Teoría de Galois de álgebras separables sobre un cuerpo

Santiago Cortés-Gómez

24 de noviembre de 2016

Índice

1. Introducción

La teoría de Galois que tiene sus raíces en el álgebra, cuenta con analogías geométricas dadas por revestimientos topológicos. Quizá, la analogía más explicita es aquella dada por los revestimientos sobre superficies de Riemann. Las anteriores analogías fueron probablemente la fuente de inspiración para tratar de generalizar la noción de ser de "Galois". El objetivo de este trabajo es explorar un pequeño apartado de esta generalización dada por teoremas enunciados en leguaje categórico similares al teorema de clasificación de Galois. Este lenguaje afectará las demostraciones clásicas de la teoría de Galois. Algunas, ciertamente, se verán envueltas en tecnicismos, que a primera vista, las hará más díficiles de seguir para un lector que no esté familiarizado con las herramientas usadas (como el producto tensorial de álgebras, y el lenguaje functorial). Este en apariencia inútil cambio de lenguaje, tendrá ciertamente consecuencias. La primera, es poder enunciar el Teorema de clasificación de Galois en términos de una antiequivalencia de categorías. La segunda es el poder fijar como objeto para enunciar la clasificación el grupo de Galois absoluto y no el de una extensión fija . Lo anterior implica que es la acción de un grupo abstracto y no una extensión del cuerpo K, la que permite realizar el enunciado de clasificación de Galois. Como consecuencia de no fijar una extensión, se generan enunciados de clasificación para extensiones infinitas o de álgebras distintas a un cuerpo. La última y más relevante consecuencia, que desafortunadamente no pudo ser abordada en este trabajo, es la posibilidad de dar el grupo de Galois como el grupo de automorfismos de un functor.

2. Álgebras separables sobre un cuerpo.

Con el objetivo que este trabajo sea autocontenido, en este capítulo se presentarán las demostraciones clásicas de algunos teoremas de la teoría de Galois clásica que son necesarias para enunciar el teorema de clasificación. De esta manera si el lector está familiarizado con la teoria de Galois sobre cuerpos si quiere puede omitirlo.

Todas las álgebras consideradas en este trabajo serán unitarias y los homomorfismos entre álgebras serán también unitarios (la imagen de la identidad multiplicativa es la identidad multiplicativa).

2.1. Elementos algebraicos

Considere un cuerpo K y L una extensión de K, ádemas sea $\alpha \in L$

Proposición 1. *Las siguientes condiciones son equivalentes :*

i. La sub-álgebra $K[\alpha]$ de L generada por α es finita sobre K.

ii. Existe un polinomio $p(x)$ no nulo en $K[x]$ tal que $p(\alpha) = 0$.

iii. las potencias de α son linealmente dependientes.

Demostración.

ii. $\implies$ iii. Es claro que si las potencias $1, \alpha, \alpha^2, ...$ fueran linealmente independientes no podría existir un polinomio $p(x)$ tal que $p(\alpha) = 0$.

i. $\implies$ iii. Se tiene que $1, \alpha, \alpha^2 ...$ generan $K[\alpha]$ como K-espacio vectorial, si este conjunto fuese linealmente independiente, $K[\alpha]$ no podría ser un K-esapcio vectorial de dimensión finita.

ii. $\implies$ i. Se sigue del homomofismo de $K[x]$ en A dado por evaluar en α.

Definición 1. *Si α satisface alguna de las anteriores condiciones, se dice que α es algebráico sobre K.*

Definición 2. *Si todos los elementos de L son álgebraicos sobre K, se dice que L es una extensión algebraica de K.*

□

Proposición 2 (Teorema chino del residuo.)**.** *Sea A un anillo , $(B_i)_{i\in I}$ una familia finita de anillos, tales que para todo $i \in I$ sea $\varphi_i : A \to B_i$ un homomorfismo dado. Si todas las aplicaciones φ_i son sobreyectivas y para todo par i, j tal que $i \neq j$ se tiene que $ker\varphi_i + ker\varphi_j = A$, entonces la aplicación $\Phi : A \to \prod_{i\in I} B_i$, definida por $\Phi(x) = (\varphi_i(x))_{i\in I}$ es sobreyectiva.*

Proposición 3. *Sea A una K-álgebra finita:*

i. El conjunto de ideales maximales de A es finito.

ii. La aplicación $\Phi : A \to \prod_{m\in Max(A)} A/m$ es sobreyectiva y su núcleo está compuesto por los elemento nilpotentes de A.

Demostración.

i. Sea $X \subset Max(A)$ finito. Por el teorema chino del residuo se tiene que $\Phi : A \to \prod_{m\in X} A/m$ es sobreyectiva, por lo tanto $\text{Card}(X) \leq \dim_K(A)$. Como X es arbitrario, implica que $\text{Card}(Max(A)) \leq \dim_K A$, de no ser así, existiría X que contradiría la primera oración.

ii. Como punto de partida se ha de probar que si A es un dominio, entonces, es un cuerpo. Es decir dado un $a \in A$, multiplicar por a es una transformacion lineal inyectiva de A en A por lo tanto, tambien ha de ser sobreyectiva. Se deduce entonces que A es un cuerpo. Con base a lo anterior, se puede asegurar que todo ideal primo de A es maximal (considere el cociente) y se sigue facilmente el resultado, pues el núcleo de Φ es la intersección de todos los maximales.

□

Proposición 4. *Sea L un extensión algebraica de K, todo K-endomorfismo de L es un automorfismo.*

Demostración. Sea $\phi : L \to L$ un endomorfismo. Como L es un cuerpo se tiene que ϕ es inyectivo. Para todo $p \in L[x]$, sea X_p el conjunto de raices de p en L, por ser un K-endomorfismo, se tiene que si $\alpha \in X_p$ entonces $0 = \phi(p(\alpha)) = p(\phi(\alpha))$. Como X_p es finito y ϕ es inyectiva, entonces en X_p ha de ser sobreyectiva. Sin embargo, como L es una extensión algebraica, se tiene que todo $\alpha \in L$ pertenece a algún X_p. □

Proposición 5. *Sea A una extensión algebraica de K, B una subextensión de A en Ω una clausura algebraica de K, todo homorfismo de B en Ω se extiende a un homomorfismo de A en Ω.*

Demostración. Sea $\mathcal{E}$ el conjunto de pares (C, h) donde C es sub-álgebra de A. Se define un orden en $\mathcal{E}$ dado por $(C, h) \leq (C', \hat{h})$ si $C \subset C'$ y $\hat{h}|_C = h$. $\mathcal{E}$ no es vacío pues $(B, f) \in \mathcal{E}$. Dada una cadena (C_i, h_i) se tiene $\bigcup C_i$ junto con $h(\alpha) = h_i(\alpha)$, donde $\alpha \in C_i$, es cota. Por el lema de Zorn, $\mathcal{E}$ tiene elementos maximales. Sea $(\overline{C}, \overline{h})$ un elemento maximal de $\mathcal{E}$, se tiene que $\overline{C} = A$. Suponga por contradicción, que no es asi y sea entonces $\alpha \in A \setminus \overline{C}$ y $p(x) = a_n x^n + ... + a_1 x + a_0$ su polinomio minimal. Se sigue que $\overline{h}(a_n)x^n + .. + \overline{h}(a_1)x + \overline{h}(a_0) \in \Omega[x]$, sea $\zeta \in \Omega$ una raíz de $\overline{h}(a_n)x^n + .. + \overline{h}(a_1)x + \overline{h}(a_0)$. Se puede definir la aplicación $\rho : \overline{C}[\alpha] \to \Omega$ definido por $\rho(\alpha) = \zeta$, ρ extiende a H, contradiciendo la maximalidad de $(\overline{C}, \overline{h})$. □

Proposición 6 (Corolario)**.** *Sea A una extensión algebraica de K, entonces existe una inmersión de A en Ω.*

Demostración. Extienda $\iota : K \to \Omega$ a A. □

Proposición 7 (Corolario)**.** *Sea Ω una clausura algebraica de K, A y B dos subextensiones de Ω. Todo homomorfismo de A en B se puede extender a un automorfismo de Ω, en partícular, todo automorfismo de A se prolonga a un automorfismo de Ω.*

Proposición 8 (Corolario)**.** *Todo par de clausuras algebraicas de K son isomorfas.*

Demostración. Gracias a la proposición 6 y 7 existe una aplicación $f : \Omega \to \Omega'$ y una aplicación $g : \Omega' \to \Omega$. Pero por la proposición 4 $f \circ g$ y $g \circ f$ son automorfismos, por lo tanto, f y g son isomorfismos. □

Proposición 9 (Corolario)**.** *Sea Ω una clausura algebráica de K y sean α y β en Ω , las siguientes afirmaciones son equivalentes:*

i. α y β tienen el mismo polinomio minimal $p(x)$.

ii. existe un automorfismo f de Ω tal que $f(\alpha) = \beta$.

Demostración.

i. $\implies$ ii. Las extensión $K[\alpha]$ y $K[\beta]$ de K son isomorfas a $K[x]/p(x)$, así $\alpha \longmapsto \beta$ es un isomorfismo entre $K[\alpha]$ y $K[\beta]$. De esta manera, se puede prolongar a un automorfismo de Ω gracias a la proposición anterior.

ii. $\implies$ i. Suponga que se tiene f automorfismo de Ω, tal que $f(\alpha) = \beta$, y suponga $p(x) \in K[x]$ el polinomio minimal de α. se tiene que:

$$0 = f(0) = f(p(\alpha)) = p(f(\alpha)) = p(\beta)$$

y se sigue el resultado.

□

La teoría presentada está sujeta al lenguaje algebraico estandar. Esta será el punto de partida para el desarrollo de los siguientes apartados.

3. Álgebras finitas

En esta sección, se desarrollarán herramientas útiles para rehacer las demostraciones dela teoría de Galois. Los elementos aquí presentados, tales como el concepto de álgebra diagonal, necesario para la definición de álgebra etal, son de vital importancia ya que componen el lenguaje usado en las demostraciones de lo que resta del trabajo.

3.1. Álgebras diagonales.

Sea A una K-álgebra y X =Hom(A, K) el conjunto de homomorfismos de K-álgebras de A en K. Para todo elemento $a \in A$, se define la aplicación $ev_a : \mathrm{Hom}_K(A, K) \to K$ dada por $\varphi \longmapsto \varphi(a)$. Naturalmente, se obtiene una aplicación de A en K^X dado, por $a \longmapsto ev_a$ Esta aplicación es conocida como la aplicación de Gelfand [1].

Lema 1. *La aplicación de Gelfand, dada por $a \longmapsto ev_a$, es un homomorfismo de álgebras.*

Demostración. Se sigue de manera directa de las definiciones. □

Lema 2. *Si A es una K-álgebra finita, entonces la transformación de Gelfand es sobreyectiva, en partícular Card(Hom$_K(A, K)) \leq deg_K A$.*

Demostración. Si A es una K-álgebra finita entonces el conjunto $\mathrm{Hom}_K(A, K)$ es un conjunto finito. Para ello, se inyectará dicho conjunto en el conjunto de ideales maximales de A, que gracias a la proposición 3 es un conjunto finito. Sea :

$$\begin{aligned} \rho : \mathrm{Hom}_K(A, K) &\to Max(A) \\ \phi &\to ker(\phi) \end{aligned}$$

ρ está bien definida pues ϕ es sobreyectiva, ya que es K-lineal y la imagen del 1 en A el 1 en K. Por ende su núcleo es un ideal maximal. Para cualquier tal homomorfismo $\phi : A \longrightarrow K$, se tiene $A \cong \ker\phi \oplus K1_A$ como espacio vectorial. Como, $\ker\phi = \ker\varphi$ implica $\phi = \varphi$, entonces la aplicación ρ es inyectiva. El lema chino muestra, si A es una K-álgebra finita, que ese conjunto es finito (la parte ii. de la proposición 3), de cardinal menor o igual a la dimensión de A como K-espacio vectorial.

Se tiene que $\mathrm{Hom}_K(A, K)$ es un conjunto finito es decir $\{f_1, f_2, .., f_n\} = \mathrm{Hom}_K(A, K)$, así, si $f_i \in \mathrm{Hom}_K(A, K)$ defina:

$$F : A \to K^n$$
$$F(a) = (f_1(a), ..., f_n(a))$$

Sean $f \neq g$, se tiene que $ker(f) + ker(g) = 1$, pues por ser estas últimas sobreyectivas y su imagen un cuerpo su núcleo ha de ser un ideal maximal (además como parte de la demostración del lema 2 se deduce que $f \neq g$ implica $ker(f) \neq ker(g)$). De esta manera las hipótesis del teorema chino se cumplen y, por lo tanto, F es sobreyectiva. Esto implica que existen a_i tal que $F(a_i) = e_1 = (0, .., 1_i, ..., 0)$. Así pues por ser la transformación de Gelfand un homomorfismo de álgebras(lema 1), para cualquier elemento $\varphi \in K^{Hom_K(A,K)}$ existe un elemento $a \in A$ tal que Gelfand de a es precisamente φ. □

Como se demostró se puede obtiene una caracterización de la dimensión finita de la K-álgebra A en términos de la transformación de Gelfand. Para dar la definición de álgebra diagonal es necesario establecer más enunciados equivalentes:

Proposición 10. *Sea A una K-álgebra finita y sea d su dimensión sobre K y $X = Hom_K(A, K)$, las siguientes condiciones son equivalentes:*

i. A es isomorfo a un álgebra de funciones sobre un conjunto finito.

ii. La transformación de Gelfand es un isomorfismo de K-álgebras.

iii. Para todo $a \in A$, $a \neq 0$, existe $f \in X$, tal que $f(a) \neq 0$.

iv. La cardinalidad de X es d.

v. La cardinalidad de X es mayor o igual a d

Demostración. ~~i.~~ ⟹ iv. La aplicación de Gelfand es un homomorfismo de K-álgebras, en partícular es una transformación K-lineal. Por lo tanto, si la transformación de Gelfand es un ismorfismo, las dimensiones de A y de K^X han de coincidir y, si X es finito entonces $dim_K(K^X) = |X|$, se sigue el resultado.

ii. $\implies$ i. K^X es precisamente una K-álgebra de funciones sobre un conjunto finito.

i. $\implies$ iii. Sea Y un conjunto finito. Como $a \neq 0$, donde $a \in K^Y$. Como a no es el vector nulo, entonces existe $y \in Y$ tal que $a_y = a(y) \neq 0$. Sea $f \in \mathrm{Hom}_K(A, K)$, dada por $f(x) = x_y$, es decir la y-ésima proyección. Por construcción se tiene que $f(a) = a(y) \neq 0$.

iii. $\implies$ v. Afirmar que la transformación de Gelfand es inyectiva, gracias al lema 1 , es lo mismo que verificar que su núcleo es trivial. Es decir, que para todo elemento no trivial $a \in A$, existe una $f \in \mathrm{Hom}_K(A, K)$ tal que $f \neq 0$, que cumple $f(a) \neq 0$. Así iii. implica que Gelfand es una inyección entre A y K^X. Por ende $|X| \leq d$ y junto con el lema 2 se tiene el resultado buscado .

v. $\implies$ ii. Por hipótesis $|X| \geq d$. Por el lema 2 $d \leq |X|$. Por tanto $|X| = d$. Ccomo Gelfand es una aplicación lineal sobreyectiva entre espacios vectoriales de la misma dimensión, entonces es un isomorfismo.

iv. $\implies$ v. es evidente.

□

Definición 3. *Sea A una K-álgebra, se dice que A es diagonal sobre K si existe un $n \geq 1$ tal que $A \cong K^n$ como K-álgebra.*

De lo anterior, se deduce que una K-álgebra diagonal es necesariamente finita sobre K. Adicionalmente si alguna de las condiciones equivalentes de la proposición 10 se cumple, A es un álgebra diagonal.

Proposición 11. *Sea A una K-álgebra, A es diagonal sobre K si y solamente si A es finita sobre K y la aplicación de Gelfand es inyectiva. En tal caso, dicha aplicación es un isomorfismo.*

Demostración. Se sigue directamente de las equivalencias probadas anteriormente. □

3.2. Algebras etales

Definición 4. *Sea A una K-álgebra finita, y sea L una extensión de K, se dice que L diagonaliza a A si $L \otimes_K A$ es un L-álgebra diagonal.*

Esta definición es técnica, su importancia radica en que en ella está contenida la definición de álgebra etal. Para hacer un vínculo entre esta definición y los teoremas de la subsección anterior es necesario desarrollar algunas caracterizaciones que se usarán en las demostraciones venideras.

Lema 3. *Existe una biyección entre $Hom_K(A, L)$ y $Hom_L(A \otimes_K L, L)$*

Demostración. Primero se inyectará $\mathrm{Hom}_K(A, L)$ en $\mathrm{Hom}_K(A \otimes_K L, L)$. Para ello, para todo $\varphi \in \mathrm{Hom}_K(A, L)$ se definirá una extensión $\hat{\varphi}$ dada por $\hat{\varphi} : l \otimes a \longmapsto lf(a)$. Por ser una multiplicacion es bilineal sobre $L \times A$ y usando la propiedad universal del producto tensorial es claro que $\hat{\varphi}$ es la extensión de dicha multiplicación y, por lo tanto está bien definida.

Dicha extensión es, en efecto, L-lineal:

$$\hat{\varphi}(l_2(l_1 \otimes a_1)) = l_2 l_1 \otimes a.$$

Se define la función f entre $\mathrm{Hom}_K(A, L)$ y $\mathrm{Hom}_L(A \otimes_K L, L)$ como $\varphi \longmapsto \hat{\varphi}$. f es inyectiva ya que si $\varphi \neq \varphi'$ por definición de f , $\hat{\varphi} \neq \hat{\varphi'}$. Esta inyección es sobreyectiva, para todo $\varphi \in \mathrm{Hom}_L(A \otimes_K L, L)$ se tiene que por L-linealidad para todo tensor básico, $\hat{\varphi}(l \otimes a) = l\hat{\varphi}(1 \otimes a)$, así $\hat{\varphi}$ está totalmente determinado por la inclusión de A en $L \otimes_K A$.

□

La siguiente es una caracterización que servirá como heramienta para simplificar algunas pruebas que se realizarán más adelante.

Proposición 12. *Para que L diagonalize a A es necesario y suficiente que $|Hom_K(A, L)| = deg_K A$*

Demostración. Lo anterior se tiene ya que $L \otimes_K A$ es L diagonal si y solo si $deg_L(L \otimes_K A) = |\mathrm{Hom}_L(L \otimes_K A, L)|$. No obstante $deg_L(L \otimes_K A) = deg_K(A)$, Pues la colección $\{1 \otimes v_i\}$, donde v_i son base de A como K espacio vectorial, es base de $L \otimes_K A$ como L espacio vectorial. Conversamente por el lema anterior (3) card $\mathrm{Hom}_K(A, L)$ =card $\mathrm{Hom}_L(L \otimes_K A, L) = deg_K(A)$.

□

El siguiente lema puede ser considerado el más importante del capítulo, porque si bien es técnico, es el puente entre el concepto de separabilidad y ser diagonal.

Lema 4. *Sea $p \in K[x]$ un polinomio de grado d y sea L una extensión de K. Para que L diagonalice $K[x]/(p)$, es suficiente y necesario que tenga d raices distintas en L.*

Demostración. Primero se probará $L \otimes_K (K[x]/(p)) \cong L[x]/(p)$:

Para ello se define:

$$f : K[x]/pK[x] \otimes L \to L[x]/p(L[X])$$
$$X^n mod_{K[x]} p \otimes \lambda \longmapsto \lambda x^n mod_{L[x]} p$$

Esta aplicación está bien definida en $K[x]/pK[x] \times L$, pues si $q + pK[x] = m + pK[x]$, por la unicidad del algoritmo de la división euclidiana,$\lambda q = \lambda B_1 P + \lambda r$,

$\lambda m = \lambda B_2 p + \lambda r$. Al factorizar el λ asegura que ambos comparten el mismo residuo, pues es un polinomio en $K[x]$ y el cociente y el residuo obtenidos por el algoritmo de la división han de ser únicos. Es posible concluir la buena definición sobre las clases en $K[x]/pK[x] \otimes L$ y entonces por la propiedad universal del producto tensorial el homomorfismo f está entonces bien definido.

Ahora se define:

$$f^{-1} : L[x]/p(L[X]) \to: K[x]/pK[x] \otimes L$$
$$x^n mod_{L[x]} p \longmapsto X^n mod_{K[x]} p \otimes 1$$

Esta aplicación está bien definida por la misma razón que f, pues los x^n son polinomios en $K[x]$ por la unicidad del algortimo de la división cualquier representante de está clase tendrá residuo en $K[x]$. Copiando el argumento aplicado a f se garantiza su buena definición.

Es claro que ambas aplicaciones son inversas una de la otra. Los elementos del dominio de f^{-1} son los generadores de las álgebras $K[x]/pK[x] \otimes L$ y $L[x]/pL[X]$, así como $f \circ f^{-1}$ y $f^{-1} \circ f$ son la identidad en los generadores han de ser al identidad sobre todo el producto tensorial y por lo tanto se tiene el isomorfismo querido.

Una vez probado el isomorfismoa nterior se procederá a realizar la prueba del lema 4. Cualquier homorfismo de álgebras unitarias φ de $L[x]/(p)$ a L estádeterminado por la imagen de $[x] := x + (p)$. Como, $x + (p) \in L[x]/(p)$ es raíz de $p(x)$, la imagen de $\varphi(x + (p))$ ha de ser raíz de $p(x)$. Así mismo, se puede ver que cada raíz de p en L determina un homomorfismo de $L[x]/(p)$ a L, dado por $x + (p) \mapsto \alpha$, donde α es raíz de p. Así $L[x]/(p)$ es diagonal si y solamente si $|Hom_L(L[x]/(p), L)| = d$. Esto último es si y solamente si p tiene d raíces en L. De esta manera, por el isomorfismo L diagonaliza a $K[x]/(p)$ si y solamente si p tiene d raíces en L.

□

A continuación se demostrarán tres equivalencias que permitirán enunciar la definición de álgebra etal.

Proposición 13. *Sea $\overline{K}$ una clausura algebráica de K y sea A una K-álgebra finita. Las siguientes condiciones son equivalentes:*

i. Existe una extensión L de K que diagonaliza a A.

ii. Existe una extensión finita L de K que diagonaliza A.

iii. $\overline{K}$ diagonaliza A.

Demostración.

ii. $\implies$ *iii.* , L se sumerge en $\overline{K}$, pues todas las clausuras algebráicas son isomofas (esto fué probado en la proposición 8), por lo tanto $L \otimes_L \overline{K} \cong \overline{K}$. Por lo

anterior $A \otimes_K \overline{K} \cong (A \otimes_K L) \otimes_L \overline{K}$, como $A \otimes_K L \cong L \oplus \cdots \oplus L$ por hipótesis, se tiene:

$$\begin{aligned} A \otimes_K \overline{K} &\cong (A \otimes_K L) \otimes_L \overline{K} \\ &\cong (\bigoplus_{1 \leq i \leq n} L_i) \otimes_L \overline{K} \\ &\cong \bigoplus_{1 \leq i \leq n} (\overline{K} \otimes_L L_i) \\ &\cong \overline{K}^n \end{aligned}$$

iii. $\implies$ *.i* Es evidente.

i. $\implies$ *ii.* Sea d el grado de A sobre K. Por la caracterización dada en la proposición 12, $|Hom_K(A, L)| = d$. Sean $\zeta_1, ..., \zeta_d$ los d elementos de $\mathrm{Hom}_K(A, L)$dichos homomorfismos. Defino L' como la sub-álgebra de L generada por $\zeta_1(A), ..., \zeta_d(A)$. Como cada una de ellas es finitamente generada como K-espacio vectorial, puesto que A mismo lo es, se tiene que L' es finita.
Cada uno de los ζ_i es un homomorfismo de K-álgebras de L', así $d \leq |\mathrm{Hom}_K(A, L')|$. $L' \subset L$, por lo tanto $\mathrm{Hom}_K(A, L') \subset \mathrm{Hom}_K(A, L)$, asi $|\mathrm{Hom}_K(A, L')| \leq d$ y por la proposición 12 se obtiene el resultado deseado.

□

Definición 5. *Si A cumple alguna de las anteriores equivalencias , se dice que A es una K-álgebra etal.*

Proposición 14. *Sea $p(x) \in K[x]$, las siguientes condiciones son equivalentes:*

i El álgebra $K[x]/(p(x))$ es etal.

ii Las raíces de $p(x)$ en Ω son distintas.

Demostración. Gracias a la definición de K-álgebra etal $p(x)$ es separable si y solamente si Ω diagonaliza a $K[x]/(p(x))$ y esto es si y solo si $p(x)$ es separable gracias al lema 4.

□

En este punto es indispensable hacer énfasis en que toda K-álgebra etal es finita:

Esto se debe a que si A es una K-álgebra etal, por la equivalencia ii de la proposoición 13, L puede ser escogido como una extención finita de K. Así, $L \otimes_K A$ es una K-álgebra finitamente generada, y ya que A es isomorfa a una subalgebra de $A \otimes_K L$, A ha de ser también finitamente generada.

Para finalizar el capítulo se demostrarán algunas propieades de las álgebras etales.

Lema 5. *Cualquier sub-álgebra de un álgebra etal es etal.*

La condicion iii. de la proposición 10 se cumple para cualquier sub-álgebra de un álgebra diagonal, pues todo $\zeta \in \mathrm{Hom}(A, K)$ se puede restringir a una subalgebra B de A. De esta manera, toda sub-álgebra de una álgebra diagonal es diagonal. Por lo tanto, si $L \otimes_K A$ es etal, como $L \otimes_K B$ es sub-álgebra, está también es diagonal y, por lo tanto, B es etal.

Lema 6. *Sea A un álgebra etal y C y B dos sub-álgebras etales de A, entonces la sub-álgebra de A generada por B yC es etal.*

Demostración. Por la defínción de la multiplicación en el producto tensorial de álgebras para $\sum_i b_i c_i \in BC$, se tiene que $l \otimes \sum_i b_i c_i = \sum_i l \otimes b_i c_i = \sum_i (l \otimes b_i)(1 \otimes c_i)$. Por lo anterior, se puede concluir que la L-álgebra $L \otimes_K BC$ es generada por los elementos $1 \otimes b$ y los elementos $1 \otimes c$ con $b \in B$ y $c \in C$. De esta manera, si L diagonaliza a B y C, se tiene que $L \otimes_K BC$ es la L-álgebra generada por $L \otimes_K B \cong L^d$ y $L \otimes_K C \cong L^m$. Por lo tanto, y se deduce que L diagolaiza a BC y, se concluye que esta última es etal.

□

La siguiente proposición como resultado de toda la teoría desarrollada ,muestra ya de manera explicita la relación entre ser separable y ser etal.

Proposición 15. *Sea A una K-álgebra. Para que A sea etal, es suficiente y necesario que A sea finita y separable.*

Demostración. Asúmase primero A etal, de forma tal que es una K-álgebra finita y por lo tanto $A \cong K[\alpha_1, ..., \alpha_n]$. Si $\alpha \in A$, $K[\alpha]$ es una sub-álgebra de A, en consecuencia es etal, pero por el lema 5 eso hace de p el polinomio mínimal de α separable. Para la otra implicación se tiene que todos los elementos de A son separables y, además, $A \cong k[\alpha_1, .., \alpha_n]$. Esta última es la K-álgebra generada por $K[\alpha_i]$, todas álgebras etales por el lema 4. Por lo tanto por el lema 6 A mismo es etal. □

En la siguiente proposición se muestra la existencia de un objeto intrínseco de la geometria algebraica, el anillo coordenado de una variedad algebraica. Esta proposición sirve como ejemplo de los vinculos existentes entre objetos geometricos y algebraicos.

Proposición 16. *Sea A una K-álgebra finita, si K es perfecto, A es etal si y solamente si A es reducida.*

Demostración. Para una dirección,se tiene que $A \hookrightarrow A \otimes_K K \hookrightarrow A \otimes_K L$. Sea L es una extensión finita de K que diagonaliza a A. Ya que $L \otimes_K A$ es isomorfa a L^d, A no puede poseer elementos nilpotentes, pues si L^d los tuviera L mismo tambien los tendria. Conversamente, si A es reducido y finito, A es isomorfo a un producto de extensiones finitas de K(por el teorema chino del residuo 3) y separables pues K es perfecto por hipótesis, asi como producto de álgebras etales es etal, se sigue el resultado. □

4. Teoria de Galois de álgebras etales

En este capítulo se enunciará el teorema de clasificación de Galois. Para ello se usarán todas las herramientas desarrolladas en los capítulos anteriores.

Definición 6. *Sea L una extensión finita de K, se dice que L es galoisiana si L se diagonliza ella misma.*

Definición 7. *Si L es una extensión Galoisiana de K, el grupo $G = Aut_K L$ es llamado el grupo de Galois de L sobre K.*

Sea L una extensión finita de K y $\overline{K}$ una clausura algebraica de K, sea $d = deg_K L$ y $Fix_G L = \{x \in L | (\forall g \in G) g(x) = x\}$.

Proposición 17. *Las siguientes condiciones son equivalentes:*

i. L es galoisiana.

ii. Card $G = d$.

ii'. Card $G \geq d$.

iii. L es etal y todo K-homomorfismo de L a $\overline{K}$ tiene su imagen en L mismo. es subconjunto L.

iv. $Fix_G L = K$

v. para todo $x \in L$ las raices en $\overline{K}$ del polinomio minimal de x son simples y pertenecen a L.

Demostración.

i $\implies$ ii Gracias al lema 4 se tiene que $d = deg_K L =$ card $\mathrm{Hom}_K(L \otimes_K L, L)$ =card $\mathrm{Hom}_K(L, L)$. De esta manera si L es galoisina implica que en particular que por v de la proposición 10 que card $(\mathrm{Hom}_K(L, L)) \geq d$. Note ademas que todo $\varphi \in \mathrm{Hom}_K(L, L)$ es un particular un homomorfismo de cuerpos que como es unitario no es el homomorfismo cero y por lo tanto es inyectivo, asi card $(G) =$ card($\mathrm{Hom}_K(L, L)) \geq d$.

ii $\implies$ i Ahora note que card $G \geq d$ implica por 10 y el hecho que card $G =$ $\mathrm{Hom}_K(L, L)$, que $L \otimes_K L$ es diagonal y por lo tanto L es galoisiana.

i $\implies$ iii L es etal, entonces card $(\mathrm{Hom}_K(L, \overline{K})) = d$. Lo anterior se sigue de la parte iii. de la proposición 10 y de la caracterización dada por la proposición 12 como $G = \mathrm{Hom}_K(L, L) \subset \mathrm{Hom}_K(L, \overline{K})$. L es galoisinana si y solamente si card $G = d$, se tiene entonces que card $G =$card $\mathrm{Hom}_K(L, \overline{K})$ y por lo tanto estos dos conjuntos han de ser iguales , se concluye de esta manera iii.

iii $\implies$ ii L es etal entonces Card $(\mathrm{Hom}_K(L, \overline{K})) = d$. Por la proposición 7 se sabe que cualquier aplicación en este conjunto se puede levantar a una en $\mathrm{Hom}_K(\overline{K}, \overline{K}) = \mathrm{Aut}_K(\overline{K})$ y por lo tanto $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Aut}_K L$.

iii $\implies$ iv Es claro que por definición de $\mathrm{Hom}_K(L, L) = G$ todos los puntos en K están fijos por G. Ahora suponga que no son todos, es decir tome $x \in Fix_G(L/K)$ y sea p_x su polinomio minimal. Como $x \notin K$ y L es etal, por el lema 4 p_x es por lo menos de grado 2 y separable. De esta manera sea y otra raíz de p_x se define $\varphi K[x] \to \overline{K}$ pero de nuevo podemos extender φ a un automorfismo de $\overline{K}$ que al restringir a L produce un autmorfismo de este último que no fija a x, una clara contradicción.

iv $\implies$ v Sea $\alpha \in L$ y sean α_i todos los cojugados de α en L. defino $p(x) = \prod_i (x - \alpha_i)$, sea $g \in G$, obtengo por ser este último un homorfismo de álgebras en particular respeta polinomios y por lo tanto $g(p(x)) = \prod_i (x - g(\alpha_i))$. Esto último es igual a $\prod_i (x - \alpha_i)$ por la definición de conjugado. Pero lo anterior implica que los coeficientes de $p(x)$ son invariantes bajo G es decir $p(x) \in K[x]$ por hipótesis. Por la definición de polinomio mínimal este último divide a $p(x)$: sea m_x el ploinomio minimal de x. α es raíz de $p(x)$ y ademas toda raíz de $p(x)$ es raíz de m_x asi el grado del minimal ha de ser igual al de $p(x)$ (por minimalidad del grado de m_x) y por ser ambos mónicos entonces han de ser iguales.

v $\implies$ iii La porpocisión 14 implica que L es etal. Para todo φ en $\mathrm{Hom}_K(L, \overline{K})$ y todo $x \in L$, $\varphi(x)$ ha de ser raíz del polinomio minimal de x y por hipótesis $\varphi(x) \in L$, asi se tiene iii.

□

La teoria desarrollada hasta este punto generaliza la teoría de Galois clásica. La nueva formulación es más flexible y permite realizar teoremas de clasificación más generales que la correspondencia de Galois. Gracias a la noción de álgebra diagonal y a la de acción de grupo se pueden enunciar teoremas de clasificación para álgebras separables distintas a un cuerpo.

Para poder empezar a centar las bases de para poder enunicar otros teoremas de clasificación usando lenguaje categórico el primer paso es definir una acción del grupo $\mathrm{Aut}_K(L)$ en los embebimientos de una extensión L en una clausura algebráica. Si bien esto también es abordado por la teoria de Galois clásica, el lector encontrará un drástico cambio de lenguage.

Sea L una extensión Galosiana de K y A una K-álgebra finita diagonalizada por L, Sea $G = Aut_K(L)$ y $X = \mathrm{Hom}_K(A, L)$. Gracias a la caracterización dada por la proposición 12 entonces $X \cong \mathrm{Hom}_K(L \otimes_K A, L)$. Por otra parte, para todo $g \in G$ y y $\zeta \in X$ se tiene que $g \circ \zeta \in \mathrm{Hom}_K(A, L)$, asi esta operacion define una acción del grupo G sobre el conjunto X.

Para hacer más comoda la notación, se llamará $\hat{a}$ a la imagen de un elemento $a \in A$ en una K-álgebra A arbitraria bajo la transformación de Gelfand y, γ a la aplicación de Gelfand. Para todo $t = \lambda \otimes a$ en $L \otimes_K A$, se tiene que $\lambda \hat{\otimes} a(\zeta) = \zeta(\lambda \otimes a) = \lambda\zeta(a)$. Esta última igualdad está dada por ser $\lambda \hat{\otimes} a \in \mathrm{Hom}_K(L \otimes_k A, L)$ asi $\zeta(\lambda \otimes a) = \lambda\zeta(1 \otimes a)$ ahora gracias a 3 tenemos que gracias a la identificación de A con su inclusión en $L \otimes A$, entonces $\lambda(1 \otimes a) = \lambda\zeta(a)$. Gracias a que G actua sobre L, se puede definir una acción de G sobre $L \otimes_K A$ dada por $g_*(\lambda \otimes a) = g_*(\lambda) \otimes a$. Asi puedo definir una acciø'n de G sobre L^X denotada $(g, f) \longmapsto g \perp f$, como aquella que hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} L \otimes_K A & \xrightarrow{\gamma} & L^X \\ {\scriptstyle g_* = g \otimes 1_A}\downarrow & & \downarrow{\scriptstyle f \to g \perp f} \\ L \otimes_K A & \xrightarrow{\gamma} & L^X \end{array}$$

Conmuta.

Note que el diagrama si conmuta pues por hipótesis la transformación de Gelfand de $L \otimes_K A$ a L^X es un isomorfismo 10 pues A es diagonalizada por L.

Proposición 18. *La acción $\perp$: $G \times L^X \to L^X$ está dada por la formula:*

$$(g \perp f)(\zeta) = g(f(g^{-1} \circ \zeta))$$

Demostración. Sea $\zeta \in X$ y $g \in G$. Gracias a la conmutatividad del diagrama la aplicación $\varphi : f \to (g \perp f)(\zeta)$ de L^X sobre L es un homomorfismo de K-álgebras. Su núcleo es un ideal máximal de L^X ,por lo tanto de la forma $ker_{ev(\eta)}$, con $\eta \in X$. En el anterior diagrama conmutativo g_* es g-lineal, como γ es L-lineal, $f \to g \perp f$ es g-lineal. Lo anterior en otras palabras quiere decir que para todo $l \in L$ y $f \in L^X$, $\varphi(lf) = g(l)\varphi(f)$.

Por otra parte,toda $f \in L^X$ se escribe de la forma $f(\eta) + f'$ con $f' \in ker_{ev(\eta)}$. De esta manera , $\varphi(f) = g(f(\eta))$.

Falta determinar η para acabar la demostración.

Sea $l \in L$ y $a \in A$, por definición de $\perp$:

$$(g \perp l \hat{\otimes} a)(\zeta) = g(l \hat{\otimes} a)(\zeta) = g(l)\zeta(a)$$

Por otra parte:

$$(g \perp l \hat{\otimes} a)(\zeta) = \varphi(l \hat{\otimes} a) = g(l \hat{\otimes} a)(\eta) = g(l\eta(a)) = g(l)g(\eta(a))$$

En particular si $l = 1$, $\zeta(a) = g(\eta(a))$, asi $\eta = g^{-1} \circ \zeta$ y por lo tanto $\varphi(f) = g(f(\eta)) = g(f(g^{-1} \circ \zeta)$ □

Sea L una extensión galoisiana de K y G su grupo de Galois. Defino $G-con$ la categoria de conjuntos finitos donde G actua, los morfismos en está categoria se denotaran $\mathrm{Hom}_G(X, Y)$ son aquellas funciones φ tales que para todo $x \in X$ y todo $g \in G$ $\varphi(gx) = g\varphi(x)$.

Sea D la categoria de K-álgebras finitas que son diagonalizadas por L.

Defino el functor $\mathcal{G} : D \to G$-con como $\mathcal{G}(A) = \mathrm{Hom}_K(A, L)$ y para todo $f : A \to B$, defino $\mathcal{G}(f) : \mathcal{G}(B) \to \mathcal{G}(A)$, como $f^* = \mathcal{G}(f)(\eta) = \eta \circ f$

Teorema 1. *El functor $\mathcal{G} : D \to G$-con, es una anti-equivalencia de categorias.*

Demostración. La demostración está dada en los lemas 8 y 9. □

Lema 7. *Para todo objeto $A \in \mathcal{D}$ los elementos fijos de la ación de G sobre $(L \otimes_K A)$ es isomorfo a A.*

Demostración. se tienen que $A \cong K^d$ como espacio vectorial, asi $K^d \cong A \cong 1 \otimes A \subset L \otimes_K A \cong L^d$, asi por se tiene el resultado querido. □

Lema 8. *el functor $\mathcal{G}$ es plenamente fiel.*

demostración. Primero note que para todo objeto $A \in D$, $Fix_G(L \otimes_K A) = A$.

Sea $\phi : \mathcal{G}(B) \to \mathcal{G}(A)$ un morfismo de G-con, puedo asignar a esta aplicación un morfismo de L-
algebras ϕ^* dado por $\phi^*(h) = h \circ \phi$. El homomorfismo ϕ es compatible con la operacion $\perp$, para todo $\zeta \in S(A)$:

$$\begin{aligned}\phi^*(g \perp h)(\zeta) &= (g \perp h)(\phi(\zeta)) = g(h(g^{-1} \circ \phi(\zeta))) \\ &= g(h(\phi(g^{-1^{\iota}} \circ \zeta)) = (g \perp (h \circ \phi))(\zeta) \\ &= (g \perp \phi^*(h))(\zeta)\end{aligned}$$

(recuerde que por hipótesis ϕ conmuta con los elementos de G).

Por definición de D se tiene que las trasnformaciónes de Gelfand:

$\gamma_A : L \otimes_K A \to L^{\mathcal{G}(A)}$, $\gamma_B : L \otimes_K B \to L^{\mathcal{G}(B)}$ son isomorfismos. Por lo tanto existe una aplicación $\phi^{\otimes} : L \otimes_K A \to L \otimes_K B$ tal que el diagrama:

$$\begin{array}{ccc} L \otimes_K A & \xrightarrow{\gamma_A} & L^{\mathcal{G}} \\ {\scriptstyle \phi^{\otimes}}\downarrow & & \downarrow{\scriptstyle \phi^*} \\ L \otimes_K B & \xrightarrow{\gamma_B} & L^{\mathcal{G}} \end{array}$$

Conmuta.

$\phi^{\otimes}$ es compatible con las operaciones de G entonces induce un homomorfismo de K-álgebras $f : A = Fix_G(L \otimes_K A) \to B = Fix_K(L \otimes_K B)$. Lo anterior se debe a que si $gx = x$ entonces bajo cualquier mapa h que respete la acción, se tiene que $h(x) = h(gx) = gh(x)$, es decir una aplicación que conmute con la accı'on de g, implica que induce una aplicación entre los elementos fijos por la misma. De esta manera por el lema anterior obtengo $f^* : \mathcal{G}(B) \to \mathcal{G}(A)$.

Se demostrará ahora que $\forall \eta \in \mathrm{Hom}_K(B, L)$, $\eta \circ f = \phi(\eta)$, es decir que $f^* = \phi$.

Sea $ev_\eta : L^{\mathcal{G}(B)} \to L$, definida por $ev_\eta(h) = h(\eta)$. De esta manera se tiene que por la definición de la transformación de Gelfand, $\eta = ev_\eta \circ \gamma_B \circ \iota_B$, donde $\iota_B : B \to L \otimes_K B$ es la inyección canónica. De esta manera :

$$\begin{aligned} \eta \circ f &= ev_\eta \circ \gamma_B \circ \iota_B \circ f \\ &= ev_\eta \circ \gamma_B \circ \phi^{\otimes} \circ \iota_A \\ &= ev_\eta \circ \phi^* \circ \gamma_A \circ \iota_A \\ &= ev_\eta \circ \gamma_A \circ \iota_A = \phi(\eta) \end{aligned}$$

asi $f^* = \eta$, asi la aplicación que envia $f \longmapsto f^*$ es sobreyectiva.

Solo resta mostrar que si f es de al forma ρ^* donde $\rho : A \to B$, entonces $f = \rho$, esto es equivalente a mostrar que $\rho \longmapsto \rho^*$ es inyectiva. Así, sea $\eta \in \mathcal{G}(B)$:

$$\begin{aligned} ev_\eta \circ \gamma_B \circ \iota_B \circ \rho = \eta \circ \rho = \rho^*(\eta) \\ = ev_{\phi(\eta)} \circ \gamma_A \circ \iota_A \\ = ev_\eta \circ \phi^* \gamma_A \circ \iota_A \\ = ev_\eta \circ \gamma_B \circ \iota_B \circ f \end{aligned}$$

Como $\bigcap_{\eta \in \mathcal{G}(B)} ker(ev_\eta) = 0$ y $\gamma_B \circ \iota_B$ es inyectiva se tiene que $\rho = f$. □

Lema 9. *El functor $\mathcal{G}$ es esencialmente sobreyectivo*

Demostración. Sea H un subgrupo de G y considere el cuerpo $F = Fix_H(L)$, se tiene que:

$$\begin{aligned} res : G &\to \mathrm{Hom}_K(F, L) \\ \sigma &\longmapsto \sigma|_F \end{aligned}$$

es sobre, como consecuencia del teorema de extensión de automorfismos a la clausura algebráica o a cualquier extensión algebráica

Sea entonces f y g tales que $res(f) = res(g)$, esto último es equivalente a que $g = f \circ h$ con $h \in ker(res)$. D esta manera tenemos que $\mathcal{G}(F) = \mathrm{Hom}_K(F, L)$ se identifica con el conjunto G/H.

Por otra parte considere $A, B \in D$, se tiene que $\mathcal{G}(A \times B) = \mathcal{G}(A) \sqcup \mathcal{G}(B)$:

Considere $L \otimes_K A \cong L^X$ y $L \otimes_K B \cong L^Y$ con $X = \mathcal{G}(A)$ y $Y = \mathcal{G}(B)$, entonces :

$$L \otimes_K (A \times B) \cong (L \otimes_K A) \times (L \otimes_k B) = L^{X \sqcup Y}$$

Por lo tanto $\mathcal{G}(A \times B) = X \sqcup Y$.

Con estos resultados ya se puede proceder a construir ,para cada objeto X en $G - con$,un álgerba en la categoria $\mathcal{D}$ cuya imagen bajo el functor $\mathcal{G}$ e isomorfa a X. Todo G-con finito es de la forma $\sqcup_{i \in I} X_i$ donde cada X_i es una orbita. Gracias al teorema orbita-estabilizador se tiene que I es finito y de nuevo por el mismo teorema $X \cong G/H$ donde H es un subgrupo de G, y más aún H es isomorfo al estabilizador de un elemento. Asi por los dos resultados probados anteriormente se tiene primero que $\mathcal{G}(F_i) = \mathrm{Hom}_K(F_i, L) \cong X_i$ y por lo tanto $\mathcal{G}(F_1 \times ... \times F_n) = \mathcal{G}(F_1) \sqcup \cdots \sqcup \mathcal{G}(F_n)$ □

El teorema anterior es un ejemplo de un teorema de clasificación haciendo uso de lenguage categórico. Este sirve como punto de partida para la demostración de otros enunciados de clasificación y, en general, para el desarrollo de la teoría de álgebras etales.

5. Teoria de Galois de álgebras separables

En esta sección se explora la teoria de Galois de extensiones infinita y se extiende la acción usada en el teorema de clasificación al grupo de Galois de una clausura algebraica. Por esto es necesario el uso de herramientas propias del área de la topología, como por ejemplo el concepto de grupo profinito. Resumiendo el objetivo del siguiente capítulo es gracias a estas herramientas, poder ennunciar desafortunadamente sin demostración enunciados similares al teorema 1.

5.1. Extensiones puramente inseparables

Con el ánimo de poder extender este lenguage a extensiones infinitas de un cuerpo K hace falta considerar algunas condiciones de separabilidad por ello ya que toda extensión de un cuerpo de caracterisitica 0 es separable se asumirá por el resto de esta sub-sección que K tiene caracteristica $p > 0$.

Definición 8. *Sea L una extensión de K y $x \in L$. Se dice que x es radical sobre K si existe un entero r tal que $x^{p^r} \in K$. Se dice que L es una extensión puramente inseparable de K si todo elemento de L es radical sobre K.*

Proposición 19. *Sea Ω una clausura algebráica de K y $p(x) \in K[x]$ un polinomio mónico e ireducible. Las siguientes condiciones son equivalentes:*

i. El polinomio $p(x)$ tiene una única raíz (enventualmente multiple) sobre Ω.

ii. Existe $r \in \mathcal{N}$ y $a \in K$ tal que $p(x) = x^{p^r} - a$.

Demostración.

i $\implies$ ii Sea r el mayor número entero tal que $p(x) = q(x^{p^r})$. $q(y) \notin K[y^p]$, pues de lo contrario $p(x) = q(x^{p^{r+1}})$. Por otra parte se tiene que $q(x)$ es irreducible pues $p(x)$ lo es, pero esto implica que $(q(x), q'(X))) = 1$ pues ha de ser un divisor de $q(x)$. No obstante el grado de $q'(x)$ es estrictamente menor al de $q(x)$. Al ser $q(x)$ primo relativo con su derivada es separable, sin embargo, como $p(x)$ solo tiene una raíz por hipótesis, entonces $q(x)$ ha de ser de grado uno y termina la prueba.

ii $\implies$ i Considere el homomorfismo de Frobenius dado por $\alpha \longmapsto \alpha^p$ de Ω en Ω. Por ser K de caracterisitica p, se tiene que $x^{p^r} - a = (x - \sqrt[p^r]{a})^{p^r}$.

□

Proposición 20. *Sea L una extensión puramente inseparable de K y Ω una clausura algebraica de K. Las siguientes condiciones son equivalentes:*

i. L es puramente inseparable.

ii. solo hay un homomorfismo de K-álgebras de L en Ω.

Demostración.

i $\implies$ ii Sea $\alpha \in L$, entonces existe $n \in \mathbb{N}$ y $a \in K$ tales que $\alpha^{p^r} = a$. Gracias a la proposición anterior, se tiene que para todo $\sigma : L \to \Omega$ por ser σ automorfismo la imagen de cualquier raíz de un polinomio p dado ha de ser raíz del mismo polinomio. No obstante α es la única raiz de $x^{p^r} - a$, asi por definición de puramente inseparable ha de ser la identidad en L.

ii $\implies$ i Suponga $\alpha \in L$ un elemento no radical . Entonces por la proposición anterior el polinomio minimal de α admite dos raices distintas. Así, $\alpha \longmapsto \alpha$ y $\alpha \longmapsto \beta$ determinan dos automorfismos distintos de L en Ω(proposición 9).

□

Proposición 21. *Toda extensión algebraica L de K, es una extensión puramente inseparable de L_{sep}.*

Demostración. Sea $\alpha \in L$ y sea $p(x)$ su polinomio minimal. De esta manera escoja r el mayor número natural tal que $p(x) = q(x^{p^r})$. Entonces si $q(x) \notin K(x^p)$ entonces $q(x)$ es irreducible y separable y por lo tanto $\alpha^{p^r} \in L_{sep}$. □

Definición 9. *Sea K un cuerpo y sea Ω una clausura algebráica del mismo, defino $G = Gal(\Omega/K) := Aut_k\Omega$.*

Proposición 22. $G \cong Aut_k(\Omega_{sep})$

Demostración. Se sigue de las porposiciónes 20 y 21, ya que para todo $\sigma \in \text{Gal}(\Omega_{sep}/K)$ se puede extender a $\overline{\sigma} \in \text{Gal}(\Omega/K)$ pero por las propocisiónes 20 y 21, $\overline{\sigma} \in \text{Gal}\ (\Omega/\Omega_{sep})$ es la identidad, asi G esta completamente determinado por $Gal(\Omega_{sep}/K)$. □

Después de la prueba de este teorema debería cobrar sentido para el lector todo este pequeño apartado de extensiones puramente inseparables. Gracias a lo probado se puede reducir la teoría de Galois sobre una clausura algebraica , a la teoría de Galois sobre la calusura separable del cuerpo en cuestión.

El siguiente teorema es el punto de partida para la teoria de Galois infinita. Ádemas proporcionara una estructura topológica que sera usada para un enunciado de correspondencia un poco más general que el probado en la sección 3.

Es de notar antes de continuar que gracias al capítulo 3 más especificamente a la proposición 17 podemos hacer uso de las herramientas de Galois usuales pues son compatibles con el lenguaje que hemos generado.

Proposición 23. *$Gal(\Omega/K) = \varprojlim_L Gal(L/K)$ donde L es uan extensión Galoisiana finita de K.*

Demostración. Defino:

$$\rho : \sigma \longmapsto ((\sigma)|_L)_L$$

primero se probará la inyectividad. Se tiene que si $\sigma \neq \tau$ es porque existe $\alpha \in \Omega_{Sep}$ tal que $\sigma(\alpha) \neq \tau(\alpha)$. De esta manera, como α es algebraico se tiene que si L es el cuerpo de descompocición del polinomio minimal de α, $p_\alpha(x)$, entonces $\sigma|_L \neq \tau|_L$.

Para la sobreyectividad sea $(\sigma_L)_L$ y defina $\sigma : \Omega_{sep} \to \Omega_{sep}$ como $\sigma(\alpha) = \sigma(\alpha)_L$, donde L es una extensión finita de Galois que contiene a $K(\alpha)$.

Es evidente que pro construcción la imagen de σ bajo ρ es la tupla $(\sigma_L)_L$ asi solo resta probar que σ como función es bien definida. Si L y L' no están relacionados no hay un problema de mala definición, asi que sin perdida de generalidad asuma $L \subset L'$. Por ser $(\sigma_L)_L \in \varprojlim_L \text{Gal}(L_/K)$ se tiene que :

$$res_{L'L}\pi_{L'}((\sigma_L)_L) = \pi_L((\sigma_L)_L) = \sigma_L$$

Donde $res_{L'L} : Gal(L'/K) \to Gal(L/K)$ está dado por $\varphi \longmapsto \varphi|_L$. De esta manera σ está bien definido y se tiene la sobreyectividad.

□

5.2. Teoría de Galois de álgebras separbales

Gracias a la proposición 23 se puede otorgarle una topología al grupo $\mathrm{Gal}(\Omega/K)$, pues $\varprojlim_L \mathrm{Gal}(L/K)$ como objeto en la categoría de grupos es un subconjunto del producto de los $\mathrm{Gal}(L/K)$. Esta topología será naturalmente la inducida como subesepacio de dicho producto con la topología producto y cada $\mathrm{Gal}(L/K)$ por ser finito con la topología discreta. Esta topología no solo permitirá añadir estructura a $\mathrm{Gal}(\Omega/K)$ y facilitar a si su estudio sino que permitirá dar una forma de caracterizar ciertos conjunto donde $\mathrm{Gal}(\Omega/K)$ actua.

Sea A una K-álgebra separable. Note que por definicion de $\mathrm{Gal}(\Omega, K)$ y de $\mathrm{Hom}_K(A, \Omega)$, para todo $\phi \in \mathrm{Hom}_K(A, \Omega)$ y para todo $\sigma \in \mathrm{Gal}(\Omega/K)$, se tiene que $\sigma \circ \phi \in \mathrm{Hom}_K(A, \Omega)$.

Proposición 24. *La acción dada por precomposición de $Gal_K(\Omega/K)$ sobre $Hom_K(A, \Omega)$ (este último con la topología discreta) es continua.*

Demostración. Gracias a la porposición 23 por el morfismo dado en dicha demostración es fácil ver que en $\mathrm{Gal}_K(\Omega/K)$ las restricciones a una extensión Galoisina finita coinciden con las proyecciones del producto $\prod_L \mathrm{Gal}(L/K)$. Así como subespacio del producto se tiene que para toda restricción de un elemento de $\mathrm{Gal}_K(\Omega/K)$ a una extensión de Galois L(un elemento de $\mathrm{Gal}_K(L/K)$) es continua. En particular la preimagen de la identidad en $\mathrm{Gal}_K(L/K)$, que es el conjunto $\mathrm{Gal}_K(\Omega/L)$, es un conjunto abierto.

Gracias a lo probado en el apéndice, para probar la continuidad de la acción, basta probar que el estabilizador de un elemento $\varphi \in \mathrm{Hom}_K(A, \Omega)$ es abierto. De esta manera sea $g \in \mathrm{Stab}(\varphi)$. Como A es de dimensión finita sea L una extensión finita de galois de K tal que $\varphi(A) \subset L$. Es claro que la anterior contencia implica que $\mathrm{Gal}_K(\Omega/L) \subset \mathrm{Stab}(\varphi)$, ahora por ser $\mathrm{Gal}_K(\Omega/K)$ un grupo topológico $g\mathrm{Gal}_K(\Omega/L)$ es un abierto contenido en $\mathrm{Stab}(\varphi)$ que contiene a g asi $\mathrm{Stab}(\varphi)$ es abierto . □

La anterior porposición permite construir un functor entre las álgebras separables y los conjuntos donde $\mathrm{Gal}(\Omega/K)$ actua. La continuidad de la acción será todo lo necesario para poder carterizar todos los conjuntos donde $\mathrm{Gal}(\Omega/K)$ actua.

Proposición 25. *Si A es un álgebra etal, entonces $Hom_K(A, \Omega)$ es un conjunto finito.*

Demostración. Gracias a la propocisión 6 se tiene una definición equivalencia a ser etal , donde A es isomorfa a un producto finito de extensiones finitas y separables de K.

De esta manera sea $A = \prod_{1 \leq i \leq n} L_i$. Note primero que cada uno de los conjuntos $\mathrm{Hom}_K(L_i, \Omega)$ es finito. Esto se sigue del hecho que, gracias al teorema del elemento primitivo, $L_i = K(\alpha_i)$. Por lo tanto , todo elemento en L_i es un polinomio en α_i con coeficientes en K. Dado un $\sigma \in \mathrm{Hom}_K(L_i, \Omega)$, $p_{\alpha_i}(\sigma(\alpha_i)) =$

$\sigma(p_{\alpha_i}(\alpha_i)) = 0$, entonces $\sigma(\alpha_i)$ ha de ser una raíz de p_{α_i}. Como el automorfismo σ está completamente determinado por la imagen de α_i y está solo puede ser una raiz de p_{α_i}, se concluye que solo puede haber finitos de ellos. De esta manera la finitud de $\mathrm{Hom}_K(A, \Omega)$ se sigue de la propiedad universal del co-producto pues se tiene que $\mathrm{Hom}_K(A, \omega) \cong \prod Hom(L_i, \Omega)$, y por lo tanto $\mathrm{Hom}_K(A, \Omega)$ es finito. □

Sea $\mathcal{E}$ la categoría de álgebras etales y sea G-con la categoría la cual consta de conjuntos finitos donde $G :=\mathrm{Gal}(\Omega/K)$ actua de manera continua. Al igual que en el teorema 1 las aplicaciones de G-con son aquellas que respetan la acción de G, es decir los morfismos en está categoria se denotaran $\mathrm{Hom}_G(X, Y)$ son aquellas funciones φ tales que para todo $x \in X$ y todo $g \in G$ $\varphi(gx) = g\varphi(x)$.

Gracias a las anteriores 2 proposiciones , se puede definir un functor $\mathcal{F}$ entre la categoria $\mathcal{E}$ y la categoria G-con dado por a todo K-álgebra etal A se le asigna el conjunto $\mathrm{Hom}_K(A, \Omega)$ y atodo morfismo $f \in \mathcal{E}$ se le asigna $f^*(\eta) = \eta \circ f$.

De esta manera se puede enunciar desafortunadamente sin demostración el siguiente teorema de clasificación , esta vez para álgebras etales:

Teorema 2. *El functor $\mathcal{F} : \mathcal{E} \to G$-con, es una antiequivalencia de categorias.*

Finalmente defino $\varinjlim \mathcal{D}$ como la categoria de sistemas proyectivos de álgebras etales, es decir de álgebras finitas y separables, sus morfismos estan dadas naturalmente por sistemas dirigidos de morfismos.

Proposición 26. *La categoria $\mathcal{A}$ de álgebras separables es equivalente a $\varinjlim \mathcal{D}$.*

Demostración. Defino el functor $\mathcal{F}((A_i)) = \varinjlim A_i$, con su casi inverso definido por $A \longmapsto \varinjlim A_i$ donde $A_i \subset A$ es finito, así como todo conjunto es limite proyectivo de sus partes finitas se tiene que los functores son casi inverso uno del otro. □

De esta manera se puede enunciar el teorema clasificación de Galois para un álgebra separable arbitraria.

Teorema 3. *La categoria $\varinjlim \mathcal{D}$ es anti-equivalente a la categoria de G-conjuntos.*

Este es el resultado final que se quería presentar en este trabajo, desafortunadamente por cuestiones de tiempo no fué posible presentar una demostración del mismo.
Para terminar, quiero decir que lo impactante de este tema es la gran cantidad de áreas que puede llegar abarcar y por lo tanto, ser un ejemplo que las matemáticas no son un conjunto de áreas independientes sino por el contrario una única teoría .

6. Posibles profundizaciones para un fúturo trabajo.

Una posible continuación de este trabajo es el desarrollo de las demostraciones de los teoremas 2 y 3 .Pues su demostración es parte fundamental del dominio del tema referente a álgebras etales y separables.

Otra posible continuación que quiero mencionar es otro ejemplo de teorema de clasificación idéntico a los enunciados en esta tesis: revestimientos de superficies de Riemann compactas. En este caso el teorema de clasificación es enunciado con la ayuda de un grupo de automorfismos, el grupo de automorfismos de las hojas del revestimiento universal. La pertinencia del anterior tema es que debido al desarrollo de ejemplos de este estilo fuera del álgebra, se puede motivar la definición de "categoria Galoisiana". Aquí, el grupo de Galois se abstrae como el grupo de automorfismos de un functor, que en el caso de la categoría de álgebras etales, es el functor $\mathcal{F}$ definido en este trabajo. De esta manera se puede dar razón de un resultado más general que los teoremas de clasificación enunciados en esta tesis.

Finalmente valdria la pena trabajar en la relación entre el grupo de Galois de una extensión de un cuerpo y el grupo de clases ideales de su anillo de enteros. En algunos casos el abelianizado de dichos grupos esta en correspondencia con extensiones no ramificadas. La anterior frase usa palabras del contexto topológico. Esto último no es una coincidencia y para entender esta conexión entre geometria y álgebra es necesario explorar la teoría de cuerpos de clases.

7. Apendice.

Una acción de un grupo G en un conjunto discreto X es continua si y solamente si el estabilizador de un elemento es abierto:

podemos descomponer la orbita de un elemento en el siguiente conjunto: $\bigcup_{y\in X} U_y = \{(g,y) : gy = x\}$. Cada uno de estos conjuntos que forman esta unión son homeomorfos al estabilizador de un punto x via la función $g \to (gh, y)$ con h tal que $hy = x$.

$(g', y) \in U_y$ i.e $g'y = x$, $y = h^{-1}x$ asi que $g'h^{-1}x = x$ y por lo tanto $gh^{-1} \in Stab(x)$ de esta manera podemos definir:

$$\begin{aligned} f : Satb(x) &\to G \times X \\ g &\to (gh, y) \\ ghy = gx = x \implies im(f) &\subset U_y \end{aligned}$$

Si definimos el siguiente mapa:

$$f^{-1} : (g', y) \to g'h^{-1}$$

obtenemos:

$$g \to (gh, y) \to ghh^{-}1 = g \tag{1}$$

$$(g, y) \to gh^{-1} \to (gh^{-1}h, y) \tag{2}$$

Asi se puede apreciar que f y f^{-1} son efectivamente inversos, y como ambos están definidos en cada componente con la operación del grupo, se puede concluir que ambos son continuos y por ende f es un homeomorfismo. De esta manera si G_x es abierto, entonces todo U_y lo es tambien y por lo tanto se obtiene el resultado. Conversamente el estabilizador es la preimagen de la siguiente composición $G \to G \times X \to X$ donde $i_x(g) = gx$, así, si la acción es continua , Stab(x) es un conjunto abierto.

Referencias

[1] R Doudady Díaz. *Algebre et théories galoisiennes*. 1977.

[2] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117. Cambridge university press, 2009.