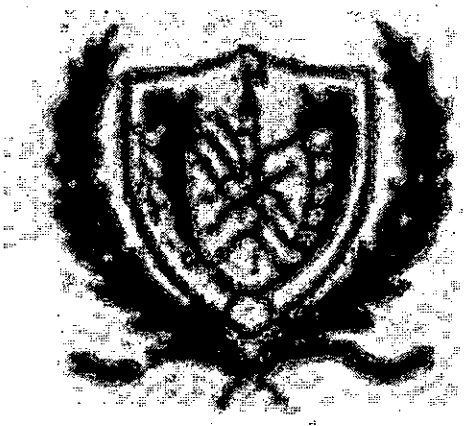
Conexiones de Galois en Categorías

CARLOS RAFAEL PAYARES GUEVARA



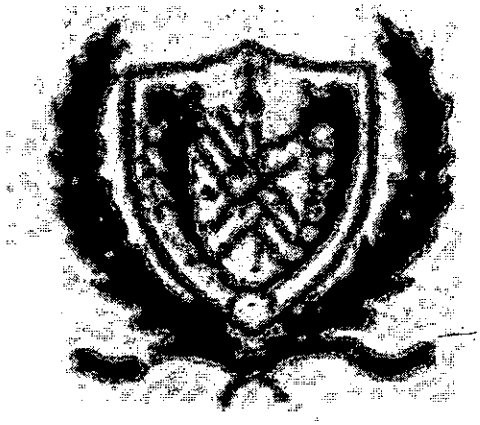
UNIVERSIDAD DE CARTAGENA
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
PROGRAMA DE MATEMÁTICAS
CARTAGENA, D.T Y C
OCTUBRE DE 2009

Conexiones de Galois en Categorías

CARLOS RAFAEL PAYARES GUEVARA

TRABAJO DE TESIS PARA OPTAR AL TÍTULO DE
ESPECIALISTA EN MATEMÁTICAS AVANZADAS

DIRECTOR
JOAQUIN LUNA TORRES



UNIVERSIDAD DE CARTAGENA
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
PROGRAMA DE MATEMÁTICAS
CARTAGENA, D.T Y C
OCTUBRE DE 2009

Dedicado a

A mi bebé... mi hermosa geometría

Índice general

Introducción

Las matemáticas, sin duda alguna son una de las obras más majestuosas y hermosas creadas por la mente humana; creaciones como éstas, que de alguna manera u otra, contribuyen a la belleza de la existencia humana son dignas de ser aprendidas no meramente como una tarea sino para ser asimilada como parte del pensamiento diario, y recordada una y otra vez con ánimo siempre renovado, hasta que nuestro espíritu contemple la verdad y la esencia del ser. E. Galois (1811-1832) desde su tumba se ríe y se asombra al ver que frecuentemente su nombre es mencionado en libros y artículos recientes de matemáticas, en tópicos que se inspiran en su trabajo original.

Bajo estas consideraciones, en este trabajo se pretende mostrar que la "filosofía Galoisiana" encarna en muchas áreas de las matemáticas, y resaltar la enorme influencia que ha tenido en algunas construcciones fundamentales de las matemáticas contemporáneas: en la obra de Alexander Grothendieck (1928 - hoy).

Una extensión de cuerpos $K \subseteq E$ es una extensión de Galois cuando todo elemento de E es la raíz de un polinomio $p(x) \in K[x]$ el cual se escinde en $E[x]$ en factores lineales y toda su raíces son distintas. El grupo de Galois $Gal(E/K)$ de esta extensión es el grupos de automorfismo de E que dejan invariantes a K puntualmente. El teorema clásico de Galois asegura que cuando $K \subseteq E$ es una extensión de Galois de dimensión finita los subgrupos $G \subseteq Gal(E/K)$ del grupo de Galois clasifican exactamente las extensiones de cuerpos intermedios $K \subseteq M \subseteq E$; y este resultado fue el que usó Galois para probar su teorema célebre.

Esta teoría que fue presentada por Galois, y que más tarde fue reconstruida en el lenguaje moderno,por E. Artin, Kaplansky, tuvo que esperar mucho tiempo para ser extendida en mundos matemáticos de naturalezas aparentemente distintas. El Diagrama 1 (pag V) manifiesta actualmente los contextos de la "*teoría de Galois*". Probablemente este esquema es incompleto si se trata de incluir descensos y cohomología de Galois, la dualidad Grothendieck - Teichmüller (manejo de teoría algebraica de números, automorfismos, superficies de Reimann, para estudiar las conexiones entre $Gal(\overline{Q}, Q)$, y grupos combinatorios y algunos otros tópicos relacionados.

Las flechas sólidas en el diagrama representan generalizaciones de varias construcciones y resultados, y las flechas punteadas representan "*inspiraciones*".

El primer paso de generalización de la Teoría clásica de Galois es reemplazar las extensiones de cuerpos intermedios $K \subseteq M \subseteq E$ por objetos más generales como son las *K-álgebras* conmutativas. Dada una extensión de cuerpos una *K-álgebra* A es *diagonal-*

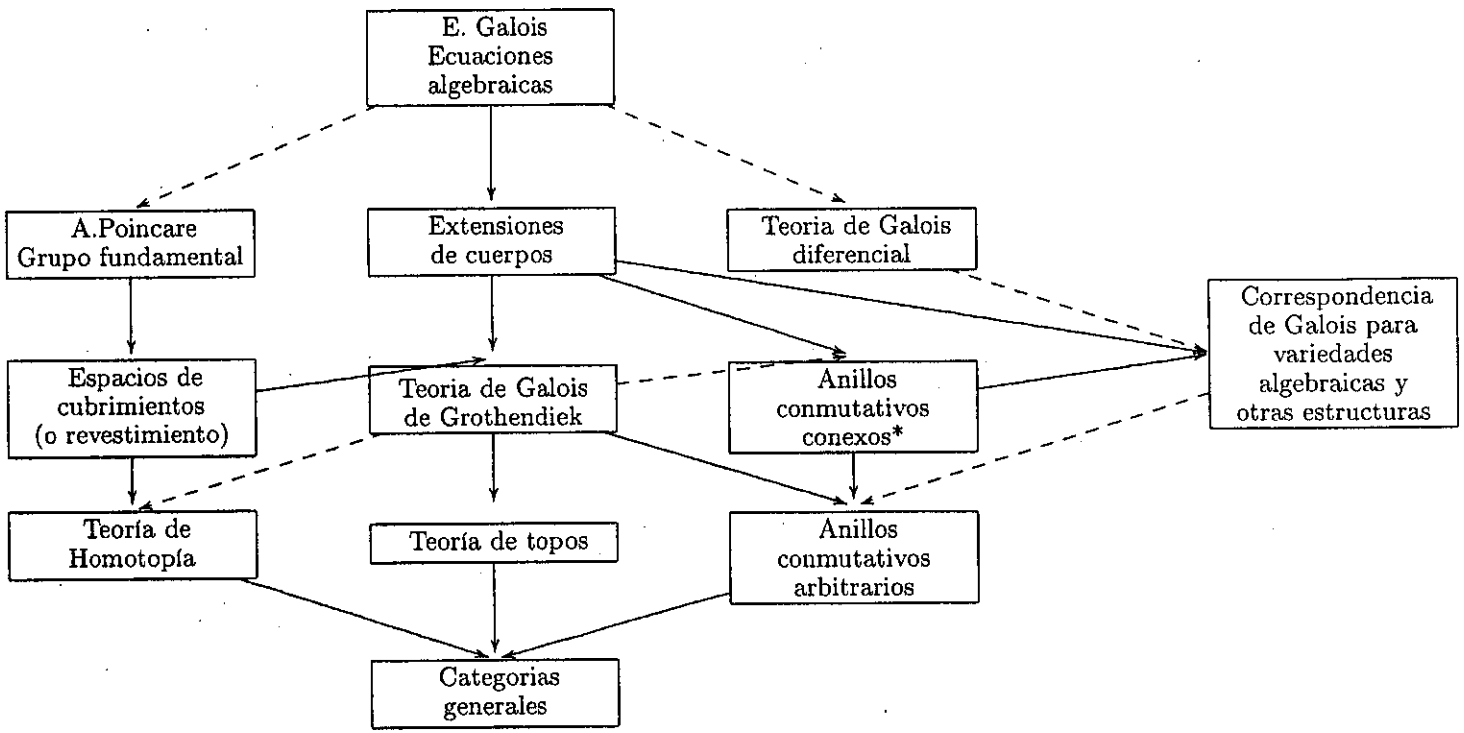


Diagrama 1: Los contextos de las teorias de Galois

*Conexos se refiere a la conexidad del espectro de zariski, que es equivalente a la ausencia de elementos idempotentes no triviales

Ejemplos de categorías

- **Conj** { Objetos: conjuntos; Morfismos: funciones
- **Cpo** { Objetos: conjuntos parcialmente ordenados; morfismos: funciones monótonas
- **Ret** { Objetos: Retículos; morfismos: homomorfismos de retículos
- **Grp** { Objetos: Grupos; morfismos: homomorfismos de grupos
- $\mathbf{Mod}_R$ { Objetos: R-módulos a derecha (R cualquier anillo); morfismos: homomorfismos de R-módulos
- **Top** { Objetos: Espacios topológicos; Morfismos: funciones continuas
- **GrpTop** { Objetos: Grupos topológicos; Morfismos: homomorfismos de grupos continuos
- **Anu** { Objetos: Anillos unitarios; Morfismos: homomorfismos de anillos que preservan unidad

- Cualquier conjunto pre-ordenado constituye otro ejemplo de categoría. Sea A un conjunto no vacío con una relación $\leq$ la cual es reflexiva y transitiva; y denotamos tal categoría por G_A donde: $Ob(G_A) = A$, y para cada $x, y \in A$ se define:

$$Mor_{G_A}(x,y) = \begin{cases} \{ x \to y \} & \text{si } x \leq y \\ \emptyset & \text{si no} \end{cases}$$

La composición de morfismo se define por la transitividad de la relación $\leq$, esto es, para $x \xrightarrow{f} y$, $y \xrightarrow{g} z$ se tiene que $g \circ f : x \to z$, pues $x \leq y$, $y \leq z$ implica $x \leq z$

En teoría de categorías las ideas vienen en parejas, cada una de las cuales es dual de la otra, en el sentido de que la definición o afirmación de la una se obtienen de la otra "invirtiendo el sentido de las flechas en los morfismos" esta observación lleva a la consideración de obtener a partir de una categoría R arbitraria otra categoría R^0, denominada la *categoría dual* (o *categoría opuesta*), y definida de la siguiente manera:

(i) $Ob(R^0) = Ob(R)$

(ii) Para cualquiera A, B en $Ob(R^0)$ se tiene $Mor_{R^0}(A,B) = Mor_R(B,A)$

- Sean R una categoría y A en $Ob(R)$ fijo, entonces se tiene el funtor contravariante:

$$Mor_R(\_, A) : R \longrightarrow Conj$$

$$\begin{array}{ccc} X & \longrightarrow & Mor_R(X, A) \\ {\scriptstyle\sigma}\downarrow & & \uparrow{\scriptstyle Mor_R(\sigma,A):f\mapsto f\circ\sigma} \\ X' & \longrightarrow & Mor_R(X', A) \end{array}$$

Si $R = {}_RMod$ (la categoria de los *R-módulos* a izquierda), entonces para todo X en $Ob(R)$: $Mor_R(X, A) = Hom_R(X, A) := \{f : X \to A : f(a + b) = f(a) + f(b), f(ra) = rf(a), \forall a, b \in X, \forall r \in R\}$ es un objeto de ${}_{\mathbb{Z}}Mod$ (la categoría de los grupos abelianos), analogamente, si $R = Mod_R$.
El funtor $Mor_R(\_, A)$ se suele denotar por $Hom_R(\_, A)$

  - En la categoría de los *R-módulos* (a izquierda o derecha) el funtor$Hom_R(_, A)$ es exácto a izquierda.
  - un *R-módulo* P es *proyectivo* si el funtor $Hom_R(\_, P)$ es exácto (para más detalles ver[12])

- El *producto tensorial* de A en $Ob(Mod_R)$ y B en $Ob({}_RMod)$ es un objeto $A \otimes_R B$ de la categoría ${}_{\mathbb{Z}}Mod$ y una función bilineal y R-balanceada $h : A \times B \to A \otimes_R B$ tal que para todo G en $Ob({}_{\mathbb{Z}}Mod)$ y toda funcion $f : A \times B \to G$ bilineal y *R-balanceada* existe un único homomorfismo $g : A \otimes_R B \to G$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} A \times B & \xrightarrow{h} & A \otimes_R B \\ {\scriptstyle f}\downarrow & \swarrow_{g} & \\ G & & \end{array}$$

Se puede demostrar que tal objeto existe (ver[12], teorema 1.4 pag.11)

Sea A en $Ob(Mod_R)$ fijo, existe un funtor aditivo dado por:

$$A \otimes_R \_ : {}_RMod \longrightarrow {}_{\mathbb{Z}}Mod$$

$$\begin{array}{ccc} B & \longmapsto & A \otimes_R B \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle A\otimes_R f:=1_A\otimes f} \\ C & \longmapsto & A \otimes_R C \end{array}$$

Similarmente, para $B \in Ob({}_RMod)$ fijo, existe un funtor aditivo:

$$\_ \otimes_R B : Mod_R \longrightarrow {}_{\mathbb{Z}}Mod$$

$$\begin{array}{ccc} A & \longmapsto & A \otimes_R B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g\otimes_R B:=g\otimes 1_B} \\ C & \longmapsto & C \otimes_R B \end{array}$$

Los funtores $A \otimes_R \_$, $\_ \otimes_R B$ son covariantes y exactos a derecha.

- Un elemento x en el G-objeto X se llama *invariante* o *G-invariante* si x queda fijo bajo toda transformación $\sigma_g : \sigma_g(x) = x$ para toda $g \in G$. Un subconjunto $M \subseteq X$ es invariante si $\sigma_g(M) \subseteq M$ para todo $g \in G$

- Sean G y G' grupos y R una categoria, X un G-objeto de R con respecto a un homomorfismo $\sigma : G \to Aut(X)$, X' un G-objeto de R con respecto a un homomorfismo $\sigma' : G' \to Aut(X')$. Un *morfismo θ-equivariante* con respecto a un homomorfismo $\theta : G \to G'$ es un morfismo $\varphi : X \to X'$ de R tal que para todo $g \in G$ el siguiente diagrama conmuta:

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & X' \\ \downarrow & & \downarrow{\scriptstyle \sigma_{\theta(g)}} \\ X & \xrightarrow[\varphi]{} & X' \end{array}$$

• Si $G = G'$ y $\theta = id_G$ solo diremos una aplicación *equivariante*

Ejemplo 2. SI X' es un G-conjunto y X es un G-conjunto con la acción del ejemplo 1. Entonces la aplicacion $\varphi : X \to X'$ es *θ-equivariante* si y sólo si el siguiente diagrama conmuta:

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ \downarrow{\scriptstyle \theta \times \varphi} & & \downarrow{\scriptstyle \varphi} \\ G \times X' & \longrightarrow & X' \end{array}$$

Si X, X', X'' son G, G', G''-objetos respectivamente, $\theta : G \to G'$, $\theta' : G' \to G''$ homomorfismos y $\varphi : X \to X'$, $\varphi : X' \to X''$ morfismos θ, θ'-equivariantes respectivamente, entonces $\varphi' \circ \varphi$ es un morfismo $\theta \circ \theta'$-equivariante.

Para un grupo G fijo, los *G-objetos* de una categoría R forman una categoría denotada R^G con los morfismos equivariantes como morfismos.

Ejemplo 3. Sea $R = Conj\ Fin$ la categoría de los conjuntos finitos, se tiene que:

$$Conj\ Fin^G$$

Es una subcategoría plena de $Conj^G$

- R^G, puede ser considerada como una categoría de funtores (interpretando a G como una categoría constituida de un sólo objeto y morfismos $g, g \in G$, con la ley de composición natural) donde los morfismos equivariantes son las trasformaciones naturales.

- Sea X un G-conjunto y $x \in X$, el subgrupo de $G : E(x) := \{g \in G : \tau_g(x) = x\}$ se llama el *grupo estabilizador* de x.

Sea X un G-conjunto con respecto a $\tau : G \to Aut(X)$. La *órbita o G-órbita* de $x \in X$, bajo la operación dada es el conjunto $\eta(x) := \{\tau_g(x) : g \in G\}$.

Afirmación. Si X es un G-conjunto, las diferentes órbitas forman una partición de X en conjuntos disyuntos, en efecto: como $x \in \eta(x)$, $X = \cup_{x \in X} \eta(x)$.
Sea $y \in \eta(x) \cap \eta(x'), x, x' \in X$, entonces $y = \tau_g(x)$, $y = \tau_{g'}(x')$. Para $z \in \eta(x) : z = \tau_a(x)$ se tiene $z = (\tau_a \circ \tau_{g^{-1}} \circ \tau_{g'})(x') \in \eta(x')$, esto es, $\eta(x) \subseteq \eta(x')$. Esto demuestra que $\eta(x) = \eta(x')$. Dado $x \in X$, se sigue que $\eta(x)$ es un *sub-G-conjunto* de X isomorfo a un G-conjunto cociente de G, esto es: $p : G \twoheadrightarrow \eta(x)$, $g \mapsto gx$.

Por lo tanto, tenemos que:

Proposición 1.2.2. Sea G un grupo. Todo G-conjunto X es la unión disyunta de *G-conjuntos* cocientes de G.

Consideremos otro ejemplo importante de *G-objeto*.

Ejemplo 4 (*G-espacios*)
Sea $G \in Ob(GrpTop)$ fijo. Un *G-espacio* X es un espacio topológico el cual es un G-conjunto con respecto a la aplicación $G \times X \to X$. Además esta aplicación se supone continua.

Es claro que el grupo G está actuando por homeomorfismos sobre X, asi que X es un G-objeto en la categoría Top.

Sea X un *G-espacio*, X' un *G'-espacio* y $\rho : G \to G'$ un morfismo de $GrpTop$. Un morfismo ρ-equivariante con respecto a $\rho : G \to G'$ es un morfismo $\varphi : X' \to X'$ de Top tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ {\scriptstyle \rho \times \varphi}\downarrow & & \downarrow{\scriptstyle \varphi} \\ G' \times X' & \longrightarrow & X' \end{array}$$

φ es continuo y por lo tanto $\rho \times \varphi$ tambien es continua, esto se sigue por la propiedad universal de la topología producto.

- Sea X un espacio topológico y G el grupo de homeomorfismos de X. La topología discreta sobre G hace a X un G-espacio

Observación. Note que dado un grupo topológico, un G-conjunto X discreto, aún finito, no tiene por que ser un G-espacio topológico, puesto que la acción $G \times X \to X$ ya

Ejemplo. Todo anillo es una $\mathbb{Z}$-*álgebra*

Ejemplo. Dado un conjunto X, el conjunto K^X de las funciones de X en K tiene una estructura natural de K-*álgebra*, definiendo las operaciones puntualmente. Ésta es un álgebra asociativa conmutativa y con unidad, que tambien se denota $F(X,K)$

Ejemplo. Sea $E \in Ob(Ext(K))$. Si B es una E-*álgebra* cualquiera, entonces B es una K-*álgebra* por restricción de multiplicación escalar a los elementos de K.

Ejemplo. Sea $E \in Ob(Ext(K))$, y A una K-*álgebra* entonces $E \otimes_K A$ es una E-*álgebra* Definida por

$$(e \otimes a) \cdot (e' \times a') = (ee') \otimes (aa')$$
$$e(e' \otimes a) = (ee') \otimes a$$

Se tiene la siguiente categoría:

- **K-Alg** $\left\{ \begin{array}{rl} \text{Objetos:} & K\text{-}\textit{álgebra} \\ \text{morfismos:} & \text{homomorfismos de } K\text{-}\textit{álgebras.} \end{array} \right.$

Proposición 1.3.1. Sea $E \in Ob(Ext(K))$, B una E-*álgebra* y A una K-*álgebra*. Entonces

$$Hom_{E-alg}(E \underset{K}{\otimes} A, B) \cong Hom_{K-alg}(A, B).$$

Es decir: (en lenguaje de categoría)

$$E - Alg \underset{F}{\overset{G}{\rightleftarrows}} K - Alg$$

donde:

$$F : A \longmapsto E \underset{K}{\otimes} A$$
$$G : B \longmapsto B$$

F es adjunto izquierdo de G (con extensiones naturales para morfismos). (ver [12], pag 37)

Demostración. Dadas B, A y E, K-*álgebras* respectivamente, defínase

$$Hom_{E-alg}(E \underset{K}{\otimes} A, B) \longrightarrow Hom_{K-alg}(A, B)$$

Así: dado $f : E \otimes_K A \to B$, considérese

■

Colorario 1.3.5 Sea A una *K-álgebra* y $I(A) := \{M \subseteq A : M$ es un ideal máximal de $A\}$. Entonces existe una biyección entre $Hom_{K-alg}(A, K)$ e $I(A)$.

Demostración. Todo *K-homomorfismo* $A \xrightarrow{f} K$ es sobre: $a = a \cdot 1 = a \cdot f(1) = f(a \cdot 1)$; luego $A/Ker(f) \cong K$. Como K es un cuerpo, entonces por proposición 1.3.4 $Ker(f)$ es ideal máximal de A.

■

Sea K un cuerpo y A una *K-álgebra*. Un elemento $a \in A$ es algebraico si existe $p(x)$ en $K[x]$ tal que $p(a) = 0$. La *K-álgebra* A se dice *algebraica* cuando todos sus elementos sean algebraicos sobre K.

Proposición 1.3.6 Sea K un cuerpo. Toda *K-álgebra* de dimensión finita es algebraica.

Demostración. Dado $a \in A$, la sucesión de elementos $1, a, a^2, a^3, \ldots, a^n, \ldots$ conllevarán a que la relación $a_n a^n + a_{n-1}a^{n-1} + \ldots + a_2 a^2 + a_1 a + a_0 = 0$ para algún $a_i \neq 0$ en K, puesto que $dim_K(A) < \infty$ (dimensión de A sobre K). Tomando $p(x) = \sum_{i=0}^{n} a_{n-i}x^{n-i}$ se tiene $p(a) = 0$.

■

Proposición 1.3.7 Sea K un cuerpo, A una *K-álgebra* y $0 \neq a \in A$ un elemento algebraico. Entonces existe un único polinomio $p(x) \in K[x]$ tal que:

(i) $p(x)$ es mónico

(ii) $p(a) = 0$

(iii) si $g(x) \in K[x]$ con $g(a) = 0$, entonces $p(x)|g(x)$.

Este polinomio $p(x)$ se llama polinomio mínimal de a.

Ejemplo (*Un polinomio mínimal reducible*)
Sea K un cuerpo y considerese la *K-álgebra* K^2, de dimensión 2 sobre K. Dado $k \in K$, la única raíz del polinomio de primer grado $x - k$ en K^2 es $k \cdot 1$, donde $1 = (1, 1)$ es la unidad de K^2. En particular el polinomio minimal del elemento es una raíz en K^2 de $x^2 - x$, el cual es su polinomio mínimal. Obsérvese que este polinomio es reducible: $x^2 - x = x(x-1)$.

Proposición 1.3.8. Sea A una *K-álgebra* y $a \neq 0$ en A un elemento algebraico. Si el álgebra A es un dominio de integridad, el polinomio mínimal de a es irreducible.

Demostración. Sea $p(x)$ el polinomio minimal de a. Si $p(x) = r(x)g(x)$, entonces $0 = r(a)g(a)$, puesto que A es un dominio de integridad $r(a) = 0$ o $g(a) = 0$. Por la minimalidad del grado de $p(x)$ se sigue que $r(x)$ o $g(x)$ es constante.

■

$$eV_\alpha : K[x]/\langle p(x)\rangle \longrightarrow E, \qquad [g[x]] \longmapsto g(\alpha)$$

Por otro lado, dado un morfismo $f : K[x]/\langle p(x)\rangle \to E$ de *K-álgebras*, escoja $\alpha = f([x])$, donde $[x]$ denota la clase de equivalencia de el polinomio $x \in K[x]$. Se tiene que α es una raíz de $p(x)$ puesto que

$$p(\alpha) = p(f([x])) = f(p([x])) = f([p(x)]) = f(0) = 0$$

Ya que, f es un homomorfismo de *K-álgebras* , fija los elementos de K, por tanto los coeficientes de $p(x)$.
Empezando, con una raíz α de $p(x)$, es inmediato que $eV_\alpha([x]) = \alpha$.
Luego, con f, como arriba, para todo polinomio $g(x) \in K[x]$,

$$eV_{f([x])}([g(x)]) = g(f([x])) = f(g([x])) = f([g(x)])$$

Nuevamente, puesto que f fija puntualmente a K, y por tanto a los coeficientes de $g(x)$.

Teorema 1.3.15. *Sea $E \in Ob(Ext(K))$ y A una K-álgebra. Los homomorfismos de K-álgebras $A \to E$ son linealmente independientes sobre K, en el espacio vectorial $L_K(A, E)$.*

Demostración. Por colorario 1.3.2

$$Hom_{K-alg}(A, E) \cong Hom_{E-alg}(E \underset{K}{\otimes} A, E)$$

Por tanto es suficiente probar que para toda *E-álgebra* B, los homomorfismos de *E-álgebras* $B \to E$ son linelamente independiente sobre E, y por tanto la independencia lineal sobre K se tiene.
Si $f, g : B \twoheadrightarrow E$ son homomorfismos distintos de *B-álgebras*, ellos son aplicaciones cocientes y por lo tanto $Ker(f) \neq Ker(g)$; por la maximalidad de estos núcleos, $ker(f) + Ker(g) = B$.
Ahora bien, considerese una familia finita $f_i : B_i \twoheadrightarrow E$ de homomorfismos de *K-álgebras* distintos, tales que $\sum_{1\leq i\leq n} \alpha_i f_i = 0$, para algún $\alpha_i \in E$. Aplicando el teorema chino del residuo a la aplicación

$$B \longrightarrow E^n \ , \ b \longmapsto (f_i(b_i))_{1\leq i\leq n}$$

ésta es sobreyectiva. Si al menos un α_i es no nulo, se contradice la sobreyectividad. ∎

1.4. Extensiones de Galois

Se busca estudiar objetos muy especiales en la categoría $Ext(K)$, (K cualquier cuerpo) que son las extensiones normales y separables y de Galois.
Si $E \in Ob(Ext(K))$ (E una extensión del cuerpo K), se denotara E/K; puesto que E es una *K-álgebra* escribimos $[E : K]$ para la dimensión de E como *K-espacio* vectorial.

Proposición 1.4.5. Sean E/K una extensión normal de dimensión finita. Entonces las siguientes condiciones son equivalentes:

(i) $\alpha_1, \alpha_2 \in E$ son conjugados sobre K.

(ii) Existe un *K-automorfismo* $f : E \to E$ tal que $f(\alpha_1) = \alpha_2$.

Demostración. (Ver [7] ó [14]) ∎

- Una extensión de cuerpo es de *Galois* (o *galoisiana*) cuando es normal y separable. El grupo $Aut_K(E)$ se llama el *grupo de Galois* de esta extensión y se denota por: $Gal(E/K)$.

Proposición 1.4.6. Sea $K \subseteq M \subseteq E$ Extensiones de cuerpos. Si E/K es una extensión de Galois entonces E/M es una extensión de Galois.

Demostración. Por proposiciones 1.4.2, 1.4.3 . ∎

Lema 2.1. Si $A \underset{g}{\overset{f}{\rightleftarrows}} B$ es una conexión de Galois, entonces para todo $(a,b) \in A \times B$, $a \leq g(b) \Leftrightarrow b \leq f(a)$.

Demostración. Si $a \leq g(b)$, entonces por antitonía de f, $f(a) \geq f(g(b))$, $f(a) \geq (f \circ g)(b)$, y la extensividad de $f \circ g$, implica $f(a) \geq b$; y analogamente el reciproco. ∎

En realidad, detrás de una conexión de Galois hay mucha más información estructural, como se infiere de la siguiente proposición.

Proposición 2.1. Sean $(A, \leq)$ y $(B, \leq)$ conjuntos ordenados. Entonces $A \underset{g}{\overset{f}{\rightleftarrows}} B$ es una conexión de Galois $\Leftrightarrow$ $G_B \underset{f}{\overset{g}{\rightleftarrows}} G_A$ es una adjunción categórica, es decir f es un funtor adjunto izquierdo de g.

Demostración. (ver [13], Sección 5, Teorema 1, pag 93) ∎

EJEMPLOS

2.1. Teoría de Galois Clásica

El aporte de Evariste Galois al desarrollo de la matemática ha sido fundamental. El álgebra abstracta debe a este cientifico invaluables resultados. Este ejemplo, ha sido la fuente de inspiración para crear nuevas teorías en matemáticas, de ahí radica su importacia histórica y filosófica.

Considérese E/F una extensión de cuerpos. Sea $Ext(E/F) := \{K \text{cuerpo} : F \subseteq K \subseteq E, \text{K}\}$ el conjunto de los cuerpos intermedios entre E y F, y sea $Sub(Gal(E/F) := \{H : H \text{es un subgrupo de } Gal(E/F)\}$ el conjunto de los subgrupos de $Gal(E/F)$.

- $(Ext(E/F), \leq)$ es conjunto parcialmente ordenado: $B \leq C$, para todo B, C en $Ext(E/F) \Leftrightarrow B$ es un subcuerpo de C
- $(Sub(Gal(E/F)), \leq)$ es un conjunto parcialmente ordenado: $H \leq K$ para todo H y K en $Sub(Gal(E/F)) \Leftrightarrow H$ es subgrupo de K

El par de aplicaciones:

$$Ext(E/F) \underset{Fix}{\overset{Gal}{\rightleftarrows}} Sub(Gal(E/F))$$

Demostración (Ver[7], Teorema 2.3,pag 251). ∎

Todo cuerpo F viene acompañado por extensión de Galois canónica: $\overline{F}/F$, su grupo de Galois se llama grupo de Galois absoluto de F. La extensión $\overline{F}/F$ tiene grado infinito en casi todo los casos. Demostraremos que el teorema 2.1.1 no siempre se tiene para la extensión $\overline{F}/F$. Mas precisamente, no es del todo cierto que, dado cualquier subgrupo U en $Sub(Gal(\overline{F}/F))$, exista un subcuerpo K en $Ext(\overline{F}/F)$ tal que $U = Gal(K)$, como veremos en lo que sigue. (ver ejemplo 1).

Definición 2.1.1 Sea E/F una extensión de cuerpos. K en $Ext(F/F)$ es llamado un subcuerpo cerrado si $K = Fix(H)$, para algún H en $Sub(Gal(E/F))$ se dice que es cerrado si existe K en $Ext(E/F)$ tal que $H = Gal(K)$.

Sean:
$Sub_c(Gal(E/F)) := \{H \in Sub(Gal(E/F)) : H \text{ es cerrado}\}$.
y
$Ext_c(E/F) := \{K \in Ext(E/F) : K \text{ es cerrado}\}$

Luego, tenemos las siguientes afirmaciones:

a)

$$Sub_c(Gal(E/F)) \underset{Gal}{\overset{Fix}{\rightleftarrows}} Ext_c(E/F)$$

Es una correspondencia de Galois (ver[7], Teorema 2.7, pag 247)

b) Si E/F es una extensión de Galois, $[E : F] < \infty$ entonces cualquier K en $Ext(E/F)$ es cerrado, y todo H en $Sub(Gal(E/F))$ es cerrado. (ver[7], lema 2.10(iii), pag 249). Asi que, (a) y (b) implican el Teorema 2.1.1.

c) E/F es una extensión de Galois $\Leftrightarrow$ F es cerrado.

Ahora bien, invocamos a las extensiones de Galois de dimensión infinita: el siguiente ejemplo demuestra que el Teorema 2.1.1 no es válido para ese tipo de extensiones.

Ejemplo 1. Para este ejemplo, se suponen conocidos los hechos de que: para toda potencia de primo p^d, existe un cuerpo finito $GF(p^d)$, llamado *cuerpo de Galois* de orden p^d, cuando $d = 1$, $GF(p) = \mathbb{Z}_p$; ademas $GF(p^d) \leq GF(p^r)$ si y sólo si $d|r$.(Ver [14], cap 5, pag 244-247).

Refiriendonos a la Fig 2.1. (pag 21) Sea $F := \mathbb{Z}_p = GF(p)$, y sea $E := Clau\,Alg(\mathbb{Z}_p) = \overline{\mathbb{Z}}_p$ (clausura algebraica de $\mathbb{Z}_p$) puesto que F es una cuerpo finito, este es perfecto y por tantoE/F es una extensión separable.
Puesto que E es algebraicamente cerrada, E es una extensión normal de F. por lo tanto

¿Como obtener una caracterización de los subgrupos cerrados de $Gal(E/F)$ de tal manera que exista una correspondencia de Galois?

Este problema fue resuelto en 1928 por Krull publicado en el artículo:

- "Galoissche Theorie der unendlichen algebraischen", Math. Ann., 100(1928) , pp. 687-698.

El observó que $Gal(E/F)$ puede ser dotado con una topología τ de tal forma que un subgrupo H de $Gal(E/F)$ es cerrado en el sentido algebraico de la definición si y sólo si H es topológicamente cerrado con respecto a la topología τ. Tal topología es llamada *topología de Krull.*

Una manera, de construir este grupo topológico es:

Sea E/F una extensión de Galois, no necesariamente finita. En el grupo $Gal(E/F)$ se define una topología, de dos maneras equivalentes:

a) Un sistema fundamental de vecindades de id_E se forma por los "subgrupos grandes", esto es por los subgrupos H de $Gal(E/F)$ tal que $[Gal(E/F) : H] < \infty$.(Ver [9], Teorema 21,pag. 60).

b) Identificándose cada $\sigma \in Gal(E/F)$ con una familia $(\sigma(\alpha))_{\alpha \in E} : Gal(E/F)$ se torna en un subespacio del producto cartesiano topológico $\prod_{\alpha \in E} E_\alpha$, siendo $E_\alpha = E$ con la topología discreta.

Con esta topología $Gal(E/F)$ es un grupo topológico compacto, Hausdorff y totalmente disconexo.

Así que, hemos invocado, " a la teoria de galois infinita", que consiste en una generalización del teorema 2.1.1 a extensiones galoisianas infinitas.

2.2. Teoría de Galois Infinita

Gracias a la topología de KRULL, se tiene el siguiente resultado:

Teorema 2.2.1. (Teorema Fundamental de la teoría de Galois infinita) *Sea E/F una extensión de Galois (finita o infinita) con grupo de Galois $Gal(E/F)$. Entonces existe una correspondencia de Galois entre:*

- Si a es un punto en $\mathbb{R}^2$ $\{a\}^{\perp}$ = { rectas que pasan por a }
- Si $\triangle$ es una recta en $\mathbb{R}^2$ ${}^{\perp}\{a\}$ = { puntos que estan en $\triangle$ }
- Si $A = B = G$, donde $(G, \cdot)$ es un grupo, R la relación de conmutatividad $aRb \Leftrightarrow a \cdot b = b \cdot a\}$ para $X \subseteq G$, $X^{\perp} = Cent(X)$ (subgrupo centralizador de X)

B) Sea $(\mathbb{H}, \leq)$ una álgebra de Heyting (es decir: un retículo distributivo con operación de residuación $(\Rightarrow) : a \wedge b \leq c \; ssi \; a \leq (b \Rightarrow c)$)

$$(\mathbb{H}, \leq) \underset{a \Rightarrow (\;)}{\overset{a \wedge (\;)}{\rightleftarrows}} (\mathbb{H}, \leq)$$

Es una conexión de Galois:

$$a \wedge x \leq y \text{ si y sólo si } x \leq (a \Rightarrow y)$$

Casos particulares:

B_1) $\mathbb{H} = (\{$ proposiciones $\}, \wedge, \vee, F, \Rightarrow)$, $\overset{\longmapsto}{inf}$ deducibilidad intucionista.F(falsedad).
$p \wedge q \overset{\longmapsto}{inf} r$ si y sólo si $p \overset{\longmapsto}{inf} (q \Rightarrow r)$ Teorema de deducción

B_2) $\mathbb{H} = (P(X), \cap, \cup, \emptyset, \Rightarrow), \subseteq$ contenencia conjuntista, se tiene que si A, B, C son subconjuntos de X se debe verificar: $A \cap B \subseteq C \; ssi \; A \subseteq (B \Rightarrow C)$, $(B \Rightarrow C)$ debe ser el máximo subconjunto de X que al intersectarse con B recae en C, es decir $(B \Rightarrow C) = C \cup B'$, en efecto:

$$A \cap B \subseteq C \text{ si y sólo si } A \subseteq C \cup B'$$

B_3) Sea (X, τ) un espacio topologíco y sea η la colección de abiertos en (X, τ).
$\mathbb{H} = (\eta, \cap, \cup, \emptyset, \Rightarrow)$, $\subseteq$ contenecia conjuntista.
Se tiene que si A, B, C estan en η, $(B \Rightarrow C)$ debe ser el máximo abierto que al intersectar con B recae en C; luego $(B \Rightarrow C) = \overset{\circ}{\widehat{C \cup B'}}$ (interior de $C \cup B'$) asi que : $A \cap B \subseteq C$ si y sólo si $A \subseteq \overset{\circ}{\widehat{C \cup B'}}$, en efecto:
$A \cap B \subseteq C \Rightarrow A \subseteq C \cup B' \Rightarrow A \subseteq \overset{\circ}{\widehat{C \cup B'}}$ (maximo abierto contenido en $C \cup B'$)
Viceversa:
$A \subseteq \overset{\circ}{\widehat{C \cup B'}} \Rightarrow A \cap B \subseteq (\overset{\circ}{\widehat{C \cup B'}} \cap B) = (\overset{\circ}{\widehat{C \cup B'}}) \cap B^{\circ} = (\overset{\circ}{\widehat{C \cup B'}}) \cap B = (\overset{\circ}{\widehat{C \cup B}}) \subseteq C$

C) C_1) Sea S un anillo, R un subanillo de S, y sean
$\Upsilon := \{I : I$ es un ideal de $R\}$
$\Gamma := \{J :$ es un ideal de $S\}$, considerando Υ como conjunto ordenado por la inclusión y Γ ordenado por la inclusión inversa (esto es, $J_1 \leq J_2 \Leftrightarrow J_1 \supseteq J_2$), se tiene que

- Sur Équations Différentielles et les Groupes Algébriques des Transformations (Sobre las Ecuaciones Diferenciales Lineales y los Grupos Algebraicos de Transformaciones), publicado en 1887 por la universidad de Toulouse.
- Traité d'Analyse, Tome III (tratado de análisis, tomo III) publicado por Gauthiers Villars en 1928.

Vessiot, por su parte, publicó muchos artículos, pero su más grande contribución fue su tesis doctoral titulada L'Intégrations des Équations Différentielles Linéaires (sobre la integración de las ecuaciones diferenciales lineales), publicado en 1892 por parte de la escuela normal superior de París.

Picard y Vessiot se propusieron crear, para las ecuaciones diferenciales, una teoría como la de Galois y Jordan para las ecuaciones polinómicas; hay quienes creen que comparado con el de Lie, el logro de Picard y Vessiot es más certero. Es posible pensar que la teoría de Picard - Vessiot nombrada así por la influencia de estos matemáticos, es la más apropiada teoría de Galois para las ecuaciones diferenciales.

Vessiot continuó su teoría con la colaboración de Jules Drach, formándose así la teoría de Drach - Vessiot que consiste en la teoría de Galois para ecuaciones diferenciales parciales. En esa teoría se utilizan los pseudo-grupos de transformaciones.

En fin, se puede hablar y hacer tratados extensos sobre el estudio de métodos algebraicos para analizar ecuaciones diferenciales; donde las teorías de Lie, Picard - Vessiot y Drach - Vessiot son, por el momento, las ramas de ese árbol. En adelante, hablaremos de la teoría de Picard - Vessiot. En 1932, Joseph Fels Ritt (1893-1951) publicó el libro Equations Differential from the Algebraic Standpoit (Ecuaciones Diferenciales desde el punto de Vista Algebraico), libro que le da especial tratamiento a los polinomios diferenciales y a las variedades algebraicas diferenciales. En 1950 publicó el clásico Differential Algebra (Algebra Diferencial) título que según él fue sugerido por Ellis Kolchin . Kolchin pública varios artículos alrededor de este tema, uno de ellos lo escribió con Ritt, pero su obra cumbre fue el libro Differential Algebra and Algebraic Groups (Algebra Diferencial y Grupos Algebraicos), publicado en 1973. Kolchin traslada a la teoría de Picard - Vessiot el lenguaje moderno de las extensiones de campos diferenciales, demostrando el teorema de existencia y unicidad de las extensiones de Picard - Vessiot.
Kolchin también extendió la teoría de Galois diferencial a algunas ecuaciones diferenciales no lineales especiales en un cierto sentido, en donde las extensiones son denominadas fuertemente normales. Entre 1940 y 1970, la teoría de Galois diferencial fue estudiada solamente por la escuela de Kolchin. En 1976, Irwing Kaplansky publica An Introduction to Differential Algebra (Una introducción al Algebra Diferencial) una pequeña monografía que es considerada muy buena por parte de los entendidos en la materia y que contribuyó en una forma esencial al desarrollo de este campo. En un sentido homenaje por la muerte de Kolchin en el otoño de 1991, Andy Magid, quien se desempeñó como instructor de J.F Ritt en la universidad de Columbia, pública de 1994 su obra Lectures on Differential Galois Theory (Lecciones en Teoría de Galois Diferencial).

normalmente escribimos:$a' = \delta(a)$, $a'' = \delta(\delta(a)), \ldots, a^{(n)} = \frac{\delta(\delta \ldots (\delta(a)))}{n-veces}$ esta última es la n-ésima derivada de a.

Ejemplos de Cuerpos Diferenciales.

a) Si F es un cuerpo, F es un cuerpo diferencial en el cual todos los elementos son constantes.

b) Si F es un cuerpo, podemos ver que $F(X)$, el cuerpo de fracciones con coeficientes en F en la indeterminada X con la derivación formal $\frac{\delta R(X)}{\delta X}$ para fracciones, es un cuerpo diferencial.

De ahora en adelante consideraremos solamente los cuerpos diferenciales de característica cero.

c) Dado un cuerpo diferencial F, definimos el anillo diferencial $F[X]_d$ de los polonomios diferenciales en una variable X con coeficientes en el cuerpo F, de la siguiente manera:

$$F[X]_d = F[X, X', X'', \ldots, X^{(n)}, \ldots]$$

es el anillo de polinomios con coeficientes en F en infinitas enumerables variables, para las cuales valen las relaciones:

$$X = X^{(0)}, X' =^{(1)}, X'' =^{(2)}, \ldots, X^{(n)}, \ldots$$

En general, si $P(X) \in F[X]_d$, entonces

$$P(X)' = P^*(X) + \sum X^{(n+1)} \frac{\delta P}{\delta X^{(n)}},$$

donde P^* denota el polinomio obtenido por derivación de los coeficientes de P (no hay que olvidar que los coeficientes de P, elementos de F, no necesariamente son constantes) y donde $\frac{\delta P}{\delta X^{(n)}}$ denota la derivada parcial en el sentido usual de P con respecto a la variable $X^{(n)}$. Como $F[X]_d$ es un dominio de integridad, existe el cuerpo diferencial de fracciones, el cual se denota $F(X)_d$.

- ¿Existe, para los cuerpos diferenciales, el concepto análogo al de cuerpo algebráicamente cerrado?, y si la respuesta es afirmativa,
- ¿Existe la clausura diferencial de un cuerpo diferencial?

Ecuaciones Diferenciales Lineales en una Indeterminada.

Definición 2.4.2. **(i)** Un operador diferencial lineal homogeneo sobre el cuerpo diferencial F es un operador L de la forma:

Consideremos ahora las extensiones apropiadas en la teoría de Galois Diferencial, las llamadas extensiones de Picard - Vessiot, donde este fenómeno no ocurre.

Definición 2.4.3. Una extensión diferencial E/F es una extensión de Picard - Vessiot para L si

a) E es generado sobre F como un cuerpo diferencial por las soluciones de $L = 0$ en E.

b) Las constantes de E son las costantes de F.

c) $L = 0$ tiene soluciones en E, las cuales son linelamente independientes sobre las constantes.

Observación. La definición anterior es al análogo el concepto de *cuerpo de ruptura para un polinomio* , en la clásica Teoría de Galois.

Lema 2.4.2. Si E/F es una extensión de Picard - Vessiot para L y $F \subseteq K \subseteq E$ es un cuerpo diferencial. Entonces E/K es una extención de Picard - Vessiot para L.

De ahora en adelante se utilizarán las siguientes convenciones:

⋆ C es el cuerpo de las constantes F

⋆ F es de característica cero

⋆ C es algebraicamente cerrado.

Nota. Sea R un anillo diferencial con derivación $'$. Un *ideal diferencial* I de R es un ideal tal que $f' \in I$ para todo $f \in I$.

El siguiente resultado nos da una condición para no admitir nuevas constantes.

Teorema 2.4.1. Suponga que R es una dominio de integridad diferencial, $R \supseteq F$. Si $Q(R)$, el cuerpo de fracciones de R, tiene una nueva constante, entonces R contiene un ideal diferencial primo no nulo.

Colorario 2.4.2. Sea $P \subseteq F[y_{i,j}] = R$, P un ideal diferencial primo maximal, donde R es como en la proposición 2.4.1. Entonces $E = Q(R/P) \supseteq F$, donde E es el cuerpo de fracciones de R/P, satisface (a) y (b) de la definición de una extensión de $Picard-Vessiot$.

Desmostración. Como R es un anillo noetheriano (por ser un anillo de Polinomios y F es un cuerpo) existen ideales diferenciales primos maximales. Si P es uno de ellos, entonces R/P no tiene ideales diferenciales primos no nulos, luego por Teorema 2.4.1, $Q(R/P)$ no tiene nuevas constantes. Tambien se tiene que F diferencialmente generada sobre F por las soluciones de $L = 0$, de la misma forma para R/P y E.

que $V = \sigma_i(V_i)$. Se sigue entonces de la condición (a) para extensiones de Picard - Vessiot que $\sigma_1(E_1) = \sigma_2(E_2)$.
Usando la propiedad de normalidad de las extensiones de Picard - Vessiot, podemos probar su unicidad.

Teorema 2.4.5. Cualquier par de extensiones de Picard - Vessiot de F para L son isomorfas sobre F.

Demostración. Sean E_1,E_2 extensiones de Picard - Vessiot. Considerese el anillo diferencial $T = E_1 \otimes E_2$ con derivación dada por: $(e_1 \otimes e_2)' := e_1' \otimes e_2 + e_1 \otimes e_2'$. T es una F-álgebra finitamente generada, es decir, un anillo noetheriano. Sea M un ideal diferencial $E = Q(T/M)$ no tiene nuevas constantes, y dadas la inyecciones diferenciales $O_i : E_i \to E$ tales que $O_1(s) = s \otimes 1$ y $O_2(e) = 1 \otimes e$, por la propiedad de normalidad se tiene que $O = O_2 O_1^{-1}$ es un isomorfismo de E_1 a E_2 ∎

Ejemplo 1. Las extensiones de Galois finita son extensiones de Picard - Vessiot.

- **El grupo de Galois diferencial y la correspondencia de Galois.**

Sea (F, δ) un cuerpo diferencial. Un automorfismo diferencial $\alpha : E \to F$ es un automorfismo de tal forma que el diagrama

$$\begin{array}{ccc} F & \xrightarrow{\alpha} & F \\ {\scriptstyle\delta}\downarrow & & \downarrow{\scriptstyle\delta} \\ F & \xrightarrow[\alpha]{} & F \end{array}$$

es conmutativo

Definición 2.4.5. (Grupo de Galois Diferencial.)
Si E es una extensión diferencial de F, el grupo de todos los automorfismos diferenciales de E en E que dejan fijos (o invariantes) los elementos de F se denomina el *grupo de Galois diferencial de E sobre F* y es denotado por $Gal(E/F)$.

EL siguiente teorema muestra una propiedad básica de los grupos de Galois diferenciales:

Teorema 2.4.6. Si E es una extensión de Picard - Vessiot de F para L entonces $G(E/F)$ es un grupo lineal algebraico sobre C.

Supóngase que E/F es una Extensión diferencial, y considérense los siguientes conjuntos:

En analogía con el teorema de Galois para ecuaciones algebraicas se tiene el siguiente resultado.

Teorema 2.4.9. Si E es una extensión Liouville de F, entonces el grupo de Galois diferencial $Gal(E/F)$ es soluble.

2) Se puede hacer una teoría de Galois para un sistema de ecuaciones diferenciales: $Y' = AY$ donde $A \in M_{n\times n}(K)$, K cuerpo diferencial, como se hace en [8]. En nuestro ejemplo, trabajamos con el operador diferencial homogéneo $L(y) = D^n y + \ldots + a_0 y = 0$, que es equivalente a la ecuación matricial diferencial $y' = Cy$, donde

$$C = \begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & & & & \vdots \\ -a_0 & -a_1 & & \ldots & & -a_{n-1} \end{bmatrix}$$

La matriz compañera de L

2.5. Teoría de Galois de Anillos Conmutativos

La noción de extension de Galois de anillos conmutativos fue definida primero (independientemente de A. Grothendieck) por M. Auslander y O. Goldman(M.Auslander y O. Goldman, The Brauer group of commutative ring, Trans. Amer. Math. Soc. 97, 1960, 367-409), y la teoría de Galois de estas extensiones fue desarrollada por S.U. Chase, D.K. Harrison y A. Rosenberg (ver[4]) y G.J. Janusz (G.J. Janusz, Separable algebras over commutative rings, Trans Amer. Math. Soc. 122, 1996, 461 - 479).

El artículo [4] es citado en cualquier libro reciente sobre este tema y es el artículo que hemos tomado como guia principal en la elaboración de este ejemplo.

Los anillos base, en esta teoría de Galois, son anillo conmutativos; las extensiones son siempre álgebras conmutativas separables; esto es, si R es el anillo base las extensiones son R-álgebras conmutativas S , con S un $S \otimes_R S$ − módulo proyectivo. Una simplificación ocurre para los anillos en donde 0 y 1 son los únicos elementos idempotentes; puesto que en la teoría clásica de Galois (la de cuerpos) esto no es necesario ; el método usado por estos matemáticos es dar una aproximación alternativa a esta teoría.

El prerrequisito que demanda esta teoría es un curso de álgebra homológica (y cohomologica) de las K-álgebras asociativas y su dimensión homólogica. Para un tema tan especializado como este, nuestras afirmaciones y resultados, estan soportadas, en un excelente texto como lo es [5].

Extensiones de Galois de Anillos conmutativos

f_j son fuertemente distintas para $i \neq j$, se tiene que $f_i(e_j) = \delta_{ij}$.
Finalmente , $e_i e_j = f_j(e_i)e_j = \delta_{ij}$, asi que $e_1, e_2, \ldots, e_n$ son ortogonales por parejas. ∎

Sea A un anillo conmutativo, G un subgrupo finito de $(Aut(A), \circ)$, y el subanillo R de A, definido como: $R = A^G = \{a \in A : g(a) = a \text{ para todo } g \in G\}$.
Ahora bien, intoduciremos dos R-álgebras auxiliares.

- Sea $D = D(A, G)$ denotando el producto cruzado tivial de A con G. Esto dice que D es un A-módulo libre con generador U_σ (σ en G), con estructura de R-álgebra definida por la formula

$$(sU_\sigma)(tU_t) = s\sigma(t)U_{\sigma\tau}(s, t \in A; \sigma, \tau \in G)$$

  La indentidad de A es U_1, y se denotara por el simbolo 1.

- $g : D \longrightarrow Hom_R(A, A)$
  $sU_\sigma \longmapsto g(sU_\sigma) : A \longrightarrow A$
  $a \longmapsto g(sU_\sigma)(a) := s\,\sigma(a)$
  Para todo s, a en A y σ en G es una homomorfismo de R-álgebras.

- Recuerde que $E = F(G, A)$ es una A-álgebra. Si $V_\sigma : G \to A$ es la función dada por $V_\sigma(\tau) = \delta_{\sigma\tau}$, se tiene que $E = \sum_{\sigma \in G} \oplus A V_\sigma$ y V_σ son ortogonales por pareja, idempotentes en E cuya suma es 1.

- Recuerde que $A \otimes_R A$ es una A-álgebra y se tiene que: $h : A \otimes_R A \to E$, dada por $h(a \otimes t)(\sigma) = a\,\sigma(t)$ es un homomorfismo de A-álgebra.

Teorema 2.5.1. Sea A un anillo conmutativo, G subgrupo finito de $Aut(A)$, y $R = A^G$. Entonces las siguientes condiciones son equivalentes:

(a) *A es una R-álgebra separable (y los elementos de G son fuertemente distintas).*

(b) *Existen elementos $x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n$ en A tal que $\sum_{i=1}^n x_i\sigma(y_i) = \delta_{1,\sigma}$, para todo σ en G.*

(c) *A es un R-módulo proyectivo finitamente generado y g es un isomorfismo.*

(d) *Sea M un D-módulo a izquierda, el cual tambien es un G-módulo a izquierda con $\sigma(m) = U_\sigma(m)$.*

(e) *$h : A \otimes_R A \to E$ es un isomorfismo de A-álgebras.*

(f) *Dado σ en G y P un ideal maximal de A, existe $s = s(P, \sigma)$ en A con $s - \sigma(s) \notin P$.*

Definición 2.5.3. Si G es un grupo finito de automorfismo de un anillo conmutativo A y $R = A^G$, Se dice que A es una *extensión de Galois* de R con grupo de Galois G si satisface cualquiera de las condiciones equivalentes del teorema 2.5.1.

Observación

Correspondencia de Galois

Definición 2.5.4. Sea A una extensión de Galois de R con grupo de Galois G, y sea T un subanillo de A. Se dice que T *es G-fuerte* si la restricción a T de dos elementos cualesquiera de G son iguales o fuertemente distintos como funciones de T a A.

- Esta condición es vacuamente verdadera si A no tiene elementos idempotentes además de 0 y 1

Proposición 2.5.1. Sea A una extensión de Galois de R con grupo de Galois G, H un subgrupo de G y $T = A^H$. Entonces T es una R-álgebra separable G-fuerte, A es una extensión de Galois de T con grupo de Galois H y $H = \{\sigma \in G : \sigma(t) = t \text{ para todo } t \in T\}$. Si $H \trianglelefteq G$, entonces T es una extensión de Galois de R con grupo de Galois G/H.

Demostración. Sean $x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n$ en A satisfaciendo la condición (b) del teorema 2.5.1. Entonces $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{i,\sigma}$, para todo σ en H, esto demuestra que A es una extensión de Galois de T con grupo de Galois H. Luego por el teorema 2.5.1.c , A es un T-módulo proyectivo finitamente generado. Aplicando [5], IX, 2.5 se obtiene que $A \otimes_R A$ es un $T \otimes_R T$-módulo proyectivo. Pero por el teorema 2.5.1.a A es una R-álgebra separable esto es, A es un $A \otimes_R A$-módulo proyectivo, así que, A es un $T \otimes_R T$-módulo proyectivo.
Por otro lado , T es un T-módulo sumando directo de A, por lema 2.5.2 y por ser A una extensión de Galois de T. Entonces T es también un $T \otimes_R T$-módulo sumando directo de A, como A es un grupo $T \otimes_R T$-módulo proyectivo, y todo sumando directo de un módulo proyectivo es proyectivo (ver [12], teorema 3.14, pag 63), se tiene que T es un $T \otimes_R T$-módulo proyectiva. Esto es, T es una R-álgebra separable. Sea $H' := \{g \in G : g(t) = t \ \forall t \in T\}$, H' es un subgrupo de G, donde $H \subseteq H'$ y $A^{H'} = A^H = T$.
Sean $n = o(H)$ y $n' = o(H')$. Por lo anterior, A es una extesión de Galois de T con grupos de Galois H y H'. Por lo tanto, por teorema 1.e $A \otimes_T A$ es un A-módulo libre de dimensión n y tambien de dimensión n'. Ahora bien, como los anillos conmutativos son dimensionales (ver[12], Teorema 3.4 pag 58) entonces $n = n'$, y así $H' = H$. ∎

Nota. Puesto que A es una extensión de Galois de T con grupo de Galois H, aplicando el lema 2.5.2, es posible obtener que $\sum_{\rho \in H} \rho(c) = 1$.

Veamos que T es G-fuerte: sean $x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n$ satisfaciendo el teorema 2.5.1.b para A y G. Haciendo $x_i' = \sum_{\rho \in H} \rho(x_i c), y_i' = \sum_{\rho \in H} \rho(y_i)$ para $i \leq n$. x_i', y_i' están en $A^H = T$ y además para σ en G

$$\sum_{i=1} x_i' \sigma(y_i') = \begin{cases} 1, & \text{si } \sigma \in H \\ 0, & \text{en otro caso} \end{cases}$$

Aplicando la función $tra \otimes 1$ y el lema 2.5.2, obtenemos que $A^H \subseteq T$.

Las proposiciones 2.5.1 y 2.5.2 , conllevan al teorema fundamental de esta teoría de Galois; pero antes de enunciarlo, se hará la siguiente convención: sea A una extensión de Galois de R, con grupo de Galois G, se define:

$$\Delta_A := \{T : T \text{ es } R\text{-subalgebra separable (la cual es } G\text{-fuerte) de } A\}$$

$$H_T := \{\sigma \in G : \sigma(t) = t \text{ para todo } t \in T\}$$

Teorema 2.5.2. (Teorema fundamental de la teoría de Galois de anillos conmutativos) *Sea A una extensión de Galois de R, con Grupo de Galois G. Entonces existe una correspondencia de Galois entre*

$$\Delta_A \rightleftarrows Sub(G)$$

dada por:

$$T \longmapsto H_T \quad y \quad K \longmapsto A^K$$

para todo T en Δ_A y para todo K subgrupo de G. Esta correspondencia preserva la acción de G de la siguiente forma: si $\sigma \in G$ y $T \in \Delta_A$, entonces $H_{\sigma(T)} = \sigma T \sigma^{-1}$. $H \trianglelefteq G$ si y sólo si A^H es invariante bajo G, en tal caso A^H es una extensión de Galois de R con grupo de Galois G/H.

2.6. Problema Inverso de la Teoría de Galois

¿Es todo grupo finito, el grupo de Galois de una extension de $\mathbb{Q}$?
Esto es:

¿Cuales son los grupos finitos G, tales que exista una extensión E de $\mathbb{Q}$, con $Gal(E/\mathbb{Q})$ isomorfismo a G ?

¡Este problema aún no ha sido resuelto completamente!

Se conocen algunos casos particulares, por ejemplo:

(a) ¿Para que valores de n existe un polinomio sobre $\mathbb{Q}$ cuyo grupo de Galois es $S_n(A_n)$? (Una prueba para S_n, ver: Handock Charles R; Field Theory and its classical problems, Pag 210)

(b) Salvo isomorfismo existen cinco grupos de orden 8, que son:

$$\mathbb{Z}_8\,,\ \mathbb{Z}_4 \times \mathbb{Z}_2\,,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

D_4 (grupo de simetrías del cuadrado) y $\mathbb{Q}_8$ (el grupo de los cuaterniones)

(1) *La teoría de Galois de* $M_n(K)$

Sea $L = M_n(K)$, $K = GF(P^t)$ cuerpo de Galois, $p \in \mathbb{N}$ primo, y $A = Aut(L)$ supongasé que:

$$S^* = \{S | S \text{ es un subanillo simple de } L\}$$

$$G^* = \{G | G \text{ es un subgrupo regular de } A\}$$

$$Aut_A(R) = \{\Lambda \in A : \ \Lambda(\alpha) = \alpha \text{ para todo } \alpha \text{ en } R\}$$

$$Rng_L(G) = \{\sigma \in L : \ \Lambda(\sigma) = \sigma \text{ para todo } \Lambda \text{ en } G\}$$

Entonces

$$S^* \underset{Rng_L}{\overset{Aut_A}{\rightleftarrows}} G^*$$

Es una correspondencia de Galois.
(Ver [3], teorema (VIII. 18) , pag 155).

(2) *Teoría de Galois para anillos de división*

Ver [15]

(3) *Teoría de Galois para anillos conmutativos en categorías*

(Ver [6] capítulo III, Sección 3.6,2)

3.1. Álgebras Diagonalizables

En la teoría clásica de Galois, en el caso de una extensión de Galois E/K, las extensiones intermedias M pueden verse como:

- K-álgebras algebraicas sobre K.
- aquellas en las que los polinomios minimales de elementos $M(\in K[x])$ se factorizan en $E[x]$ en factores de grado uno y con raices distintas.

Definición 3.1.1. Sea E/K una extensión de cuerpos y A una K-álgebra. Se dice que E diagonaliza el álgebra A cuando:

(i) El álgebra A es algebraica sobre K.

(ii) Los polinomios minimales $p(x) \in K[x]$ de elementos de A se factorizan en $E[x]$ con factores de grado 1 y raices distintas.

Un caso particular es el siguiente:

Proposición 3.1.1. Sea E/K una extensión de cuerpo. Entonces las siguientes condiciones son equivalentes.

(a) E/K es una extensión de Galois.

(b) E diagonaliza a E (como K-álgebra).

Dada la extensión de cuerpos E/K se construye la categoría:

- $Diag(E/K) = \begin{cases} \text{Objetos:} & \text{K-álgebras diagonalizadas por } E \\ \text{Morfismos:} & \text{Homomorfismos de K-álgebras} \end{cases}$

La categoría cuyos objetos son las K-álgebras de dimensión finita diagonalizadas por E y los morfismos son homomorfismos de K-álgebras se representaran por(que es una subcategoría plena de $Diag(E/K)$) $Diag\,Fin(E/K)$.

Definición 3.1.2. (Transformación de Gelfand) Sea A una K-álgebra, se define la función:

$$\begin{array}{rcl} Gel : A & \longrightarrow & K^{Hom_{K-alg}(A,K)} \\ a & \longmapsto & Gel(a) : Hom_{K-alg}(A,K) \longrightarrow K \\ & & \varphi \longmapsto Gel(a)(\varphi) := \varphi(a). \end{array}$$

que se le llama *Transformación de Gelfand.*

Proposición 3.1.2. Sea A una K-álgebra.

K-espacios vectoriales) si τ es un isomorfismo, entonces:

$$mn = dim_K(E \otimes A) = dim_K(E^{Hom(E\otimes A,E)}) = m\ card(Hom(E \underset{K}{\otimes} A, E))$$

Asi que: $n = card(Hom_E(E \otimes_K A, E))$
(vi) $\Rightarrow$ (iv). Se debe probar que $Card(Hom_{E-alg}(E^n, E)) = n$ obsérvese que las proyecciones

$$p_i : E^n \longrightarrow E$$

forman n homomorfismos distintos de E-álgebras linealmente independientes sobre E, por el teorema 1.3.15 puesto que $dim_E(L_E(E^n, E)) = n$, las p_i son todos los morfismos de E-álgebras, por el teorema 1.3.15.
(ii) $\Leftrightarrow$ (vii). La condición (vii) expresa la inyectividad de τ, la cual se sabe que es sobreyectiva.
Falta ver (i) $\Leftrightarrow$ (ii), para tal fin, probemos el siguiente colorario. ∎

Colorario 3.1.4. En las condiciones del teorema 3.1.3, la clase de estas K-algebras satisfaciendo las condiciones equivalentes (ii) a (vii) son estables bajo subobjetos cocientes, productos finitos y productos tensoriales. Además si una K-álgebra A admite dos sub-álgebras A_1, A_2 satisfaciendo las condiciones (ii) a (vii), lo mismo se cumple para las sub-álgebras de A generadas por elementos de A_1, A_2.

Demostración. La condición (vii) es trivialmente estable bajo subobjetos.
Considerando ahora un cociente $A \overset{f}{\twoheadrightarrow} Q$ de un K-álgebra A de dimensión n, el cual satisface las condiciones de (ii) a (vii) del teorema, tensorizando con E, obtenemos un cociente de E-álgebras:

$$E^n \cong E \underset{K}{\otimes} A \xrightarrow{id\otimes f} E \underset{K}{\otimes} Q$$

El $Ker(id \otimes f) \subseteq E^n$ es un ideal de la forma:

$$J := Ker(id \otimes f) = \{(l_i)_{1\leq i\leq n} \mid \forall i \in X\ l_i = 0\}, X \subseteq \{1, \ldots, n\}\}$$

Tomando $x = Card(X)$, llegamos a $E \otimes_K Q \cong E^n/J \cong E^{n-x}$ y por la condición (vi) del teorema, resta probar que Q tiene dimensión $n-x$ sobre K. Puesto que E tiene dimensión m sobre K y E^n/J tiene dimensión $n-x$ sobre E, se sigue que E/J tiene dimensión $m(n-x)$ sobre K. Por otro lado $E \otimes_K Q$ tiene dimensión $m \cdot dim_K(Q)$ sobre K, y del cual, $dim_K Q = n - x$, puesto que $E \otimes_K Q \cong E^n/J$ al tratar el caso de productos finitos, obsérvese primero que tensorizando con E, el funtor

$$E \underset{K}{\otimes} \_ : Vect_K \to Vect_E$$

entre categorías de espacios vectoriales, es aditivo, preservando productos finitos, por lo tanto si A, A' son K-álgebras de dimensiones n, n' respectivamente y satisfaciendo las

es una equivalencia contravariante de categorías con $Gal(E/K)$ actuando por composición sobre $Hom_{K-alg}(A,E)$ para cualquier A en $Ob(Diag\,Fin(E/K))$.

Obsérvese que el hecho anterior señala que:

$$\boxed{Diag\,Fin(E/K) \approx (Conj\,Fin)^{Gal(E/K)^{op}}}$$

Es decir:
Diagonalizar álgebras corresponde esencialmente a hacer actuar el grupo el Galois.

Demostración

- **F está bien definido.**
  Si A está en $Ob(Diag\,Fin(E/K))$, entonces $F(A) = Hom_{K-alg}(A,E)$ es finito, por teorema 3.1.3,(v).
  Además la acción de $Gal(E/K)$ está dada por $Gal(E/K) \times Hom_{K-alg}(A,E) \to Hom_{K-alg}(A,E), (g,f) \mapsto g \circ f$. Por lo tanto, $F(A)$ es un $G(E/F)$-objeto de la categoría $Conj\,Fin^{Gal(E/K)}$

- **F es pleno:** Esto es, dadas A, B en $Ob(Diag\,Fin(E/K))$ para todo $F(B) \xrightarrow{g} F(A)$ morfismo en $Conj\,Fin^{Gal(E/K)}$ existe $A \xrightarrow{f} B$ morfismo de K-álgebra tal que $g = Hom(f,E)$. Observemos los siguientes traslados de acciones:

  (a) $Gal(E/K)$ actúa sobre E naturalmente:

  $$Gal(E/K) \times E \longrightarrow E$$
  $$(g,\alpha) \longmapsto g \cdot \alpha := g(\alpha)$$

  (b) $Gal(E/K)$ opera sobre $E \otimes_K A$ via (a):

  $$Gal(E/K) \times E \underset{K}{\otimes} A \longrightarrow E \underset{K}{\otimes} A$$
  $$(g, \lambda \otimes a) \longmapsto g \cdot (\lambda \otimes a) := (g\lambda) \otimes a$$

  (c) $Gal(E/K)$ actúa sobre $E^{Hom_{E-alg}(E \otimes A, E)}$ via (b) y el isomorfismo de Gelfand:

  $$Gal(E/K) \times E^{Hom_{E-alg}(E \otimes A, E)} \longrightarrow E^{Hom_{E-alg}(E \otimes A, E)}$$
  $$(g,\varphi) \longmapsto [\,\overline{f} \longmapsto g(\varphi(g^{-1} \circ \overline{f}))] \qquad (3.2)$$

Recordando la forma del isomorfismo

$$E^n \xrightarrow{\sim} E \otimes K^n$$
$$(\alpha_i) \longmapsto \sum_{k=1}^{n} \alpha_k \otimes e_k$$

donde e_i es el i-ésimo vector de la base canonica de K^n, obtenemos que:

$$\begin{aligned} Fix_{Gal(E/K)}(E \underset{K}{\otimes} K^n) &\cong \left\{ \sum_{k=1}^{n} k_i \otimes ei \mid k_i \in K \right\} \\ &\cong \{1 \otimes \left(\sum_{k=1}^{n} k_i ei \right) \mid k_i \in K\} \\ &\cong A \end{aligned}$$ ■

Abordemos la prueba de (b).
Sea $F(B) \xrightarrow{\varphi} F(A)$ morfismo en $ConjFin^{Gal(E/K)}$, luego se tiene que:

$$\begin{array}{ccc} F(B) & \xrightarrow{\quad\varphi\quad} & F(A) \\ \downarrow \wr & & \downarrow \wr \\ Hom_{E-alg}(E \otimes_K B, E) & \underset{\text{(identificación)}}{\dashrightarrow} & Hom_{E-alg}(E \otimes_K A, E) \end{array}$$

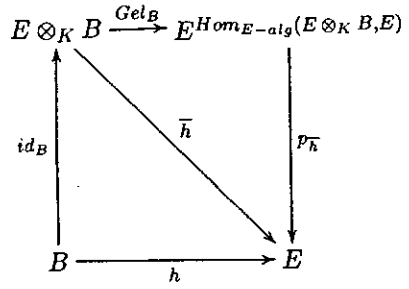
Definiendo: $E^{F(A)} \xrightarrow{\varphi^*} E^{F(B)}$ por: $\varphi^*(\alpha) := \alpha \circ \varphi$ para todo α en $E^{F(A)}$.

$$\begin{array}{ccc} F(A) & \xrightarrow{\alpha} & E \\ {\scriptstyle\varphi}\uparrow & \equiv & \nearrow \\ F(B) & & \end{array}$$

Se tiene que, φ^* es morfismo en $Conj\,Fin^{Gal(E/K)}$ via la acción (c):

$$\begin{array}{ccc} Gal(E/K) \times E^{Hom_{E-alg}(E \otimes A, E)} & \xrightarrow{\bullet} & E^{Hom_{E-alg}(E \times A, E)} \\ \downarrow {\scriptstyle id \times \varphi^*} & & \downarrow {\scriptstyle \varphi^*} \\ Gal(E/K) \times E^{Hom_{E-alg}(E \otimes B, E)} & \xrightarrow{\bullet} & E^{Hom_{E-alg}(E \otimes B, E)} \end{array}$$

en efecto:
$\varphi^*(g \cdot \alpha)(\overline{f}) = (g \cdot \alpha) \circ \varphi(\overline{f}) = g(\alpha(g^{-1} \circ \varphi(\overline{f})) = g(\alpha\varphi(g^{-1} \circ \overline{f})) = g(\varphi^*(\alpha)(g^{-1} \circ \overline{f})) =$
$(g \cdot \varphi^*(\alpha))(\overline{f})$.



$id_B(b) := 1 \otimes b$
$p_{\overline{h}}(\alpha) := (\alpha \overline{h})$
(proyección)
evaluación

que es conmutativo:

$(p_{\overline{h}} \circ Gel_B \circ id_B)(b) = (p_{\overline{h}} \circ Gel_B)(1 \otimes b) = p_{\overline{h}}(Gel_B(1 \otimes b)) = h(b)$, para todo b en B.
El siguiente diagrama es conmutativo por definición de θ y $\overline{\varphi}$:

$$\begin{array}{ccccc} A & \xrightarrow{id_A} & E \otimes_K A & \xrightarrow[\cong]{Gel_A} & E^{Hom_{E-alg}(E \otimes A, E)} \\ \downarrow{\scriptstyle \theta} & \equiv & \downarrow{\scriptstyle \varphi} & \equiv & \downarrow{\scriptstyle \varphi^*} \\ B & \xrightarrow[id_B]{} & E \otimes_K B & \xrightarrow[Gel_B]{\cong} & E^{Hom_{E-alg}(E \otimes B, E)} \end{array}$$

Asi que:

$$\begin{aligned} Hom(\theta, E)(h) &= h \circ \theta \\ &= p_h \circ Gel_B \circ id_B \circ \theta \\ &= p_h \circ Gel_B \circ \overline{\varphi} \circ id_A \\ &= p_h \circ \varphi^* \circ Gel_A \circ id_A \\ &= p_{\overline{\varphi(h)}} \circ Gel_A \circ id_A \\ &= \varphi(h) \end{aligned}$$

- **F es fiel:**

Sean A, B cualesquieras en $Ob(Diag\, Fin(E/K))$ y sean θ y α morfismos de A en B tales que $F(\theta) = F(\alpha)$, esto es, $Hom(\theta, E) = Hom(\alpha, E)$.
Veamos que $\theta = \alpha$:
Para todo $h \in F(B) = Hom_{K-alg}(B, E)$ se tiene
$p_h \circ Gel_B \circ id_B \circ \theta = h \circ \theta = Hom(\theta, E)(h) = Hom(\alpha, E)(h) = h \circ \alpha = p_h \circ Gel_B \circ id_B \circ \alpha$
Como $p_h(f) = p_h(f')$ para todo $h \in F(B)$ se tiene $f = f'$ (puesto que $p_h(f) = (f(h))$ y $p_h(f') = f'(h)$, para todo h, luego $f = f'$), entonces $Gel_B \circ id_B \circ \theta = Gel_B \circ id_B \circ \alpha$ como $Gel_B \circ id_B$ es 1-a-1 se tiene que $\theta = \alpha$.

$$F(A) \rightarrowtail F(A \times B) \leftarrowtail F(B)$$

esto es:

$$Hom_{K-alg}(A, E) \rightarrowtail Hom_{K-alg}(A \times B, E) \leftarrowtail Hom(B, E)$$

ya que $F = Hom(-, E)$.
Luego se tiene que: (por teorema 3.1.3)

$$\begin{aligned} Card(Hom_{K-alg}(A \times B, E)) &= Card(Hom_{K-alg}(E \underset{K}{\otimes}(A \times B), E) \\ &= Card(Hom_{K-alg}((E \underset{K}{\otimes} A) \times (E \underset{K}{\otimes} B), E) \\ &= Card(Hom_{E-alg}(E^n \times E^m, E) \\ &= n + m \\ &= Card(Hom_K(A, E)) + Card(Hom_K(B, E)) \end{aligned}$$

Esto concluye la prueba del teorema ■

Observación importante
El teorema 2.1.1 es un caso particular del teorema demostrado anteriormente. En efecto: la equivalencia contravariante del teorema, implica en particular, la existencia de un isomorfismo entre el retículo de subobjetos M.

$$K \rightarrowtail M \rightarrowtail E$$

En $Diag\, Fin(E/K)$, y el retículo de cocientes $Hom_{K-alg}(M, E)$

$$Gal(E/K) \cong Hom_K(E, E) \twoheadrightarrow Hom_{K-alg}(M, E) \twoheadrightarrow Hom_{K-alg}(K, E) \cong \{id\}$$

en $Gal(E/K) - Conj\, Fin$

Por las proposiciones 1.3.13, 1.2.1 esto es precisamente la correspondencia clásica de Galois.

3.3. Teoría de Galois Infinita

En este contexto la idea general es invertir la forma de proceder de la topología algebraica (dados objetos topológicos, construir adecuados invariantes algebraicos: $Top \rightarrow Alg$) Es decir, dada una situación algebraica, crear objetos topológicos que permitan razonar geométricamente ($Alg \rightarrow Top \rightarrow Geom$):

- Teoría de Galois infinita.
- Teoría de esquemas (Grothendieck)
- Geometría no conmutativa (Connes)

En este capítulo, desarrollaremos una teoría de Galois para extensión de Galois cualesquiera de cuerpo $K \subseteq E$, no necesariamente de dimensión finita.

- Usando la notación previa, desde la suposición, logramos un isomorfismo $\overline{f} : \overline{M} \to \overline{M}$ extendiendo a f. Puesto que E es algebraica sobre K, $K \subseteq E \subseteq \overline{K}$. Falta Probar que $\overline{f}(E) \subseteq E$: Dado $\alpha \in E$ con polinomio mínimo $p(x) \in F[x]$, se tiene:

$$p(\overline{f}(\alpha)) = \overline{f}(p(\alpha)) = \overline{f}(0) = 0$$

Puesto que f, y por tanto $\overline{f}$, fijan los coeficientes de $p(x)$. Asi $\overline{f}(\alpha)$ es una raíz de $p(x)$, y puesto que E/K es una extensión de Galois, $\overline{f}(\alpha) \in E$ ∎

Colorario 3.3.3. Sea E/K una extensión de Galois. Entonces:

$$K = \{\alpha \in E \mid \forall f \in Gal(E/K) \quad f(\alpha) = \alpha\} = Fix(Gal(E/K))$$

Proposición 3.3.4. Sea E/K una extensión de Galois. El cuerpo E es la union filtrada conjuntista de las subextensiones $M \in Ext(E/K)$, donde M/K es una extensión de Galois de dimensión finita.

Demostración. Si $\alpha \in E$ tiene polinomio mínimal $p(x) \in K[x]$ con raices $\alpha_1, \alpha_2, \ldots, \alpha_n$ en E, entonces por la proposición 3.3.1

$$\alpha \in K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq E$$

donde $K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K$ es una extensión de Galois de dimensión finita. Asi el cuerpo E es en efecto la unión conjuntista de subextensiones de Galois de Dimensión finita. Falta ver que esta unión es filtrante. Para esto escójase

$$K \subseteq M_1 \subseteq E, \quad K \subseteq M_2 \subseteq E$$

con M_1/K y M_2/K extensiones de Galois de dimensión finita. la K-subálgebra $M_3 \subseteq E$ generada por M_1 y M_2 es de dimensión finita sobre K. Puesto que M_1/K es una extensión de Galois, el polinomio minimal de $\alpha \in M_1$, se factoriza en M_1, y por tanto tambien en M_3 en distintos factores de grado 1; el mismo argumento para M_2. Esto demuestra que M_3 diagonaliza tanto a M_1 como a M_2, así M_3 diagonaliza a M_3, por el lema 3.1.4 por proposición 3.1.1 se tiene que M_3/K es una extensión de Galois. ∎

Proposición 3.3.5. Sea E/K una extensión de Galois supóngase que E diagonaliza la K-álgebra A. Entonces para toda K-subalgebra de dimensión finita $B \subseteq A$, existe un subextensión de Galois de dimensión finita M en $Ext(E/K)$ que diagonaliza a B

Demostración. La subálgebra B es generada sobre K por un número finito de elementos $b_1, b_2, \ldots, b_n$. Cada uno de estos b_i tienen un pòlinomio minimal $p_i(x) \in K[x]$, admitiendo en E las raices $\alpha_1^i, \alpha_2^i, \ldots, \alpha_{m_i}^i$. La extensión

Por otro lado: $E = \varinjlim \Delta$, entonces

$$\begin{aligned} Gal(E/K) &= Hom_K(E,E) \\ &\cong Hom_K(\varinjlim \Delta, E) \\ &\cong \varprojlim_{M\in\Delta} Hom_K(M,E) \quad \text{(ver [12], Teorema 2.2.7, pag 56)} \\ &\cong \varprojlim_{M\in\Delta} Hom_K(M,M) \quad (M \text{ es de Galois}) \\ &\cong \varprojlim_{M\in\Delta} Gal(M/K) \end{aligned}$$

■

Definición 3.3.7. Sea E/K una extensión de Galois. El grupo de Galois topológico de esta extensión es el grupo $Gal(E/K)$ dotado de la topología inducida por las proyecciones (Topología inicial)

$$\begin{aligned} Gal(E/K) \cong \varprojlim_{M\in\Delta} Gal(M/K) &\longrightarrow Gal(M/K) \\ f &\longmapsto f|_M \end{aligned}$$

poniendo en $Gal(M/K)$ (finito) la topología discreta para cada M en Δ. $f|_M \in Gal(M/K)$ gracias a que M es de Galois.

El grupo de Galois $Gal(E/K)$ es así un grupo topológico, que resulta como límite (co-indutivo) de grupos finitos discretos:

$$\{Gal(M'/K) \longrightarrow Gal(M/K) : M \subseteq M' :\in \Delta\}$$

Lema 3.3.8. Sea E/K una extensión de Galois. Los subgrupos $Gal(E/M) \subseteq Gal(E/K)$, para cada M en $Ext(E/K)$ una subextensión de Galois de dimensión finita, forman un sistema fundamental de vecindades abiertas y cerradas de id_E.

Demostración. Un subconjunto fundamental abierto de $Gal(E/K)$ es de la forma

$$U = P_{M_1}^{-1}(X_1) \cap \ldots \cap P_{M_n}^{-1}(X_n)$$

donde $X_i \subseteq Gal(M_i/K)$ es un subconjunto (abierto) arbitrario y P_{M_i} es la correspondiente proyección. Note que U es a la vez abierto y cerrado, puesto que cada X_i lo es. Un subconjunto cualquiera abierto de $Gal(E/K)$ es la unión de tales subconjuntos fundamentales abiertos. Para U siendo vecindad fundamental de id_E, se tiene que $1_{M_i} = P_{M_i}(1_E) \in X_i$ para todo $i = 1, 2, \ldots, n$. En ese caso U contiene a

$$V = P_{M_1}^{-1}(\{1_{M_1}\}) \cap \ldots \cap P_{M_n}^{-1}(\{1_{M_n}\})$$

se tiene que:

$$P = \{h \in Gal(E/K) : h|_M(\alpha) = \alpha\}$$

y por lo tanto

$$\begin{aligned} eV_\alpha^{-1}(\{\alpha_0\}) &= \{f \in Gal(E/K) : g^{-1} \circ f \in P\} \\ &= \{g \circ h \mid h \in P\} \end{aligned}$$

el cual es la imagen del subconjunto $P \subseteq Gal(E/K)$ por el homeomorfismo

$$\begin{aligned} Gal(E/K) &\longrightarrow Gal(E/K) \\ h &\longmapsto g \circ h \qquad (*) \end{aligned}$$

heredada de la estructura del grupo topológico puesto que $Gal(M/K)$ está dotado con la topológia discreta, $Gal(M/K(\alpha))$ es a la vez abierto y cerrado en $Gal(E/K)$, via el homeomorfismo (*) , esto implica que $eV_\alpha^{-1}(\{\alpha_0\})$ es abierto y cerrado, como se quería.
La topología del lema 3.3.9 está contenida en la topología del lema 3.3.8, reciprocamente es suficiente probar que las vecindades abiertas fundamentales $Gal(E/K)$ de id_E en el lema 3.3.8 contiene una vecindad de id_E para la topología del lema 3.3.9 en efecto M está generada por $\alpha_1, \alpha_2, \ldots, \alpha_n$. Dada f en $Gal(E/K)$, la condición $f \in Gal(E/M)$ reduce a $f(\alpha_1) = \alpha_1, \ldots, f(\alpha_n) = \alpha_n$. Esto es equivalente a

$$f \in eV_{\alpha_1}^{-1}(\{\alpha_1\}) \cap \ldots \cap eV_{\alpha_n}^{-1}(\{\alpha_n\})$$

y esta es una vecindad de id_E para la topología del lema 3.3.9, puesto que así lo es cada $eV_{\alpha_i}^{-1}(\alpha_i)$ ∎

Colorario 3.3.10. Sea E/K extensión de Galois. Para todo $f \in Gal(E/K)$, los subconjuntos

$$V_M(f) = \{g \in Gal(E/K) \ : \ g|_M = f|_M\} \subseteq Gal(E/K)$$

donde M recorre las extensiones de dimensión finita, constituyen un sistema fundamental de vecindades de f.

Demostración. Si M es generada por $\alpha_1, \alpha_2, \ldots, \alpha_n$

$$\begin{aligned} V_M(f) &= \{g \in Gal(E/K) \ : \ g(\alpha_1) = f(\alpha_1), \ldots, g(\alpha_n) = f(\alpha_n)\} \\ &= eV_{\alpha_1}^{-1}(f(\alpha_1)) \cap \ldots \cap eV_{\alpha_n}^{-1}(f(\alpha_n)) \end{aligned}$$

el cual es una vecindad de f para la topología del lema 3.3.9.
Recíprocamente, toda vecindad V de f contiene por el lema 3.3.9 una vecindad de la forma

Proposición 3.3.13. Sea E/K una extensión de Galois cualquiera. Para toda extensión de dimensión finita $M \in Ext(E/K)$

$$Gal(E/M) = \{f \in Gal(E/K) \ : \ \forall m \in M \quad f(m) = m\}$$

es un subgrupo abierto y cerrado de $Gal(E/K)$

Demostración. Citando la proposición 3.3.4 y considerando $K \subseteq M \subseteq N \subseteq E$, $[N : K] < \infty$, N/K extensión de Galois se sigue que $id_E \in Gal(E/N) \subseteq Gal(E/M)$, y por lema 3.3.8 se sabe que $Gal(E/N)$ es una vecindad abierta y cerrada de id_E, y por la proposición 1.2.3, se concluye la prueba. ∎

Colorario 3.3.14. Sea E/K una extensión de Galois para todo M en $Ext(E/K)$.

$$Gal(E/M) = \{f \in Gal(E/K) \mid \forall m \in M \quad f(m) = m\}$$

es un subgrupo cerrado de $Gal(E/K)$.

Demostración. Se tiene que:

$$\begin{aligned} Gal(E/M) &= \{f \in Gal(E/K) \mid \forall m \in M \quad f(m) = m\} \\ &= \{f \in Gal(E/K) \mid \forall m \in M \quad f \in Gal(E/K(m))\} \\ &= \bigcap_{m \in M} Gal(E/K(m))\} \end{aligned}$$

Como $[K(m) : K] < \infty$, entonces por la proposición 3.3.13 se tiene que: $Gal(E/K(m))$ es un subgrupo cerrado de $Gal(E/K)$ pero la intersección de subgrupos cerrados es cerrada (topológicamente), por tanto $G(E/M)$ es un subgrupo cerrado de $Gal(E/K)$. ∎

Lema 3.3.15. Sea E/K una extensión de Galois arbitraria y $G \subseteq Gal(E/K)$ un subgrupo cerrado. Ademas, supóngase que

$$K = Fix(G) = \{\alpha \in E \mid \forall g \in G \quad g(\alpha) = \alpha\}$$

entonces $G = Gal(E/K)$.

Demostración. Primero considerese el subgrupo

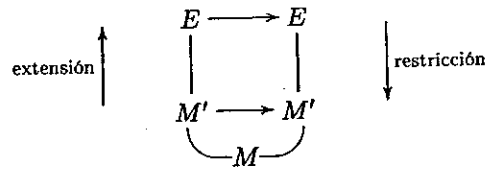
$$H_M := \{f|_M \mid f \in G\} \subseteq Gal(M/K),$$

para todo $M \in \Delta$. Luego:

$$\begin{aligned} Fix(H_M) &= \{m \in M \mid \forall h \in H_M \quad h(m) = m\} \\ &= \{m \in M \mid \forall f \in G \quad f(m) = m\} \\ &= K \end{aligned}$$

$$M \subseteq Fix(Gal(E/M)) \subseteq E$$

y E/M es una extensión de Galois, por que así lo es E/K. Dado $\alpha \in Fix(Gal(E/M))$, considérese por la proposición 3.3.4 una extensión de Galois finita M'/M, con $M \subseteq M' \subseteq E$, $\alpha \in M'$, por la proposición 3.3.2



todo M-automorfismo de M' es la restrición de un M-automorfismo de E. Puesto que α queda fijado por todo elemento de $Gal(E/M)$, tambien queda fijado por todo elemento de $Gal(M'/M)$. Por el teorema fundamental de la teoría clásica de Galois, (caso finito):

$$\alpha \in Fix(Gal(M'/M)) = M$$

■

3.4. G-espacios Profinitos

El estudio de la teoría de Galois infinita para cuerpos a la manera de Grothendieck, es necesario introducir los espacios topológicos profinitos, por tanto recomendamos ver[2], especialmente las secciones 2.8 y 2.9 del capítulo 2.

Sea $\{X_i\}$ un sistema de conjuntos indizados por un conjunto parcialmente ordenado I, el cual es dirigido, en el sentido que, dado $i, j \in I$, existe un $k \in I$ tal que $i \leq k$ y $j \leq k$. Supóngase que para todo par $i, j \in I$ con $i \leq j$, es dada una función

$$f_{ij} \ : \ X_j \longrightarrow X_i$$

tal que:

(i) $f_{ii} = id_{X_i}$, para todo $i \in I$

(ii) para todo $i \leq j \leq k$ en I, se tiene $f_{ij} \circ f_{jk} = f_{ik}$

Entonces el sistema

$$\{X_i, f_{ij} \mid i, j \in I\}$$

se llama un *sistema proyectivo*

(ii) El espacio topológico subyacente a G es profinito.

Si estas condiciones son satisfacidas, se dice que G es un *Grupo profinito*

Consideremos a $Grp\,Prof$ como la categoría de grupos topológicos profinitos (que es una subcategoría plena de la categoría $Grp\,Top$) y a $\underleftarrow{Grp\,Fin}$ como la categoría de sistemas proyectivos de grupos finitos.
Luego, la equivalencia categórica anterior se extiende (coherencia con compatibilidades de subgrupos) a una equivalencia:

$$\underleftarrow{Grp\,Fin} \approx Grp\,Prof$$
$$(G_i)_{i\in I} \longmapsto \varprojlim G_i$$

Un ejemplo típico, de grupo profinito es el grupo de Galois de una extensión de Galois: aqui:

$$Gal(E/K) = \varprojlim(E_i/K)$$

donde E_i/K recorre todos las sub extensiones de Galois de E/K, de dimensión finita. (Ver la proposición 3.3.6)

Recordemos que, dado un grupo G fijo, y R cualquier categoria, R^Grepresenta la categoria de los $G-objetos$ y sus morfismos equivariantes. Por ejemplo:

- Si $G \in Ob(Grp)$, se tiene que $Conj^G$ es la categoría de los G-conjuntos.
- si $G \in Ob(Grp\,Top)$, se tiene que Top^G es la categoría de los G-espacios.
- Si $G \in Ob(Grp)$, $Conj\,Fin^G$ es la categoría de los G-conjuntos finitos.

Ahora bien, Sea $G \in Ob(Grp\,Prof)$, un G-espacio topológico profinito es entonces el limite proyectivo de un sistema proyectivo de G-espacios topológicos finitos discretos. Asi

$$Top\,Prof^G$$

es la categoría de los G-espacios topológicos profinitos (o G-espacios profinitos);
y se tiene la equivalencia categórica:

$$\underleftarrow{Grp\,Fin^G} \approx Top\,Prof^G$$

Esto conlleva a:

$$Hom_{K-alg}(A,E) \cong Hom_{K-alg}(\varinjlim \Omega_A, E)$$
$$\cong \varprojlim_{B\in\Omega_A} Hom_{K-alg}(B,E)$$

Falta ver que $Hom_K(B,E)$ es finita para cada $B \in \Omega$. Por la proposición 3.3.5 existe $M \in \Delta$ tal que diagonaliza a B. Todo K-homomorfismo $f : B \to E$ es tal que, para todo $b \in B$ con polinomio mínimo $p(x) \in K[x]$, $p(f(b)) = f(p(b)) = f(0) = 0$, asi $f(b)$ es una raíz de $p(x)$ en E y por lo tanto $f(b) \in M$. Esto prueba que $Hom_{K-alg}(B,E) \cong Hom_{K-alg}(B,M)$, y este último conjunto es finito por teorema 3.1.3.

Lema 3.5.3. Sea E/K una extensión de Galois. Para todo A en $Ob(diag(E/K))$, la función $Gal(E/K) \times Hom_{K-alg}(A,E) \xrightarrow{\sigma} Hom_{K-alg}(A,E)$, $(g,f) \mapsto g \circ f$ es una acción continua de el grupo topológico $Gal(E/K)$ (con la topologia heredada de la defnición 3.3.7) sobre el espacio topológico profinito $Hom_{K-alg}(A,E)$ (dotado de la topológia profinita heredado del lema 3.5.2)

Prueba. Por la asociatividad de la composición σ es una acción de grupo.

Probar la continuidad, se reduce a demostrar que para todo $B \in \Omega_A$, la composición $P_B \circ \sigma$ es continua, donde P_B es la proyección canonica de el límite

$$P_B \ : \ Hom_{K-alg}(A,E) \cong \varprojlim_{B\in\Omega_A} Hom_{K-alg}(B,E) \to Hom_{K-alg}(B,E)$$

Por la proposición 3.3.5 existe $M \in \Delta$ tal que diagonaliza a B. Por la demostración del lema 3.5.2, se tiene $Hom_{K-alg}(B,E) \cong Hom_{K-alg}(B,M)$ y es un espacio finito discreto. Ahora bien, considerese el diagrama:

$$\begin{array}{ccc}
Gal(E/K) \times Hom_{K-alg}(A,E) & \xrightarrow{\sigma} & Hom_{K-alg}(A,E) \\
\downarrow{\scriptstyle P_M \times id} & & \\
Gal(M/K) \times Hom_{K-alg}(A,E) & & \downarrow{\scriptstyle P_B} \\
\downarrow{\scriptstyle id \times P_B} & & \\
Gal(M/K) \times Hom_{K-alg}(B,M) & \xrightarrow{\varphi} & Hom_{K-alg}(B,M)
\end{array}$$

puesto que P_M, y P_B son continuos por definición, la composición $(id \times P_B) \circ (PM \times id)$ es continua. La flecha $\varphi : (f,g) \mapsto f \circ g$ es continua, puesto que está definida entre espacios finitos discretos. Por tanto σ es continua.

donde

$$g\left(\sum_{i=1}^{n} k_i c_i\right) = \sum_{i=1}^{n} k_i b_i$$

Puesto que S_{B_0} es inyectiva y f es un homomorfismo de álgebras, se tiene que g es un homomorfismo de álgebras. El diagrama anterior demuestra que $f = \rho([g])$, probando que ρ es sobreyectiva. Para probar la inyectividad de ρ, considérese un homomorfismo $g' : C \to B$, tal que $f = \rho([g'])$. Por la filtración, podemos examinar como son los valores de g y g' en B_2; como S_{B_0} es inyectiva $g = g'$ en B_2. Esto dice que $[g] = [g']$ es el límite directo. ■

Sean $A, B \in Ob(Diag(E/K))$. Por definición 3.1.1 y lema 3.5.1, se puede escribir

$$A = \varinjlim C \ , \ C \subseteq A \ ; \ B = \varinjlim D \ , \ D \subseteq B \ , \ C \in \Omega_A \ , \ D \in \Omega_B$$

Por la proposición 3.3.5, para cada par C y D existen extensiones de Galois finita M_C y M_D que diagonaliza a C y D respectivamente. Por lo proposición 3.3.4 existe una extensión de Galois finita M_{CD} que diagonaliza tanto a C como a D, por tanto:

$$K \subseteq M_C \subseteq M_{CD} \subseteq E \ , \ K \subseteq M_D \subseteq M_{CD} \subseteq E$$

Como se observó en la prueba de 3.5.2

$$Hom_{K-alg}(C, E) \cong Hom_{K-alg}(C, M_{CD}) \ , \ Hom_{K-alg}(D, E) \cong Hom_{K-alg}(D, M_{CD})$$

$$Diag^{fin}_{\mu(B)}$$

la categoría de álgebras *étales* sobre $\mu(B)$.

Se tiene la siguiente equivalencia contravariante de categorías:

$$\boxed{SupRiem^{fin}_{B} \approx \left(Diag^{fin}_{\mu(B)}\right)^{op}}$$

Para mas información ver [2]

(2) A.R. Magid en (A.R. Magid, the separable Galois theory of conmutative rings, Marcel Dekker, 1974), desarrolla la teoría de Galois de Grothendieck para anillos conmutativos, en su forma mas general). En [6],se propone una aproximación a esta teoría de Galois de anillos, inspirado por A.R. Magid en forma categórica, donde usan el funtor espectro de Pierce y sus adjuntos,para relacionar la categoría de anillos conmutativos con la de los espacios topológicos profinitos.

[12] Rotman J. An Introduction to Homological Algebra, Academic Press, 1974.

[13] Saundars Mc. Lane, Categories for the Working Mathematician, New York, Springer-Verlang, 1998.

[14] Serge Lang, Algebra, Springer-Verlang, New York, 2002.

[15] Jacobson, N. Structure of Ring, Amer. Math. Soc., Colloquium Publications XXXVII, Providence, 1964.

[16] Miller G.A. Blichfeldt, H.F., and Dickson, L.E., Theory and Aplications of Finite Groups, Dover, 1961.