Miscelánea Matemática **53** (2011) 23–32 SMM

De la teoría de Galois a las teorías de torsión

Rogelio Fernández-Alonso

rfg@xanum.uam.mx

Departamento de Matemáticas
Universidad Autónoma Metropolitana - Iztapalapa
México D.F.

Resumen

Se definen las conexiones de Galois y se presentan sus propiedades básicas. Se presentan los principales resultados que llevan al teorema fundamental de la teoría de Galois desde la perspectiva de una conexión de Galois específica, de hecho, una polaridad entre dos conjuntos potencia. Se presenta la definición de este concepto y el de teoría de torsión en el contexto de una polaridad particular sobre las subclases de la clase de módulos sobre un anillo R.

1. Introducción.

La teoría de Galois, que se desarrolló a partir de las brillantes ideas de Evariste Galois, es coronada por el llamado teorema fundamental de la teoría de Galois, que establece, bajo ciertas condiciones de una extensión de campos, una correspondencia biunívoca entre extensiones intermedias y subgrupos del grupo de Galois de dicha extensión. Esta correspondencia biunívoca invierte el orden entre ambas estructuras dado por la contención. En buena medida este resultado es impactante por la estrecha conexión que establece entre "mundos" tan diferentes.

La abstracción de esta situación lleva a una definición simple que genera una gama muy amplia de ejemplos de este tipo de conexiones. Se trata de las conexiones de Galois, que se presentan en la siguiente sección, junto con otros conceptos muy relacionados, como los operadores cerradura e interior y los sistemas de cerrados y de abiertos. En la sección 2 se llega al teorema fundamental de la teoría de Galois con las proposiciones que usualmente se exponen en los libros de texto, pero

se enuncian utilizando los conceptos y la notación desarrollados en la sección 1. En la sección 3 se describe una clase de conexiones de Galois que incluyen a la conexión de Galois del teorema fundamental, llamadas polaridades. Finalmente se presentan las teorías de torsión asociadas a un anillo, definidas en [**1**] por Dickson, como un caso particular de estas polaridades. Las demostraciones se omiten por ser muy sencillas y naturales, o como en la sección 3, por ser resultados conocidos, de los cuales se incluye la referencia a algún texto.

2. Conexiones de Galois, operadores y sistemas.

Recuérdese que un *conjunto parcialmente ordenado (copo)* es una estructura $\langle P, \leq \rangle$ donde P es un conjunto y $\leq$ es una relación de orden parcial sobre P. Un *morfismo* del copo $\langle P, \leq \rangle$ al copo $\langle Q, \preccurlyeq \rangle$ es una función $f : P \to Q$ tal que para todo $p, p' \in P$ tales que $p \leq p'$ se tiene que $f(p) \preccurlyeq f(p')$. Un morfismo de copos $f : \langle P, \leq \rangle \to \langle Q, \preccurlyeq \rangle$ se llama *isomorfismo* si existe un morfismo de copos $g : \langle Q, \preccurlyeq \rangle \to \langle P, \leq \rangle$ tal que $g \circ f = 1_P$ y $f \circ g = 1_Q$. En este caso también llamaremos *isomorfismo* a la cuarteta $\langle P, f, g, Q \rangle$. El concepto de conexión de Galois generaliza al de isomorfismo de copos.

Definición 2.1 *Una* conexión de Galois *es una cuarteta* $\langle P, f, g, Q \rangle$ *donde* $\langle P, \leq \rangle$ *y* $\langle Q, \preccurlyeq \rangle$ *son copos,* $f : P \to Q$ *y* $g : Q \to P$ *son funciones tales que para todo* $p \in P$, $q \in Q$ *sucede que* $f(p) \preccurlyeq q$ *si y sólo si* $p \leq g(q)$.

A continuación se establece una definición alternativa de este concepto.

Proposición 2.2 *Dados los copos* $\langle P, \leq \rangle$ *y* $\langle Q, \preccurlyeq \rangle$ *y las funciones* $f : P \to Q$ *y* $g : Q \to P$*, son equivalentes:*

1. $\langle P, f, g, Q \rangle$ *es una conexión de Galois.*
2. *(a) Para todo* $p \in P$ *se tiene* $p \leq gf(p)$ *y para todo* $q \in Q$ *se tiene* $fg(q) \preccurlyeq q$.
   (b) f *y* g *son morfismos de copos.*

Corolario 2.3 *Si* $\langle P, f, g, Q \rangle$ *es una conexión de Galois entonces:*

1. $f \circ g \circ f = f$.

2. $g \circ f \circ g = g$.

Las conexiones de Galois tienen una estrecha relación con el concepto de cerradura (interior) que aparece en muchas áreas de las matemáticas, no sólo en la topología. A continuación se presenta la definición de ambos conceptos para copos.

Definición 2.4 *Sea $\langle P, \leq \rangle$ un copo. Un* operador cerradura (interior) *sobre P es una función $h : P \to P$ que cumple las siguientes condiciones:*

1. *h es un morfismo de orden.*
2. *Para todo $p \in P$ sucede que $p \leq h(p)$ ($h(p) \leq p$).*
3. *$h \circ h = h$.*

En pocas palabras, un operador cerradura (interior) sobre un copo es un endomorfismo creciente (decreciente) e idempotente. Una manera alternativa de definir estos conceptos es refiriéndose a los elementos cerrados o abiertos.

Definición 2.5 *Sea $\langle P, \leq \rangle$ un copo. Un* sistema de cerrados (abiertos) *de P es un subconjunto Q de P tal que para todo $p \in P$ el conjunto $\{q \in Q \mid p \leq q\}$ ($\{q \in Q \mid q \leq p\}$) tiene elemento menor (mayor), denotado por $\bar{p}$ (p°). Los elementos de Q se llaman* cerrados (abiertos)[1].

En efecto, un operador cerradura (interior) induce un sistema de cerrados (abiertos), e inversamente.

Proposición 2.6 *Sea $\langle P, \leq \rangle$ un copo.*

1. *Si h es un operador cerradura (interior) sobre un copo, entonces $h(P)$ es un sistema de cerrados (abiertos) de P.*
2. *Si Q es un sistema de cerrados (abiertos) de P, entonces la función*
   $h : P \to P$ definida como $h(p) := \bar{p}$ ($h(p) := p^\circ$) es un operador cerradura (interior) sobre P.

También sucede que un operador cerradura sobre un copo induce naturalmente una conexión de Galois.

[1] La nomenclatura y la notación provienen de la topología.

Proposición 2.7 *Sea h un operador cerradura (interior) sobre un copo $\langle P, \leq \rangle$. Sea $\bar{P} = h(P)$ ($P^\circ = h(P)$)el sistema de cerrados (abiertos) correspondiente. Sea $\bar{h} : P \to \bar{P}$ ($h^\circ : P \to P^\circ$) la correstricción de h en su imagen y sea $i : \bar{P} \to P$ ($j : P^\circ \to P$) la inclusión natural. Entonces $\langle P, \bar{h}, i, \bar{P} \rangle$ ($\langle P^\circ, j, h^\circ, P \rangle$) es una conexión de Galois.*

Recíprocamente, una conexión de Galois induce naturalmente un operador cerradura y un operador interior en los copos que forman parte de esta.

Teorema 2.8 *Si $\pi = \langle P, f, g, Q \rangle$ es una conexión de Galois entonces:*

1. *$g \circ f$ es un operador cerradura sobre P.*
2. *$\bar{P} = g(Q) = gf(P)$ es un sistema de cerrados de P.*
3. *$f \circ g$ es un operador interior sobre Q.*
4. *$Q^\circ = f(P) = fg(Q)$ es un sistema de abiertos de Q.*

A los elementos de $\bar{P}$ les llamaremos π-*cerrados*, y a los de Q° les llamaremos π-*abiertos*. Resulta que el sistema abierto y el sistema cerrado que están implícitos en una conexión de Galois son copos isomorfos.

Proposición 2.9 *Si $\langle P, f, g, Q \rangle$ es una conexión de Galois entonces las restricciones de f a $\bar{P}$ y de g a Q° inducen un isomorfismo de copos $\langle \bar{P}, f', g', Q^\circ \rangle$.*

3. Teorema fundamental de la teoría de Galois.

Como ya se dijo en la introducción, el teorema fundamental de la teoría de Galois establece, *bajo ciertas condiciones* de una extensión de campos, una correspondencia biunívoca (que invierte la contención) entre extensiones intermedias y subgrupos del grupo de Galois de dicha extensión. Pero de hecho no se necesitan condiciones adicionales para ya tener una conexión de Galois.

Proposición 3.1 *Sea E/F una extensión de campos y sea $\mathcal{P}$ el copo de extensiones intermedias entre F y E ordenadas con la contención. Sea $G = G(E/F)$ el grupo de todos los automorfismos de E que dejan fijos a todos los elementos de F y sea $\mathcal{Q}$ el copo de todos los subgrupos de G*

ordenados por la contención invertida. Sean $f : \mathcal{P} \to \mathcal{Q}$ *y* $g : \mathcal{Q} \to \mathcal{P}$ *definidas como sigue:*

$$f(K) = G(E/K) = \{\sigma \in G \mid \forall x \in K, \sigma(x) = x\}$$
$$g(H) = E_H = \{x \in E \mid \forall \sigma \in H, \sigma(x) = x\}$$

Entonces $\pi_{\mathrm{Gal}} = \langle \mathcal{P}, f, g, \mathcal{Q} \rangle$ *es una conexión de Galois*[2].

En este caso específico los copos $\mathcal{P}$ y $\mathcal{Q}$ son retículas completas[3]. Además en cada copo hay funciones que le asocian a cada elemento un cardinal. En $\mathcal{P}$ se puede considerar el grado $[E : K]$ de la extensión E/K y en $\mathcal{Q}$ puede considerarse el orden $o(H)$ del subgrupo H de $G(E/F)$. El siguiente resultado relaciona ambos números en el caso finito.

Proposición 3.2 *[2, teo. 4.9.3] Sea* E *un campo y sea* $H \leq Aut(E)$ *un subgrupo finito. Entonces* $o(H) = [E : E_H]$.

Esto tiene como consecuencia la siguiente propiedad de la conexión de Galois π_{Gal}.

Proposición 3.3 *Sea* E/F *una extensión de campos. Si* H *es un subgrupo finito de* $G(E/F)$ *entonces* $H = G(E_H/F) = fg(H)$*, es decir,* $H \in \mathcal{Q}^\circ$.

En particular, todos los subgrupos son finitos cuando el grupo $G(E/F)$ lo es. Por lo tanto en este caso todos los elementos de $\mathcal{Q}$ son abiertos.

Corolario 3.4 *Si* $G(E/F)$ *es un grupo finito entonces:*

1. $\mathcal{Q} = \mathcal{Q}^\circ$.
2. $f \circ g = 1_{\mathcal{Q}}$.
3. f *es suprayectiva y* g *es inyectiva.*

La hipótesis de la proposición anterior se tiene cuando la extensión de campos es finita.

Proposición 3.5 *[3, teo. 5.6.2] Si* E/F *es una extensión finita entonces* $G(E/F)$ *es un grupo finito y* $o(G(E/F)) \leq [E : F]$.

[2] A menudo este tipo de conexiones de Galois, donde el orden de uno de los copos está invertido, se llaman *antítonas*, a diferencia de las ya definidas aquí que se llaman *monótonas*.

[3] Una retícula *completa* es un copo tal que para todo subconjunto existe su ínfimo (menor cota superior) y su supremo (mayor cota inferior).

Recuérdese que una extensión algebraica E/F se llama:

- *normal* si todo polinomio irreducible $p(x) \in F[x]$ con una raíz en E se descompone completamente en E;
- *separable* si para todo $\alpha \in E$, el polinomio mónico irreducible que tiene a α como raíz es separable, esto es, no tiene raíces múltiples;
- *extensión de Galois* si es normal y separable.

Proposición 3.6 *[**5**, teo. 3.26] Para una extensión finita E/F son equivalentes:*

(a) E/F es una extensión de Galois.

(b) E es el campo de descomposición de un polinomio separable $p(x) \in F[x]$.

(c) $F = gf(F)$, es decir, $F \in \bar{\mathcal{P}}$ (F es cerrado en $\mathcal{P}$).

La equivalencia entre las condiciones (a) y (b) de la proposición 3.6 implica que las extensiones intermedias heredan la misma propiedad.

Corolario 3.7 *Dada una extensión finita E/F y un campo intermedio $F \leq K \leq E$, si E/F es una extensión de Galois entonces E/K es una extensión de Galois.*

Aplicando la condición (c) de la proposición 3.6 a todas las extensiones intermedias E/K se obtiene finalmente que si E/F es una extensión de Galois tenemos del lado de las extensiones intermedias un resultado análogo al corolario 3.4.

Proposición 3.8 *Para una extensión finita E/F son equivalentes:*

(a) $F \in \bar{\mathcal{P}}$ (F es cerrado en $\mathcal{P}$).

(b) $\mathcal{P} = \bar{\mathcal{P}}$ (todos los elementos de $\mathcal{P}$ son cerrados).

(c) $g \circ f = 1_{\mathcal{P}}$.

Como consecuencia de las proposiciones 3.4 y 3.8, y aplicando la proposición 2.9, tenemos el teorema dundamental de la teoría de Galois.

Corolario 3.9 *(**Teorema fundamental de la teoría de Galois**) Si E/F es una extensión de Galois finita entonces $\mathcal{P} = \bar{\mathcal{P}}$, $\mathcal{Q} = \mathcal{Q}^{\circ}$ y la conexión de Galois π_{Gal} es un isomorfismo.*

4. Polaridades.

La conexión de Galois π_{Gal} descrita en la sección anterior es un caso particular de un tipo más amplio de conexiones de Galois, inducidas por una relación binaria.

Definición 4.1 *Sean A y B conjuntos. Una* polaridad *entre los conjuntos potencia $\wp(A)$ y $\wp(B)$, ordenados por la contención es una conexión de Galois $\langle \wp(A), f, g, \wp(B)^{\text{op}} \rangle$.*

Las polaridades resultan ser correspondientes con relaciones binarias, de manera muy sencilla.

Teorema 4.2 *Sean A y B conjuntos.*

1. *Toda relación $R \subseteq A \times B$ induce una polaridad $\pi_R = \langle \wp(A), f, g, \wp(B)^{\text{op}} \rangle$ dada por las funciones:*

$$f_R(X) = \{b \in B \mid \forall x \in X, (x, b) \in R\}, \qquad \text{para } X \subseteq A;$$
$$g_R(Y) = \{a \in A \mid \forall y \in Y, (a, y) \in R\}, \qquad \text{para } Y \subseteq B.$$

2. *Toda polaridad $\pi = \langle \wp(A), f, g, \wp(B)^{\text{op}} \rangle$ induce la relación:*

$$R_\pi = \{(a, b) \in A \times B \mid b \in f(\{a\})\}$$

3. *Dada una relación $R \subseteq A \times B$ se tiene R_{π_R}=R. Dada una polaridad $\pi = \langle \wp(A), f, g, \wp(B)^{\text{op}} \rangle$ se tiene $\pi_{R_\pi} = \pi$. Por tanto hay una correspondencia biunívoca entre las relaciones de A en B y las polaridades entre $\wp(A)$ y $\wp(B)$.*

Dada una extensión de campos E/F y el grupo de automorfismos $G = G(E/F)$, la proposición 3.1 establece una conexión de Galois π_{Gal}. Obsérvese la similaridad entre las definiciones de las funciones f y g que componen π_{Gal} y las del teorema 4.2. De hecho se puede considerar la relación

$$R = \{(x, \sigma) \in E \times G \mid \sigma(x) = x\}.$$

Según el teorema 4.2, a dicha relación de E en G le corresponde una polaridad π_R entre $\wp(E)$ y $\wp(G)$, definida precisamente como en la proposición 3.1, pero donde ahora K y H representan subconjuntos *arbitrarios* de E y G respectivamente. En tal caso también $f(K)$ resulta ser un subgrupo de G y $g(H)$ resulta ser un subcampo intermedio de E/F, de tal forma que según el teorema 2.8, el sistema de π_R-cerrados

y el sistema de π_R-abiertos son $\bar{\mathcal{P}}$ y $\mathcal{Q}^\circ$, es decir, coincide con el sistema de π_{Gal}-cerrados y con el sistema de π_{Gal}-abiertos, respectivamente.

Las polaridades pueden definirse de la misma forma entre retículas completas L y L', aunque a fin de cuentas estas pueden considerarse como ciertas polaridades entre $\wp(L)$ y $\wp(L')$. Para una explicación más detallada de esto véase [**4**].

5. Teorías de torsión.

La correspondencia dada por el teorema 4.2 puede aplicarse también a relaciones $\mathcal{R}$ de una clase $\mathcal{A}$ a otra clase $\mathcal{B}$, aún cuando estas no sean conjuntos. En tal caso la polaridad $\pi_{\mathcal{R}}$ inducida por $\mathcal{R}$ se establece entre $\wp(\mathcal{A})$ y $\wp(\mathcal{B})$ donde ahora se denotan así las clases que constan de todas las subclases de $\mathcal{A}$ y $\mathcal{B}$, respectivamente. Sea R un anillo asociativo con uno y sea R-Mod la clase de todos los R-módulos izquierdos. La relación sobre R-Mod dada por

$$\mathcal{H} = \{(M, N) \in R\text{-Mod} \times R\text{-Mod} \mid \text{Hom}_R(M, N) = 0\},$$

induce una polaridad $\pi_{\mathcal{H}}$ sobre $\wp(R\text{-Mod})$ dada por las siguientes asignaciones definidas para subclases $\mathcal{A}$ y $\mathcal{B}$ de R-Mod:

$$f_{\mathcal{H}}(\mathcal{A}) = \{N \in R\text{-Mod} \mid \forall M \in \mathcal{A}, \text{Hom}_R(M, N) = 0\},$$
$$g_{\mathcal{H}}(\mathcal{B}) = \{M \in R\text{-Mod} \mid \forall N \in \mathcal{B}, \text{Hom}_R(M, N) = 0\}.$$

De acuerdo al teorema 2.8, las subclases de R-Mod $\pi_{\mathcal{H}}$-cerradas son aquellas $\mathcal{A}$ tales que $g_{\mathcal{H}}f_{\mathcal{H}}(\mathcal{A}) = \mathcal{A}$ y las subclases $\pi_{\mathcal{H}}$-abiertas son aquellas $\mathcal{B}$ tales que $f_{\mathcal{H}}g_{\mathcal{H}}(\mathcal{B}) = \mathcal{B}$.

Llegamos pues al concepto de teoría de torsión introducido por Dickson en [**1**]. De hecho él define en [**1**, §3, p. 228] los operadores $f_{\mathcal{H}}$ y $g_{\mathcal{H}}$ y demuestra que la siguiente condición es una definición alternativa al concepto que presenta al principio de su artículo.

Definición 5.1 *Dado un anillo R, una* teoría de torsión *es una pareja $(\mathcal{A}, \mathcal{B})$ de subclases de R-Mod tales que $\mathcal{B} = f_{\mathcal{H}}(\mathcal{A})$ y $\mathcal{A} = g_{\mathcal{H}}(\mathcal{B})$.*

En otras palabras, una teoría de torsión es una pareja $(\mathcal{A}, \mathcal{B})$ donde $\mathcal{A}$ es una subclase $\pi_{\mathcal{H}}$-cerrada y $\mathcal{B}$ es la subclase $\pi_{\mathcal{H}}$-abierta que le corresponde de manera biunívoca, según la proposición 2.9. Consideremos las siguientes *propiedades de cerradura* que puede tener una clase de R-módulos.

Definición 5.2 *Una subclase $\mathcal{C}$ de R-Mod es* cerrada bajo*:*

1. epimorfismos *si para cada epimorfismo* $M \twoheadrightarrow L$ *tal que* $M \in \mathcal{C}$ *se tiene* $L \in \mathcal{C}$*;*

2. monomorfismos *si para cada monomorfismo* $N \rightarrowtail M$ *tal que* $M \in \mathcal{C}$ *se tiene* $N \in \mathcal{C}$*;*

3. sumas directas *si para cada conjunto* $\{M_i\}_{i\in I}$ *de* R*-módulos en* $\mathcal{C}$ *se tiene que su suma directa* $\bigoplus_{i\in I} M_i$ *está en* $\mathcal{C}$*;*

4. productos directos *si para cada conjunto* $\{M_i\}_{i\in I}$ *de* R*-módulos en* $\mathcal{C}$ *se tiene que su producto directo* $\prod_{i\in I} M_i$ *está en* $\mathcal{C}$*;*

5. extensiones *si para cada sucesión exacta* $0 \to N \to M \to L \to 0$ *tal que* $N, L \in \mathcal{C}$ *se tiene* $M \in \mathcal{C}$*.*

Las subclases $\pi_{\mathcal{H}}$-cerradas y $\pi_{\mathcal{H}}$-abiertas pueden caracterizarse en términos de ciertas propiedades de cerradura como sigue.

Proposición 5.3 *Sea* $\mathcal{C}$ *una subclase de* R*-Mod.*

1. $\mathcal{C}$ *es una subclase* $\pi_{\mathcal{H}}$*-cerrada si y sólo si es cerrada bajo epimorfismos, sumas directas y extensiones.*

2. $\mathcal{C}$ *es una subclase* $\pi_{\mathcal{H}}$*-abierta si y sólo si es cerrada bajo monomorfismos, productos directos y extensiones.*

A las subclases $\pi_{\mathcal{H}}$-cerradas de R-Mod se les llama *clases de torsión*. A las subclases $\pi_{\mathcal{H}}$-abiertas se les llama *clases libres de torsión*. Aplicando la proposición 2.9 tenemos el siguiente resultado.

Corolario 5.4 *Existe una correspondencia biunívoca entre las clases de torsión y las clases libres de torsión, que invierte la contención de clases.*

6. Conclusiones y preguntas.

El concepto de conexión de Galois es lo suficientemente básico para permear diversas áreas de las matemáticas, como se puede apreciar en la larga lista de ejemplos en [**4**]. Eso nos lleva a preguntar si la interesante situación del teorema fundamental de la teoría de Galois ocurre en otros ámbitos. Como hemos visto aquí, dicha situación se da gracias a que con ciertas condiciones muy especiales, todos los elementos de los dos copos involucrados son cerrados o abiertos, respectivamente. En otro tipo de conexiones de Galois no tendremos la misma fortuna, y cabe preguntar

¿qué condiciones debemos añadir para que la conexión de Galois sea un isomorfismo? De todos modos sigue existiendo un isomorfismo que hace corresponder los cerrados de un copo con los abiertos del otro. Así que un par de preguntas importantes ante cualquier conexión de Galois $\langle P, f, g, Q\rangle$ es ¿cuáles son los cerrados de P? ¿cuáles son los abiertos de Q? Hemos visto que en el caso de la conexión de Galois $\pi_{\mathcal{H}}$ usada para definir las teorías de torsión, se caracterizan estos elementos en términos de propiedades intrínsecas. ¿En qué otros casos se puede hacer esto? Todas estas preguntas ofrecen una interesante perspectiva.

Bibliografía

1. S. E. Dickson, A torsion theory for abelian categories, *Trans. Amer. Math. Soc.* **121** (1966) 223–235.
2. G. Ehrlich, *Fundamental Concepts of Abstract Algebra*, PWS-KENT, 1991.
3. I. N. Herstein, *Topics in Algebra*, John Wiley and Sons, 1975.
4. A. M. M. Erné, J. Koslowski y G. E. Strecker, A primer on galois connections, *Ann. New York Acad. Sci.* **704** (1993) 103–125.
5. F. Zaldívar, *Teoría de Galois*, Anthropos-UAM, 1996.