Extensiones finitas separables y cerraduras de Galois

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos el concepto de cerradura de Galois. Naturalmente, si L/F es una extensión de campos, definiremos la cerradura de Galois de L/F como la extensión mas chica de L que es Galois sobre F. Intuitivamente esto es correcto, pero como no todas las extensiones de un campo son comparables vía la inclusión, debemos tener cuidado a que nos referimos cuando decimos "la extensión mas *chica*".

Cuando definimos el concepto de campo de descomposición de un polinomio, intuitivamente lo pensamos como la extensión mas chica en donde el polinomio se descompone. Formalmente, pedimos que no existiera ninguna extensión estrictamente mas pequeña (en términos de la inclusión) en donde el polinomio se descompusiera. Después vimos que esta definición era adecuada demostrando que podemos encajar cualquier campo de descomposición en cualquier campo en donde el polinomio se descompusiera.

Recordemos que esto fue consecuencia inmediata del siguiente resultado:

Si K/F es un campo de descomposición de $f(x) \in F[x]$ sobre F, y K'/F es una extensión de campos en donde $f(x)$ se descompone, entonces existe un homomorfismo $\varphi : K \to K'$ tal que $\varphi\restriction_F = \mathrm{id}_F$.

Con esto en mente, procedamos a definir el concepto de cerradura de Galois.

Cerradura de Galois

Definición

Supongamos que L/F es una extensión de campos. Decimos que M **es una cerradura de Galois de** L/F si M es una extensión de L tal que

1. M/F es de Galois y
2. Si M' es una extensión de L tal que M'/F es de Galois, entonces existe $\varphi : M \to M'$ homomorfismo de campos tal que $\varphi\restriction_L = \mathrm{id}_L$.

Notemos que el homomorfismo φ de la propiedad (2) es inyectivo[1] y por lo tanto la propiedad (2) implica que

Si M es una cerradura de Galois de L/F y M'/L es tal que M'/F es de Galois, entonces podemos encajar a M en M'.

[1] Pues $0 \in L$ y por lo tanto $\varphi(0) = 0$.

Existencia de cerraduras de Galois para extensiones de la forma $F(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n$ separables

Proposición 1

Supongamos que L/F es una extensión de campos y que $L = F(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in L$ separables sobre F. Mas aun, supongamos que

$$\{m_{\alpha_1,F}(x), \ldots, m_{\alpha_n,F}(x)\} = \{f_1(x), \ldots, f_l(x)\} \text{ donde } f_i(x) \neq f_j(x) \text{ si } i \neq j$$

En palabras, $f_1(x), \ldots, f_l(x)$ son todos los distintos elementos de $\{m_{\alpha_1,F}(x), \ldots, m_{\alpha_n,F}(x)\}$. Usando esto, definimos

$$f(x) = f_1(x) f_2(x) \cdots f_l(x) \in F[x].$$

En palabras, $f(x)$ es el producto de todos los distintos polinomios mínimos de los $\alpha_1, \ldots, \alpha_n$.

Si M es el campo de descomposición de $f(x) = f_1(x) \cdots f_l(x)$ sobre L, entonces M es una cerradura de Galois de L/F.

Demostración. Antes que nada, veamos que $f(x)$ es separable. Como L/F es separable, entonces cada uno de los $m_{\alpha_i,F}(x)$ es separable. Usando esto y la definición de $f(x)$ es fácil ver que para demostrar que $f(x)$ es separable, basta probar que $f_i(x)$ y $f_j(x)$ no comparten raíces si $i \neq j$.

A manera de contradicción, supongamos que existen i, j distintos tales que $f_i(x)$ y $f_j(x)$ que comparten una raíz, llamémosle β. Es fácil ver que esto implicaría que $f_i(x) = m_{\beta,F}(x)$ y $f_j(x) = m_{\beta,F}(x)$ de donde $f_i(x) = f_j(x)$, contradiciendo nuestra elección de los $f_i(x)$'s.

Ahora si, veamos que M es una cerradura de Galois de L/F verificando las dos condiciones de la definición.

1. *M/F es de Galois.*

   Como $f(x)$ es separable, basta probar que M es el campo de descomposición de $f(x)$ sobre F. Por definición, M es el campo de descomposición de $f(x)$ sobre L y por lo tanto, si denotamos por $\beta_1, \ldots, \beta_m \in M$ a las raíces de $f(x)$, entonces tendremos

   $$M = L(\beta_1, \ldots, \beta_m). \tag{1}$$

Veamos que

$$L(\beta_1, \ldots, \beta_m) = F(\beta_1, \ldots, \beta_m). \tag{2}$$

$\supset$) Es consecuencia inmediata de que $L \supset F$.

$\subset$) Antes que nada notemos que

$$\alpha_1, \ldots, \alpha_n \in \{\beta_1, \ldots, \beta_m\}$$

porque (i) $\beta_1, \ldots, \beta_m \in M$ son las raices de $f(x)$, (ii) $f(x) = f_1(x) \cdots f_l(x)$, y (iii) $f_i(x) \in \{m_{\alpha_1,F}(x), \ldots, m_{\alpha_n,F}(x)\}$ (por hipótesis).

Lo anterior implica que

$$L = F(\alpha_1, \ldots, \alpha_n) \subset F(\beta_1, \ldots, \beta_m)$$

donde la primera igualdad es por hipótesis.

En particular, $F(\beta_1, \ldots, \beta_m)$ es un subcampo de M que contiene a L y a $\beta_1, \ldots, \beta_m$ y por lo tanto, $L(\beta_1, \ldots, \beta_m) \subset F(\beta_1, \ldots, \beta_m)$.

Juntando (1) y (2) obtenemos que $M = F(\beta_1, \dots, \beta_m)$ y por lo tanto, M es el campo de descomposición de $f(x)$ sobre F (c.f. proposición 2.9.2). Como $f(x)$ es separable, lo anterior implica que M/F es de Galois.

2. *Si M' es una extensión de L tal que M'/F es de Galois, entonces existe $\varphi : M \to M'$ homomorfismo de campos tal que $\varphi \restriction_L = \mathrm{id}_L$.*

   Supongamos que M' es una extensión de L tal que M'/F es de Galois. En particular, M'/F es normal y por lo tanto, para toda $i \in \{1, \dots, n\}$ tenemos que $m_{\alpha_i,F}(x)$ se descompone en M'/F ($m_{\alpha_i,F}(x)$ es un polinomio irreducible en $F[x]$ que tiene una raíz en M': $\alpha_i \in L \subset M'$).

   Como $f(x) = f_1(x) \cdots f_l(x)$ y $f_j(x) \in \{m_{\alpha_1,F}(x), \dots, m_{\alpha_n,F}(x)\}$, entonces lo anterior implica que $f(x)$ se descompone en M'/F. Supongamos que $\gamma_1, \dots, \gamma_m \in M'$ son las raíces de $f(x)$. Entonces $L(\gamma_1, \dots, \gamma_m) \subset M'$ es un campo de descomposición de $f(x)$ sobre L y por unicidad de los campos de descomposición, existe un isomorfismo

$$\varphi : M = L(\beta_1, \dots, \beta_m) \to L(\gamma_1, \dots, \gamma_m) \subset M'$$

   que es la identidad en L. Considerando a φ como un homomorfismo de M en M' obtenemos lo deseado.

$\square$

Una caracterización de las extensiones finitas separables

Corolario 2

Supongamos que L/F es una extensión de campos. Entonces L/F es finita separable si y solo si $L = F(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in L$ separables sobre F.

En particular, si L/F es finita separable, entonces existe una cerradura de Galois de L/F.

Demostración.

$\Longrightarrow$) Supongamos que L/F es finita separable. Como es finita, existen $\alpha_1, \ldots, \alpha_n \in L$ tales que $L = F(\alpha_1, \ldots, \alpha_n)$. Pero como L/F es separable, entonces $\alpha_1, \ldots, \alpha_n \in L$ son separables sobre F.

$\Longleftarrow$) Supongamos que L/F es tal que $L = F(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in L$ separables sobre F. Por la proposición anterior, existe una extensión M de L tal que M/F es de Galois. En particular, M/F es separable. Como M es una extensión de L lo anterior también implica que L/F es separable.

$\square$

Comentario

Se puede demostrar que la cerradura de Galois de una extensión finita separable es única salvo isomorfismo. Es decir, que si M y M' son cerraduras de Galois de L/F (con L/F finita separable), entonces $M \cong M'$ (c.f. Cox, Galois Theory, Exercise 7.1.5).

Por eso, si L/F es una extensión finita separable a veces decimos "*la* cerradura de Galois de L/F" en vez de "*una* cerradura de Galois de L/F".

Finalizamos esta sección con una consecuencia inmediata de la caracterización de extensiones finitas separables.

La suma, resta, multiplicación, y división de elementos separables es separable

Corolario 3

Supongamos que L/F es una extensión de campos. Si $\alpha, \beta \in L$ son separables sobre F y $\beta \neq 0$, entonces

$$\alpha \pm \beta, \quad \alpha\beta, \quad \alpha/\beta$$

también son separables sobre F. En particular, el conjunto de los $\gamma \in L$ que son separables sobre F es un subcampo de L.

Demostración. Supongamos que $\alpha, \beta \in L$ son separables sobre F y considera $F(\alpha, \beta)$. Por el corolario anterior $F(\alpha, \beta)/F$ es separable y como

$$\alpha \pm \beta, \;\; \alpha\beta, \;\; \alpha/\beta \in F(\alpha, \beta)$$

obtenemos lo deseado. $\square$