TEORÍA DE GALOIS

Anexo Hoja 3. El Teorema del Elemento Primitivo.

Teorema del Elemento Primitivo. *Sea E/K una extensión de cuerpos finita y separable. Entonces la extensión E/K es simple, i.e., existe $\Theta \in E$ tal que $E = K(\Theta)$.*

---

1. El objetivo de este ejercicio es dar una demostración de este teorema cuando K es infinito (el caso en el que K es finito lo veremos en clase).

a) Demuestra que basta probar el teorema en el caso en el que $E = K(\alpha, \beta)$ con $\alpha, \beta \in E$ separables sobre K.

b) Sean $p_\alpha(x), p_\beta(x) \in K[x]$ los polinomios mínimos de α y β sobre K (respectivamente). Sea L el cuerpo de descomposición de $p_\alpha(x) \cdot p_\beta(x)$ sobre K. Entonces en $L[x]$,

$$p_\alpha(x) = (x - a_1) \cdots (x - a_n), \quad p_\beta(x) = (x - b_1) \cdots (x - b_m) \tag{1}$$

con $a_1, \ldots, a_n, b_1, \ldots, b_m \in L$ y $a_i \neq a_j$ para $i \neq j$; $b_i \neq b_j$ para $i \neq j$. Supongamos que $a_1 = \alpha$ y $b_1 = \beta$. Demuestra que existe un elemento $c \in K$ tal que:

$$c \neq \frac{a_i - \alpha}{\beta - b_j} \tag{2}$$

para $i = 1, \ldots, n$ y $j = 2, \ldots, m$.

c) Definimos

$$\Theta := \alpha + c\beta. \tag{3}$$

Prueba que para concluir la demostración del teorema basta ver que $\beta \in K(\Theta)$.

d) Demuestra que β es una raíz común de los polinomios:

$$p_\alpha(\Theta - cx),\ p_\beta(x) \in K(\Theta)[x]. \tag{4}$$

e) Definimos:

$$d(x) := \text{m.c.d}_{K(\Theta)[x]}(p_\alpha(\Theta - cx),\ p_\beta(x)) \in K(\Theta)[x]. \tag{5}$$

Usando el apartado anterior demuestra que el grado de $d(x)$ es mayor o igual que 1. Usando la factorización en (1) y la definición de c en (2) concluye que el grado de $d(x)$ es exactamente uno.

f) Deduce del apartado anterior que $\beta \in K(\Theta)$.

2. Revisa la demostración del ejercicio 1. Responde de manera razonada a las siguientes preguntas:

a) ¿Dónde se usa que K es infinito?

b) ¿Dónde se usa la hipótesis de la separabilidad?

c) ¿Habría valido la misma desmostración si no suponemos que α es separable sobre K?

d) Usando tus respuestas a los apartados anteriores, ¿crees que se puede debilitar alguna de las hipótesis del teorema?

3. Encuentra elementos primitivos en el caso de las siguientes extensiones:

a) $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$;

b) $\mathbb{Q}(\sqrt{2}, i, \sqrt[3]{5})/\mathbb{Q}$;

c) $\mathbb{Q}(\sqrt{2}, i, \sqrt[3]{2})/\mathbb{Q}(i)$.