Introducción a los Números Algebraicos
Clase 9: Cuerpos ciclotómicos II

Gonzalo Tornaría

17 de abril, 2007

6.2 Enteros algebraicos

Recordemos que $\Delta(\zeta_p) = \pm p^{p-2}$ (ejercicio 19). Es posible calcular una fórmula similar para $\Delta(\zeta_m)$ en general, pero es complicada y para nuestros propósitos nos alcanzará con

Proposición 6.2.1. $\Delta(\zeta_m) \mid m^{\varphi(m)}$.

Demostración. Como ζ_m es raíz de X^m-1, y $\Phi_m(X)$ es su polinomio minimal, se sigue que $X^m-1 = \Phi_m(X)g(X)$ con $g(X) \in \mathbb{Z}[X]$. Derivando y evaluando en ζ_m obtenemos

$$m\zeta_m^{m-1} = \Phi_m'(\zeta_m)g(\zeta_m).$$

Como $\zeta_m^m = 1$, es lo mismo

$$m = \zeta_m\Phi_m'(\zeta_m)g(\zeta_m).$$

Tomando normas, como $N(\zeta_m) = 1$ y $\Delta(\zeta_m) = N(\Phi_m'(\zeta_m))$, resulta

$$m^\varphi(m) = \Delta(\zeta_m)N(g(\zeta_m)),$$

lo que demuestra la proposición, pues $N(g(\zeta_m)) \in \mathbb{Z}$. □

Ahora estamos listos para determinar el anillo de enteros de $K_m = \mathbb{Q}[\zeta_m]$.

Teorema 6.2.2. $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$.

Demostración, caso $m = p^r$. Denotaremos $n = \varphi(m)$ al grado de K_m sobre $\mathbb{Q}$. Observemos que, claramente, $\mathbb{Z}[\zeta_m] = \mathbb{Z}[1-\zeta_m]$. Por la proposición anterior, $\Delta(\zeta_m) = \Delta(1-\zeta_m)$ es una potencia de p. Se sigue que el índice de $\mathbb{Z}[1-\zeta_m]$ en $\mathcal{O}_{K_m}$ es también una potencia de p, y por lo tanto todo elemento de $\mathcal{O}_{K_m}$ puede escribirse como

$$\frac{t_1 + t_2(1-\zeta_m) + \cdots + t_n(1-\zeta_m)^{n-1}}{p^r},$$

con $t_i \in \mathbb{Z}$. Supongamos por absurdo que $\mathbb{Z}[1-\zeta_m] \neq \mathcal{O}_{K_m}$. Entonces existe $\alpha \in \mathcal{O}_{K_m}$ tal que

$$p\alpha = t_k(1-\zeta_m)^{k-1} + \cdots + t_n(1-\zeta_m)^{n-1},$$

con $t_i \in \mathbb{Z}$ y $p \nmid t_k$. Como $(1-\zeta_m)^n \mid p$ (verificar), concluimos que

$$(1-\zeta_m)^k \mid t_k(1-\zeta_m)^{k-1}.$$

Pero tomando normas resulta $p^k \mid (t_k)^n p^{k-1}$ lo que es absurdo pues $p \nmid t_k$. □

Para probar el teorema en general necesitamos un resultado sobre anillos de enteros en cuerpos compuestos (ejercicio 40).

Proposición 6.2.3. *Sean K y L cuerpos de números de grado m y n, y supongamos que KL tiene grado mn. Entonces*

$$\mathcal{O}_K\mathcal{O}_L \subseteq \mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L,$$

donde $d = \operatorname{mcd}(\Delta(\mathcal{O}_K), \Delta(\mathcal{O}_L))$.

Corolario 6.2.4. *Si* $[KL:\mathbb{Q}] = [K:\mathbb{Q}][L:\mathbb{Q}]$, *y* $\operatorname{mcd}(\Delta(\mathcal{O}_K), \Delta(\mathcal{O}_L)) = 1$, *entonces* $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$.

Demostración del teorema, caso general. Ya hemos probado el teorema en el caso en que m es potencia de un primo. En otro caso, podemos escribir $m = m_1m_2$ con $\operatorname{mcd}(m_1, m_2) = 1$. Por inducción en m, podemos asumir que $\mathcal{O}_{K_{m_i}} = \mathbb{Z}[\zeta_{m_i}]$. Como $\varphi(m) = \varphi(m_1)\varphi(m_2)$ (pues φ es multiplicativa), y puesto que $\Delta(\mathcal{O}_{K_{m_i}}) \mid m_i^{\varphi(m_i)}$, estamos en las hipótesis del corolario. Luego

$$\mathcal{O}_{K_m} = \mathcal{O}_{K_{m_1}}\mathcal{O}_{K_{m_2}} = \mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}] = \mathbb{Z}[\zeta_{m_1}, \zeta_{m_2}] = \mathbb{Z}[\zeta_m].$$

□

Para la demostración de la Proposición 6.2.3 (ejercicio 40) se sugiere utilizar el siguiente lema de teoría de cuerpos

Lema 6.2.5. *Suponiendo $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$, si σ es un monomorfismo de K y τ es un monomorfismo de L, existe un (único) monomorfismo de KL cuya restricción a K es σ y cuya restricción a L es τ.*

Sea $\{\alpha_1, \ldots, \alpha_m\}$ una base entera de $\mathcal{O}_K$, de discriminante $\Delta = \Delta(\mathcal{O}_K)$. Si $\alpha \in \mathcal{O}_{KL}$, podemos escribir $\Delta\alpha = \sum \alpha_i \beta_i$, donde $\beta_i \in L$. Por el lema, cada monomorfismo σ de K extiende a un único monomorfismo, que también llamamos σ, que deja fijo todos los elementos de L. Conseguimos así m ecuaciones que involucran los β_i. Usar la regla de Cramer para despejar los β_i y probar que son enteros (¿dónde aparece Δ?), etc.

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. Continuará... □