez corresponden a través del isomorfismo con ideales en $(\mathbb{Z}/(p))[X]$ que contienen a $\widetilde{F}(X)$, i.e. factores de $\widetilde{F}(X)$ (pues $(\mathbb{Z}/(p))[X]$ es un dominio principal). Para obtener $f_i = \mathrm{gr}\,\widetilde{F}_i(X)$ alcanza con mirar los cuerpos residuales a través de la correspondencia. □

Corolario 3.6.3. *En la hipótesis del teorema, p es ramificado si y solamente si $p \mid \Delta(\alpha) = \pm \prod_{i<j} (\alpha_i - \alpha_j)^2$.*