UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

EXTENSIONES DE GALOIS

T E S I N A

QUE PARA OBTENER EL TÍTULO DE:

MATEMÀTICO

P R E S E N T A:

JOSÉ GUSTAVO HERNÁNDEZ ABASCAL

DIRECTOR DE TESIS:
D. EN C. EUGENIA O'REILLY REGUEIRO
2010

1. Datos del Alumno
   Hernández
   Abascal
   José Gustavo
   53 64 50 16
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Matemático
   87528073
2. Datos del Tutor
   Dr.
   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
   Extensiones de Galois
   24 p
   2010

Agradecimientos

✓**A mis padres de quien he recibido apoyo incondicional toda mi vida y por enseñarme a guiar mí camino por la senda del respeto y la honestidad.**

✓**A mis amigos que me tendieron su mano cuando más lo necesite.**

✓**A mis profesores, por trasmitirme sus conocimientos dentro y fuera del aula, porque me ayudaron a construir mi formación académica.**

✓**A la Dra. Eugenia O'Reilly Regueiro quien me dio la oportunidad de culminar mi profesión, por sus enseñanzas y su paciencia en todo momento.**

✓**A dios, por escuchar siempre mis oraciones.**

Agradecimientos

A los sinodales, que tuvieron la gentileza de revisar mí trabajo, exter narme su opinión y sugerencias

Dr. José Ríos Montes

Dr. Hugo Alberto Rincón Mejía

Dr. Alejandro Javier Díaz Barriga

Dr. Alejandro Alvarado García.

Índice general

Introducción

Evariste Galois (25 de octubre de 1811- 31 de mayo de 1832) fue un joven matemático nacido en Bourg-la Reine una comuna a las afueras de París, su padre fue Nicolás Gabriel Galois y su madre Adelaide- Marie. Hasta los doce años, Evariste, fue educado por su madre, junto con su hermana mayor Nathalie-Theodore, consiguiendo una sólida formación en latín y griego.

Su educación académica comezó a la edad de 12 años cuando ingresó en el liceo Royal de Louis-le-Grand, de Paris, Ahí tuvo sus primeros escarceos de tintes políticos, su primer contacto con las matemáticas fue a la edad de 15 años gracias a el curso impartido por Ms Vernier, quien despertó el genio matemático de Galois, estudió la Geometría de Legendre y el Álgebra de Lagrange, enfrascándose más en el estudio del Álgebra, que en esa epoca tenía muchas lagunas y cuestiones oscuras.

Siendo estudiante de Louis-le-Grand, Galois, logró publicar su primer trabajo (una demostración de un teorema sobre fracciones continuas periódicas) y poco después dio con la clave para resolver un problema que había mantenido en jaque a los matemáticos durante más de un siglo (las condiciones de resolución de ecuaciones polinómicas por radicales). Sin embargo, sus avances más notables fueron los relacionados con el desarrollo de una teoría nueva cuyas aplicaciones desbordaban con mucho los límites de las ecuaciones algebraicas: la teoría de grupos. Mientras aún era un adolescente, fue capaz de determinar la condición necesaria y suficiente para que un polinomio sea resuelto por el método de radicales, dando una solución a un problema que había permanecido insoluble, analizando todas las permutaciones posibles de las raíces de una ecuación que cumplieran con las condiciones determinadas. Mediante dicho proceso, que en terminología actual equivale al de hallar el grupo de automorfismos de un campo, sentó las bases de la moderna teoría de grupos, una de las ramas más importantes del álgebra.

Galois intuyó que la solubilidad mediante radicales estaba sujeta a la solubilidad del grupo de automorfismos relacionado. A pesar de sus revolucionarios descubrimientos, todas las memorias que publicó con sus resultados fueron rechazadas por la Academia de Ciencias, algunas de ellas por matemáticos tan eminentes como

Cauchy, Fourier o Poisson. Pasó un tiempo en prisión por ofensas políticas, y fue muerto en un duelo a la edad de 20 años, poco después de haber sido liberado 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 termino "grupo" en un contexto matemático.

En este trabajo, veré una parte de la Teoría de Galois, LAS *EXTENSIONES DE GALOIS*, tema que forma parte importante de lo desarrollado por Galois, en lo particular me es muy intresante ver cómo se utilizan las herramientas de la teoría de grupos y la teoría de campos para construir una nueva teoría muy vasta e importante para dar solución a una ecuación. Es decir, dada una ecuación particular en un campo en donde no tiene solución, construir una "extensión" de ese campo en donde sí tenga solución y, muy interesante, ver que esa extensión es nuevamente un campo, con todas las operaciónes inducidas por el campo inicial.

Recordaré en el primer capítulo algunas definiciones y resultados importantes, de la teoría de campos y anillos, en el segundo capítulo veré extensiones de campos, monomorfismos y automorfismos de campos, recordaré la definición de cerradura algebraica, campos algebráicamente cerrados y para finalizar, en el tercer capítulo las extensiones separables y normales, y las extensiones de Galois, algunos resultados y aplicaciones

Cauchy, Fourier o Poisson. Pasó un tiempo en prisión por ofensas políticas, y fue muerto en un duelo a la edad de 20 años, poco después de haber sido liberado 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 termino "grupo" en un contexto matemático.

En este trabajo, veré una parte de la Teoría de Galois, LAS *EXTENSIONES DE GALOIS*, tema que forma parte importante de lo desarrollado por Galois, en lo particular me es muy intresante ver cómo se utilizan las herramientas de la teoría de grupos y la teoría de campos para construir una nueva teoría muy vasta e importante para dar solución a una ecuación. Es decir, dada una ecuación particular en un campo en donde no tiene solución, construir una "extensión" de ese campo en donde sí tenga solución y, muy interesante, ver que esa extensión es nuevamente un campo, con todas las operaciónes inducidas por el campo inicial.

Recordaré en el primer capítulo algunas definiciones y resultados importantes, de la teoría de campos y anillos, en el segundo capítulo veré extensiones de campos, monomorfismos y automorfismos de campos, recordaré la definición de cerradura algebraica, campos algebráicamente cerrados y para finalizar, en el tercer capítulo las extensiones separables y normales, y las extensiones de Galois, algunos resultados y aplicaciones

Capítulo 1

Teoría de Anillos y Campos

1.1. Definición y Propiedades de Anillos

En esta sección se verán dos conjuntos en los cuales se definen dos operaciones binarias suma y multiplicación, y, algunas propiedades importantes de los mismos, a estos conjuntos se les define como Anillos y Campos.

Definición 1.1.1. *Un* Grupo $\langle G, * \rangle$ *es un conjunto* G *junto con una operación binaria *, que satisface:*

- *La operación binaria es asociativa*
- *Existe* $e \in G$ *tal que* $e * x = x * e = x$ *para todas las* $x \in G$
- *se cumple que* $\forall a \in G$ *existe* $a' \in G$ *tal que:* $a * a' = a' * a = e$ (Elemento inverso)

Definición 1.1.2. *Un* Anillo $\langle R, +, * \rangle$ *es un conjunto* R *junto con dos operaciones binarias + y *, que llamaremos suma y multiplicación respectivamente, tales que satisfacen:*

- *La multiplicación es asociativa*
- $\langle R, + \rangle$ *es un grupo conmutativo* i.e. abeliano
- *se cumple que* $\forall a, b, c \in R$ $(a + b)c = ac + bc$ *y* $a(b + c) = ab + ac$ *la* ley distributiva

Definición 1.1.3. *Un anillo en donde la multiplicación es conmutativa, es decir* $\forall a, b \in R\ ab = ba$ *es un* anillo conmutativo *y, si en* R *existe 1, tal que* $\forall x \in R$ $1x = x1 = x$ *ese elemento es llamado* elemento unitario *y el anillo es un* anillo con unitario.

Teorema 1.1.1. *Si* R *es un* anillo con unitario *entonces ese elemento unitario es único*

Demostración 1.1.1. *Suponemos que 1 y 1'son unitarios.*
Como 1 es unitario, en particular
1(1')=1'
Y como 1' es unitario,
1'(1)=1
por tanto
1=1 □

Definición 1.1.4. *Sea R un anillo con unitario. Un elemento* $u \in R$ *es una* ***unidad*** *de R si tiene inverso multiplicativo, es decir:*
Existe u^{-1} *tal que* $uu^{-1} = 1$*, donde 1 es el elemento unitario de R.*

1.2. Ideales de Anillos

Para algunas demostraciones se utiliza frecuentemente el concepto de "clases laterales" por eso es importante la definición siguente:

Definición 1.2.1. *Sea H un subgrupo de un grupo G y sea* $a \in G$*. La clase lateral izquierda aH de H es el conjunto* $\{ah \mid h \in H\}$*. La clase lateral derecha Ha, se define de manera similar.*

Los subgrupos aditivos $\langle N, + \rangle$ de un anillo R que tengan la característica de que $rN \subseteq N$ y $Nr \subseteq N$ para todas las $r \in R$, veremos mas adelante que, tienen gran importancia en la teoría de anillos y campos, por eso, la importancia de estudiarlos ahora.

Definición 1.2.2. *Un subgrupo aditivo* $\langle N, + \rangle$ *de un anillo R que satisface que* $rN \subseteq N$ *y* $Nr \subseteq N$ *para todas las* $r \in R$ *es un* ***IDEAL****.*

Definición 1.2.3. *Si N es un ideal, Una clase lateral* $r + N$ *de un anillo* $\langle R, +, * \rangle$ *es el conjunto* $\{r + h \mid h \in N\}$*, con* $r \in R$*.*

Definición 1.2.4. *Si N es un ideal en un anillo R, entonces el anillo de las clases laterales $r + N$ bajo las operaciones inducidas por el anillo R de suma y producto (+ y *), es llamado el* ***anillo cociente,anillo factor*** *o el* ***anillo de las clases residuales de R módulo N*** *y se denota por* $\boldsymbol{R/N}$

Definición 1.2.5. *Si R un anillo conmutativo con unitario y $\alpha \in R$, sea el ideal $\langle\alpha\rangle = \{r\alpha | r \in R\}$, se dice que N es un* ***ideal principal*** *si $N = \langle\alpha\rangle$*

Teorema 1.2.1. *Si R es un* anillo con unitario *y N es un* ideal *de R tal que $u \in N$ para u unidad de R. entonces $N = R$*

Demostración 1.2.1. *Sea N un ideal de R, suponemos que $u \in N$ para alguna unidad u en R, entonces, la condición $rN \subseteq N$ para todas las $r \in R$, implica, si tomamos $r = u^{-1}y$ $u \in N$, que $1 = u^{-1}u$ esta en N. Pero, $rN \in R$, para todas las $r \in R$, esto implica que $r1 = r$ está en N para todas las $r \in R$, de modo que $N = R$.*

1.3. Definición y Propiedades de Campos

Definición 1.3.1. *Si R es un anillo conmutativo con unitario e , que tiene la propiedad de que $\forall a \in R \setminus \{0\}$ $\exists$ $a' \in R$ tal que $a * a' = e$ entonces R es llamado* CAMPO.

Definición 1.3.2. *Si R es un campo un subcampo se define como un subconjunto de R que es a su vez un campo bajo las operaciones inducidas por el campo R.*

Para un campo C es interesante saber si existe algún entero positivo n tal que $n \cdot a = 0$ para todas las $a \in R$.

Definición 1.3.3. *Si C es un campo y existe un entero positivo n tal que $n \cdot a = 0$ $\forall a \in C$, entonces el menor de esos enteros es la* característica de C, *si no existe dicho entero decimos que C es de* característica 0.

Teorema 1.3.1. *La característica de un campo es 0 ó es un número primo*

Demostración 1.3.1. *Sea C un campo, Si la característica no es 0, entonces, por la definición 2.3.3, es de caracterśtica n, con n entero positivo mínimo que cumple que $n \cdot a = 0$ $\forall a \in C$*

p.d. n es primo, es decir sólo es divisible entre él mismo y 1.

Suponemos que n no es primo, en ese caso $\exists m$ y $u' \in \mathbb{Z}$ tal que $n = m \cdot u'$ con $1 < m < n$ y $1 < u' < n$

Como $n \cdot a = 0 \ \forall a \in C$ *en particular para* $a = e$ *donde* e *es el elemento neutro de* C*, que existe puesto que* C *es campo.*

$\Rightarrow$ *como* $n \cdot e = (m \cdot u')e = 0$

$\Rightarrow (m \cdot e)(u' \cdot e) = 0$

$m \cdot e \neq 0$ *ya que* $m < n$ *y por hipótesis* n *es el menor entero tal que* $n \cdot a = 0$

$\Rightarrow u' \cdot e = 0$ *con* $m < n$ *lo que contradice la hipótesis de que* n *es el menor entero tal que* $n \cdot a = 0$

Por lo tanto, n *es primo* $\square$

1.4. Isomorfismos, Homorfismos y Monomorfismos de Campos

A lo largo de este trabajo, se hablará constantemente acerca de isomorfismo, homomorfismo y, especialmente de monomorfismo entre Campos, por tanto es conveniente definirlos desde esta sección.

Definición 1.4.1. *Un HOMOMORFISMO ϕ de un anillo C en un anillo L es una función $\phi : C \longrightarrow L$ tal que $\forall a, b \in C$*

- $\phi(a + b) = \phi a + \phi b$
- $\phi(ab) = (\phi a)(\phi b)$

Definición 1.4.2. *Un MONOMORFISMO es un Homomorfismo $\phi : C \longrightarrow L$ que es Inyectivo o uno a uno, es decir, $\forall a, b \in C$, $\phi(a) = \phi(b) \Longrightarrow a = b$,*

Un concepto interesante en la teoría de Grupos y Anillos es saber cuándo podemos decir que dos de ellos son ESTRUCTURALMENTE iguales, excepto por el nombre de sus elementos, esto nos lleva a la siguiente definición:

Definición 1.4.3. *Un ISOMORFISMO ϕ de un campo C en un campo L es un Monomorfismo tal que $\forall b \in L \ \exists \ a \in C$ tal que:*
$\phi(a) = b$

Definición 1.4.4. *El núcleo de un homomorfismo ϕ de un anillo R en un anillo L es el conjunto de todos los elementos de R cuya imagen es la identidad 0 de L bajo ϕ.*

En adelante se manejará constantemente el concepto de polinomio, ya que uno de los objetivos principales de este trabajo, vía los estudios de Galois es encontrar las raíces de polinomios, tal como los conocemos, pero generalizaremos la teoría a un campo R cualquiera.

Definición 1.4.5. *Sea R un anillo. Un* ***polinomio f(x) con coeficientes en R*** *es una suma formal infinita*

$$\sum_{i=0}^{\infty} a_i x^i \tag{1.4.1}$$

tal que $a_i \in R \ \forall i$ y $\exists \ \ m \in \mathbb{N}$ para la que $a_n = 0 \ \ \forall n > m$.

Definición 1.4.6. *Sea R un anillo conmutativo. denotamos por $R[x]$ al conjunto de todos los polinomios con coeficientes en R y con indeterminada x y son el conjunto de expresiones de la forma: $p(x) = p_0 + p_1x + ... + p_nx^n + ...$*

Definición 1.4.7. *Dados los polinomios*
$f(x) = a_0 + a_1x + ... + a_nx^n + ...$
y
$g(x) = b_0 + b_1x + ... + b_nx^n + ...$
definimos la suma como:
$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n + ...$
y la multiplicación
$f(x)g(x) = c_0 + c_1x + ... + c_nx^n + ...$
donde

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} \tag{1.4.2}$$

Con las operaciones de suma y producto arriba definidas, el siguiente teorema demostrará que $R[x]$ es un anillo

Teorema 1.4.1. *El conjunto $R[x]$ de polinomios en una indeterminada x con coeficientes en el campo R, es un anillo bajo la suma y multiplicación de polinomios.*

Demostración 1.4.1. *Para demostrarlo hay que ver que $\langle R[x], + \rangle$ es grupo*

- *Asociatividad:*

  $f(x) + [g(x) + h(x)] = a_0 + a_1x + ... + a_nx^n + ... + [b_0 + b_1x + ... + b_nx^n + ... + c_0 + c_1x + ... + c_nx^n + ...]$

  coma $a_i, b_i y c_i \in R$ (anillo)

  $= a_0 + a_1x + ... + a_nx^n + ... + (b_0 + c_0) + (b_1 + c_1)x + ... + (b_n + c_n)x^n + ... = (a_0 + b_0 + c_0) + (a_1 + b_1 + c_1)x + ... + (a_n + b_n + c_n)x^n + ... = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n + ... + c_0 + c_1x + ... + c_nx^n + ... = [a_0 + a_1x + ... + a_nx^n + ... + b_0 + b_1x + ... + b_nx^n +]... + c_0 + c_1x + ... + c_nx^n + ... = [f(x) + g(x)] + h(x)$

- *Elemento neutro Sea $p(x) = 0$ el elemento neutro y $p(x) \in R[x]$, es claro que:*

  $f(x) + p(x) = f(x)\ \forall f(x) \in R[x]$

- *Inverso si $f(x) = a_o + a_1x + ... + a_nx^n$, sea $f'(x) = -a_0 + (-a_1)x + ... + (-a_n)x^n + ...$ el elemento inverso.*

  este elemento existe ya que $a_i \in R$ y, como R es campo, para cada $a_i, existe - a_i$

Ahora

$f(x) + f'(x) = a_o + a_1x + ...a_nx^n + ... + -a_0 + (-a_1)x + ... + (-a_n)x^n + ... = (a_0 - a_0) + (a_1 - a_1)x + ...(a_n - a_n)x^n + ... = 0 = p(x)$

si

$$f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{j=0}^{\infty} b_j x^j, yh(x) = \sum_{k=0}^{\infty} a_k x^k \tag{1.4.3}$$

Aplicando las propiedades de campo para los coeficientes $a_i, b_i yc_i$ se puede demostrar la ley asociativa y distributiva para la multiplicación de polinomios. □

Definición 1.4.8. *Dado un polinomio p(x) en un anillo K[x] con coeficientes en K, sea α un elemento de K, decimos que α es una raiz de p(x) si p evaluado en α es el elemento neutro de K, es decir $p(\alpha) = 0$.*

Definición 1.4.9. *Un polinomio $f(x) \in F[x]$, es un* ***polinomio irreducible*** *en $F[x]$, si no puede expresarse como producto de dos polinomios $g(x)h(x)$, con $g(x)$ y $h(x) \in F[x]$, de grado menor que $f(x)$*

Capítulo 2

Extensiones y Monomorfismos

Un tema importante en la Teoría de Galois es el concepto de extensiones, es decir si tenemos un polinomio f(x) en un anillo K[x] con coeficientes en un campo K, en donde, no todas sus raíces están en ese campo, quisiéramos construir un conjunto, (que se demostrará que también tiene la estructura de campo), que contenga a K, pero que contenga también a las raíces del polinomio f(x).

2.1. Extensiones

Definición 2.1.1. *Sea L un campo, y K un subcampo de L. Decimos que L es* ***una extensión de*** *K y lo denotamos por L/K.*

Definición 2.1.2. *Si un campo de extensión L de un campo K es de dimensión finita* ***n*** *como espacio vectorial sobre K, entonces L es una extensión finita de grado n sobre K, y lo denotamos por* $[L : K] = n$.

Definición 2.1.3. *Dadas dos extensiones L/K y M/L decimos que L/K es una subextensión de M/K y, en ocasiones escribiremos* $L/K \leq M/K$.

Un resultado importante y que constantemente se usa para las demostraciones de la Teoría de Galois es dada una subextensión de una extensión, que relación existe entre los grados de las extensiones.

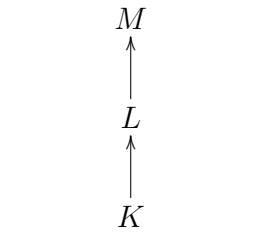
Teorema 2.1.1. [1] *Sea L/K una subextensión de M/K sucede que:*
$[M : K] = [L : K][M : L]$, *además:*

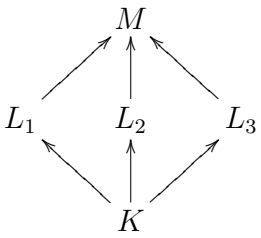
[1] La demostración se podrá consultar en: **Andrew Baker** *An Introduction to Galois Theory* Departament of Mathematics, Univerity of Glasgow.2008. http://www.maths.gla.ac.uk/ ajb/course-notes.html.p.p.26

- *Si* $[M : K]$ *es finito también lo son* $[L : K]$ *y* $[M : L]$
- *Si ambos grados* $[L : K]$ *y* $[M : L]$ *son finitos,* $[M : K]$ *es finito.*

.

Podemos ver gráficamente a las extensiones y subextensiones como una torre ó en ocasiones como un árbol como se muestra en las gráficas siguientes.





Definición 2.1.4. *Un campo de extensión L de un campo K es llamado extensión simple si,* $\exists\ u \in L$ *tal que L es el campo de extensión más pequeño que contiene a K y al elemento u , lo denotamos* $L = K(u)$*. K(u,v) es el campo de extensión de K(u) más pequeño que contiene a v, en general,* $K(u_1, u_2, ...u_n)$ *es el campo de extensión más pequeño de K que contiene a los elementos* u_i

Proposicion 2.1.2. *Sean K(u)/K y K(u,v)/K(u) extensiones simples. Entonces se cumple que:*

- $K(u, v) = K(u)(v) = K(v)(u)$ *ó en general*
- $K(u_1, ...u_n) = K(u_1, ...u_{n-1})(u_n)$

Este resultado es muy importante cuando queremos conocer el grado de una extensión, la podemos descomponer en extensiones simples.

Vamos a ver un ejemplo:

En la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ quisiéramos conocer cuál es su grado.

Sabemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]=2$ por la proposición anterior ya que 1 y $\sqrt{2}$ son una base para $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$

Ahora,$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3})$

y si u $\in \mathbb{Q}(\sqrt{2},\sqrt{3})$, entonces u $= a + b\sqrt{3}$ para algunas a,b $\in \mathbb{Q}(\sqrt{2})$, es decir $\{1,\sqrt{3}\}$ es una base de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$

por tanto,

$[\mathbb{Q}(\sqrt{2},\sqrt{3})/\ \mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3})/\ \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2})/\ \mathbb{Q}]=2\cdot 2=4$

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ {\scriptstyle [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\sqrt{2}]=2}\uparrow \\ \mathbb{Q}(\sqrt{2}) \\ {\scriptstyle [\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2}\uparrow \\ \mathbb{Q} \end{array}$$

La siguiente proposición es muy importante y nos va a permitir conocer la dimensión de algunas extensiones que cumplan ciertas características, sin tener que hacer muchos cálculos.

Proposicion 2.1.3. *Sean $p_1,....,p_n$ una sucesión de números primos distintos, con $p_i > 0$. Entonces*

Como $\sqrt{p_n}$ no está en $\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_{n-1}})$ se tiene que:

$[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1},...,\sqrt{p_{n-1}})]=2$

y

$[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_n}) : \mathbb{Q}]=2^n$

2.2. El Elemento Algebraico y Campos Algebraicamente Cerrados

2.2.1. Elemento Algebraico

Definición 2.2.1. *Un elemento $t \in L$ es **algebraico sobre K** si existe un polinomio $p(x) \in K[x]$ tal que $p(t) = 0$, en caso contrario diremos que t es **trascendente sobre K**.*

Si consideramos **R** como campo de extensión de **Q** sabemos que $\sqrt{2}$ es algebraico sobre Q pues es un cero de el polinomio x^2-2, pero también es cero de x^3-2x y de x^4-3x^2+2, pero notemos que estos polinomios son múltiplos de x^2-2, generalizando, hablaremos aquí del **polinomio irreducible**, que está determinado de manera única salvo un factor constante sobre el campo.

Definición 2.2.2. *El **homomorfismo de evaluación** $\phi_\alpha : F[x] \to E$ donde F es un subcampo del campo E y $\alpha \in E$ está definido por:*
$\phi_\alpha(a_0 + a_1x + ... + a_nx^n) = a_0 + a_1\alpha + ... + a_n\alpha^n$

Teorema 2.2.1. *ϕ_α es un homomorfismo*

Demostración 2.2.1. *si $f(x) = a_0 + a_1x + ... + a_nx^n$ y*
$g(x) = b_0 + b_1x + ... + b_mx^m$, suponemos que $m \geq n$ sin pérdida de generalidad. Entonces
$f(x) + g(x) = c_0 + c_1x + ... + c_mx^m$ donde $c_i = a_i + b_i$
por tanto
$\phi_\alpha(f(x) + g(x)) = c_0 + c_1\alpha + ... + c_m\alpha^m$
$= c_0 + c_1\alpha + ... + c_m\alpha^m = a_0 + a_1\alpha + ... + a_n\alpha^n + b_0 + b_1\alpha + ... + b_m\alpha^m = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$
por otro lado, si
$f(x)g(x) = d_0 + d_1x + ... + d_rx^r$
entonces
$\phi_\alpha(f(x)g(x)) = d_0 + d_1\alpha + ... + d_r\alpha^r$
y
$\phi_\alpha(f(x))\phi_\alpha(g(x)) = a_0 + a_1\alpha + ... + a_n\alpha^n + b_0 + b_1\alpha + ... + b_m\alpha^m$
como

$$d_j = \sum_{i=0}^{j} a_i b_{j-i} \tag{2.2.1}$$

es claro que
$\phi_\alpha(f(x)g(x)) = \phi_\alpha(f(x))\phi_\alpha(g(x))$
por tanto ϕ_α es un homomorfismo. □

Teorema 2.2.2. *Sea L un campo de extensión de K y sea $\alpha \in L$ donde α es algebraico sobre K. Entonces, existe un polinomio irreducible $p(x) \in K[x]$ que denotaremos por $irr(\alpha, K)$ tal que $p(\alpha) = 0$ y está determinado de manera única salvo un factor constante en K y es un polinomio de grado mínimo $\geq 1 en\ K[x]$ que tiene a α como raíz. Si $f(\alpha) = 0$ para $f(x) \in K[x]$ con $f(x) \neq 0$, entonces p(x) divide a f(x)*

Demostración 2.2.2. *Sea ϕ_α el homomorfismo de evaluación de $K[x]$ en L, el núcleo N de ϕ_α es un ideal y, como K es campo es un ideal principal es decir, existe algún $p(x) \in K[x]$ de grado mínimo ≥ 1 tal $\langle p(X)\rangle = N$,Como $\langle p(x)\rangle$ consta de todos los elementos de $K[x]$ que tienen como raíz a α, si existe un polinomio $f(x) \neq 0$ tal que $f(\alpha) = 0$ entonces $f(x) \in \langle p(x)\rangle$ por lo tanto $f(x) = ap(x)$ para alguna $a \in K$ es decir, p(x) divide a f(x).*

P.d. p(x) es irreducible.

Suponemos p(x) no es irreducible $\Rightarrow$

$p(x) = r(x)s(x)$ para algunos $r(x)$ y $s(x) \in K[x]$ con grado menor que $p(x)$ uno de los cuales tiene a α como raíz puesto que L es un campo, lo cual contradice el hecho de que $p(x)$ es de grado mínimo.

Por lo tanto p(x) es irreducible.$\square$

Definición 2.2.3. *El grado de $irr(\alpha, K)$ es* ***el grado*** *de α sobre K y se denota $grad(\alpha, K)$*

Proposicion 2.2.3. [2] *Si $t \in L$ es algebraico sobre K entonces:*

$[K(t) : K] = grad(\alpha, K)$

Teorema 2.2.4. *Sea L un campo de extensión de K y sea $\alpha \in L$ algebraico sobre K. Si $grad(\alpha, K) = n$ entonces $K(\alpha)$ es un espacio vectorial n-dimensional sobre K con base $\{1, \alpha, ..., \alpha^{n-1}\}$, más aún, todo elemento β de $K(\alpha)$ es algebraico sobre K y $grad(\beta, K) \leq grad(\alpha, K)$.*

Demostración 2.2.3. *Sea L campo de extensión de K y $\alpha \in L$ algebraico sobre K.*

Como $grad(\alpha, K) = n$ entonces existe $f(X) \in K[X]$ polinimio irreducible tal que:

$f(X) = p_0 + p_1X + ... + p_nX^n$, con $p_i \in K$ y $f(\alpha) = 0 \Rightarrow p_0 + p_1(\alpha) + ... + p_n(\alpha)^{n-1} \neq 0$ entonces $\{1, \alpha, ..., \alpha^{n-1}\}$ son linealmente independientes en $K(\alpha)$ y, además todo elemento $\beta \in K(\alpha)$ se puede expresar como combinación lineal de $\{1, \alpha, ..., \alpha^{n-1}\}$ así que $\{1, \alpha, ..., \alpha^{n-1}\}$ forman una base para $K(\alpha)$ sobre K, es decir, $K(\alpha)$ es un espacio vectorial sobre K, generado por los vectores $\{1, \alpha, ..., \alpha^{n-1}\}$ y la dimensión de $K(\alpha)$ como espacio vectorial sobre K es n.

Por otro lado, si $\beta \in K(\alpha)$, tomamos el conjunto de elementos $\{1, \beta, \beta^2, ..., \beta^n\} \in K(\alpha)$, como $grad(\alpha, K) = n$, para que sean linealmente independientes en $K(\alpha)$, no pueden ser $n + 1$ elementos distintos ya que $\{1, \alpha, ..., \alpha^{n-1}\}$ es una base para $K(\alpha)$ con n elementos distintos.

[2] La demostración se podrá consultar en: **Andrew Baker** *An Introduction to Galois Theory* Departament of Mathematics, Univerity of Glasgow.2008. http://www.maths.gla.ac.uk/ ajb/course-notes.html.p.p.31

Por lo tanto $1 + b_1\beta + ... + b_n\beta^n = c$ *para alguna* $c \in K$ *, con no todas las* $b_i = 0$ *es decir:*

$b_0 + b_1\beta + ... + b_n\beta^n = 0$, *donde* $b_0 = 1 - c$, *sea* $f(x) = b_0 + b_1x + ... + b_nx^n$ *un elemento en* $K[x]$ *distinto de cero tal que* $f(\beta) = 0$, *por tanto* β *es algebraico sobre* K *y* $grad(\beta, K) \leq grad(\alpha, K)$ $\square$

Definición 2.2.4. *Dada la extensión L/K, si todo elemento* $a \in L$ *es algebraico sobre K diremos que L es una* ***extensión algebraica de K****.*

Teorema 2.2.5. *Si L es un campo de extensión finita de un campo K, entonces L es una extensión algebraica.*

Demostración 2.2.4. *Sea* $\alpha \in L$, *p.d.* α *es algebraico en K, como L es finita, Por la definición 3.1.4 si [L:K]=n, por otro lado como* $K \leq K(\alpha) \leq L \Rightarrow [K(\alpha) : K]$ *es finita, por lo tanto* $\{1, \alpha, .., \alpha^{n-1}\}$ *son linealmente independientes, es decir existen* $a_i \in K$ *tal que:*

$a_o + a_1x + ... + a_n = 0$ *con no todas las* $a_i = 0$, *sea*

$f(x) = a_o + a_1x + ... + a_n$, *f(x) es un polinomio distinto de cero en K[x] y* $f(\alpha) = 0$, *por tanto* α *es algebraico sobre K.*$\square$

2.2.2. Cerradura Algebraica y Campos Algebraicamente Cerrados

Dada una extensión L de K, nos interesarán de manera particular aquellos elementos α de L que sean algebraicos sobre K ya que nuestra finalidad son las raíces de los polinomios $p(x) \in K[x]$.

Sería excelente que existiera un campo en donde cualquier polinomio f(x) NO CONSTANTE de F[x] tuviera una raíz, es decir que f(x) tuviera una raíz en ese campo, ¿Existe?, SI EXISTIERA SERIA LA SOLUCIÓN A MUCHOS PROBLEMAS!. Todos sabemos que todo polinomio no constante en $\mathbb{C}[x]$ tiene una raíz en $\mathbb{C}$, esto se conoce en álgebra, como *El teorema fundamental del álgebra*

Definición 2.2.5. *Se dice que un campo K es* ***algebraicamente cerrado*** *si todo polinomio no constante* $f(x) \in K[x]$, *tiene una raíz en K.*

Definición 2.2.6. *Sea K un campo, Un campo de extensión L/K es* ***cerradura algebraica de K*** *si L es algebraico sobre K y algebraicamente cerrado.*

Definición 2.2.7. *Sea L un campo de extensión del campo K, definimos el conjunto*

$$L^{alg} = \{\alpha \in L \mid \alpha \text{ es algebraico en } K\} \tag{2.2.2}$$

como ***la cerradura algebraica de K en L***

Teorema 2.2.6. *Sea L un campo de extensón de un campo K, L^{alg}, es un subcampo de L*

Demostración 2.2.5. *Si $\alpha, \beta \in L^{alg}$,como $K(\alpha, \beta)$ es una extensión finita de K por el teorema 2.2.5 todos los elementos de $K(\alpha, \beta)$ son algebraicos sobre K*
es decir $K(\alpha, \beta) \subseteq L^{alg}$, por tanto,
$\alpha + \beta, \alpha - \beta, \alpha\beta$ y $\alpha/\beta para \beta \neq 0$,están en L^{alg}
por lo tanto

L^{alg} es un subcampo de L □

Teorema 2.2.7. *Todo campo K tiene una* ***cerradura algebraica****, es decir, una extensión algebraica $\bar{K}$ que es algebraicamente cerrada.*

2.3. Campos de Descomposición

Una de las preguntas que dieron origen a toda esta teoría, aprovechando el conocimiento de la existencia de los campos de extensión de un campo K nos preguntaremos: Dado un polinomio p(x) con coeficientes en K que no tenga raíces en el campo K, ¿Existe algun campo de extension L/K para el cual p(x) tenga una raíz?, más aun, ¿Existe dicho campo de extension en el cual p(x) se pueda descomponer en producto de factores lineales $(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$?

Definición 2.3.1. *Decimos que $p(x) \in K[x]$ se descompone en L/K si se puede factorizar en producto de factores lineales en $L[x]$*

Por la definición 2.1.4, dado un campo K y una raíz α que no esté en K, existe un campo de extensión $K(\alpha)/K$ que contiene a K y al elemento α y, si $\alpha_1, ...\alpha_n$ son las raíces del polinomio p(x) existe un campo $K(\alpha_1, ...\alpha_n)/K$, en donde se cumple que en este nuevo campo se puede factorizar a p(x) en producto de factores lineales además, es el subcampo más pequeño que contiene al campo K y a las raíces de polinomio.

La segunda version de el Teorema de Kronecker nos enuncia este resultado:

Teorema 2.3.1. [3] *TEOREMA DE KRONECKER: Sean K un campo, y* $p(x) \in K[x]$ *un polinomio de grado positivo. Entonces existe un campo de extensión* E/K *que es un campo de descomposición de p(x) en K.*

Este teorema nos garantiza que siempre podemos construir un campo en donde el polinomio p(x) se puede descomponer en producto de factores lineales, es decir, en donde estén todas las raíces del polinomio. ¡QUE INTERESANTE!.

2.4. Monomorfismos entre Extensiones

En la Teoría de Galois, se utilizan frecuentemente los Monomorfismos de extensiones para relacionarlos con las raíces de polinomios, es decir, dada una raiz t_0 de un polinomio $p(x) \in K[x]$ en un campo de extensión L, existe una biyección entre el conjunto de raíces de un polinomio en el campo de extensión L con el conjunto de monomorfismos del campo de extensión simple $K(t_0)$ y el campo de extensión L. Por eso consideré necesario incluir ese tema en el presente trabajo.

Recordemos que un MONOMORFISMO de un campo L en un campo K es una transformación $\phi : L \longrightarrow K$ tal que $\forall a, b \in L$

- $\phi(a+b) = \phi a + \phi b$
- $\phi(ab) = (\phi a)(\phi b)$

que es inyectiva o uno a uno, es decir, $\forall a, b \in L$, $\phi(a) = \phi(b) \Longrightarrow a = b$

La idea es, dado un polinomio $f(x) \in K[x]$, si L es una extensión algebraica de K y α en L es una raíz de f(x), poder viajar, via una transformación, a otra raíz β en L de el mismo polinomio, pero que esa transformación deje fijos a los elementos del campo K. ¿Podrá ser esto posible?.

Definición 2.4.1. *Sea L extensión algebraica de un campo K. Decimos que* α *y* β *son* ***conjugados sobre K*** *si* $irr(\alpha, K) = irr(\beta, K)$*, es decir, si* α *y* β *son raices del mismo polinomio irreducible sobre K.*

De manera más general:

Definición 2.4.2. *Sean* α *y* β *en* $\bar{K}$ *de un campo K. Decimos que* α *y* β *son* ***conjugados sobre K*** *si existe un monomorfismo* $\varphi : \bar{K} \longmapsto \bar{K}$ *donde* $\beta = \varphi(\alpha)$.

[3] La demostración se podrá consultar en: **John B. Fraleigh** *Álgebra Abstracta* Delawer, E.U, Addison-Wesley Iberoamericana. 1987. p.p.321

Definición 2.4.3. *Si φ es un monomorfismo de un campo L en un campo F, y sea $a \in L$, entonces decimos que a queda* ***fijo bajo*** *φ si $\varphi a = a$.*

Definición 2.4.4. *Sean L_1 y L_2 extensiones de un campo K, y sea φ un monomorfismo $\varphi : L_1 \longmapsto L_2$, decimos que φ* ***deja fijo a K*** *si para cada $a \in K$ queda fijo bajo φ, es decir $\varphi a = a \ \forall a \in K$.*

Por la definición 2.4.2, vemos que si L es una extensión algebraica de K y, que si α y $\beta \in L$ son conjugados sobre K entonces hay un monomorfismo $\varphi : K(\alpha) \longmapsto K(\beta)$, además, $K(\alpha) \leq L$ y $K(\beta) \leq L$ son extensiones simples de K, aquí nos preguntaremos si dada esta transformacion ¿podemos extender el dominio $K(\alpha)$ a un campo más grande?, ¿tal vez a todo L?, es decir **extender la transformación φ a una transformación** $\phi : L \longmapsto L$ mas ambicioso sería preguntarse si $K(\beta)$ se puede extender a la cerradura algebraica $\bar{K}$, recordando que $L \leq \bar{K}$. La respuesta a estas preguntas es SÍ, esto nos lo garantiza el **Teorema de extensión de monomorfismos**

Teorema 2.4.1. [4] ***TEOREMA DE EXTENSIÓN DE MONOMORFISMOS*** *M/K extensión algebraica y $L/K \leq M/K$. Supongamos que $\varphi_0 : L \longmapsto \bar{K}$ es un monomorfismo que fija a los elementos de K, entonces existe un a extensión de φ_0 a un monomorfismo $\varphi : M \longmapsto \bar{K}$*

Definición 2.4.5. *Sea L una extensión finita de un campo K, el número de monomorfismos de L en $\bar{K}$que dejan fijo a K se denota por:* $\mid Mono_K(L, \bar{K}) \mid$

[4]La demostración se podrá consultar en:**Andrew Baker***An Introduction to Galois Theory* Departament of Mathematics, Univerity of Glasgow.2008. http://www.maths.gla.ac.uk/ ajb/course-notes.html.p.p.40

Capítulo 3

Extensiones de Galois

3.1. Extensiones Separables y Normales

En esta sección se tratarán extensiones que tienen características especiales y que son base para la teoría que desarrolló Evariste Galois.
Si $f(x) \in K[x]$ y $\alpha \in K$ es una raíz de f(x) es decir $f(\alpha) = 0$ podemos factorizar f(x) como $f(x) = (x - \alpha)f_1(x)$ para alguna $f_1(x) \in K[x]$

Definición 3.1.1. *Sea $f(x) \in K[x]$, y $\alpha \in \bar{K}$ tal que $f(\alpha) = 0$, α* ***es una raíz de f(x) de multiplicidad v*** *si v es el mayor entero tal que $f(x) = (x - \alpha)^v f_1(x)$ para alguna $f_1(x) \in \bar{K}[x]$, si $v = 1$ decimos que α es* ***raíz simple*** *de f(x)*

Ahora sabemos que en un polinomio podemos encontrar raíces simples, pero en ocasiones hay raíces que son de multiplicidad mayor a uno, es decir, son raíces múltiples, nos interesará estudiar en esta sección, aquellas extensiónes L/K que contengan sólo las raices de los polinomios irreducibles en $K[x]$ y además, que todas sean raíces **simples**.

Definición 3.1.2. *Un polinomio $p(x) \in K[x]$ irreducible se dice que es* ***separable sobre K*** *si cada raíz de p(x) en una extensión L/K es simple.*

Definición 3.1.3. *Sea L/K una extensión, un elemento algebraico $\alpha \in L$ se dice que es* ***separable*** *si el $irr(\alpha, K) \in K[x]$ es separable.*

Definición 3.1.4. *Una extensión algebraica L/K se llama* ***separable*** *si cada elemento de L es separable sobre K.*

Definición 3.1.5. *Si L es una extensión de K, el grado de separabilidad de L sobre K es la cardinalidad de el conjunto de monomorfismos de L en la cerradura algebraica $\bar{K}$ que dejan fijo a los elementos de K y lo denotamos por:*
$\{L : K\} = |Mono_K(L, \bar{K})|$

En particular para una extensión simple $K(\alpha)/K$,
$\{K(\alpha) : K\}$ es el número de las distintas raíces de $irr(\alpha, K)$
Ver que:
Si una extensión finita L/K es separable entonces $\{L : K\} = [L : K]$
Es decir, si L es un campo de extensión de un campo K, es de dimensión finita n como espacio vectorial sobre K, el número de elementos de la base es igual al número de monomorfismos de L en $\bar{K}$ que dejan fijo a K.

Definición 3.1.6. *Si L es una extensión finita de K, se dice que L es una* ***extensión normal de K*** *si L es un campo de descomposición separable sobre K.*

Teorema 3.1.1. *Sean E/L y L/K extensiones finitas. Si E/K es normal entonces E/L es normal.*

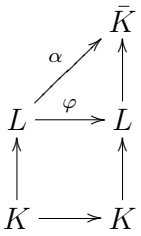
Demostración 3.1.1. *Como E es una extensión normal de K, E es campo de descomposición separable sobre K, es decir, existe $\{f_i(x), i \in I\}$ un conjunto de polinómios de K[x], como $K \leq L \leq E$, E es campo de descomposición sobre L[x] del mismo conjunto de polinómios considerados como elementos de L[x] y como E es separable sobre K, E es separable sobre L, por lo tanto E es una extensión normal de L.*

3.2. Extensiones de Galois

Se sabe, hasta aquí, sobre las extensiones de un campo dado y, cuando se dice que son separables y/o normales, nos interesarán en especial aquellas extensiones que tienen ambas características, pues este tipo de extensiones son con las que Galois, desarrolló su teoría. Al cumplir ambas características, nos interesarán aquellas extensiones L de un campo K, tal que, dado un polinomio f(x) en K[x], contenga a todas las raíces del polinomio y, además sean raíces simples.

Definición 3.2.1. *Una extensión finita E/K se llama* ***extensión de Galois*** *si cumple que es* ***normal y separable****.*

Si L/K es una extensión de Galois sabemos que $[L : K] = \{L : K\}$, es decir, cada monomorfismo $\phi : L \mapsto \bar{K}$ que deja fijo a K, manda a L en sí mismo, esto se restringe a estudiar los automorfismos $\varphi : L \mapsto L$ que dejan fijo a K, $Aut_K(L)$.



Definición 3.2.2. *Sea L/K , una extensión finita de Galois,* ***El grupo de Galois*** *de la extensión es el grupo de automorfismos de L que dejan fijo a K. y es denotado por:*

$Gal(L/K) = Aut_K(L)$

Definición 3.2.3. *Sea L/K una extensión finita de Galois y $u, v \in L$, decimos que v es conjugado de u si hay un $\varphi \in Gal(L/K)$ para la cual $v = \varphi(u)$*

Definición 3.2.4. *Sea L/K una extensión de Galois, suponemos que si $K \leq E \leq L$, es decir, $E/K \leq L/K$, entonces L/E es también una extensión de Galois y su Grupo de Galois correspondiente Gal(L/E), es llamado el* ***Grupo Relativo de Galois*** *de las extensiones L/K y E/K.*

Definición 3.2.5. *Sea L/K una extensión de Galois finita, Definimos:*
$SG(L/K)$ como el conjunto de todos los subgrupos de Galois $Gal(L/K)$, y
$SE(L/K)$ como el conjunto de todos las subextensiones E/K, de L/K

El **TEOREMA PRINCIPAL DE LA TEORÍA DE GALOIS** dice que existe una biyección entre SG(L/K) y SE(L/K) de lo que se desprende el siguiente corolario.

Corolario 3.2.1. *Sea L/K una extensión finita de Galois. Entonces existe un número finito de subextensiones $E/K \leq L/K$.*

Demostración 3.2.1. *Como el conjunto SG(L/K) es finito, y debido al teorema principal de la teoría de Galois, implica que SE(L/K)(conjunto de subextensiones E/K de L/K) es finito.*□

Finalizaré con el siguiente ejemplo, en donde se ve la construcción de una extensión para las raíces del polinomio $f(x) = (x^2 - 2)(x^2 - 3)$, que, resultará ser una extensión de Galois, y la relación que guardan las raíces con el grupo de automorfismos de la extensión:

Tomemos el campo $\mathbb{Q}$, y el polinómio $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$, si lo factorizamos, $f(x) = (x^2 - 2)(x^2 - 3)$, es claro que en $\mathbb{Q}$, este polinomio no tiene solución, ya que sus raíces $\{\sqrt{2}, \sqrt{3}, -\sqrt{2}, -\sqrt{3}\}$ no están en $\mathbb{Q}$, por lo tanto es un polinómio irreducible sobre $\mathbb{Q}$. tomamos la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, ver que los elementos $\{\sqrt{2}, \sqrt{3}, -\sqrt{2}, -\sqrt{3}\}$ ya están en esta extensión, una base para la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$ es $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ por lo tanto $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, ó visto de otra manera

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$

Por otro lado, los automorfismos de L que dejan fijo a $\mathbb{Q}$ son

ϕ_1 : La identidad

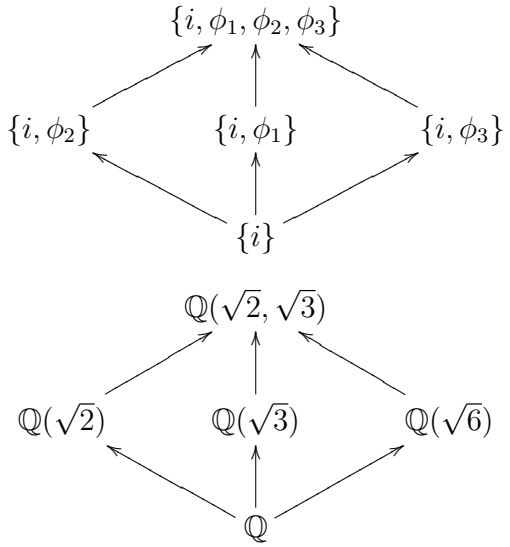
ϕ_2 : El automorfismo que transforma $\sqrt{2}$ en $-\sqrt{2}$ y deja fijos a los demás

ϕ_3 : El automorfismo que transforma $\sqrt{3}$ en $-\sqrt{3}$ y deja fijos a los demás

ϕ_4 : El automorfismo que transforma $\sqrt{2}$ en $-\sqrt{2}$ y $\sqrt{3}$ en $-\sqrt{3}$ y deja fijos a los demás.

Por tanto el número de automorfismos $\{L : K\} = 4$ que coincide con el número de raíces del polinomio f(x).

como $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = \{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\}$ por la definición 3.1.5, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es una extensión separable, además $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es campo de descomposición de f(x) sobre $\mathbb{Q}$, por lo tanto es normal. Por la definición 3.2.1 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es extensión de Galois.



Capítulo 4

Conclusiones

✓Al estudiar un polinomio con coeficientes en un campo K, en donde no todas sus raíces estén dentro del campo K, siempre podemos construir una extensión de ese campo que contenga a la ó las raíces del polinomio y, así formar un nuevo campo, **un campo de extensión de K**.

✓Dado un campo K, siempre podemos construir una extensión algebraica que contenga las raíces de todo polinomio en $K[x]$.

✓Evariste Galois estudió en particular extensiones L/K que cumplen ciertas características:
Que son **separables**, es decir, extensiones en donde cada polinomio irreducible en K[x] sus raíces son simples
Que son **Normales**, es decir, que contenga a todas las raíces de cualquier polinomio en K[x].

Bibliografía

[1] **John B. Fraleigh** *Álgebra Abstracta*, Delawer, E.U, Addison-Wesley Iberoamericana. 1987.

[2] **John R, Durbin** *Modern Algebra and Introduction*, John Wiley and Sons. New York, 1979.

[3] **Andrew Baker** *An Introduction to Galois Theory*, Departament of Mathematics, Univerity of Glasgow.2008. http://www.maths.gla.ac.uk/ ajb/course-notes.html

[4] **Ian Stewart** *Galois Theory*, Chapman and Hall/CRC, 3a. Edición, 2004.

[5] **Javier Fresán** *Del otro lado de los sueños*, en Clarín,XI, no. 63, Julio 2006. 1987.

[6] **Tony Rothman** *Évariste Galois*, en Investigación y Ciencia. Edición Especial: Grandes Matemáticos.

[7] **Leopold Infeld** *El elegido de los Dioses*,Siglo XXI editores. Novela bibliográfica sobre la vida de Evariste Galois.