UNA CARACTERIZACION DE LAS EXTENSIONES DE GALOIS MEDIANTE LA TRAZA DE LA EXTENSION

por

EMILIO BUJALANCE

En el presente trabajo se da una caracterización de las extensiones de Galois mediante la traza de la extensión, en el caso de extensiones algebraicas finitas, y suponiendo que la característica del cuerpo de la extensión es distinta del grado de ésta.

Definición 1.

Una extensión E de un cuerpo F se denomina de Galois si el grupo G de automorfismos de E, que dejan fijo a F, tiene como cuerpo fijo a F.

Definición 2.

Dada una extensión separable E de F, se denomina fibra de un elemento $x \in F$ a

$$T_{E/F}^{-1}(x)$$

donde $T_{E/F}$ es la traza de la extensión.

Definición 3.

Dada una extensión separable E de F, se dice que automorfismo f de E conmuta con la traza si $T_{E/F}\, f = T_{E/F}$.

Proposición 1.

Sea una extensión separable E de F, entonces el conjunto de automorfismos que conmutan con la traza es un grupo. Lo denominaremos G(E/F).

TEOREMA

Dada una extensión separable E de F, el grupo de automorfismos de E que dejan fijo a F, que designaremos por G(E, F) coincide con G(E/F).

Demostración. Sean $\{f_i\}_{i=1, \ldots, n}$ los homomorfismos inyectivos que definen a $T_{E/F}$. Entonces

$$\forall g \in G(E, F) \; T_{E/F}\, g = \sum_{i=1}^{n} f_i \cdot g$$

Como los $\{f_i \cdot g\}_{i=1, \ldots, n}$ son n homomorfismos inyectivos distintos, serán los mismos $\{f_i\}_{i=1, \ldots n}$. Luego:

$$T_{E/F}(g) = \sum_{i=1}^{n} f_i \cdot g = \sum_{i=1}^{n} f_i = T_{E/F} \Longrightarrow g \in G(E/F)$$

luego $G(E, F) \subset G(E/F)$.

Sea ahora $g \in G(E/F) \Longrightarrow T_{F/F}\, g = T_{F/F}$.

Hay que probar que $\forall a \in F \Longrightarrow g(a) = a$.

Supongamos que $g(a) = b$. Puede ser $b \in F$ ó $b \in E - F$.

Si $b \in F \Longrightarrow T_{E/F}\; g(a) = T_{E/F}\,(a) = T_{F/F}\,(b) \Longleftrightarrow na = nb \Longrightarrow$ $\Longrightarrow n(a - b) = 0 \Longrightarrow a = b$.

Si $b \in E - F$ existe un polinomio irreductible:

$$p(x) = x^m + a_{m-1}\, x^{n-1} + \ldots + a_0 \text{ con } m \geqslant 0$$

tal que $p(b) = 0$.

Por tanto, $(g(a))^m + a_{m-1}\,(g(a))^{m-1} + \ldots + a_0 = 0$ y entonces $T_{E/F}((g(a))^m + a_{m-1}\,(g(a)^{m-1}) + \ldots + a_0) = 0$.

Por las propiedades de la traza, se tiene

$$T_{F/F}(a^m) + a_{m-1}\, T_{E/F}(a^{m-1}) + \ldots + n\, a_0 = 0$$

Luego $n\, a^m + n\, a_{m-1}\, a^{m-1} + \ldots + n\, a_0 = 0 \Longrightarrow a^m + a_{m-1}\, a^{m-1} +$ $+ \ldots + a_0 = 0$, en contradicción con el hecho de ser $p(x)$ irreductible en F.

Así, pues, $b \in F$ y como hemos visto antes, $b = a$, con lo que se verifica $G(E/F) \subset G(E, F)$ y por tanto $G(E/F) = G(E, F)$.

Definición 4.

Dada una extensión separable E de F, se dice que $T_{E/F}$ es regular si cada fibra tiene un solo punto fijo para G(E/F).

Proposición 2.

Dada una extensión separable E de F, se verifica que $T_{E/F}$ es regular sí y sólo si la extensión es de Galois.

Demostración:

$\Leftarrow$) Sea E una extensión de Galois de F y sea $\{f_i\}_{i=1,\ldots,n}$ el conjunto de homomorfismos inyectivos que definen $T_{E/F}$, si existe un $a \in F$ tal que

$$T^{-1}_{E/F}(a)$$

tuviese dos puntos fijos para G(E/F), como la extensión es de Galois $G(E/F) = \{f_i\}_{i=1,\ldots n}$, entonces

$$b, c \in T^{-1}_{E/F}(a)$$

tal que $f_i(b) = b$ y $f_i(c) = c \ \forall i = 1, \ldots, n$ por lo cual $T_{E/F}(b) = nb = T_{E/F}(c) = nc \Rightarrow n(b - c) = 0 \Rightarrow b = c$.

$\Rightarrow$) Supongamos que E no es de Galois de F. Por lo tanto, $a \in E - F$, tal que si $\{f_i\}_{i=1,\ldots,n} = G(E/F) \, f_i(a) = a \ \forall i = 1, \ldots, n$.

Si $T_{E/F}(a) = b$ y $|E, F| = p$, el elemento

$$\frac{b}{pu}$$

(donde u es la unidad de E) es tal que

$$T_{E/F}\left(\frac{b}{pU}\right) = b$$

y además como

$$\frac{b}{pU} \in F,$$

se tiene que

$$f_i\left(\frac{b}{pU}\right) = \frac{b}{pU} \quad i = 1, \ldots, n$$

luego $T_{E/F}$ no es regular.

Proposición 3.

Sea E una extensión separable de K y F un cuerpo intermedio.

Si $T_{E/F}$ y $T_{F/K}$ son regulares, entonces $\forall g \in G(E/K)$ las aplicaciones

$$T_{E/F} \, g T^{-1}_{E/F}$$

pertenecen a G(F/K).

Demostración. Dado

$$g \in G(E/K)\ \forall a \in E\ T_{E/F}\ g T_{E/F}^{-1}(a)$$

Si designamos

$$T_{E/F}^{-1}(a)$$

por A, se tiene que $\forall y \in A$

$$T_{E/F}\ g(y) = T\ g(E)/g(F)\ g(y) = g[T_{E/F}(y)] = g(a)$$

Luego

$$T_{E/\Gamma}\ g\ T_{E/F}^{-1}(a) = g(a),$$

por lo que

$$T_{E/F}\ g\ T_{E/F}^{-1}$$

es aplicación y automorfismo al serlo g y ser $g(F) = F$. Por último, veamos que conmuta con $T_{F/K}$.

$$T_{F/K}\ T_{E/F}\ g T_{E/F}^{-1} = T_{E/K}\ g T_{E/F}^{-1} = T_{\Gamma/K} \cdot T_{E/F}^{-1} = T_{\Gamma/K}.$$

BIBLIOGRAFIA

1. ARTIN, E.: *Galois Theory,* Notre Damme, Indiana, 1959.
2. LANG, S.: *Algebra,* Adison-Wesley, Reading, 1965.
3. MAC CARTHY, P. J.: *Algebraic Extensions of Fields,* Blairdell, Wathmann, 1966.