Introducción a los Números Algebraicos

Clase 10: Cuerpos ciclotómicos III

Gonzalo Tornaría

19 de abril, 2007

6.3 Factorización de primos

Investiguemos ahora la factorización de primos racionales en K_m Sea $p \in \mathbb{Z}$ un primo. Como $K_m/\mathbb{Q}$ es normal, sabemos que

$$(p) = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g)^e,$$

donde los $\mathfrak{p}_i$ son distintos ideales primos de $\mathbb{Z}[\zeta_m]$, todos con el mismo grado de inercia f. Además tenemos que $efg = \varphi(m)$.

Teorema 6.3.1. *Sea $m = p^k m_0$, con $p \nmid n$. Entonces $e = \varphi(p^k)$, y f es el orden (multiplicativo) de p módulo m_0.*

Demostración. Sea $n = \varphi(m)$ el grado de K_m sobre $\mathbb{Q}$.

Primer caso: $m = p^k$. En este caso, tenemos que $p = u(1-\zeta_m)^n$ (ejercicio 43). Se sigue que $(p) = \mathfrak{p}^n$, donde $\mathfrak{p} = (1-\zeta_m)$ es el único ideal primo arriba de p, y tiene grado 1, es decir que p ramifica completamente en K_m.

Segundo caso: $m = m_0$. Como en este caso $p \nmid \Delta(\mathcal{O}_K)$ (Proposición 6.2.1), tenemos que p no ramifica (Corolario 3.6.3), de modo que

$$(p) = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g.$$

donde los $\mathfrak{p}_i$ son distintos ideales primos, todos con el mismo grado de inercia f, y donde $fg = n$.

Recordemos que $G = \mathrm{Gal}(K_{m_0}/\mathbb{Q})$ es canónicamente isomorfo a $(\mathbb{Z}/m_0)^\times$. Llamemos σ_p al automorfismo de K_{m_0} correspondiente a p mod m_0, que está determinado por $\sigma_p(\zeta_{m_0}) = \zeta_{m_0}^p$. Debemos probar que σ_p tiene orden f en G.

Fijemos cualquier $\mathfrak{p} = \mathfrak{p}_i$; el cuerpo finito $\mathbb{Z}[\zeta_{m_0}]/\mathfrak{p}$ tiene grado f sobre $\mathbb{Z}/p$ por definición. Luego, el grupo de Galois de $\mathbb{Z}[\zeta_{m_0}]/\mathfrak{p}$ sobre $\mathbb{Z}/p$ es cíclico de orden f, generado por el automorfismo $\tau(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}$.

Para terminar de probar este caso, alcanza mostrar que $\sigma_p^a = 1$ sii $\tau^a = 1$, pues en tal caso se sigue que el orden de σ_p es igual al orden de τ. El paso clave es ver que $1, \zeta_{m_0}, \zeta_{m_0}^2, \ldots, \zeta_{m_0}^{n-1}$ son todos diferentes módulo $\mathfrak{p}$.

Otra forma de verlo es mostrar que $\sigma_p\mathfrak{p} = \mathfrak{p}$, y por lo tanto hay un mapa natural

$$\langle\sigma_p\rangle \longrightarrow \mathrm{Gal}(\mathbb{Z}[\zeta_{m_0}]/\mathfrak{p}, \mathbb{Z}/p),$$

inducido por la proyección $\mathbb{Z}[\zeta_{m_0}] \to \mathbb{Z}[\zeta_{m_0}]/\mathfrak{p}$, que manda σ_p en τ (y por lo tanto es sobreyectivo). Este mapa es inyectivo pues si $\zeta_{m_0}^{p^a} \equiv \zeta_{m_0} \pmod{\mathfrak{p}}$, entonces $p^a \equiv 1 \pmod{n}$ por lo antes dicho ($1, \zeta_{m_0}, \zeta_{m_0}^2, \ldots, \zeta_{m_0}^{n-1}$ son todos diferentes módulo $\mathfrak{p}$).

Finalmente, podemos probar el caso general: sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ los primos de $\mathbb{Z}[\zeta_{m_0}]$ arriba de p, y fijemos primos $\mathfrak{P}_1 \ldots, \mathfrak{P}_g$ arriba de éstos. Entonces $f(\mathfrak{P}_i|p) \geq f(\mathfrak{p}_i|p)$. Por otra parte, como $(1-\zeta_{p^k})$ es el único primo en $\mathbb{Z}[\zeta_{p^k}]$ arriba de p, se sigue que los $\mathfrak{P}_i$ están arriba de $(1-\zeta_{p^k})$, y por lo tanto $e(\mathfrak{P}_i|p) \geq e(1-\zeta_{p^k}|p)$. El resultado se sigue pues el grado de $\mathbb{Q}[\zeta_m]$ sobre $\mathbb{Q}$ es $\varphi(m) = \varphi(p^k)\varphi(m_0)$ y las desigualdades que hemos probado son necesariamente igualdades. □

Corolario 6.3.2. *Supongamos $p \nmid m$, y sea $D_\mathfrak{p} = \{\sigma \in G : \sigma\mathfrak{p} = \mathfrak{p}\}$. Entonces $D_\mathfrak{p}$ es cíclico de orden f, generado por σ_p.*

Demostración. Ya vimos que $\sigma_p \in D_\mathfrak{p}$ tiene orden f. Como $G/D_\mathfrak{p}$ actúa transitivamente sobre los primos arriba de p, su orden es al menos g, pero $fg = n$, así que necesariamente $\langle\sigma_p\rangle = D_\mathfrak{p}$. □

6.4 La Ley de Reciprocidad Cuadrática

Sea p un primo impar y consideremos el cuerpo $K_p = \mathbb{Q}[\zeta_p]$. Este cuerpo contiene la raíz cuadrada de $p^* = (-1)^{(p-1)/2}p$ (ejercicio 20). Sea $g \in K_p$ tal que $g^2 = p^*$. Aunque no la usaremos aquí, es posible dar una expresión explícita para g como una *suma de Gauss*, a saber $g = \sum_{a=1}^{p}\left(\frac{a}{p}\right)\zeta_p^a$.

Supongamos que $q \neq p$ es otro primo impar. Consideremos el automorfismo σ_q de K_p. Entonces $\sigma_q g = \pm g$, donde el signo es $+$ si y solo si $\sigma_q \in \mathrm{Gal}(K_p/\mathbb{Q}[g])$. Como el grupo $G = \mathrm{Gal}(K_p/\mathbb{Q})$ es isomorfo a $(\mathbb{Z}/p)^\times$, grupo cíclico de orden $p-1$, vemos que $\sigma_q g = g$ si y solamente si σ_q es un cuadrado en G, si y solamente si q es un cuadrado módulo p. Dicho de otro modo

$$\sigma_q g = \left(\frac{q}{p}\right) g.$$

Consideremos ahora un ideal primo $\mathfrak{q}$ en K_p arriba de q. Entonces

$$\sigma_q g \equiv g^q \pmod{\mathfrak{q}},$$

y se sigue que $\left(\frac{q}{p}\right) g \equiv g^q \pmod{\mathfrak{q}}$, por lo tanto

$$\left(\frac{p^*}{q}\right) \equiv (p^*)^{(q-1)/2} \equiv g^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{\mathfrak{q}}.$$

Esto último demuestra (ya que $2 \notin \mathfrak{q}$) la primer parte de

Teorema 6.4.1 (Ley de Reciprocidad Cuadrática)**.** *Sean $p \neq q$ primos racionales impares. Entonces $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$, donde $p^* = \pm p \equiv 1 \pmod 4$. Además $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ y $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.*

Corolario 6.4.2. *Sea Δ un discriminante fundamental. Entonces $\left(\frac{\Delta}{p}\right)$ depende solamente de $p \bmod \Delta$. Más aún, existe un subgrupo H de $(\mathbb{Z}/\Delta)^\times$ de índice 2 tal que $\left(\frac{\Delta}{p}\right) = 1$ sii $p \in H$.*

Demostración. Alcanza con probarlo para un *discriminante primo*, es decir p^* con p primo impar, -4 y ± 8. Esto se sigue directamente de la Ley de Reciprocidad Cuadrática. $\square$