Introducción a los Números Algebraicos

Clase 13: Ramificación

Gonzalo Tornaría

3 de mayo, 2007

4.5 Ramificación

Teorema 4.5.1. *Sea K un cuerpo de números, y sea p primo racional. Entonces p ramifica en K sii $p \mid \Delta(\mathcal{O}_K)$.*

Demostración. Sea $\{\alpha_1, \dots, \alpha_n\}$ una base entera de $\mathcal{O}_K$. Denotemos $\sigma_1, \dots, \sigma_n$ los monomorfismos de K en $\mathbb{C}$, donde n es el grado de K, que extendemos a automorfismos de la clausura normal L de K. Denotemos $G = \mathrm{Gal}(L/\mathbb{Q})$.
($\rightarrow$) Sea $\mathfrak{p} \mid p$ con $e(\mathfrak{p}|p) > 1$. Entonces podemos escribir $(p) = \mathfrak{p}I$, donde I es un ideal de K que es múltiplo de todos los primos arriba de p.

Sea $\alpha \in I - (p)$, es decir que α es múltiplo de todos los primos de K arriba de p, sin ser múltiplo de p. Podemos escribir $\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n$, donde $m_i \in \mathbb{Z}$ y, reordenando los α_i si es necesario, podemos suponer $p \nmid m_1$. Entonces

$$\Delta(\alpha, \alpha_2, \dots, \alpha_n) = m_1^2 \Delta(\mathcal{O}_K),$$

y como $p \nmid m_1$ alcanza probar que $p \mid \Delta(\alpha, \dots)$. Pero α es múltiplo de todos los primos de K arriba de p, luego es múltiplo de todos los primos de L arriba de p. Fijemos un primo $\mathfrak{q} \mid p$ en L. Como $L/\mathbb{Q}$ es normal, entonces $\sigma_i(\alpha) \in \sigma_i(\sigma_i^{-1}(\mathfrak{q})) = \mathfrak{q}$ para todo i. Entonces $\Delta(\alpha, \dots) \in \mathfrak{q} \cap \mathbb{Z} = (p)$, como afirmamos.
($\leftarrow$) Supongamos $\Delta(\mathcal{O}_K) = \det(T^K(\alpha_i\alpha_j)) \equiv 0 \pmod p$. Entonces, por álgebra lineal sobre el cuerpo $\mathbb{Z}/p$, existe un $\alpha \in \mathcal{O}_K$ tal que $T^K(\alpha\alpha_i) \equiv 0 \pmod p$ para todo i, es decir que $T^K(\alpha\mathcal{O}_K) \subseteq p\mathbb{Z}$, con $\alpha \notin p\mathcal{O}_K$. Un poco más de álgebra lineal muestra que, además

$$T^L(\alpha\mathcal{O}_L) = T^K(T^L_K(\alpha\mathcal{O}_L)) = T^K(\alpha T^L_K(\mathcal{O}_L)) \subseteq T^K(\alpha\mathcal{O}_K) \subseteq p\mathbb{Z}.$$

Supongamos que p no es ramificado en K. Por 4.1.4 tampoco lo será en L, y como $\alpha \notin p\mathcal{O}_K = p\mathcal{O}_L \cap K$, debe haber un ideal primo $\mathfrak{q} \mid p$ en L tal que $\alpha \notin \mathfrak{q}$ (¿cómo se usa que p no ramifica en L?). Más aún, podemos suponer que α está en todos los otros primos de L arriba de p (si no multiplicarlo por $\beta \in \mathcal{O}_L$ con $\beta \notin \mathfrak{q}$ pero en todos los otros primos de L arriba de p, que existe por el Teorema Chino de los Restos).

Entonces tenemos

1. $T^L(\alpha\mathcal{O}_L) \subseteq p\mathbb{Z} \subseteq \mathfrak{q}$.
2. $\sigma(\alpha\mathcal{O}_L) \subseteq \mathfrak{q}$ para todo $\sigma \in G - D_{\mathfrak{q}}$ (pues $\sigma^{-1}(\mathfrak{q}) \neq \mathfrak{q}$ para un tal σ).

Concluimos que $\sum_{\sigma \in D_{\mathfrak{q}}} \sigma(\alpha\gamma) \in \mathfrak{q}$ para todo $\gamma \in \mathcal{O}_L$. Pero como estamos suponiendo que p no es ramificado en L, se sigue que $I_{\mathfrak{q}}$ es trivial, y tenemos $D_{\mathfrak{q}} \xrightarrow{\sim} \overline{G} = \mathrm{Gal}(k_{\mathfrak{q}}/\mathbb{F}_p)$. Luego,

$$\sum_{\overline{\sigma} \in \overline{G}} \overline{\sigma}(\overline{\alpha}\,\overline{\gamma}) = 0$$

en $k_{\mathfrak{q}}$, lo que es lo mismo, pues γ es arbitrario,

$$\sum_{\overline{\sigma} \in \overline{G}} \overline{\sigma}(x) = 0$$

para todo $x \in k_{\mathfrak{q}}$. Esto es una contradicción, pues los automorfismos de un cuerpo son linealmente independientes por el siguiente Lema. □

Lema 4.5.2. *Sea F un cuerpo cualquiera. Distintos automorfismos $\sigma_1, \dots, \sigma_n$ de F son siempre linealmente independientes (como funciones de F en F).*

Demostración. Ejercicio (3p. como parte de la entrega 4). Suponer que $a_1\sigma_1 + \ldots + a_n\sigma_n = 0$ con $a_i \in F$ no todos cero, y con n minimal. Sea $x \in F$ tal que $\sigma_1(x) \neq \sigma_n(x)$. Mostrar que $\sum a_i\sigma_i(x)\sigma_i = 0$ y por otra parte $\sum a_i\sigma_1(x)\sigma_i = 0$, obtener una contradicción a la minimalidad de n. □