UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

MONOMORFISMOS ENTRE EXTENSIONES DE CAMPOS

T E S I N A

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C A

P R E S E N T A:

MAURA PATRICIA MIRANDA MONROY

ASESORA DE TESIS:
DRA. EUGENIA O'REILLY REGUEIRO

2010

Hoja de Datos del Jurado

1. Datos del alumno
   Miranda
   Monroy
   Maura Patricia
   57 30 26 54
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Matemáticas
   302262647

2. Datos del tutor
   Dra.
   Eugenia
   O'Reilly
   Regueiro

3. Datos del sinodal 1
   Dr.
   José
   Ríos
   Montes

4. Datos del sinodal 2
   Dr.
   Hugo Alberto
   Rincón
   Mejía

5. Datos del sinodal 3
   Dr.
   Alejandro Javier
   Díaz Barriga
   Casales

6. Datos del sinodal 4
   Alejandro
   Alvarado
   García

7. Datos del trabajo escrito.
   Monomorfismos entre extensiones de campos
   22 p
   2010

A G R A D E C I M I E N T O S

"Las palabras jamás podrán decir todo lo que un corazón agradecido siente"

Solo me queda decir "GRACIAS"
A mi amado CREADOR y SEÑOR,
A mi querida e inigualable FAMILIA,
A mis apreciables AMIGOS,
A mi distinguido ASESOR ESPÍRITUAL,
A mis solidarios COMPAÑEROS Y MAESTROS,
A mis originales AYUDANTES,
A mi linda ASESORA
Y a tí, mi querida Paty.

GRACIAS POR TODO.

I N D I C E

1 INTRODUCCIÓN

En matemáticas, la **Teoría de Galois** es una colección de resultados que conectan la Teoría de campos con la Teoría de grupos. La Teoría de Galois tiene aplicación a diversos problemas de la Teoría de campos, que gracias a dicha Teoría, pueden ser reducidos a problemas más sencillos de la Teoría de grupos. La Teoría de Galois debe su nombre al matemático francés Évariste Galois (1811-1832), muerto a la edad de 20 años aproximadamente.

El nacimiento de la Teoría de Galois estuvo motivado por el intento de responder a la siguiente cuestión:

> *¿Por qué no existe una fórmula para la resolución de ecuaciones polinómicas de quinto grado (o superior) en términos de los coeficientes del polinomio, usando operaciones algebraicas (suma, resta, multiplicación, división) y la extracción de raíces (raíces cuadradas, cúbicas, etc.); tal como existe para las ecuaciones de segundo, tercer y cuarto grado?*

El Teorema de Abel-Ruffini que es parte de la Teoría de Galois da una respuesta a esta pregunta. La Teoría de Galois proporciona no sólo una elegante respuesta a esta cuestión, sino que también explica en detalle por qué es posible resolver ecuaciones de grado inferior al cuarto, y por qué las soluciones son expresables mediante operaciones algebraicas y extracción de raíces.

Évariste Galois (25 de octubre de 1811 - 31 de mayo de 1832) fue un joven matemático francés nacido en Bourg-la-Reine. Mientras aún era un adolescente, fue capaz de determinar la condición necesaria y suficiente para que un polinomio pueda resolverse por radicales, dando una solución a un problema que había permanecido insoluble. Su trabajo ofreció las bases fundamentales para la teoría que lleva su nombre, una rama principal del álgebra abstracta. Fue el primero en utilizar el término "grupo" en un contexto matemático.

La Teoría de Galois es muy extensa, lo que trabajaremos aquí son monomorfismos entre extensiones de campo.

2 PRELIMINARES

La mayoría de las demostraciones de los resultados aquí mencionados, en preliminares, pueden ser vistas en [1] y [2]

Definición 2.1. Un *anillo* es un sistema $(R,+,\cdot)$ que consiste en un conjunto no vacio R y dos relaciones binarias + y · definidas sobre R y tales que

a) $(R,+)$ es un grupo abeliano
b) $(R,\cdot)$ es un semigrupo
c) La multiplicación, por ambos lados se distribuye sobre la suma.

Recordatorio 2.2.

2.2.1. $(R,+)$ es un grupo abeliano si:

2.2.1.1. Existe un elemento $0 \in R$ tal que $0 + a = a + 0 = a, \forall a \in R$

2.2.1.2. $a + (b + c) = (a + b) + c \quad \forall a, b, c \in R$

2.2.1.3. $\forall a \in R$ existe $-a \in R$ tal que $a + (-a) = (-a) + a = 0$

2.2.1.4. $a + b = b + a \quad \forall a, b \in R$ (abeliano)

2.2.2. $(R,\cdot)$ es un semigrupo si:

2.2.2.1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

2.2.3. La multiplicación se distribuye sobre la suma por ambos lados

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Definición 2.3. Un *anillo conmutativo* $(R,+,\cdot)$ es un anillo tal que $a \cdot b = b \cdot a \ \forall a, b \in R$.

Definición 2.4. Un anillo $(R,+,\cdot)$ se llama con *unidad* o con *identidad* si existe un elemento $1 \in R$ tal que $1 \cdot a = a \cdot 1 = a \ \ \forall a \in R$.

Definición 2.5. Si R es un anillo y $0 \neq a \in R$ entonces se dice que a es un *divisor izquierdo (derecho) de cero*, si existe algún elemento en R, $b \neq 0$ tal que $a \cdot b = 0$ $(b \cdot a = 0)$.

Nota 2.6. Un divisor de cero es cualquier elemento de R que es tanto divisor derecho como divisor izquierdo de cero.

Definición 2.7. Sea R un anillo conmutativo con identidad. Si R no tiene divisores de cero, entonces se dice que R es un *dominio entero*.

Definición 2.8. Sea $(R,+,\cdot)$ un anillo y sea S un subconjunto de R. Se dice que S es un *subanillo* de R si $(S\ ,\ +|_{S\times S}\ ,\ \cdot\ |_{S\times S})$ es en sí mismo un anillo.

Nota 2.9. Es decir, $(S,+,\cdot)$ es un subanillo de R si:

2.9.1. $(S,+)$ es un subgrupo de $(R,+)$.

2.9.2. $(S,\cdot)$ es un subsemigrupo de $(R,\ \cdot)$.

Definición 2.10. Sea R un anillo arbitrario. Si existe un entero positivo n tal que $n\cdot a=0$ $\forall a\in R$ entonces al entero positivo más pequeño con esta propiedad se le conoce como *la característica del anillo*. Si no existe tal entero (es decir, si $n=0$ es el único entero para el cual $n\cdot a=0$ para todo $a\in R$) entonces se dice que R es un anillo de *característica cero*.

Se denota la característica del anillo por *char*.

Definición 2.11. Sea I un subconjunto no vacío de un anillo R. Entonces I es un *ideal derecho* de R si:

2.11.1. $a,b\in I$ implica $a-b\in I$

2.11.2. $r\in R$ y $a\in I$ implica $a\cdot r\in I$

Análogamente para el ideal izquierdo. Y se escribe ideal cuando nos referimos a un ideal bilateral.

Definición 2.12. Consideremos un anillo arbitrario R y S un subconjunto no vacio de R. Denotamos por

$$(S)=\cap\{I|I\ es\ ideal\ de\ R\ y\ S\subset I\}$$

Llamamos a (S) al *ideal generado* por S, ya que si J es un ideal de R y $S\subset J$, entonces $(S)\subset J$. Es decir (S) es el ideal de R más pequeño que contiene a S.

Definición 2.13. Sea R un anillo y $S=\{a_1\}\subset R$, entonces se dice que $(\{a_1\})$ es un *ideal principal*.

Definición 2.14. Se dice que un anillo R es un *anillo de ideales principales* si cada ideal I de R es de la forma $I=(a)$ para algún $a\in R$.

Definición 2.15. Sean R y R'anillos. Por un *homomorfismo* de anillos de R a R' entendemos una función $f: R \longrightarrow R'$ tal que:

2.15.1. $f(a+b) = f(a) + f(b)$

2.15.2. $f(ab) = f(a)f(b) \ \ \forall a, b \in R$

Además:

2.15.3. f es un *monomorfismo* si f es inyectiva.

2.15.4. f es un *isomorfismo* si f es biyectiva.

2.15.5. Si $f: R \longrightarrow R$ y f es un homomorfismo, entonces se dice que f es un *endomorfismo*.

2.15.6. Si $f: R \longrightarrow R$ es además isomorfismo, entonces se dice que f es un *automorfismo*.

2.15.7. Si $f: R \longrightarrow R'$ es un homomorfismo de anillos, entonces se dice que $f(R) = \mathrm{Im} f$ es una *imagen homomorfa* de R.

Teorema 2.16. Sean R y R' dos anillos y $f: R \longrightarrow R'$ un homomorfismo. Entonces los siguientes enunciados son ciertos:

2.16.1. $f(0_R) = 0_{R'}$

2.16.2. $f(-a) = -f(a) \ \ \forall a \in R$

2.16.3. Si R y R' tienen identidad y f es suprayectiva $(f(R) = R')$ entonces $f(1_R) = 1_{R'}$

2.16.4. $f(a^{-1}) = f(a)^{-1}$ (R y R' tienen identidad) para a invertible en R y $f(R) = R'$

Teorema 2.17. Sea f un homomorfismo del anillo R al anillo R'. Entonces

2.17.1. Para cada subanillo S de R, $f(S)$ es un subanillo de R'.

2.17.2. Para cada subanillo S' de R', $f^{-1}(S')$ es un subanillo de R.

Definición 2.18. Sea f un homomorfismo de un anillo R a un anillo R'. *El kernel o núcleo* de f, denotado por $Nuc(f)$, consiste de todos los elementos en R que van a cero bajo f *ie*:

$$Nuc(f) = \{r \in R | f(r) = 0_{R'}\}$$

Observación 2.19. $Nuc(f) \neq \emptyset$, ya que $0_R \in Nuc(f)$

Teorema 2.20. Un homomorfismo f de un anillo R a un anillo R' es monomorfismo sí y sólo sí en el kernel o núcleo está solamente el cero, $Nuc(f) = \{0_R\}$

Definición 2.21. Dado un anillo R y un ideal I de R, denotamos al conjunto de todas las *clases laterales* de I en R por:

$$R/I \coloneqq \{a + I | a \in R\}$$

Teorema 2.22. Sea I un ideal del anillo R, entonces R/I es un anillo y se le conoce como el *anillo cociente* de R por I(o de I en R).

Definición 2.23. Un anillo K se dice que es un *campo* si el conjunto $K \setminus \{0\}$ es un grupo conmutativo bajo la multiplicación en K.

Teorema 2.24. Todo campo K es un dominio entero.

Definición 2.25. Por un *subcampo* K' de un campo K entendemos un subanillo K' de K que en sí mismo es un campo

Definición 2.26. Sea K un campo; *el anillo de polinomios* en X sobre K, que siempre se expresará como $K[X]$, es el conjunto de todas las expresiones formales $p(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n$, donde los a_i, llamados coeficientes del polinomio $p(X)$, están en K. En $K[X]$ se definen igualdad, suma y producto de dos polinomios para hacer de $K[X]$ un anillo conmutativo.

Lema 2.27. $K[X]$ es un dominio entero.

Definición 2.28. Si $p(X) = a_0 + a_1X + \cdots + a_nX^n$ y $a_n \neq 0$, entonces el *grado* de $p(X)$, denotado por grd $p(X)$, es n.

Teorema 2.29 (ALGORITMO DE LA DIVISIÓN). Dados los polinomios $f(X), g(X) \in K[X]$, donde $g(X) \neq 0$, se cumple entonces que existen $q(X), r(X) \in K[X]$ tales que

$$f(X) = q(X)g(X) + r(X),$$

y $r(X) = 0$ o bien grd $r(X) <$ grd $g(X)$.

Definición 2.30. $f(X) \in K[X]$ es un *polinomio mónico* si el coeficiente de su potencia más alta es 1.

Así que si $f(X)$ es mónico significa que

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

Definición 2.31. Un polinomio $p(X) \in K[X]$ de grado positivo es *irreducible* en $K[X]$ si no puede factorizarse como producto de polinomios de manera que todos ellos tengan grado

menor que grd $p(X)$. Es decir si $p(X) = r(X) \cdot q(X)$ entonces ha de ser $r(X) \in K$ o $q(X) \in K$ (es decir, alguno de ellos es un polinomio constante)

Teorema 2.32. (Propiedad de la Evaluación del Homomorfismo). Sea $\varphi: R \longrightarrow S$ un homomorfismo de anillos.

i. Para cada $s \in S$ existe un único homomorfismo de anillos $\varphi_s: R[X] \longrightarrow S$ el cual:
   a. $\varphi_s(r) = \varphi(r) \quad \forall r \in R,$
   b. $\varphi_s(X) = s.$

ii. Para $n \geq 1$ y $s_1, \dots, s_n \in S,$ existe un único homomorfismo $\varphi_{s_1,\dots,s_n}: R[X_1, \dots, X_n] \longrightarrow S$ el cual

   a. $\varphi_{s_1,\dots,s_n}(r) = \varphi(r) \ \forall r \in R,$
   b. $\varphi_{s_1,\dots,s_n}(X_i) = s_i \ \text{ con } i = 1, \dots, n.$

Para la demostración ver [3] p.6

Definición 2.33. Sea $t \in K$ donde K es un campo y $p(X) \in K[X]$. Decimos que t es *raíz* de $p(X)$ si $p(t) = 0$

Definición 2.34. Un ideal propio M de un anillo K es un *ideal máximo* si los únicos ideales de K que contienen a M son el mismo M y K.

Teorema 2.35. Si $p(X) \in K[X]$, entonces el ideal $\langle p(X) \rangle$ generado por $p(X)$ en $K[X]$ es un ideal máximo de $K[X]$ si y sólo si $p(X)$ es irreducible en $K[X]$. (Demostración en [2] p. 159-160)

Teorema 2.36. Sea K un campo.

i. El anillo cociente $K[X]/\langle p(X) \rangle$ es un dominio entero si y sólo si $p(X) = 0$ o $p(X)$ es irreducible en $K[X]$.
ii. El anillo cociente $K[X]/\langle p(X) \rangle$ es un campo si y sólo si $p(X)$ es irreducible en $K[X]$.

Demostración en [3] p.9

Definición 2.37. Sean K y L campos tales que $K \subseteq L$ es un subanillo. Entonces decimos que K es *subcampo* de L; también decimos que L es una *extensión del campo* K.

Notación 2.38. Para indicar que L es una extensión del campo K escribimos $K \leq L$ o L/K y $K < L$ si K es un subcampo propio de L, es decir, si $K \neq L$.

Observación 2.39. Un hecho importante sobre las extensiones de campo L/K es que L es un espacio vectorial sobre el campo K donde la suma es la suma en el campo L mientras el

producto por escalares está definido por $u \cdot x = ux \quad (u \in K, x \in L)$. (Es decir el producto por escalares es la restricción del producto en L).

Definición 2.40. A la *dimensión* de L como espacio vectorial sobre K la llamaremos el *grado* de la extensión de L sobre K y usaremos la siguiente notación:

$$\dim_K L = [L : K].$$

Una extensión de campo L/K es finita (dimensionalmente) si $[L : K] < \infty$, de otro modo es infinita (dimensional).

Definición 2.41. Sea F un campo y $K \leq F$. Dados los elementos $u_1, \dots, u_r \in F$ nosotros podemos formar el siguiente conjunto

$$K(u_1, \dots, u_r) = \bigcap_{\substack{K \leq L \leq F \\ u_1, \dots, u_r \in L}} L$$

el cual es el campo en F más pequeño que contiene a K y a los elementos $u_1, \dots, u_r$. La extensión $K(u_1, \dots, u_r)/K$ se llama *la extensión generada por los elementos* $u_1, \dots, u_r$; también decimos que $K(u_1, \dots, u_r)/K$ es una extensión finita generada de K. Una extensión de la forma $K(u)/K$ es llamada una *extensión simple* de K con *generador* u.

Podemos extender esto al caso de una sucesión infinita $u_1, \dots, u_r, \dots$ en F y denotada por $K(u_1, \dots, u_r, \dots) \leq F$ la extensión más pequeña del campo K que contiene a todos los elementos u_r.

Teorema 2.42. Para una extensión simple $K(u)/K$, solamente una de las siguientes condiciones se cumple:

> (i) El homomorfismo evaluación en u $\varepsilon_u : K[X] \longrightarrow K(u)$ es un monomorfismo y al pasarlo al campo de cocientes da un isomorfismo $(\varepsilon_u)_* : K(X) \longrightarrow K(u)$. Se refiere al campo de cocientes de polinomios $K(X) = \{f(X)/g(X) | f(X), g(X) \in K[X], g(X) \neq 0\}$. En este caso, $K(u)/K$ es infinito y decimos que u es trascendente sobre K.
>
> (ii) El homomorfismo evaluación en u $\varepsilon_u : K[X] \longrightarrow K(u)$ tiene un núcleo no trivial $Nuc(\varepsilon_u) = \langle p(X) \rangle$ donde $p(X) \in K[X]$ es polinomio mónico irreducible de grado positivo y el homomorfismo cociente $\tilde{\varepsilon}_u : K[X]/\langle p(X) \rangle \longrightarrow K(u)$ es un isomorfismo. En este caso $K(u)/K$ es finita con $[K(u) : K] = \text{grd } p(X)$ y decimos que u es algebraico sobre K.

(La demostración de este teorema se encuentra en [3] p.27-28)

Definición 2.43. Sea L/K una extensión de campo. Decimos que un elemento $t \in L$ es *algebraico* sobre K si hay un polinomio $p(X) \in K[X]$ no nulo para el cual $p(t) = 0$.

El Teorema 2.42 nos permite caracterizar los elementos algebraicos de la siguiente manera:

Proposición 2.44. Sea $t \in L$. Entonces las siguientes condiciones son equivalentes:

i. t es algebraico sobre K
ii. El homomorfismo evaluación $\varepsilon_t : K[X] \longrightarrow L$ tiene un núcleo no trivial.
iii. La extensión $K(t)/K$ es de dimensión finita.

Definición 2.45. Si $t \in L$ es algebraico sobre K entonces por la Proposición 2.44

$$Nuc(\varepsilon_t) = \langle \text{minpoly}_{K,t}(X) \rangle \neq \langle 0 \rangle,$$

donde $\text{minpoly}_{K,t}(X) \in K[X]$ es un polinomio mónico irreducible llamado el *polinomio mínimo de t sobre K*. El grado de $\text{minpoly}_{K,t}(X)$ es llamado *el grado de t sobre K* y está denotado por $\text{grd}_K\, t$.

Proposición 2.46. Si $t \in L$ es algebraico sobre K entonces

$$[K(t) : K] = \text{grd minpoly}_{K,t}(X) = \text{grd}_K\, t$$

La demostración de esta Proposición se sigue del Teorema 2.43(ii).

Definición 2.47. La extensión L/K es *algebraica* o L es *algebraico sobre K* si todo elemento $t \in L$ es algebraico sobre K

Definición 2.48. Sea L/K una extensión entonces:

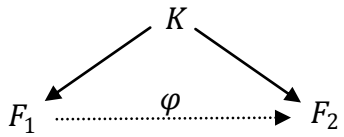
$$L^{alg} = \{t \in L | t \; es \; algebraico \; sobre \; K\} \subseteq L$$

Definición 2.49. Sea K un campo. Una extensión F/K es llamada una *cerradura algebraica de K* si F es algebraico sobre K y cerrado algebraicamente.

Notación: Para referirnos a *la cerradura algebraica del campo K* escribiremos $\overline{K}$

Teorema 2.50. Sea K un campo

i. Hay una cerradura algebraica de K.
ii. Sean F_1 y F_2 cerraduras algebraicas de K. Entonces hay un isomorfismo $\varphi : F_1 \longrightarrow F_2$ que deja fijos los elementos de K.



Entonces las cerraduras algebraicas son esencialmente únicas.

Demostración. Ver [1] que usa Lema de Zorn (ver axioma 2.53)

Definición 2.51. Un *conjunto parcialmente ordenado* $(X, \preccurlyeq)$ consiste de un conjunto X y una relación binaria $\preccurlyeq$ tal que $\forall x, y, z \in X$,

- $x \preccurlyeq x$;
- Si $x \preccurlyeq y$ y $y \preccurlyeq z$ entonces $x \preccurlyeq z$;
- Si $x \preccurlyeq y$ y $y \preccurlyeq x$ entonces $x = y$

$(X, \preccurlyeq)$ es *totalmente ordenado* si para toda pareja $x, y \in X$, se cumple $x \preccurlyeq y$ o $y \preccurlyeq x$.

Definición 2.52. Sea $(X, \preccurlyeq)$ un conjunto parcialmente ordenado y $Y \subseteq X$.

- $\bar{y} \in X$ es una *cota superior para* Y si $\forall y \in Y, y \preccurlyeq \bar{y}$.
- Un elemento $x \in X$ es un *elemento máximo* de X si

$$x \preccurlyeq y \quad \Longrightarrow \quad y = x$$

Axioma 2.53 (Lema de Zorn). Sea $(X, \preccurlyeq)$ un conjunto parcialmente ordenado en el cual todo subconjunto totalmente ordenado tiene una cota superior. Entonces X tiene un elemento máximo.

Este Axioma es equivalente al Axioma de Elección como se menciona en [4].

3 MONOMORFISMOS ENTRE EXTENSIONES

Definición 3.1. Para extensiones F/K y L/K, sea $\mathrm{Mono}_K(L,F)$ que denota el *conjunto de todos los monomorfismos* $L \longrightarrow F$ los cuales dejan fijos a los elementos de K.

$$\mathrm{Mono}_K(L,F) = \{\alpha | \alpha: L \longrightarrow F, \alpha \text{ es monomorfismo y } \alpha(x) = x \ \forall x \in K\}$$

Observación 3.2. Siempre se tiene que $\mathrm{Aut}_K(F)$ está contenido en $\mathrm{Mono}_K(F,F)$.

Donde $\mathrm{Aut}_K(F)$ denota el conjunto de todos los automorfismos de la extensión F/K.

$$\mathrm{Aut}_K(F) = \{\beta | \beta: F \longrightarrow F, \beta \text{ es automorfismo y } \beta \text{ fija los elementos de } K\}$$

Y $\mathrm{Mono}_K(F,F)$ es cerrado bajo composición

Demostración:

Sean $\alpha, \beta \in \mathrm{Mono}_K(F,F)$ entonces $\alpha \circ \beta \in \mathrm{Mono}_K(F,F)$

$\alpha: F \longrightarrow F, \beta: F \longrightarrow F$ son homomorfismos inyectivos. Por demostrar que $\alpha \circ \beta: F \longrightarrow F$ es homomorfismo inyectivo.

Sean $a, b \in F$

$$(\alpha \circ \beta)(a+b) = \alpha\big(\beta(a+b)\big) = \alpha\big(\beta(a) + \beta(b)\big) = \alpha\big(\beta(a)\big) + \alpha(\beta(b))$$

Análogo para $a \cdot b$, por lo tanto $\alpha \circ \beta$ es homomorfismo.

Ahora veamos que $\alpha \circ \beta$ inyectiva. Sean $a, b \in F$ y $a \neq b$.

Por demostrar que $(\alpha \circ \beta)(a) \neq (\alpha \circ \beta)(b)$

$$(\alpha \circ \beta)(a) = \alpha(\beta(a)) \text{ y } (\alpha \circ \beta)(b) = \alpha(\beta(b))$$

como β es inyectiva y $a \neq b$ entonces $\beta(a) \neq \beta(b)$, como α es inyectiva

$$\alpha\big(\beta(a)\big) \neq \alpha\big(\beta(b)\big).$$

Por lo tanto $\alpha \circ \beta(a) \neq \alpha \circ \beta(b)$. Por lo tanto $\alpha \circ \beta$ es inyectiva. Con esto tenemos que $\alpha \circ \beta \in \mathrm{Mono}_K(F,F)$; es decir, $\mathrm{Mono}_K(F,F)$ es cerrado bajo composición. □

Ya vimos que la composición es cerrada pero no siempre es un grupo ya que los elementos no son necesariamente invertibles.

Sea $\alpha \in \mathrm{Mono}_K(F,F)$; $\alpha^{-1}: \alpha(F) \longrightarrow F$ como α no necesariamente es sobre se puede dar el caso de que $\alpha(F) \neq F$ entonces α^{-1} no pertenece a $\mathrm{Mono}_K(F,F)$.

Observación: Si F/K es finita entonces tenemos que $\mathrm{Mono}_K(F,F) = \mathrm{Aut}_K(F)$ ya que cada transformación $K-$lineal inyectiva es suprayectiva y, por lo tanto, invertible.

Definición 3.3. Sea F/K una extensión y $p(X) \in K[X]$ tenemos

$$\mathrm{Roots}(p,F) = \{u \in F | p(u) = 0\}$$

el cual es el *conjunto de todas las raíces* de $p(X)$ en F.

Este conjunto siempre es finito; lo cual es una de las consecuencias del Teorema del Factor. (Todo polinomio de grado positivo n tiene a lo más n raíces). Y también este conjunto puede ser vacío (esto pasa precisamente cuando $p(X)$ no tiene raíces en F).

Ahora supongamos que $p(X) \in K[X]$ es un polinomio irreducible y podemos suponer que también es Mónico, y sea F/K una extensión. Entonces si t es una raíz de $p(X)$ podemos obtener a partir del homomorfismo $\varepsilon_t: K[X] \longrightarrow F$ el monomorfismo cociente siguiente:

$$\tilde{\varepsilon}_t: K[X] \,/\, \langle p(X) \rangle \longrightarrow F$$

cuya imagen es $K(t) \leq F$. Veamos que es homomorfismo:

Con la Suma:

$$q(X) + \langle p(X) \rangle, f(X) + \langle p(X) \rangle \in K[X] \,/\, \langle p(X) \rangle$$

$$\tilde{\varepsilon}_t: (q(X) + \langle p(X) \rangle + f(X) + \langle p(X) \rangle) =$$

$$\tilde{\varepsilon}_t(q(X) + f(X) + \langle p(X) \rangle) =$$

$$q(t) + f(t) =$$

$$\tilde{\varepsilon}_t(q(X) + \langle p(X) \rangle) + \tilde{\varepsilon}_t(f(X) + \langle p(X) \rangle)$$

Con el producto:

$$\tilde{\varepsilon}_t([q(X) + \langle p(X) \rangle] \cdot [f(X) + \langle p(X) \rangle]) =$$

$$\tilde{\varepsilon}_t(q(X) \cdot f(X) + \langle p(X) \rangle) =$$

$$q(t) \cdot f(t)$$

Por otro lado

$$\tilde{\varepsilon}_t(q(X) + \langle p(X)\rangle) \cdot \tilde{\varepsilon}_t(f(X) + \langle p(X)\rangle) =$$

$$q(t) \cdot f(t).$$

Por lo tanto $\tilde{\varepsilon}_t$ es homomorfismo.

Entonces la imagen de $\tilde{\varepsilon}_t$ es $K(t)$ pues $\forall t$ raíz de $p(X)$ tenemos que:

$$q(X) + \langle p(X)\rangle \in K[X] / \langle p(X)\rangle$$

$$\tilde{\varepsilon}_t(q(X) + \langle p(X)\rangle) = q(t)$$

Donde $q(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ es decir, los coeficientes están en K

$$a^i \in K$$

Entonces $q(t) = a_0 + a_1t + \cdots + a_nt^n$

es una combinación lineal de potencias de t con coeficientes en K, eso implica que

$$q(t) \in K(t)$$

de esta manera la imagen de $\tilde{\varepsilon}_t$ es $K(t) \leq F$

Y por lo tanto, para cada raíz de $p(X)$ en F hay un monomorfismo

$$t_1 \curvearrowright K(t_1)$$

$$t_2 \curvearrowright K(t_2)$$

Ahora, si fijamos una raíz t_0 y obtenemos:

$$\tilde{\varepsilon}_{t_0}: K[X]/\langle p(X)\rangle \longrightarrow K(t_0) \text{ es un isomorfismo.}$$

Con lo anterior $\tilde{\varepsilon}_{t_0}$ es un homomorfismo.

a) Por demostrar que $\tilde{\varepsilon}_{t_0}$ es sobre:

   Sea $\alpha \in K(t_0) \Rightarrow \alpha = \alpha_0 + \alpha_1t_0 + \cdots + \alpha_j + t_0^j$ con $\{1, t_0, t_0^2, \ldots, t_0^j\}$ base de $K(t_0)$ y $\alpha_0, \ldots, \alpha_j \in K$

   Entonces nos tomamos

   $\alpha_0 + \alpha_1x + \alpha_2x^2 + \cdots + \alpha_jx^j + \langle p(X)\rangle \in K[X]/\langle p(X)\rangle$

Vemos que al aplicar $\tilde{\varepsilon}_{t_0}$ obtenemos lo siguiente

$$\alpha_0 + \alpha_1 t_0 + \cdots + \alpha_j t_0^j$$

Por lo tanto $\tilde{\varepsilon}_{t_0}$ es sobre.

b) Por demostrar que $\tilde{\varepsilon}_{t_0}$ es inyectiva

$$K[X]/\langle p(X)\rangle \longrightarrow K(t_0)$$

$$f(X) + \langle p(X)\rangle \longmapsto f(t_0) \text{ y } q(X) + \langle p(X)\rangle \longmapsto q(t_0)$$

$$f(X) = \sum_{i=0}^{n} a_i X^i \quad , \quad q(X) = \sum_{i=0}^{m} b_i X^i$$

$$f(X) \neq q(X)$$

$$\sum_{i=0}^{n} a_i X^i \xrightarrow{\tilde{\varepsilon}_{t_0}} \sum_{i=o}^{n} a_i t_0^i \qquad\qquad \sum_{i=0}^{m} b_i X^i \xrightarrow{\tilde{\varepsilon}_{t_0}} \sum_{i=0}^{m} b_i t_0^i$$

Donde

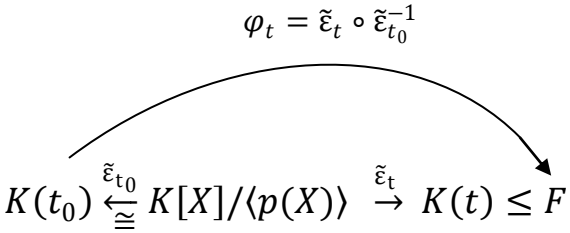
$$\sum_{i=0}^{n} a_i t_0^i \neq \sum_{i=0}^{m} b_i t_0^i$$

Ya que $\{1, t_0, \ldots, t_0^j\}$ es linealmente independiente sobre K.

Así que $\tilde{\varepsilon}_{t_0}$ es inyectiva y por lo tanto $\tilde{\varepsilon}_{t_0}$ es biyección.

$$K[X]/\langle p(X)\rangle \cong K(t_0)$$

De lo anterior tenemos el siguiente esquema:



ie: dada una raíz t_0 de $p(X)$ se da paso a un monomorfismo

$$\varphi_t = \tilde{\varepsilon}_t \circ \tilde{\varepsilon}_{t_0}^{-1} : \mathrm{K}(\mathrm{t}_0) \longrightarrow \mathrm{F}$$

$$\varphi_t(t_0) = \tilde{\varepsilon}_t \circ \tilde{\varepsilon}_{t_0}^{-1}(\mathrm{t}_0) =$$

$$\tilde{\varepsilon}_t(X + \langle p(X) \rangle) = t$$

Por lo tanto $\varphi_t(t_0) = t$

La función me lleva de una raíz a otra.

Ahora dado φ monomorfismo tendríamos una raíz.

Sea $\varphi: K[X]/\langle p(X) \rangle \longrightarrow F$ monomorfismo tal que $\varphi|_K = id$

Tomamos $0 \in K[X]/\langle p(X) \rangle$

$$0 = p(X) + \langle p(X) \rangle$$

Como φ es homomorfismo entonces $\varphi(0) = 0$

$$p(X) = \sum_{i=0}^{j} k_i X^i$$

$$\varphi(p(X) + \langle p(X) \rangle) = \sum_{i=0}^{j} k_i \varphi(X)^i = 0$$

$\therefore \varphi(X)$ es raíz de $p(X)$

Todo lo anterior se resume en el siguiente resultado:

Proposición 3.4. *Sea F/K una extensión de campo. Sea $p(X) \in K[X]$ un polinomio irreducible con $t_0 \in F$ una raíz de $p(X)$*

Entonces hay una biyección

$$\text{Roots } (p, F) \leftrightarrow \text{Mono}_K(K(t_0), F)$$

Dada por $t \leftrightarrow \varphi_t$ Donde $\varphi_t: K(t_0) \longrightarrow F$ es tal que $\varphi(t_0) = t$.

Proposición 3.5. *Sea F/K* y *L/K extensiones.*

(i) *Para* $p(X) \in K[X]$, *cada monomorfismo* $\alpha \in \mathrm{Mono}_K(L,F)$ *restringe a una función* $\alpha_p : \mathrm{Roots}(p,L) \longrightarrow \mathrm{Roots}(p,F)$ *la cual es una inyección.*

(ii) *Si* $\alpha \in \mathrm{Mono}_K(L,L)$, *entonces* $\alpha_p : \mathrm{Roots}(p,L) \longrightarrow \mathrm{Roots}(p,L)$ *es una biyección.*

Demostración: (i) Para $u \in \mathrm{Roots}(p,L)$ tenemos

$$p(u) = 0 \qquad p(u) = \sum_{i=0}^{j} a_i u^i \quad \text{con } a_i \in K$$

$$\alpha\big(p(u)\big) = \sum_{i=0}^{j} a_i \alpha(u)^i = 0 \quad \text{entonces} \quad \alpha(u) \text{ es raíz de } p(X) \text{ en } F$$

Por eso α manda $\mathrm{Roots}(p,L)$ en $\mathrm{Roots}(p,F)$

Ya que α es una inyección, su restricción a $\mathrm{Roots}(p,L) \subseteq L$ es también una inyección.

(ii) $\alpha : L \longrightarrow L$ monomorfismo, $\alpha_p : \mathrm{Roots}(p,L) \longrightarrow \mathrm{Roots}(p,L)$ es biyectiva.

De (i), $\alpha_p : \mathrm{Roots}(p,L) \longrightarrow \mathrm{Roots}(p,L)$ es una función inyectiva (solo hacemos $F = L$) de un conjunto finito (pues dijimos que $\mathrm{Roots}(p,L)$ es finito como consecuencia del Teorema del Factor) a sí mismo entonces este α_p es también suprayectiva.

Por lo tanto $\alpha_p : \mathrm{Roots}(p,L) \longrightarrow \mathrm{Roots}(p,L)$ es biyectiva. □

Proposición 3.6. *Sea* L/K *una extensión y* $\alpha \in \mathrm{Mono}_K(L,L)$. *Entonces* α se *restringe a un automorfismo*

$$\alpha^{alg} : L^{alg} \longrightarrow L^{alg}$$

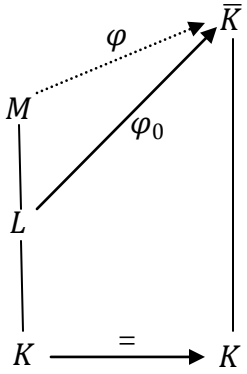
Demostración: Sea $u \in L^{alg}$, entonces $p(u) = 0$ para algún $p(X) \in K[X]$ de grado positivo.

Pero $p(u) = \sum_{i=0}^{j} a_i u^i$ y $\alpha\big(p(u)\big) = \alpha\big(\sum_{i=0}^{j} a_i u^i\big) = \sum_{i=0}^{j} a_i \alpha(u)^i = 0$. Así que $\alpha(u)$ es raíz de $p(X)$.

Por lo anterior α envía $L^{alg} \subseteq L$ en sí mismo y, por lo tanto, induce por restricción $\alpha^{alg} : L^{alg} \longrightarrow L^{alg}$ que también es un monomorfismo. Debemos demostrar que α^{alg} es biyectiva, para esto demostraremos que es suprayectiva.

Sea $u \in L^{alg}$ y supóngase que $q(u) = 0$ para algún $q(X) \in K[X]$ de grado positivo. Ahora $\mathrm{Roots}(q,L) \neq \emptyset$ pues $u \in \mathrm{Roots}(q,L)$ y también es finito. Entonces $\alpha_q : \mathrm{Roots}(q,L) \longrightarrow \mathrm{Roots}(q,L)$ es una biyección por la proposición $3.5(ii)$, entonces $u = \alpha_q(w)$ $p.a.$ $w \in \mathrm{Roots}(q,L) \subseteq L^{alg}$ Esto muestra que $u \in Im\ \alpha$ y que también α^{alg} es suprayectiva. □

Teorema 3.7 (Teorema de Extensión de Monomorfismo). *Sea M/K una extensión algebraica y $L/K \leq M/K$. Supongamos que $\varphi_0 : L \longrightarrow \overline{K}$ es un monomorfismo que fija los elementos de K. Entonces hay una extensión de φ_0 a un monomorfismo $\varphi : M \longrightarrow \overline{K}$.*



Demostración:

Recordar que con $\overline{K}$ nos referimos a la cerradura algebraica de K.

Consideremos el conjunto X que tiene como elementos (F, θ), donde $F/L \leq M/L$ y $\theta : F \longrightarrow \overline{K}$ que extiende φ_0. Ordenamos X usando la relación $\preccurlyeq$ para cada $(F_1, \theta_1) \preccurlyeq (F_2, \theta_2)$ donde $F_1 \leq F_2$ y θ_2 extiende a θ_1. Entonces $(X, \preccurlyeq)$ es un conjunto parcialmente ordenado.

Supongamos que $Y \subseteq X$ es un subconjunto totalmente ordenado. Sea

$$\tilde{F} = \bigcup_{(F,\theta) \in Y} F$$

Entonces $\tilde{F}/L \leq M/L$. También hay una función $\tilde{\theta} : \tilde{F} \longrightarrow \overline{K}$ definida por

$$\tilde{\theta}(u) = \theta(u)$$

con $u \in F$ para algún $(F, \theta) \in Y$. Es directo verificar que si $u \in F'$ con $(F', \theta') \in Y$ entonces

$$\theta'(u) = \theta(u),$$

Por lo tanto $\tilde{\theta}$ está bien definida. Entonces para cada $(F, \theta) \in Y$ tenemos que $(F, \theta) \preccurlyeq (\tilde{F}, \tilde{\theta})$, por lo cual $(\tilde{F}, \tilde{\theta})$ es una cota superior de Y. Por el Lema de Zorn debe de haber un elemento máximo de X , (M_0, θ_0). Supongamos que $M_0 \neq M$, por lo que hay un elemento $u \in M$ pero $u \notin M_0$. Como M es algebraico sobre K, también lo es sobre M_0. Si

$$\text{minpoly}_{M_0,u}(X) = a_0 + \cdots + a_{n-1}X^{n-1} + X^n,$$

entonces el polinomio

$$f(X) = \theta_0(a_0) + \cdots + \theta_0(a_{n-1})X^{n-1} + X^n \in (\theta_0 M_0)[X]$$

también es irreducible y tiene una raíz v en $\overline{K}$ (que también es una cerradura algebraica de $\theta_0 M_0 \leq \overline{K}$) (donde $\theta_0 M_0 \coloneqq \theta_0(M_0)$). La Propiedad de la Evaluación del Homomorfismo (Teorema 2.32(i)) del anillo de polinomios $M_0[X]$ aplicado al monomorfismo $\theta_0 : M_0 \longrightarrow \overline{K}$ da un homomorfismo $\theta_0' : M_0[X] \longrightarrow \overline{K}$ que es una extensión de θ_0 y además $\theta_0'(X) = v$. Tomamos el cociente $M_0[X]/\langle \text{minpoly}_{M_0,u}(X)\rangle$ y definimos el monomorfismo

$$\theta_0'' : M_0[X]/\langle \text{minpoly}_{M_0,u}(X)\rangle \longrightarrow \overline{K}$$

$$\theta_0''\left(h(X) + \langle \text{minpoly}_{M_0,u}(X)\rangle\right) = \theta_0'\left(h(X)\right) + \langle \theta_0'(\text{minpoly}_{M_0,u}(X))\rangle$$

de donde

$$\langle \text{minpoly}_{M_0,u}(X)\rangle = \langle a_0 + \cdots + a_{n-1}X^{n-1} + X^n\rangle$$

$$\theta_0'(\langle \text{minpoly}_{M_0,u}(X)\rangle) = \langle \theta_0'(a_0) + \cdots + \theta_0'(a_{n-1})\theta_0'(X^{n-1}) + \theta_0'(X^n)\rangle$$

Como $a_i \in M_0$ entonces $\theta_0'(a_i) = \theta_0(a_i)$ y $\theta_0'(X) = v$

Por lo tanto $\theta_0'(\langle \text{minpoly}_{M_0,u}(X)\rangle) = \langle \theta_0(a_0) + \cdots + \theta_0(a_{n-1})v^{n-1} + v^n\rangle = \langle f(v)\rangle = 0$

Entonces tenemos que

$$\theta_0''\left(h(X) + \langle \text{minpoly}_{M_0,u}(X)\rangle\right) = \theta_0'\left(h(X)\right) + 0$$

$$= \theta_0'\left(h(X)\right)$$

Si $h(X) = \sum_{i=0}^{n} b_i X^i$ entonces $\theta_0'\left(h(X)\right) = \sum_{i=0}^{n} \theta_0(b_i)v^i \in \overline{K}$

De esta forma θ_0'' es una extensión de θ_0.

Como $M_0[X]/\langle \text{minpoly}_{M_0,u}(X)\rangle \cong M_0(u)$ porque u es raíz de $\text{minpoly}_{M_0,u}(X)$, que es un polinomio irreducible, entonces $\text{minpoly}_{M_0,u}(X)$ es máximo (ver Teorema 2.35., Teorema 2.36(ii) y Teorema 2.42(ii)).

Y además $M_0 \leq M_0(u)$, entonces se tiene que $(M_0, \theta_0) \preccurlyeq (M_0(u), \theta_0'')$ y $(M_0, \theta_0) \neq (M_0(u), \theta_0'')$, esto contradice que (M_0, θ_0) sea máximo. Así que $M_0 = M$ y podemos tomar $\varphi = \theta_0$. ■

Como se estudia después, en los cursos de Teoría de Galois, para un polinomio $f(X) \in K[X]$ mónico separable de grado n, el Grupo de Galois de su campo de descomposición E sobre K puede ser considerado como un subgrupo del grupo simétrico S_n , que más adelante se ve como una permutación de las raíces de $f(X)$. Por ejemplo, la parte (ii) de la Proposición 3.5 dice que algún automorfismo de L/K permuta el conjunto de raíces en L de un polinomio $p(X) \in K[X]$. Así, esta proposición junto con los resultados mencionados en este trabajo, como el Teorema de Extensión del Monomorfismo, nos da un mejor entendimiento sobre los automorfismos posibles. En el caso finito, o generalmente más algebraico, en extensiones esta es la llave para entender el grupo de automorfismos y esto es una visión fundamental de la Teoría de Galois.

BIBLIOGRAFIA

[1] J. B. Fraleigh, Un primer curso en Algebra Abstracta, Addison Wesley (1999).

[2] I. N. Herstein, Álgebra Abstracta, Grupo Editorial Iberoamericana (1988)

[3] A. Baker, Una Introducción a la Teoría de Galois, Departamento de Matemáticas de la Universidad de Glasgow (pdf) http://www.maths.gla.ac.uk/~ajb/course-notes.html

[4] J. A. Amor, Teoría de Conjuntos para estudiantes de Ciencias, Las prensas de Ciencias, segunda edición (2005)