Introducción a los Números Algebraicos

# Clase 8: Cuerpos ciclotómicos

Gonzalo Tornaría

12 de abril, 2007

## 6 Cuerpos ciclotómicos

Sea $m$ un entero positivo, y sea $\zeta_m := e^{\frac{2\pi i}{m}}$ (una *raíz primitiva $m$-ésima de la unidad*. Observar que $\zeta_m$ es raíz del polinomio $X^m - 1 = 0$, y lo mismo es cierto para todas las potencias de $\zeta_m$, de las cuales hay $m$ distintas, a saber $\{\zeta_m, \zeta_m^2, \ldots, \zeta_m^m = 1\}$. Se concluye que $K_m := \mathbb{Q}[\zeta_m]$ es el cuerpo de descomposición de $X^m - 1$, y por lo tanto es una extensión de Galois de $\mathbb{Q}$, que llamamos *$m$-ésimo cuerpo ciclotómico* o alternativamente *cuerpo ciclotómico de raíces $m$-ésimas de la unidad*.

### 6.1 El grupo de Galois

Denotemos $G_m := \mathrm{Gal}(K_m/\mathbb{Q})$ el grupo de automorfismos de $K_m$.

**Proposición 6.1.1.** *Existe un monomorfismo $\theta : G_m \to (\mathbb{Z}/m)^\times$ tal que para $\sigma \in G$*

$$\sigma(\zeta_m) = \sigma_m^{\theta(\sigma)}.$$

*Demostración.* Como $\zeta_m$ es raíz de $X^m - 1$, entonces $\sigma(\zeta_m)$ también lo será, y se sigue que $\sigma(\zeta_m) = \zeta_m^{\theta(\sigma)}$, donde $\theta(\sigma)$ es un entero bien definido módulo $m$. Es claro que $\sigma \mapsto \theta(\sigma)$ es multiplicativo, y como $G$ es un grupo se sigue que la imagen de $\theta$ está contenida en $(\mathbb{Z}/m)^\times$. Finalmente, si $\theta(\sigma) \equiv 1 \pmod m$, se sigue que $\sigma(\zeta_m) = \zeta_m$, luego $\sigma = 1$ pues $\zeta_m$ genera $K_m/\mathbb{Q}$, de modo que $\theta$ es inyectivo. □





Decimos que una extensión $K/\mathbb{Q}$ es *abeliana* si es normal su grupo de Galois es abeliano.

**Corolario 6.1.2.** *$K_m/\mathbb{Q}$ es una extensión abeliana, y $[K_m : \mathbb{Q}] \mid \varphi(m)$.*

Este corolario tiene una suerte de recíproco, el Teorema de Kronecker-Weber, que afirma que cualquier extensión abeliana de $\mathbb{Q}$ está contenida en un cuerpo ciclotómico!

**Definición 6.1.3.** Sea $\Phi_m(X) := \prod_{i \in (\mathbb{Z}/m)^\times} (X - \zeta_m^i)$ el *$m$-ésimo polinomio ciclotómico*.

Las raíces de $\Phi_m(X)$ son precisamente las raíces $m$-ésimas primitivas de la unidad. Puesto que todos los conjugados de $\zeta_m$ son raíces $m$-ésimas primitivas, y lo mismo puede decirse de cualquier raíz $m$-ésima primitiva, se sigue que $\Phi_m(X) \in \mathbb{Z}[X]$.

Es claro que el grado de $\Phi_m(X)$ es $\varphi(m)$.

Mostraremos ahora que $\theta$ es sobreyectivo; equivalentemente, $[K_m : \mathbb{Q}] = \varphi(m)]$, o $\Phi_m(X)$ es irreducible.

**Lema 6.1.4.** *Si $p \nmid m$ es primo, entonces $\zeta_m^p$ es conjugado a $\zeta_m$.*

*Demostración.* Sea $f(X) \in \mathbb{Z}[X]$ el polinomio minimal de $\zeta_m$. Entonces $X^m - 1 = f(X)g(X)$ con $f(X), g(X) \in \mathbb{Z}[X]$ mónicos. Es claro que $\zeta_m^p$ es raíz de $X^m - 1$. Debemos probar que $\zeta_m^p$ es raíz de $f(X)$. Supongamos por el contrario, que $\zeta_m^p$ es raíz de $g(X)$. Entonces $\zeta_m$ es raíz de $g(X^p)$, de modo que $f(X) \mid g(X^p)$.

Considerando estos polinomios módulo $p$, y debido a que $g(X^p) \equiv g(X)^p \pmod p$, concluimos que $\overline{f}(X) \mid \overline{g}(X)^p$ en $(\mathbb{Z}/p)[X]$, que es un dominio de factorización única. Entonces $\overline{f}(X)$ y $\overline{g}(X)$ tienen un factor común, cuyo cuadrado divide a $\overline{X^m - 1} = \overline{f}(X)\overline{g}(X)$. Pero esto es imposible, pues la derivada de $\overline{X^m - 1}$ es $\overline{m}X^{m-1} \not\equiv 0 \pmod p$ (pues $p \nmid m$). □

**Teorema 6.1.5.** *El polinomio ciclotómico $\Phi_m(X)$ es irreducible.*

*Demostración.* Alcanza probar que todo $\zeta_m^i$ con $\mathrm{mcd}(i, m) = 1$ es conjugado a $\zeta_m$. En efecto, esto se sigue de aplicar el Lema reiteradas veces a los factores primos de $i$ (y observar que $\zeta_m$ conjugado a $\zeta_m^p$ implica $\zeta_m^j$ conjugado a $\zeta_m^{jp}$, etc.) □

**Corolario 6.1.6.** *El mapa $\theta$ es sobreyectivo, $[K_m : \mathbb{Q}] = \varphi(m)$, y el grupo de Galois $G_m$ es canónicamente isomorfo a $(\mathbb{Z}/m)^\times$.*