Los automorfismos de cuerpos y el Grupo de Galois

Un conjunto importante de resultados de la teoría de cuerpos puede establecerse desde propiedades simples de la teoría de grupos. Esta conexión de la teoría de cuerpos con la teoría de grupos es lo que conocemos como Teoría de Galois.

En este breve artículo tratamos los automorfismos definidos en un cuerpo L (los endomorfismos biyectivos definidos sobre L) que dejan invariantes los elementos de un subcuerpo k del mismo. Tales automorfismos los denominamos k-automorfismos de L y presentan la interesante propiedad de que constituyen un grupo, que denominamos *Grupo de Galois de la extensión de L sobre k*.

Nos encontramos, además, que todo subgrupo del Grupo de Galois de los k-automorfismos de L sobre k es, a su vez, un conjunto de k-automorfismos que dejan invariante a los elementos de un cuerpo intermedio entre k y L, y, recíprocamente, para todo cuerpo intermedio existe también el correspondiente grupo de Galois constituido por aquellos k-automorfismos de L que dejan invariantes a sus elementos, y que es subgrupo del Grupo de Galois de los k-automorfismos de la extensión de L sobre k.

Los conceptos clave que manejamos son:

Por una parte, el subconjunto del cuerpo L que queda invariante para un conjunto H dado de automorfismos de L. Veremos que tal subconjunto tiene estructura de cuerpo y se denomina *cuerpo fijo* o *cuerpo invariante* del conjunto de automorfismos H.

El cuerpo fijo o invariante del Grupo de Galois de la extensión de L sobre k no tiene porqué coincidir con el cuerpo k. Puede ser un cuerpo intermedio (cuerpo que contiene a k y es subcuerpo de L).

Asimismo, el Grupo de Galois del cuerpo fijo de un conjunto H de automorfismos no ha de coincidir obviamente con el conjunto H. Veremos en este artículo la condición que debe cumplirse para que esta situación ocurra.

Introducción:

Un conjunto k se dice que tiene estructura de cuerpo con respecto a dos leyes, que llamaremos "+" (ley aditiva) y "." (ley multiplicativa) si se verifica que:

A) (k,+) es grupo conmutativo con respecto a la ley aditiva, cuyo elemento neutro representaremos por 0.
B) (k-{0},.) es grupo con respecto a la ley multiplicativa. Si fuera grupo conmutativo diremos que el cuerpo es conmutativo. Podemos representar por e el elemento neutro de esta ley.

C) La ley multiplicativa distribuye a la ley aditiva.

Podemos utilizar la notación (k,+,.) para representar al cuerpo cuyo conjunto de elementos es k y las leyes internas son las ya indicadas. Cuando se sobreentienden tales leyes utilizaremos simplemente la notación k.

Si dos cuerpos, k y L, tienen las mismas leyes de composición interna, diremos que el cuerpo k es subcuerpo de L si k está contenido en L. También podemos decir que L es supercuerpo de k, o que L es una extensión de k.

Si L se obtiene adjuntando a k un número finito de elementos, $a_1,...,a_n$, se dice que L se obtiene por adjunción desde k: $L = k(a_1,...,a_n)$ y que L es una extensión finita de k.

Si la extensión L de k se obtiene adjuntándole a k un solo elemento $a \in L$ diremos que $L = k(a)$ es una extensión simple de k.

La extensión $L = k(a_1,...,a_n)$ se dice que es algebraica sobre k si todo elemento $a_i, i = 1,...,n$ es algebraico sobre k, es decir, si para cada $a_i, i = 1,...,n$ siempre existe algún polinomio $p(x) \in k[x]$ con coeficientes en k tal que $p(a_i) = 0$.

Si algún $a_i \in L(a_1,...,a_n)$ no es algebraico sobre k, entonces la extensión L se dice que es una extensión trascendente sobre k.

Si L es extensión de k, entonces L es espacio vectorial sobre k. La dimensión de este espacio vectorial se denomina *grado de la extensión*. Si tal grado es finito se dice que L es extensión finita de k. En otro caso se dirá que es extensión infinita. Representaremos por $(L:k)$ al grado de la extensión de L sobre k.

Sea L una extensión de k. Diremos que el cuerpo k' es un cuerpo intermedio, si k' es supercuerpo de k y subcuerpo de L. O sea, cumpliendo: $k \subseteq k' \subseteq L$.

Dados dos cuerpos, (k,+,.) y (k', Δ,x), una aplicación f de k en k' se dice que es homomorfismo de cuerpos si respeta las dos leyes internas de ambos cuerpos, es decir:

$$\forall a,b \in k,\ f(a+b) = f(a)\Delta f(b) \in k'$$
$$\forall a,b \in k,\ f(a.b) = f(a) \times f(b) \in k'$$

Si el homomorfismo f es aplicación inyectiva se denomina monomorfismo, y si f es biyectiva, isomorfismo.

Si los cuerpos k y k' son el mismo cuerpo, entonces el homomorfismo se denomina endomorfismo. Un automorfismo en k es un endomorfismo biyectivo, esto es, un isomorfismo de k en k.

Un automorfismo de cuerpos es, en definitiva, una aplicación biyectiva de un cuerpo en si mismo que respeta sus las leyes internas.

1_K-automorfismos, cuerpo fijo, Grupo de Galois:

Dados un cuerpo L y un subcuerpo k del mismo, denominamos *k-automorfismo* de L a todo automorfismo de L que deja invariantes a los elementos de k:

$$f\ k-automorfismo\ de\ L \leftrightarrow f\ automorfismo\ de\ L \wedge \forall x \in k,\ f(x)=x$$

Teorema:
a) El conjunto $G(L:k)$ de los k-automorfismos de L tiene estructura de grupo.
b) Si M es un cuerpo intermedio entre k y L, $k \subseteq M \subseteq L$, entonces el grupo de los *M*-automorfismos de L, $G(L:M)$, es subgrupo de $G(L:k)$.
Demostración:

a) Obviamente, el automorfismo identidad i de L es un k-automorfismo, y el inverso f^{-1} de un k-automorfismo f es también k-automorfismo. La composición de dos k-automorfismos, fog, es también k-automorfismo, la asociatividad es evidente por tratarse de automorfismos. En definitiva $G(L:k)$ es un grupo.
b) Si $k \subseteq M \subseteq L$, todo *M*-automorfismo de L es también k-automorfismo, pues si deja invariantes a los elementos de M también dejará invariantes a los elementos de k, ya que $k \subseteq M$. Luego $G(L:M) \subseteq G(L:k)$.

El grupo $G(L:k)$ se denomina *Grupo de Galois de L sobre k* .

Teorema:
a) Dada una familia *H* de k-automorfismos de *L*, $H \subseteq G(L:k)$, el conjunto $f(H)$ de todos los elementos de *L* que quedan invariantes por *H* es un cuerpo intermedio, $k \subseteq f(H) \subseteq L$, que se denomina *cuerpo fijo* o *cuerpo invariante* de *H*.
b) Si *H'* contiene a *H*, entonces el cuerpo fijo de *H'* está contenido en el cuerpo fijo de *H*: $H \subseteq H' \rightarrow f(H') \subseteq f(H)$.
Demostración:

a) Para probar que $f(H)$ es cuerpo bastará probar que $(f(H),+)$ es grupo aditivo y que $(f(H)-\{0\},.)$ es grupo multiplicativo:
$\varphi \in G(L:k)$, $\forall x,y \in f(\varphi)$
$\varphi(x-y)=\varphi(x)-\varphi(y)=x-y \in f(\varphi)$
$\varphi(x.y^{-1})=\varphi(x).\varphi(y^{-1})=x.y^{-1} \in f(\varphi),\ si\ y^{-1}\neq 0$
Las propiedades asociativa y distributiva se verifican siempre, pues se trata de los elementos del cuerpo L.
Finalmente, es $f(H)=\bigcap\{f(\varphi)/\varphi \in M\}$, que es subcuerpo de L.
b) Si $H \subseteq H'$, la familia de elementos que quedan fijos por todo k-automorfismo de *H'* forma parte de la familia de elementos que permanecen fijos por todo k-automorfismo de *H*. O sea, $f(H') \subseteq f(H)$.

Todo subgrupo del Grupo de Galois $G(L:k)$ tiene por cuerpo fijo un cuerpo intermedio, y todo cuerpo intermedio es el cuerpo fijo de un subgrupo del Grupo de Galois $G(L:k)$.

Teorema: Sea *L* extensión finita de *k*. El conjunto de n k-automorfismos distintos de *L* es siempre linealmente independiente.
Demostración:
Sean n *k*-automorfismos sobre el cuerpo *L*, $\varphi_1,...,\varphi_n, \varphi_j \in G(L:k), j=1,...,n$, y veamos que se ha de verificar que

$$\sum_{j=1}^{n}\lambda_j\varphi_j(x)=0, \text{ con } \lambda_j \in L,\ j=1,...,n \rightarrow \lambda_j=0,\ j=1,...,n,\ \forall x \in L$$

para ver que todos los coeficientes han de ser necesariamente nulos empleamos inducción:

- Para *n=1* se tiene que, al ser $\varphi_1(x)\neq 0$ será $\lambda_1\varphi_1(x)=0 \rightarrow \lambda_1=0$.
- Si la proposición es cierta para *n-1*, veamos que ha de ser cierta también para n, pues si suponemos que siendo cierta para *n-1* fuera falsa para *n* se tendrá que todos los coeficientes λ_j habrían de ser no nulos, pues por hipótesis de inducción es imposible que sean nulos algunos de los coeficientes sin serlo todos, con lo que

  $\sum_{j=1}^{n}\lambda_j\varphi_j(x)=0 \wedge \lambda_j\neq 0,\ j=1,...,n \rightarrow \sum_{j=1}^{n-1}\lambda_j\varphi_j(x)+\lambda_n\varphi_n(x)=0$, de lo cual

  $$\sum_{j=1}^{n-1}\frac{\lambda_j}{\lambda_n}\varphi_j(x)+\varphi_n(x)=0 \qquad [1]$$

  y siendo distintos todos los n k-automorfismos, será:

  $\varphi_j(a)\neq\varphi_n(a),\ j=1,...,n-1$, para algún $a \in L$.

  Entonces, podemos escribir:

  $\sum_{j=1}^{n-1}\frac{\lambda_j}{\lambda_n}\varphi_j(ax)+\lambda_n\varphi_n(ax)=\sum_{j=1}^{n-1}\frac{\lambda_j}{\lambda_n}\varphi_j(a)\varphi_j(x)+\varphi_n(a)\varphi_n(x)=0$, o bien:

  $$\sum_{j=1}^{n-1}\frac{\lambda_j}{\lambda_n}\varphi_j(a).\varphi_n^{-1}(a)\varphi_j(x)+\varphi_n(x)=0 \qquad [2]$$

  Si restamos la expresión [2] a la expresión [1] se tiene:

  $$\sum_{j=1}^{n-1}\frac{\lambda_j}{\lambda_n}\left[e-\varphi_j(a)\varphi_n^{-1}(a)\right]\varphi_j(x)=0$$

  por hipótesis de inducción los coeficientes de los n-1 k-automorfismos son todos nulos:

  $\frac{\lambda_j}{\lambda_n}\left[e-\varphi_j(a)\varphi_n^{-1}(a)\right]=0 \rightarrow e-\varphi_j(a)\varphi_n^{-1}(a)=0 \rightarrow \varphi_n(a)-\varphi_j(a)=0 \rightarrow$

  $\rightarrow \varphi_j(a)=\varphi_n(a),\ j=1,...,n-1$, lo que contradice la hipótesis del teorema de que todos los n k-automorfismos son distintos.
  Luego, han de ser nulos todos los *n* coeficientes, y se verifica la proposición para *n*.

Teorema:
a) Dado un conjunto $\varphi_1,\varphi_2,...,\varphi_n$ de k-automorfismos distintos de L, se cumple que si $f(H)$ es el cuerpo fijo de la familia $H=\{\varphi_1,\varphi_2,...,\varphi_n\}$, entonces el grado de la extensión de *L* sobre $f(H)$ es mayor o igual que *n*: $(L:f(H))\geq n$
b) Si el conjunto de k-automorfismos $H=\{\varphi_1,\varphi_2,...,\varphi_n\}$ es grupo, y por tanto subgrupo de $G(L:k)$, entonces es $(L:f(H))=n$.

Demostración:

a) Supongamos que la dimensión del espacio vectorial L sobre el cuerpo $f(H)$ es r. Por definición de grado de la extensión, es $(L:f(H))=r$. Consideremos una base de dicho espacio: $\{u_1,...,u_r\}$. Será $\forall w\in L,\ w=\sum_{j=1}^{r}\lambda_j u_j,\ \lambda_j\in f(H),\ j=1,...,r$

Si fuera $r<n$, las *r* ecuaciones

$$\varphi_1(u_1).x_1+...+\varphi_n(u_1).x_n=0$$
$$... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ...$$
$$\varphi_1(u_r).x_1+...+\varphi_n(u_r).x_n=0$$

tendrían soluciones $x_1,...,x_n$ no todas nulas.

Y puesto que $f(H)$ es el cuerpo fijo de los k-automorfismos $\varphi_1,\varphi_2,...,\varphi_n$ se tendrá que $\varphi_j(\lambda_i u_i)=\varphi_j(\lambda_i).\varphi_j(u_i)=\lambda_i.\varphi_j(u_i)$. Entonces, multiplicando las r ecuaciones anteriores respectivamente por $\lambda_1,...,\lambda_r$, se tiene

$$\lambda_1\varphi_1(u_1).x_1+...+\lambda_1\varphi_n(u_1).x_n=0$$
$$... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ...$$
$$\lambda_r\varphi_1(u_r).x_1+...+\lambda_r\varphi_n(u_r).x_n=0$$

o bien:

$$\varphi_1(\lambda_1 u_1).x_1+...+\varphi_n(\lambda_1 u_1).x_n=0$$
$$... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ...$$
$$\varphi_1(\lambda_r u_r).x_1+...+\varphi_n(\lambda_r u_r).x_n=0$$

por lo que, al sumar:

$$\sum_{i=1}^{r}\varphi_1(\lambda_i u_i).x_1+...+\sum_{i=1}^{r}\varphi_n(\lambda_i u_i).x_n=0\rightarrow\varphi_1(\sum_{i=1}^{r}\lambda_i u_i).x_1+...+\varphi_n(\sum_{i=1}^{r}\lambda_i u_i).x_n=0\rightarrow$$
$$\rightarrow\varphi_1(w).x_1+...+\varphi_n(w).x_n=0,\ \forall w\in L$$

con lo cual vemos que los k-automorfismos no serian linealmente independientes en contradicción con el teorema anterior. Luego no ha de ser $r<n$. Por consiguiente es $r=(L:f(H))\geq n$. O bien, denotaremos por $(L:f(H))\geq o(H)$.

b) Sabemos, pues, que $r\geq n$. Veamos que no puede ser $r>n$ si *H* tiene estructura de grupo.

Supongamos que $r>n$. Esto querría decir que hay al menos m+1 elementos de L que son linealmente independientes. Sean estos $\{u_1,...,u_{m+1}\}$ y consideremos las *m* ecuaciones lineales con m+1 incógnitas:

$$\varphi_1(u_1).y_1+...+\varphi_1(u_{m+1}).y_{m+1}=0$$
$$... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ...$$
$$\varphi_m(u_1).y_1+...+\varphi_m(u_{m+1}).y_{m+1}=0$$

Se trata de un sistema de ecuaciones lineales homogéneo constituido por m ecuaciones, una por cada automorfismo, y m+1 incógnitas, por lo que habrán soluciones para el sistema, no todas nulas.

Como *H* es grupo, uno de los automorfismos ha de ser la identidad. Sea, por ejemplo, φ_1. La ecuación correspondiente a este automorfismo quedaría como $u_1.y_1+...+u_{m+1}.y_{m+1}=0$, siendo los $y_i, i=1,...,m+1$ no todos nulos, contra la hipótesis de que los elementos $\{u_1,...,u_{m+1}\}$ son linealmente independientes.

Por otra parte, si consideramos entre todas las soluciones del sistema anterior de ecuaciones lineales aquella que tenga el menor número *p* de elementos no nulos, por ejemplo $(q_1,...,q_p,0,...,0)$, necesariamente ha de ser *p>1*, pues si fuera *p=1* se tendría que $\varphi_1(u_1).q_1 = u_1.q_1 = 0 \rightarrow u_1 = 0$, lo que también es absurdo, pues los elementos $\{u_1,...,u_{m+1}\}$ son linealmente independientes y por tanto ninguno puede ser nulo.

Si hacemos $q_p = e$ (elemento neutro de la ley multiplicativa), se tiene:

$$\sum_{i=1}^{p} q_i \varphi_k(u_i) = \sum_{i=1}^{p-1} q_i \varphi_k(u_i) + \varphi_k(u_p) = 0, \;\; k = 1,...,m \qquad [3]$$

donde no todas las soluciones $q_1,...,q_p$ están en el cuerpo fijo, pues uno de los automorfismos es la identidad. Sea, por ejemplo, $q_1 \notin f(H) \rightarrow \exists \varphi_h \in H / \varphi_h(q_1) \neq q_1$ por lo que aplicando φ_h a la igualdad [3] será:

$$\sum_{i=1}^{p-1} \varphi_h(q)_i (\varphi_h \circ \varphi_j)(u_i) + (\varphi_h \circ \varphi_j)(u_p) = 0, \;\; j = 1,...,m$$

y como *H* es grupo, siempre puede elegirse j de modo que $\varphi_h \circ \varphi_j = \varphi_k$, con lo que

$$\sum_{i=1}^{p-1} \varphi_h(q_i) \varphi_k(u_i) + \varphi_k(u_p) = 0, \;\; k = 1,...,m$$

restando esta expresión a [3]:

$$\sum_{i=1}^{p-1} [q_i - \varphi_h(q_i)] \varphi_k(u_i) = 0, \;\; k = 1,...,m$$

donde cada coeficiente es no nulo: $q_i - \varphi_h(q_i) \neq 0$, luego existe solución con al menos p-1 elementos no nulos, en contradicción con la suposición de que era *p* el menor número de elementos no nulos, luego, no es posible que $r > n$, de lo que se deduce que ha de ser $r = n$. Esto es, $(L : f(H)) = o(H)$

Corolario 1:

Si es L extensión finita de k, el cuerpo fijo del grupo de Galois de L sobre k, $f(G(L:k)))$, es tal que el grado de la extensión de L sobre él, $(L : f(G(L:k)))$, es igual al orden del grupo de Galois:

$$(L : f(G(L:k)))) = oG(L:k)$$

Demostración:

Si es $G(L:k)$ el Grupo de Galois de L sobre k (conjunto de todos los automorfismos en L que dejan invariantes a los elementos de k), y es $f(G(L:k)))$ el cuerpo fijo de $G(L:k)$, es decir el cuerpo constituido por todos los elementos de L que quedan invariantes por los autormorfismos de $G(L:k)$ (todos, no solo los elementos de k), se cumple:

$$k \subseteq f(G(L:k))) \subseteq L$$

Si llamamos $oG(L:k)$ al orden del grupo de Galois, es decir, al número de automorfismos que constituyen el grupo, se tiene, al aplicar el teorema anterior:

- por a): $(L : f(G(L:k))) \geq oG(L:k)$
- por b), siendo $G(L:k)$ grupo: $(L : f(G(L:k))) = oG(L:k)$

Corolario 2:
Si es L extensión finita de k, H un subgrupo del Grupo de Galois, $G = G(L : f(G))$ y f(H) su cuerpo fijo, entonces todo k-automorfismo de $G(L:k)$ que deja invariante a todo elemento de f(H) pertenece a H, y H es el Grupo de Galois de L sobre f(H): $H = G(L : f(H))$. En particular es $G = G(L : f(G))$.
Demostración:
Por el anterior teorema, es $o(H) = (L : f(H))$. Si suponemos que existe un k-automorfismo φ^* que sin ser elemento de H dejase fijo a f(H), podríamos llamar entonces $H' = H \cup \{\varphi^*\}$, y resulta que $f(H') = f(H)$, y sin embargo se tiene que

$$(L : f(H')) = (L : f(H)) = o(H) < o(H)+1 = o(H') \rightarrow (L : f(H')) < o(H')$$

lo que, como es obvio, contradice al teorema anterior. En definitiva, todo k-automorfismo que deja fijo a f(H) pertenece a H.

De todo ello, H será precisamente el Grupo de Galois de la extensión de L sobre f(H), $H = G(L : f(H))$ y, en particular, es

$$G(L:k) = G(L : f(G))$$

Bibliografía:

01. Artin, E., "Teoría de Galois". Vicens-Vives, 1970.
02. Atiyah, M.F., Macdonald, I.G., "Introducción al Álgebra conmutativa". Ed. Reverté.
03. Carrega, J.C., "Théorie des corps. La règle et le compas". Hermann, Paris, 1981.
04. Childs, L.N., "A Concrete Introduction to Higher Algebra". Springer UTM, New York, 1979.
05. Dorronsoro, J. y Hernández, E., "Números, grupos y anillos". Addison-Wesley./Universidad Autónoma de Madrid, 1996.
06. Garling, D.J.H., "A course in Galois Theory". Cambridge University Press.
07. Herstein, I. N., "Álgebra moderna : grupos, anillos, campos, teoría de Galois". Ed. Trillas, México, 1973.
08. Kostrikin, A. I., "Introducción al álgebra". McGraw-Hill, Madrid, 1992.
09. Lang, S., "Álgebra". Ed. Aguilar, Madrid, 1971.
10. Milne, J.S., "Fields and Galois Theory", http://www.jmilne.org/math/CourseNotes/math594f.html
11. Stewart, I., "Galois Theory". Chapman and Hall, London, 1973.
12. Van der Waerden, B.L., "Modern Algebra" Vol I. Frederick Ungar, New York, 1964.
13. Xambó Descamps, S., Delgado de la Mata, F. y Fuertes, C., "Introducción al Álgebra: anillos, factorización y teoría de cuerpos". Universidad de Valladolid. Manuales y Textos Universitarios. Ciencias nº 29, 1998.