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 $\gamma \in E$ tal que $E = K(\gamma)$.*

El objetivo de este ejercicio es dar una demostración de este teorema en el caso en que K es infinito (cuando K es finito, el resultado es una consecuencia casi directa del hecho de que $K^\times$ es un grupo cíclico, y lo veremos en clase).

A partir de ahora supondremos que K es infinito. Como E/K es una extensión finita, existen $\alpha_1, \ldots, \alpha_r \in E$ tales que $E = K(\alpha_1, \ldots, \alpha_r)$ (por ejemplo, tomando los elementos de una K-base de E).

1. Sea $E = K(\alpha_1, \ldots, \alpha_r)/K$ una extensión separable, queremos probar que es simple. Procede por inducción y muestra que la prueba se reduce al caso en que $E = K(\alpha, \beta)$.

2. Sea $E = K(\alpha, \beta)$ con $\alpha, \beta \in E$ separables (en particular, algebraicos), queremos probar que existe un $\gamma \in E$ tal que $E = K(\gamma)$.

a) Sean $p = \mathrm{Irr}(\mathrm{K}, \alpha)$ y $q = \mathrm{Irr}(K, \beta)$ los polinomios mínimos de α y β sobre K. Sea L el cuerpo de escisión de $f = pq$ sobre K, notad que $\alpha, \beta \in L$. En particular, p y q se escinden en $L[x]$. Luego

$$p(x) = (x - a_1) \cdots (x - a_n), \text{ y } q(x) = (x - b_1) \cdots (x - b_m) \tag{1}$$

donde $a_1, \ldots, a_n$ son las raíces de p en L y $b_1, \ldots, b_m \in L$ son las raíces de q en L. (Como α y β son separables, se tiene que $a_i \neq a_j$ y $b_i \neq b_j$ siempre que $i \neq j$.) Podemos suponer que $\alpha = a_1$ y $\beta = b_1$. Demuestra que existe un elemento $c \in K$ tal que

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

para $i = 1, \ldots, n$ y $j = 2, \ldots, m$. En particular $c \neq 0$.

b) Elegimos un $c \in K$ que satisfaga (2), y definimos

$$\gamma = c\beta - \alpha. \tag{3}$$

Es obvio que $K(\gamma) \subseteq K(\alpha, \beta)$. Queremos ver que estos dos cuerpos son iguales. Prueba que para concluir la demostración del teorema basta con probar que $\beta \in K(\gamma)$.

c) Ahora queremos probar $\beta \in K(\gamma)$. Empieza por demostrar que β es una raíz común de los polinomios g y q donde

$$g(x) = p(cx - \gamma) \in K(\gamma)[x] \subseteq L[x]. \tag{4}$$

d) Sea $d = \mathrm{mcd}(g, q) \in K(\gamma)[x]$ el máximo común divisor de g y q. Usando el apartado anterior concluye que $x - \beta$ divide a d. *Recuerda que el máximo común divisor de dos polinomios definidos sobre un cuerpo F no depende de la extensión de F en la que lo calculemos.*

e) Prueba que $d(x) = x - \beta$ por reducción al absurdo (si $\delta(d) > 1$ entonces g y q tienen otra raíz en común). Usa la factorización de q en (1) y la elección de c satisfaciendo (2).

f) Concluye del apartado anterior que $\beta \in K(\gamma)$ y, por tanto, $K(\alpha, \beta) = K(\gamma)$.

3. Revisa la demostración del ejercicio 2. 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? *Puedes pensar en la extensión E/K donde $K = \mathbb{F}_p(t^p, u^p)$, funciones sobre $\mathbb{F}_p$ en las variables t^p y u^p, y $E = \mathbb{F}_p(t,u) = K(u,t)$. En este caso $p(x) = x^p - t^p$ y $q(x) = x^p - u^p$. Si tomamos $c = 1$ (pues en este caso no obtenemos condiciones sobre c), ¿quiénes serían g y d? Nota que $d = g = p \in K[x]$ así que no obtenemos ninguna información sobre $\gamma = u - t$ en este caso. De hecho, la extensión E/K no es simple. Es fácil ver que $|E : K| = p^2$ y que para cada $\alpha \in E$, se tiene que $\alpha^p \in K$, por lo que E/K no tiene elemento primitivo.*

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?

4. Dada una extensión E/K finita y separable, por el Teorema del Elemento Primitivo sabemos que existe un elemento $\gamma \in E$ tal que $E = K(\gamma)$. Un elemento tal se denomina *elemento primitivo* de la extensión. Encuentra elementos primitivos para las siguientes extensiones:

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

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

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

Nota: El Teorema del Elemento Primitivo también se puede probar como consecuencia del Teorema Fundamental de Galois y un resultado de Artin que dice que una extensión E/K finita es simple si, y solo si, tiene un número finito de subcuerpos intermedios. Si el tiempo nos lo permite, lo veremos en el tema de aplicaciones.