Extensiones normales

Facultad de Ciencias UNAM

Introducción

En esta sección vamos a demostrar una propiedad importante de los campos de descomposición. Esto nos llevara al concepto de *extensión normal*.

Si un campo de descomposición tiene *una* raíz de un polinomio irreducible, entonces tiene *todas* sus raíces

Proposición 1

Supongamos que F es un campo, que $f(x) \in F[x]$, y que L es un campo de descomposición de $f(x)$. Si $p(x) \in F[x]$ es irreducible en $F[x]$ y L contiene una raíz de $p(x)$, entonces $p(x)$ se descompone en L/F.

Demostración. Supongamos que M es un campo de descomposición de $f(x)p(x) \in F(x) \subset L[x]$ sobre L. Como

1. $f(x)p(x)$ se descompone en M/F,
2. $f(x)$ se descompone en M/F (pues $L \subset M$ y L es campo de descomposición de $f(x)$), y
3. las factorizaciones en irreducibles (y en particular la factorización de la definición de "$f(x)$ se descompone en K/F") son únicas

entonces, $p(x)$ se descompone en M/F, digamos

$$p(x) = c(x - \alpha_1)^{k_1} \cdots (x - \alpha_m)^{k_m}$$

con $c \in F$, $\alpha_1, \ldots, \alpha_m \in M$, y $k_1, \ldots, k_m \in \mathbb{Z}_{\geq 0}$.

Por hipótesis, L contiene una raíz de $p(x)$. Sin perdida de generalidad, supongamos que esta raíz es α_1. Como queremos ver que $p(x)$ se descompone en L/F, basta ver que $\alpha_2, \ldots, \alpha_n \in L$. Para esto, demostraremos que si $\alpha, \alpha' \in M$ son raíces de $p(x)$, entonces

$$[L(\alpha) : L] = [L(\alpha') : L] \tag{1}$$

Antes que nada, veamos porque nos interesa esta igualdad. Específicamente, veamos que la implicación $\alpha_1 \in L \implies \alpha_2, \ldots, \alpha_n \in L$ es consecuencia inmediata de esta igualdad:
Como $\alpha_1 \in L$, entonces $[L(\alpha_1) : L] = 1$, de donde (por (1)), $[L(\alpha_j) : L] = 1$ o equivalentemente, $\alpha_i \in L$ para toda $i \in \{2, \ldots, n\}$.

Por lo tanto, solo resta probar (1). Para esto, supongamos que $\alpha, \alpha' \in M$ son raíces de $p(x)$ y consideremos las siguientes inclusiones:

$$K \subset K(\alpha) \subset L(\alpha) \subset M$$

Por lo tanto, podemos escribir $[L(\alpha) : K]$ de la siguiente manera:

$$[L(\alpha) : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K]. \tag{2}$$

Por otro lado, nota que también puedes escribir $[L(\alpha) : K]$ de la siguiente manera:

$$[L(\alpha) : K] = [L(\alpha) : L][L : K]. \tag{3}$$

Juntando (2) y (3) obtenemos

$$[L(\alpha) : K(\alpha)][K(\alpha) : K] = [L(\alpha) : L][L : K] \tag{4}$$

y análogamente,

$$[L(\alpha') : K(\alpha')][K(\alpha') : K] = [L(\alpha') : L][L : K]. \tag{5}$$

Por eso, en lo que sigue demostraremos que

$$[K(\alpha) : K] = [K(\alpha') : K] \quad \text{y} \quad [L(\alpha) : K(\alpha)] = [L(\alpha') : K(\alpha')].$$

Primero recordemos que como α y α' son raíces de $p(x)$, entonces el teorema 2.5.4 implica que $K(\alpha)$ y $K(\alpha')$ son isomorfos. Por lo tanto,

$$[K(\alpha) : K] = [K(\alpha') : K]. \tag{6}$$

Resta probar que

$$[L(\alpha) : K(\alpha)] = [L(\alpha') : K(\alpha')]. \tag{7}$$

Antes que nada, es fácil verificar que $L(\alpha)$ es el campo de descomposición de $f(x)$ sobre $K(\alpha)$ y que $L(\alpha')$ es el campo de descomposición de $f(x)$ sobre $K(\alpha')$. Como $K(\alpha)$ y $K(\alpha')$ son isomorfos, lo anterior y el teorema de unicidad de los campos de descomposición (c.f. teorema 2.10.1) implican que tenemos el siguiente diagrama conmutativo donde las flechas horizontales son isomorfismos y las flechas verticales son inclusiones.

$$\begin{array}{ccc} L(\alpha) & \longrightarrow & L(\alpha') \\ \uparrow & & \uparrow \\ K(\alpha) & \longrightarrow & K(\alpha') \end{array}$$

Usando esto, obtenemos (7). Juntando (4), (5), (6), y (7) obtenemos

$$\begin{aligned} [L(\alpha) : L][L : K] &= [L(\alpha) : K(\alpha)][K(\alpha) : K] \\ &= [L(\alpha') : K(\alpha')][K(\alpha') : K] = [L(\alpha') : L][L : K]. \end{aligned}$$

Cancelando $[L : K]$ de ambos lados obtenemos (1) y por lo explicado anteriormente, ya acabamos. $\square$

Extensiones normales

Definición

Supongamos que K/F es una extensión de campos. Decimos que K/F es **normal** si todo polinomio irreducible en $F[x]$ que tenga una raíz en K se descompone en K/F.

Recordando que podemos interpretar la condición "$p(x)$ se descompone en K/F" como que "K tiene a todas las raíces de $p(x)$", entonces podemos decir que K/F es normal si para todo $p(x) \in F[x]$ irreducible en $F[x]$ se satisface la siguiente implicación

$$K \text{ tiene } \textit{una} \text{ raíz de } p(x) \implies K \text{ tiene } \textit{todas} \text{ las raíces de } p(x).$$

Ejemplos

- La extensión $\mathbb{C}/\mathbb{R}$ es normal porque todo polinomio (irreducible o no) se descompone en $\mathbb{C}/\mathbb{R}$.
- La extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal porque el polinomio $x^3 - 2 \in \mathbb{Q}[x]$ no se descompone en $\mathbb{Q}(\sqrt[3]{2})$ $\mathbb{Q}$: En efecto, recuerda que en la sección 2.9 vimos que las otras dos raíces de este polinomio son $\zeta\sqrt[3]{2}$ y $\zeta^2\sqrt[3]{2}$, donde ζ es una 3-esima raíz primitiva de la unidad. Como $\zeta\sqrt[3]{2}$ y $\zeta^2\sqrt[3]{2}$ no son números reales[1], en particular tampoco pertenecen a $\mathbb{Q}(\sqrt[3]{2})$ y por lo tanto, la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal.
- Podemos reescribir la proposición 1 de la siguiente manera:

  Si K/F es una extensión de campos y K es un campo de descomposición de un polinomio con coeficientes en F, entonces K/F es una extensión normal.

  Juntando esto con el inciso anterior obtenemos que $\mathbb{Q}(\sqrt[3]{2})$ no es un campo de descomposición para ningún polinomio con coeficientes en $\mathbb{Q}$. En lo que sigue, veremos que si K/F es finita, el converso de la proposición 1 también es cierto.

[1] En la sección 2.9 vimos que $\zeta = \frac{-1+i\sqrt{3}}{2}$ es una 3-esima raíz primitiva de la unidad.

K/F es finita y normal $\iff$ K es un campo de descomposición sobre F

Proposición 2

Si K/F es una extensión de campos, entonces K/F es finita y normal si y solo si existe $f(x) \in F[x]$ tal que K es campo de descomposición de $f(x)$ sobre F.

Demostración.

$\Longleftarrow$) Es consecuencia inmediata de la proposición 1 y de que los campos de descomposición son extensiones finitas.

$\Longrightarrow$) Supongamos que K/F es finita y normal. Como es finita, entonces por el teorema 2.7.8 existen $\alpha_1, \ldots, \alpha_n \in F$ algebraicos sobre K tales que $K = F(\alpha_1, \ldots, \alpha_n)$. Definimos $f(x)$ como el producto de todos los polinomios mínimos (sobre F) de los α_i. Específicamente, sea

$$f(x) = m_{\alpha_1,F}(x) \cdot m_{\alpha_2,F}(x) \cdots m_{\alpha_n,F}(x)$$

Como $m_{\alpha_i,F}(x)$ pertenece a $F[x]$ para cada $i \in \{1, \ldots, n\}$, entonces $f(x)$ también pertenece a $F[x]$.

Finalmente, veamos que $K = F(\alpha_1, \ldots, \alpha_n)$ es el campo de descomposición de $f(x)$ sobre F verificando las dos condiciones de la definición de campo de descomposición:

- *$f(x)$ se descompone en K/F*: Como K es normal y $f(x)$ es un polinomio irreducible[2] que tiene una raíz en K (cualquiera de las α_i, entonces $f(x)$ se descompone en K/F.
- *No existe L campo tal que $F \subset L \subsetneq K = F(\alpha_1, \ldots, \alpha_n)$ y $f(x)$ se descompone en L/F*: Supongamos lo contrario. Como $F \subset L \subsetneq F(\alpha_1, \ldots, \alpha_n)$, entonces existe $i \in \{1, \ldots, n\}$ tal que $\alpha_i \notin L$; y como $f(x)$ se descompone en K/F, entonces existen $c \in F$ y $\beta_1, \ldots, \beta_m \in L$ tales que

$$f(x) = c \cdot (x - \beta_1)(x - \beta_2) \cdots (x - \beta_m). \tag{8}$$

  Por otro lado, como $\alpha_i \in K$ es raíz de $f(x)$, existe $g(x) \in K[x]$ tal que

$$f(x) = (x - \alpha_i)g(x). \tag{9}$$

  Usando (8), (9), y el hecho de que $K[x]$ es un DFU, obtenemos que $x - \alpha_i = x - \beta_j$ para alguna $j \in \{1, \ldots, m\}$. Esto implica $\alpha_i = \beta_j \in L$, contradiciendo $\alpha_i \notin L$. Por lo tanto, no existe L campo tal que $F \subset L \subsetneq K = F(\alpha_1, \ldots, \alpha_n)$ y $f(x)$ se descompone en E/F.

□

[2] Es fácil verificar que el producto de polinomios irreducibles es un polinomio irreducible.