Universidad Nacional Autónoma de México

Facultad de Ciencias

TEOREMA DE GALOIS PARA EXTENSIONES INFINITAS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
ANA LILIA AMAYA LUNA

DIRECTOR DE TESIS:
DRA. MARÍA DEL CARMEN GÓMEZ LAVEAGA

2009

Amaya
Luna
Ana Lilia
58-32-06-10
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas

Jurado

Dra.
Bertha María
Tomé
Arreola

Dr.
Juan
Morales
Rodríguez

Dra.
María del Carmen
Gómez
Laveaga

Mat.
Julio César
Guevara
Bravo

Mat.
Ernesto
Mayorga
Saucedo

Teorema de Galois para extensiones infinitas
75
2009

VNIVERSIDAD NACIONAL AVTONOMA DE MEXICO

FACULTAD DE CIENCIAS
Secretaría General
División de Estudios Profesionales

Votos Aprobatorios

ACT. MAURICIO AGUILAR GONZÁLEZ
Jefe de la División de Estudios Profesionales
Facultad de Ciencias
P r e s e n t e

Por este medio hacemos de su conocimiento que hemos revisado el trabajo escrito titulado:

Teorema de Galois para extensiones infinitas

realizado por **Amaya Luna Ana Lilia** con número de cuenta **4-0100026-3** quien ha decidido titularse mediante la opción de **tesis** en la licenciatura en **Matemáticas**. Dicho trabajo cuenta con nuestro voto aprobatorio.

Propietario	Dra. Bertha María Tomé Arreola	
Propietario	Dr. Juan Morales Rodríguez	
Propietario Tutora	Dra. María del Carmen Gómez Laveaga	
Suplente	Mat. Julio César Guevara Bravo	
Suplente	Mat. Ernesto Mayorga Saucedo	

Atentamente,
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, D. F., a 13 de enero de 2009
EL COORDINADOR DEL COMITÉ ACADÉMICO DE LA LICENCIATURA EN MATEMÁTICAS

M. EN C. FRANCISCO DE JESÚS STRUCK CHÁVEZ

Señor sinodal: antes de firmar este documento, solicite al estudiante que le muestre la versión digital de su trabajo y verifique que la misma incluya todas las observaciones y correcciones que usted hizo sobre el mismo.

A Ana y Javier

A Paco, Mere, Rodolfo, Pablo y Gloria

A Tadeo

A mi familia

Índice general

Introducción vii

1. Elementos de la teoría de Galois **1**
1.1. Extensiones de campos 1
1.2. El grupo de k-automorfismos 10
1.3. Extensiones Separables y Puramente Inseparables 18
1.4. Extensiones Normales 26
1.5. Extensiones de Galois 32
1.6. El teorema del elemento primitivo 36

2. Grupos Topológicos **41**
2.1. Espacios Topológicos 41
2.2. Filtros 47
2.3. Propiedades Topológicas 49
2.4. Grupos Topológicos 52

3. Extensiones infinitas de Galois **59**
3.1. Topología de Krull 59
3.2. Extensiones infinitas de Galois 68

Conclusiones **73**

Agradecimientos

Cómo agradecer a quienes no sólo te dan la vida sino que además te brindan parte de la suya... A mis padres Ana María y Javier por compartir sus experiencias y darme la oportunidad de estudiar, por creer en mi y apoyarme en todas las decisiones tomadas a lo largo de mi vida, los logros obtenidos son por ustedes.

A mis hermanos Paco, Mere, Rodolfo, Pablo y Gloria por su cariño y por confiar en mi, así como a cada una de sus familias, por quererme y apoyarme.

A Tadeo Maravilla, por su amor, apoyo y confianza.

A mi maestra Carmen Gómez Laveaga,por sus enseñanzas, por haber despertado este interés hacia el estudio de las matemáticas, por haber aceptado dirigir esta tesis, por su gran paciencia y comprensión, por sus consejos y gran apoyo, muchas gracias.

A Ernesto Mayorga Saucedo, por darme la oportunidad de trabajar junto a él, haciendo crecer los conocimientos adquiridos a lo largo de la carrera, por su gran ayuda para la realización de esta tesis, su paciencia, sus consejos y su gran apoyo.

A Rolando Gómez Macedo, por su apoyo y sus enseñanzas.

A Pablo García por aprender conmigo a lo largo de carrera.

A mis sinodales Dra. Bertha Tomé Arreola, Dr. Juan Morales Rodríguez, en especial al Mat. César Guevara Bravo, por sus comentarios y correcciones.

A los profesores con quien tuve la fortuna de llevar cursos, gracias por sus enseñanzas y por darme la oportunidad de aprender de este mundo tan maravilloso de las Matemáticas.

A mis amigas Mayte Peréz y Margarita Martínez por su gran apoyo y

cariño, gracias por su amistad.

Finalmente, agradezco a la Universidad Nacional Autónoma de México, por haberme otorgado la oportunidad de realizar mi estudio de licenciatura.

Introducción

El Teorema de Galois para extensiones finitas (normales y separables) K/k, (Teorema 3.2.3) establece una correspondencia biyectiva entre el conjunto de campos intermedios entre k y K y el conjunto de subgrupos de $G(K/k)$, el grupo de automorfismos de K que dejan fijo a k. En este trabajo presentamos una generalización de este teorema para extensiones infinitas de Galois.

Dada una extensión infinita de Galois K/k y L un campo intermedio ($k \subseteq L \subseteq K$), $G(K/L)$ es un subgrupo de $G(K/k)$, pero no necesariamente cualquier subgrupo de él es de esta forma, como se puede ver en el ejemplo que se presenta al final del Capítulo 3. La idea consiste en buscar una forma de distinguir a estos subgrupos $G(K/L)$ en el conjunto de subgrupos de $G(K/k)$.

El matemático alemán Wolfgang Krull (1899-1971) encontró la manera de hacer esta distinción definiendo una topología sobre $G(K/k)$, llamada la topología de Krull, en donde los subgrupos cerrados respecto a esta topología son exactamente lo de la forma $G(K/L)$. Es importante mencionar que cuando la extensión K/k es finita, la topología de Krull resulta ser la topología discreta y por consiguiente cada subgrupo es cerrado, por lo que el Teorema de Galois para extensiones finitas resulta ser un caso particular.

Comenzamos este trabajo haciendo un recordatorio acerca de los resultados básicos de la Teoría de Galois para extensiones finitas y generalizando algunos de ellos para extensiones infinitas. En el segundo capítulo hacemos un breve resumen de nociones topológicas, con el fin de introducir algunos conceptos de grupos topológicos, los cuales serán utilizados en el último capítulo para definir y demostrar propiedades de la topología (topología

de Krull), que será asignada a $G(K/k)$.

Finalmente, quisiera agradecer a la Dra. Carmen Gómez Laveaga, directora de esta tesis,por su interés, profesionalismo y paciencia que llevaron a buen termino este trabajo.

Ana Lilia Amaya Luna

... Los matemáticos no estudian los objetos, sino las relaciones entre los objetos; por tanto, les es indiferente reemplazar estos objetos por otros, con tal que no cambien las relaciones. La sustancia no les importa, sólo les interesa la forma.

Henri Poincaré

Capítulo 1

Elementos de la teoría de Galois

En este capítulo daremos un resumen de los conceptos básicos de la Teoría de Galois, recordando que las demostraciones de la mayoría de los resultados se ven en un curso básico de Álgebra Moderna.

1.1. Extensiones de campos

Sea k un campo.

Definición 1.1.1. *Un campo K es llamado una extensión de k si k es un subcampo de K.*

Observación 1.1.2. *Si K es una extensión de k, entonces K es un espacio vectorial sobre k*

Notación 1.1.3. *Para expresar el hecho "K es una extensión de k ", usaremos la expresión: "la extensión K/k".*

Definición 1.1.4. *Sea K es una extensión de k. El grado de K sobre k es la dimensión de la extensión K/k y se denota por $[K : k]$. En el caso en que esta dimensión sea finita diremos que la extensión es finita de grado $[K : k]$.*

Teorema 1.1.5. *Si L es una extensión de K y K es una extensión de k, entonces L es una extensión de k y $[L:k] = [L:K][K:k]$.*

Demostración. Sea $\{a_i : i \in I\}$ una base para K sobre k, y sea $\{b_j : j \in J\}$ una base para L sobre K. Consideremos el conjunto $\{a_i b_j : i \in I, j \in J\}$. Mostraremos que este conjunto es una base para L sobre k. Si $x \in L$, entonces $x = \sum_j \alpha_j b_j$, donde $\alpha_j \in K$ y casi todo $\alpha_j = 0$.

Además $\alpha_j = \sum_i \beta_{ij} a_i$, donde $\beta_{ij} \in k$ y casi todo $\beta_{ij} = 0$. Así $x = \sum_{i,j} \beta_{ij} a_i b_j$, por lo tanto $\{a_i b_j : i \in I, j \in J\}$ genera a L como un k-espacio vectorial.
Para la independencia lineal, si $\sum_{i,j} \beta_{ij} a_i b_j = 0$, con $\beta_{ij} \in k$, entonces $\sum_j (\sum_i \beta_{ij} a_i) b_j = 0$ y de la independencia lineal de los b_j sobre K, tenemos que $\sum_i \beta_{ij} a_i = 0$ para cada j. Ahora de la independencia lineal de los a_i sobre k, tenemos que $\beta_{ij} = 0$, para cada i, j. Así $\{a_i b_j : i \in I, j \in J\}$ es linealmente independiente sobre k. Por lo tanto forman una base para L sobre k y

$[L:k] = cardinalidad\ \ de\ \ \{a_i b_j : i \in I, j \in J\}$
$= cardinalidad\ \ de\ \ \{a_i : i \in I\} \cdot cardinalidad\ \ de\ \{b_j : j \in J\}$
$= [L:K][K:k]$. ■

Corolario 1.1.6. *Sean L/k una extensión finita y K un campo intermedio, es decir, $k \subseteq K \subseteq L$. Entonces $[K:k]$ divide a $[L:k]$.*

Notemos que en el caso en que K/k sea una extensión finita de grado $[K:k] = p$, con p un primo, entonces no existen campos intermedios propios entre K y k.

Ahora recordemos que dado un anillo conmutativo A, $A[x]$ denota el anillo de polinomios en x con coeficientes en A.

Definición 1.1.7. *Sea k un campo y sea $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ un polinomio en $k[x]$*

Para cada $a \in k$

$$f(a) = a_0 + a_1 a + \ldots a_n a^n \in k$$

Un elemento $a \in k$ se llama una raíz del polinomio $f(x)$ si $f(a) = 0$.

Recordemos también que un elemento $a \in k$ es raíz de $f(x) \in k[x]$ si y sólo si $(x-a)|f(x)$.

Definición 1.1.8. *Sean k un campo y $f(x)$ un polinomio en $k[x]$. Un elemento $a \in k$ se llama una raíz de multiplicidad $m \geq 1$ de $f(x)$ si $(x-a)^m \mid f(x)$ pero $(x-a)^{m+1} \nmid f(x)$.*
Si $m = 1$, diremos que a es una raíz simple. Si $m > 1$, diremos que a es una raíz de multiplicidad m.

Ahora veremos algunos resultados acerca de campos que utilizaremos posteriormente.

Observemos que si K es un campo y $\{L_\alpha\}$ es una familia de subcampos de K, entonces la intersección (que es no vacía ya que K es subcampo de K) $L = \cap_\alpha L_\alpha \subseteq K$ es nuevamente un subcampo de K.

Definición 1.1.9. *Si K es cualquier campo y $\{L_\alpha\}$ es la familia de todos los subcampos de K, la intersección de esta familia $k = \cap_\alpha L_\alpha \subseteq K$, se llama el campo primo de K.*

Teorema 1.1.10. *El campo primo de un campo K es isomorfo a $\mathbb{Q}$ o a $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, para algún primo p en $\mathbb{Z}$.*

Demostración. Sean K un campo y Δ su campo primo. Determinaremos Δ salvo isomorfismos.
Consideremos $\mathbb{Z}$ el anillo de los enteros, $e \in k$ el neutro multiplicativo y $\phi : \mathbb{Z} \to K$ definido por:

$$\phi(n) = n \cdot e = \begin{cases} e + e + \cdots + e \ \ (n - sumandos), & \text{n}> 0; \\ 0, & \text{n}= 0; \\ (-e) + (-e) + \cdots + (-e) \ \ (|n| - sumandos), & \text{n}< 0. \end{cases}$$

ϕ es un morfismo. En realidad puede verse que $\phi : \mathbb{Z} \to \Delta$, ya que $e \in \Delta$ y por lo tanto $\phi(\mathbb{Z}) \subseteq \Delta$.
El $nuc(\phi)$ no es todo $\mathbb{Z}$, ya que $\phi(1) = e \neq 0$. Por lo tanto únicamente tenemos dos casos: $nuc(\phi) = 0$ ó $0 \neq nuc(\phi) \subsetneq \mathbb{Z}$.
Caso 1. Supongamos que $nuc(\phi) = 0$, es decir, ϕ es un monomorfismo. Entonces Δ tiene un subanillo isomorfo a $\mathbb{Z}$. Como $\mathbb{Z}$ es un dominio entero

y su campo de cocientes es $\mathbb{Q}$, entonces $\phi(\mathbb{Z}) \cong \mathbb{Z}$ y por lo tanto el campo de cocientes de $\phi(\mathbb{Z})(\subseteq \Delta)$ es isomorfo al campo de cocientes de $\mathbb{Z}$ que es $\mathbb{Q}$ y por la minimalidad de Δ este debe ser Δ. Entonces $\Delta \cong \mathbb{Q}$.
Caso 2. $nuc(\phi) \neq 0$. Entonces $nuc(\phi) = n\mathbb{Z}$ para alguna $n \in \mathbb{Z}$ y $\overline{\phi} : \mathbb{Z}/n\mathbb{Z} \to \Delta$, dada por $\overline{\phi}(x+n\mathbb{Z}) = \phi(x)$ está bien definida y es un monomorfismo.
Debido a que $\overline{\phi}(\mathbb{Z}/n\mathbb{Z})$ es un subanillo de Δ, se tiene que $\overline{\phi}(\mathbb{Z}/n\mathbb{Z})$ es un dominio y por lo tanto $\mathbb{Z}/n\mathbb{Z}$ es un dominio, lo que implica que n es primo que a su vez implica que $\mathbb{Z}/n\mathbb{Z}$ es campo. Entonces $\phi(\mathbb{Z}/n\mathbb{Z})$ es campo y por la minimalidad de Δ, debe ser igual a Δ. Concluimos entonces que $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \cong \Delta$, con n primo.

■

Definición 1.1.11. *Sea K un campo. Si el campo primo de K es isomorfo a $\mathbb{Q}$, diremos que K es un campo de característica cero, y lo denotamos $carK = 0$.*
Si el campo primo de K es isomorfo a $\mathbb{Z}_p$, para un primo p, diremos que K es un campo de característica p y lo denotamos $carK = p$.

Proposición 1.1.12. *Si K/k es una extensión, entonces $carK = cark$.*

Esto es por que K y k tienen el mismo campo primo.

Ahora construiremos otros subcampos de un campo dado, haciendo uso de intersecciones de campos.

Definición 1.1.13. *Sean K una extensión de k y $X \subseteq K$. Consideremos a F como la familia de subcampos de K que contienen a k y a X. Es claro que $F \neq \emptyset$ puesto que $K \in F$. El subcampo $k(X) := \bigcap_{L \in F} L$ se llama el campo obtenido de adjuntar X a k.*
Tenemos que $k(X)$ es un campo intermedio entre k y K, es decir, $k \subseteq k(X) \subseteq K$, y también $k(X)$ es el mínimo subcampo de K que contiene a k y a X, en el sentido de que si hay otro subcampo de K que contiene a k y a X entonces contiene a $k(X)$, lo cual es evidente por la definición de $k(X)$ Si $X = \{a_1 \dots a_n\} \subseteq K$ es un conjunto finito, usaremos la notación

$$k(\{a_1 \dots a_n\}) = k(a_1 \dots a_n).$$

En particular, si $X = \{a\} \subseteq K$, diremos que $k(a)$ es una extensión simple de k. Es decir, una extensión K de k es simple si existe $a \in K$ tal que $K = k(a)$

Proposición 1.1.14. *Sean K/k una extensión y $\alpha \in K$. Sea $k(\alpha)/k$ la extensión simple obtenida al adjuntar α a k. Entonces,*

$$k(\alpha) = \left\{ \tfrac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in k[x] \;\; y \;\; g(\alpha) \neq 0 \right\}$$

Demostración. Sea $L = \{f(\alpha)/g(\alpha) : f, g \in k[x], g(\alpha) \neq 0\} \subseteq K$. Veamos que $L = k(\alpha)$. Primero observemos que con las operaciones de K, L es un subcampo de K y $k \subseteq L$ ya que si $u \in k$ y si tomamos $f(x) = u \in k(x)$ el polinomio constante u y $g(x) = 1$ el polinomio constante 1, entonces

$$u = \tfrac{f(\alpha)}{g(\alpha)} = \tfrac{u}{1} \in L.$$

Además $\alpha \in L$, basta tomar $f(x) = x$ y $g(x) = 1$. Así $k(\alpha) \subseteq L$.
Ahora, si $f(x) \in k[x]$ entonces $f(\alpha) \in k(\alpha)$, y ya que $k(\alpha)$ es un campo, si $g(x) \in k[x]$ es tal que $g(\alpha) \neq 0$, entonces $f(\alpha)/g(\alpha) \in k(\alpha)$. Así $L \subseteq k(\alpha)$.
Por lo tanto $L = k(\alpha)$ ■

Definición 1.1.15. *Sea K/k una extensión. Un elemento $\alpha \in K$ se llama algebraico sobre k si existe un polinomio no cero $f(x) \in k[x]$ tal que $f(\alpha) = 0$. En caso contrario se dice que α es trascendente sobre k.*

Dada una extensión K/k y $\alpha \in K$, denotamos por $k[\alpha]$ al subanillo de K, definido como $k[\alpha] = \{f(\alpha) | f(x) \in k[x]\}$.

Teorema 1.1.16. *Sean K/k una extensión y $\alpha \in K$ algebraico sobre k. Entonces existe un único polinomio mónico irreducible $p(x) \in k[x]$ tal que $p(\alpha) = 0$. Si $g(x)$ es cualquier polinomio en $k(x)$ tal que $g(\alpha) = 0$, entonces $p(x)$ divide a $g(x)$.*

Demostración. Definimos el mapeo $\psi : k[x] \rightarrowtail k[\alpha]$ dada por $\psi(f(x)) = f(\alpha)$. Es claro que ψ es un epimorfismo de $k[x]$ en $k[\alpha]$. Ya que α es algebraico sobre k, el núcleo de ψ es un ideal no cero de $k[x]$, como $k[x]$ es un dominio de ideales principales, cada ideal de $k[x]$ es principal, por lo tanto el núcleo de ψ es de la forma $\langle p(x) \rangle$, donde podemos asumir que

$p(x)$ es mónico, además $p(\alpha) = 0$
Ya que $k[x]/\langle p(x)\rangle$ es isomorfo a $k[\alpha]$, siendo este último un dominio entero, entonces $\langle p(x)\rangle$ es un ideal primo, lo cual implica que $p(x)$ es irreducible en $k[x]$: de hecho, $p(x)$ es el único polinomio mónico irreducible en el ideal $\langle p(x)\rangle$.
Ahora, si $g(x) \in k[x]$ es tal que $g(\alpha) = 0$, entonces $g(x) \in nuc(\psi)$, pero este núcleo es el ideal generado por $p(x)$, así $g(x) = p(x)h(x)$ para algún $h(x) \in k[x]$, así $p(x)$ divide a $g(x)$. ■

El único polinomio mónico irreducible en $k[x]$ que tiene a α como una raíz será denotado por $Irr(\alpha, k)$.

La siguiente Proposición nos dice que cuando α es algebraico sobre k, la descripción de $k(\alpha)$ en la Proposición 1.1.14 es más sencilla:

Proposición 1.1.17. *Sea $\alpha \in K$ algebraico sobre k y sea $p(x) = Irr(\alpha, k) \in k[x]$. Entonces $k(\alpha) = k[\alpha]$; más aún,*

$$k(\alpha) = \{g(\alpha) : g(x) \in k[x] \quad y \quad gr(g(x)) < gr(p(x))\}.$$

Demostración. Sea $a = \frac{f(\alpha)}{g(\alpha)} \in k(\alpha)$, con $g(\alpha) \neq 0$. Ya que $g(\alpha) \neq 0$ tenemos que $p(x)$ no divide a $g(x)$ y puesto que $p(x)$ es irreducible, el máximo común divisor $(p(x), g(x)) = 1$, así existen polinomios $s(x), t(x) \in k[x]$ tales que

$$1 = p(x)s(x) + g(x)t(x)$$

y con esto tenemos que

$$1 = p(\alpha)s(\alpha) + g(\alpha)t(\alpha) = g(\alpha)t(\alpha),$$

por lo que

$$t(\alpha) = \tfrac{1}{g(\alpha)}$$

y entonces

$$a = \tfrac{f(\alpha)}{g(\alpha)} = f(\alpha)t(\alpha) = h(\alpha)$$

donde $h(x) = f(x)t(x) \in k[x]$. Ahora lo que resta demostrar, y que es muy importante, es que $h(x)$ tiene una representación única como un polinomio de grado menor que el grado de $p(x)$, y esto resulta de aplicar el algoritmo de la división a los polinomios $h(x)$ y $p(x)$, es decir, existen polinomios únicos $q(x), r(x) \in k[x]$ tales que:

$$h(x) = p(x)q(x) + r(x) \text{ en } k[x]$$

con $r(x) = 0$ o $gr(r(x)) < gr(p(x))$ y así tenemos que $h(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, es decir, $a = h(\alpha) = r(\alpha)$, con $r(x) = 0$ o $gr(r(x)) < gr(p(x))$. Notemos además que si $f(x) \neq 0$ entonces $r(x) \neq 0$ ya que de no ser así, tendríamos que $h(x) = p(x)q(x)$, es decir, $0 = h(\alpha) = a \neq 0$, lo cual es una contradicción.

■

Teorema 1.1.18. *Si K es una extensión de k, entonces $\alpha \in K$ es algebraico sobre k si y sólo si $[k(\alpha) : k] < \infty$. Más aún $[k(\alpha) : k] = gr(Irr(\alpha, k))$.*

Demostración. Demostraremos primero que si $k(\alpha)/k$ es extensión finita, entonces α es algebraico sobre k. Supongamos que $[k(\alpha) : k] = n$ y consideremos al conjunto $1, \alpha, \alpha^2 \ldots, \alpha^n \subseteq k(\alpha)$, el cual es un conjunto linealmente dependiente sobre k, así existen $a_0, a_1, \ldots a_n \in k$ con $a_i \neq 0$ para alguna $i = 0, \ldots, n$ tales que

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$$

Así, vemos que α es raíz del polinomio no constante

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in k[x]$$

Por lo tanto α es algebraico sobre k.

Ahora supongamos que α es algebraico sobre k, y consideremos $Irr(\alpha, k)$ el polinomio mónico irreducible de α. Sea $n = gr(Irr(\alpha, k))$. Por la Proposición 1.1.17 $k(\alpha) = \{p(\alpha) : p(x) \in k[x] \quad y \quad gr(p(x)) < n\}$. Veamos que $1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in k(\alpha)$ forman una base para $k(\alpha)$ sobre k

1. $1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in k(\alpha)$ son linealmente independientes, ya que si

$$a_0 1 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$$

con $a_j \in k$, entonces $a_j = 0$ para todo $j = 0, \ldots, n-1$, porque de no ser así existiría un polinomio, a saber, $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$,distinto de cero cuyo grado es menor a n y para el cual α es raíz, lo cual contradice la minimalidad del grado de $Irr(\alpha, k)$.

2. $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ generan a $k(\alpha)$ por la forma de los elementos de $k(\alpha)$.

■

Corolario 1.1.19. *Si $\alpha \in K$ es algebraico sobre k, entonces todos los elementos de $k(\alpha)$ son algebraicos sobre k.*

Definición 1.1.20. *Una extensión K de k es llamada una extensión algebraica de k si cada elemento de K es algebraico sobre k.*

Teorema 1.1.21. *Si K es una extensión finita de k, entonces K es una extensión algebraica de k.*

Proposición 1.1.22. *Una extensión K de k es finita si y sólo si es algebraica y existen un número finito de elementos $\alpha_1, \ldots, \alpha_m \in K$ tal que $K = k(\alpha_1, \ldots, \alpha_m)$*

Demostración. Primero supongamos que K/k es finita con $[K : k] = n$, por el Teorema 1.1.21 cada elemento de K es algebraico sobre k. Además si $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ es una base de K, entonces $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$.
Ahora supongamos que la extensión K/k es algebraica y $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Como cada α_i es algebraico sobre k, tenemos, por el Teorema 1.1.18 que la extensión $k(\alpha_1)/k$ es finita. Ahora, α_2 es algebraico sobre k, entonces también lo es sobre $k(\alpha_1)$ y así $k(\alpha_1)(\alpha_2)/k(\alpha_1)$ es finita y como $k(\alpha_1)(\alpha_2) = k(\alpha_1, \alpha_2)$, tenemos, por el Teorema 1.1.5, que $k(\alpha_1, \alpha_2)/k$ es finita, por el mismo argumento $k(\alpha_1, \alpha_2, \alpha_3)/k$ también lo es y así podemos seguir con un argumento similar para cada α_i, $i = 1, 2, \ldots, n$ y como sólo hay un número finito de α_i, tenemos que la extensión $k(\alpha_1, \alpha_2, \ldots, \alpha_n)/k$ es finita. ■

Teorema 1.1.23. *Sean $k \subseteq L \subseteq K$ campos. Si L/k y K/L son algebraicas, entonces K/k es algebraica.*

Demostración. Sea $\alpha \in K$, y sea $f(x) = a_0 + a_1x + \cdots + x^n$ el polinomio mínimo de α sobre L. Ya que L/k es algebraica, por la Proposición 1.1.22, el campo $L_0 = k(a_0, a_1, \ldots, a_{n-1}) \subseteq L$ es una extensión finita de k. Ahora $f(x) \in L_0[x]$, así α es algebraico sobre L_0. Entonces por el Teorema 1.1.5 y el Teorema 1.1.18:

$$[L_0(\alpha) : k] = [L_0(\alpha) : L_0] \cdot [L_0 : k] < \infty.$$

Ya que $k(\alpha) \subset L_0(\alpha)$, vemos que $[k(\alpha) : k] < \infty$, y así α es algebraico sobre k. Debido a que esto es cierto para todo $\alpha \in K$, tenemos que K/k es algebraica. ■

Lema 1.1.24. *Sea K una extensión de k y sean $a, b \in K$ algebraicos sobre k. Entonces $a + b$, $a - b$,$a \cdot b$ y $\frac{a}{b}$ (cuando $b \neq 0$) son algebraicos sobre k. En otras palabras, el conjunto $F \subseteq K$ de todos los elementos que son algebraicos sobre k es un subcampo de K.*

Teorema 1.1.25. *Sean k un campo y $p(x) \in k[x]$ un polinomio mónico irreducible no constante. Entonces existe una extensión K de k, de grado $[K : k] = gr(p(x)) = n$ en la cual $p(x)$ contiene una raíz $\alpha \in K$, y de hecho $p(x) = Irr(\alpha, k)$ y así $K = k(\alpha)$.*

Demostración. Como $p(x)$ es irreducible, el anillo de clases residuales $K = k[x]/ < p(x) >$ es un campo ya que $< p(x) >$ es un ideal maximal de $k[x]$. Podemos considerar a k como un subanillo de $k[x]$ y si $a, b \in k$, entonces $a \equiv b\ (mod p(x))$ si y sólo si $a = b$. Así en K, $a+ < p(x) >= b+ < p(x) >$ si y sólo si $a = b$ para cualesquiera $a, b \in k$. Por lo tanto, si identificamos $a \in k$ con $a+ < p(x) > \in K$, podemos considerar a k como subcampo de K. El elemento $\alpha = x+ < p(x) >$ de K es una raíz de $p(x)$, ya que $p(\alpha) = p(x+ < p(x) >) = p(x)+ < p(x) > =< p(x) >$, el cual es el elemento cero de K y por ser $p(x)$ irreducible $p(x) = Irr(\alpha, k)$.
Además se tiene que:
$\bar{1} = 1+ < p(x) >, \alpha = x+ < p(x) >, \alpha^2 = x^2+ < p(x) >, ..., \alpha^{n-1} = x^{n-1}+ < p(x) >$ es una base de K sobre k ya que son linealmente independientes y generan a K puesto que dado cualquier polinomio $f(x) \in k[x]$ al dividirlo entre $p(x)$ se obtiene $f(x) = p(x)q(x) + r(x)$, donde $r(x) = 0$ o $gr(r(x)) \leq n - 1$ y $f(x)+ < p(x) >= r(x)+ < p(x) >$. Si escribimos

$r(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$, donde todas las c_i son cero en el caso en que $r(x) = 0$ o si $r(x) \neq 0$, $c_i = 0$ para toda $i > gr(r(x))$,tenemos que $r(x)+ < p(x) >= c_0\bar{1} + c_1\alpha + ... + c_{n-1}\alpha^{n-1}$

Como $1, \alpha, \alpha^2, ..., \alpha^{n-1}$, donde $n = gr(p(x))$, forman una base de K sobre k, entonces $K = k(\alpha)$. ■

Corolario 1.1.26. *Sea k un campo y $f(x) \in k[x]$ un polinomio de grado $n \geq 1$. Entonces existe una extensión finita K/k de grado $\leq n!$ tal que $f(x)$ tiene todas sus raíces en K.*

Demostración. Haremos la demostración por inducción sobre n.
Si $n = 1$, entonces $f(x) = x - a$, y como $a \in k$, tenemos que k es un campo en el cual $f(x)$ tiene todas sus raíces y además $[k : k] = 1$.
Supongamos que el resultado es válido para todos los polinomios de grado menor que n, es decir, si $g(x) \in k[x]$ es un polinomio de grado menor que n, entonces existe una extensión finita K/k de grado $\leq grg(x)!$ tal que $g(x)$ tiene todas sus raíces en K.
Ahora sea $f(x)$ un polinomio de grado n en $k[x]$. Consideremos a $p(x)$ un factor irreducible de $f(x)$, entonces por el Teorema 1.1.25 existe una extensión K_0 de k cuyo grado es $[K_0 : k] = gr(p(x)) \leq gr(f(x))$ y en la cual $p(x)$ tiene una raíz α. Así en $K_0[x]$ tenemos que $f(x) = (x - \alpha)q(x)$, donde $q(x) \in k_0[x]$ y $gr(q(x)) = n - 1$, entonces por hipótesis de inducción existe una extensión K/K_0 de grado $\leq (n-1)!$ en la cual $q(x)$ tiene todas sus raíces. Por lo tanto todas las raíces de $f(x)$ están en K, puesto que sus raíces son α o una raíz de $q(x)$.

Finalmente,

$$[K : k] = [K : K_0] \cdot [K_0 : k] \leq (n-1)!n = n!$$

■

1.2. El grupo de k-automorfismos

Definición 1.2.1. *Un k-isomorfismo entre dos extensiones L y K del mismo campo k, es un isomorfismo de campos $\phi : L \to K$ tal que $\phi|_k = id_k$*

Ahora teniendo esta definición daremos un resultado que ayuda a clasificar extensiones algebraicas simples, pero primero recordemos que dados K y L campos y un morfismo $\psi : K \to L$, este induce un morfismo de anillos $\widehat{\psi} : K[x] \to L[x]$ dado por

$$\widehat{\psi}(a_0 + a_1x + \cdots + a_nx^n) = \psi(a_0) + \psi(a_1)x + \cdots + \psi(a_n)x^n$$

Definición 1.2.2. *Sea K una extensión de k y sean a y b elementos de K, los cuales son algebraicos sobre k. Si $Irr(a,k) = Irr(b,k)$, entonces decimos que a y b son conjugados sobre k o $k-$conjugados.*

Antes de enunciar el Teorema que relaciona extensiones simples, daremos un resultado mas general:

Teorema 1.2.3. *Sea $\psi : K \to L$ un isomorfismo de campos y sean $K(\alpha)/K$, $L(\beta)/L$ extensiones algebraicas simples. Consideremos a $p_\alpha(x) = Irr(\alpha, K)$ y $p_\beta(x) = Irr(\beta, L)$. Sea $\widehat{\psi} : K[x] \to L[x]$ el morfismo inducido por ψ que, de hecho, es isomorfismo de anillos puesto que ψ lo es, y supongamos que $\widehat{\psi}(p_\alpha(x)) = p_\beta(x)$. Entonces existe un isomorfismo de campos $\phi : K(\alpha) \to L(\beta)$ tal que $\phi|_K = \psi$ y mas aún $\phi(\alpha) = \beta$.*

Demostración. Como mencionamos arriba, dado $\psi : K \to L$ un isomorfismo, tenemos un isomorfismo $\widehat{\psi} : K[x] \to L[x]$ definido como

$$\widehat{\psi}(a_0 + a_1x + \cdots + a_nx^n) = \psi(a_0) + \psi(a_1)x + \cdots + \psi(a_n)x^n$$

Claramente $\widehat{\psi}|_K = \psi$.
Ahora, tenemos por la Proposición 1.1.17 que si $a \in K(\alpha)$, entonces $a = f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$, con $f(x) \in K[x]$, $gr(f(x)) < gr(p_\alpha(x))$, así definimos $\phi : K(\alpha) \to L(\beta)$ como:

$$\phi(a) = \phi(f(\alpha)) = \phi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \\ \psi(a_0) + \psi(a_1)\beta + \cdots + \psi(a_n)\beta^n = \widehat{\psi}(f)(\beta).$$

1. Claramente ϕ es biyectiva

2. Si $f(\alpha), g(\alpha) \in K(\alpha)$, entonces $\phi(f(\alpha) + g(\alpha)) = \phi(f(\alpha)) + \phi(g(\alpha))$ puesto que:
   $\phi(f(\alpha) + g(\alpha))$

$= \phi((f+g)(\alpha))$
$= \widehat{\psi}(f+g)(\beta)$
$= \widehat{\psi}(f(\beta)+g(\beta))$
$= \widehat{\psi}(f)(\beta)+\widehat{\psi}(g)(\beta)$
$= \phi(f(\alpha))+\phi(g(\alpha))$

3. De igual forma como $\widehat{\psi}$ es un isomorfismo de anillos tenemos que si $f(\alpha), g(\alpha) \in K(\alpha)$, entonces $\phi(f(\alpha)g(\alpha)) = \phi(f(\alpha))\phi(g(\alpha))$

4. Además si $a \in K$, entonces $a = f(\alpha)$ con $f(x) = a$ y así tenemos que

$$\phi(a) = \phi(f(\alpha)) = \psi(a)$$

así $\phi|_K = \psi$

5. Claramente, $\alpha = f(\alpha)$ con $f(x) = x$, a si tenemos que $\phi(\alpha) = \phi(f(\alpha)) = \widehat{\psi}(f)(\beta) = \beta$

■

Ahora como caso particular del Teorema previo, tenemos el siguiente resultado:

Teorema 1.2.4. *Sea K una extensión de k y sean $a, b \in K$ conjugados sobre k. Entonces $k(a)$ y $k(b)$ son isomorfos. De hecho, existe un isomorfismo $\sigma : k(a) \to k(b)$ tal que $\sigma(a) = b$.*

Ahora teniendo en cuenta la Definición 1.2.1, vemos que un grupo natural asociado a una extensión K/k consiste del conjunto de todos los k-isomosfismos del campo K, teniendo como operación a la composición de funciones, y así, claramente se tiene un grupo. A estos k-isomorfismos de K los llamaremos *k-automorfismos* de K.

Lema 1.2.5. *Sea K/k una extensión de campos. El conjunto de k-automorfismos de K, denotado por $G(K/k)$ es un grupo con la composición de automorfismos.*

Demostración. Es claro que $id_K \in G(K/k)$. Ahora si $\sigma, \tau \in G(K/k)$ entonces $\sigma \circ \tau : K \to K$ es un isomorfismo tal que para todo $x \in k$ se tiene que $\sigma \circ \tau(x) = \sigma(\tau(x)) = \sigma(x) = x$ ya que $\tau|_k = id$ y $\sigma|_k = id$, y así $\sigma \circ \tau \in G(K/k)$.
Finalmente, si $\sigma \in G(K/k)$ entonces $\sigma^{-1} : K \to K$ es un isomorfismo, y si $x \in k$ se tiene:

$$\begin{aligned} x &= \sigma^{-1}(\sigma(x)) \\ &= \sigma^{-1}(x) \quad \text{ya que } \sigma|_k = id \end{aligned}$$

y así $\sigma^{-1} \in G(K/k)$.
Como la composición de funciones es asociativa, se sigue que $G(K/k)$ es un grupo. ■

Teorema 1.2.6. *Sean K y L campos y sean $\sigma_1, \ldots, \sigma_n$, n distintos isomorfismos de K en L. Entonces $\sigma_1, \ldots, \sigma_n$ son linealmente independientes en el sentido de que si para $a_1, \ldots a_n \in L$,*

$$(*) \quad \sum_{i=1}^{n} a_i \sigma_i(b) = 0, \text{ para toda } b \in K,$$

entonces $a_1 = \cdots = a_n = 0$.

Demostración. Haremos la demostración por inducción sobre n. Supongamos que la relación $(*)$ en la afirmación del teorema vale para todo $b \in K$. Si $n = 1$, tenemos que $a_1\sigma_1(b) = 0$ para todo $b \in K$ y en particular, si $b = 1$ obtenemos $a_1 = 0$.
Ahora supongamos que $n > 1$ y que el teorema es válido para cualesquiera $n-1$ isomorfismos de K en L. Sean $\sigma_1, \ldots, \sigma_n$ isomorfismos tales que para $a_1, \ldots, a_n \in L$

$$\sum_{i=1}^{n} a_i \sigma_i(b) = 0$$

para toda $b \in K$. Si para alguna i, $a_i = 0$, podemos suponer $a_1 = 0$, entonces:

$$\sum_{i=2}^{n} a_i \sigma_i(b) = 0$$

para todo $b \in K$ y así tenemos que $a_1 = \cdots = a_n = 0$ por nuestra hipótesis de inducción.
Supongamos pues que $a_i \neq 0$ para toda $i = 1, \ldots, n$. Debido a que σ_1 y σ_n son distintos, existe un elemento $c \in K$, $c \neq o$ tal que $\sigma_1(c) \neq \sigma_n(c)$. Entonces

$$\sigma_n(c^{-1}) \sum_{i=1}^{n} a_i \sigma_i(cb) = 0$$

para todo $b \in K$, o

$$\sum_{i=1}^{n} a_i \sigma_n(c^{-1}) \sigma_i(c) \sigma_i(b) = 0$$

para todo $b \in K$. Si restamos esto de:

$$\sum_{i=1}^{n} a_i \sigma_i(b) = 0$$

obtenemos

$$\sum_{i=1}^{n-1} a_i \left(1 - \sigma_n(c^{-1}) \sigma_i(c)\right) \sigma_i(b) = 0,$$

lo cual es cierto para todo $b \in K$. Por nuestra hipótesis de inducción, esto implica que $a_i(1 - \sigma_n(c^{-1})\sigma_i(c)) = 0$ para todo $i = 1, \ldots, n-1$. En particular, $a_1(1 - \sigma_n(c^{-1})\sigma_1(c)) = 0$ y por ser $a_1 \neq 0$ entonces $\sigma_1(c) = \sigma_n(c)$, lo cual es contrario a la elección de c. ■

Corolario 1.2.7. *Sea K una extensión de k y sean $\sigma_1, \ldots \sigma_n$ distintos k-automorfismos de K. Entonces $\sigma_1, \ldots \sigma_n$ son linealmente independientes en el sentido del Teorema 1.2.6.*

También como corolario obtenemos una cota para el orden del grupo de automorfismos de una extensión finita:

Corolario 1.2.8. *Sea K/k una extensión finita de campos. Entonces $o(G(K/k)) \leq [K : k]$*

Demostración. Sean $n = [K : k]$ y $u_1, \ldots u_n \in K$ una base de K sobre k. Supongamos que $o(G(K/k)) > n$. Entonces existen, al menos, $n + 1$ k-automorfismos de K distintos, digamos $\sigma_1, \ldots \sigma_{n+1} \in G(K/k)$. Consideremos ahora el sistema de ecuaciones lineales

$$\sum_{i=1}^{n+1} \sigma_i(u_j)x_i = 0,\ 1 \leq j \leq n$$

y como el número de ecuaciones n es menor que el número de incógnitas $n+1$, el sistema de ecuaciones tiene una solución no trivial $(a_1, \ldots, a_{n+1})$ en k^{n+1}. Así reemplazando esta solución en las ecuaciones del sistema se obtiene que:

$$\sum_{i=1}^{n+1} \sigma_i(u_j)a_i = 0,\ 1 \leq j \leq n$$

donde algún $a_i \neq 0$.
Ahora, dado $b \in K$, existen $\alpha_1, \ldots, \alpha_n \in k$ tales que:

$$b = \alpha_1 u_1 + \cdots \alpha_n u_n$$

y así

$$\sigma_i(b) = \sigma_i(\sum_{j=1}^{n} \alpha_j u_j) = \sum_{j=1}^{n} \alpha_j \sigma_i(u_j)$$

ya que los $\alpha_j \in k$ y los $\sigma_i : K \to K$ son k-automorfismos.
Se sigue que

$$a_1\sigma_1(b) + \cdots + a_{n+1}\sigma_{n+1}(b) = \sum_{i=1}^{n+1} a_i(\sum_{j=1}^{n} \alpha_j \sigma_i(u_j)) = \sum_{j=1}^{n} \alpha_j(\sum_{i=1}^{n+1} a_i\sigma_i(u_j)) = \sum_{j=1}^{n} \alpha_j \cdot (0) = 0,$$

Hemos probado que para toda $b \in K$

$a_1\sigma_1(b) + \cdots + a_{n+1}\sigma_{n+1}(b) = 0$, y por lo tanto $o(G(K/k)) \leq [K : k]$

con algún $a_i \neq 0$, en contradicción con el Corolario 1.2.7. ■

Teorema 1.2.9. *Sean K y L campos y sean $\sigma_1, \ldots \sigma_n$ distintos isomorfismos de K en L. Sea*

$$F = \{a \in K | \sigma_1(a) = \cdots = \sigma_n(a)\}$$

Entonces F es un subcampo de K y $[K : F] = r \geq n$.

Demostración. Claramente F es un subcampo de$K$.
Supongamos que $[K : F] = r < n$ y sean $b_1, \ldots, b_r$ una base de K sobre F. Consideremos el sistema de r ecuaciones con n incógnitas:

$$\sum_{j=1}^{n} \sigma_j(b_i)x_j = 0, \quad i = 1, \ldots r$$

Aquí tenemos más incógnitas que ecuaciones y por lo tanto el sistema de ecuaciones tiene una solución no trivial $c_1, \ldots, c_n$ en L. Sea $a \in K$ y escribamos $a = a_1b_1 + \cdots + a_rb_r$ donde $a_1, \ldots a_r \in F$. Multiplicando la i-ésima de las ecuaciones anteriores por $\sigma_1(a_i) = \cdots = \sigma_n(a_i)$ obtenemos:

$$\sum_{j=1}^{n} \sigma_j(a_ib_i)c_j = 0$$

Si sumamos estas ecuaciones, obtenemos

$$\sum_{j=1}^{n}(\sum_{i=1}^{r} \sigma_j(a_ib_i))c_j = 0,$$

Pero

$$\sum_{i=1}^{r} \sigma_j(a_ib_i)c_j = \sigma_j(\sum_{i=1}^{r}(a_ib_i))c_j = \sigma_j(a)c_j$$

y entonces

$$\sum_{j=1}^{n} c_j\sigma_j(a) = 0.$$

Ya que esto es cierto para toda $a \in K$, y no todas las c_j son cero, esto contradice el Teorema 1.2.6.
Por lo tanto $[K : F] = r \geq n$. ■

Definición 1.2.10. *Sean K una extensión de k, G un grupo finito de automorfismos de K y H un subgrupo de G. Definimos el campo fijo de H como el conjunto:*

$$F(H) = \{a \in K | \sigma(a) = a \ \ \forall \sigma \in H\}$$

Teorema 1.2.11. *Sea G un grupo finito de automorfismos de un campo K y sea $F(G)$ el campo fijo de G. Entonces $F(G)$ es un subcampo de K y $[K : F(G)] = o(G)$.*

Demostración. Por el teorema anterior, $F(G)$ es un subcampo de K y $[K : F(G)] \geq o(G) = n$. Supongamos que $[K : F(G)] > n$. Entonces existen $n+1$ elementos $b_1, \ldots b_{n+1}$ de K los cuales son linealmente independientes sobre $F(G)$. Sea $G = \{\sigma_1, \ldots, \sigma_n\}$ y consideremos el sistema de n ecuaciones con $n+1$ incógnitas:

$$\sum_{j=1}^{n+1} \sigma_i(b_j)x_j = 0,\ i = 1, \ldots n. \quad (1)$$

El sistema tiene mas incógnitas que ecuaciones y así, tiene una solución no trivial $a_1, \ldots, a_{n+1}$ en K. Afirmamos que al menos una de las $a_i \notin F(G)$, ya que si fuera cierto que $a_i \in F(G)$ para toda $i = 1, ..., n+1$, entonces para el elemento identidad de G, tendríamos:

$$\sum_{j=1}^{n+1} a_j b_j = 0$$

lo cual contradice el hecho de que $b_1, \ldots b_{n+1}$ son linealmente independientes sobre $F(G)$.
De entre todas las soluciones del sistema de ecuaciones (1) escogemos una con el menor número de términos no cero. Sea esta $a_1 \ldots, a_{n+1}$, donde podemos suponer que $a_j \neq 0$ para $j = 1, \ldots, r$ y $a_j = 0$ para $j = r+1, \ldots, n+1 \quad (si \quad r \neq n+1)$, $r \neq 1$, porque si $r = 1$ tendríamos , con σ_1 como la identidad de G, $a_1 b_1 = 0$, lo cual implica que $a_1 = 0$. Tenemos:

$$\sum_{j=1}^{r} a_j \sigma_i(b_j) = 0, \quad i = 1 \ldots n \quad (2)$$

Podemos suponer que $a_r = 1$, porque de otra manera podemos multiplicar cada una de las ecuaciones por a_r^{-1}. También, podemos suponer que $a_1 \notin F(G)$, así que existe un elemento $\sigma_h \in G$ tal que $\sigma_h(a_1) \neq a_1$. Si aplicamos σ_h a cada ecuación en (2) obtenemos:

$$\sum_{j=1}^{r} \sigma_h(a_j)\sigma_h\sigma_i(b_j) = 0, \quad i = 1 \ldots n.$$

Como σ_i varía en el grupo G, también $\sigma_h\sigma_i$ y podemos escribir estas ecuaciones como:

$$\sum_{j=1}^{r} \sigma_h(a_j)\sigma_i(b_j) = 0, \quad i = 1, \dots n. \quad (3)$$

Si restamos la i-ésima ecuación en (3) de la i-ésima ecuación en (2) y usando el hecho de que $a_r = 1$ obtenemos:

$$\sum_{j=1}^{r-1} (a_j - \sigma_h(a_j))\sigma_i(b_j) = 0, \quad i = 1, \dots, n.$$

Ya que $a_1 - \sigma_h(a_1) \neq 0$, esto contradice nuestra elección de la solución $a_1, \dots, a_{n+1}$ del sistema (1) como la única con el menor número de términos no cero.
Por lo tanto $[K : F(G)] = n$. ■

Corolario 1.2.12. *Sea H un subgrupo finito del grupo de automorfismos de un campo K. Sea $F(H)$ el campo fijo de H. Entonces $G(K/F(H)) = H$.*

En la siguiente sección analizaremos el concepto de *separabilidad*, cuya importancia aparece al considerar extensiones de campos de característica un primo, ya que para campos de característica cero, la separabilidad es automática, como veremos más adelante.

1.3. Extensiones Separables y Puramente Inseparables

Sea K una extensión de k y sea $a \in K$, el cual es algebraico sobre k. Sea $f(x) \in k[x]$. Existe un criterio conveniente para saber cuándo a es una raíz simple de $f(x)$, usando el concepto de derivada de un polinomio. Si $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, definimos su derivada como el polinomio $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. Es fácil verificar que si $f(x)$ y $g(x)$ son polinomios sobre el mismo campo, entonces

$$(f(x) + g(x))' = f'(x) + g'(x) \text{ y}$$
$$(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$$

Proposición 1.3.1. *Sean K una extensión de k, $a \in K$ algebraico sobre k y $f(x) \in k[x]$ un polinomio no cero,tal que $f(a) = 0$. Entonces a es una raíz simple de $f(x)$ si y sólo si $f'(a) \neq 0$.*

Definición 1.3.2. *Sea K una extensión de k. Un elemento $a \in K$ algebraico sobre k es separable sobre k si es raíz simple de su polinomio irreducible sobre k, $Irr(a, k)$.*

Decimos que la extensión K de k es una *extensión separable* sobre k si esta es algebraica sobre k y cada uno de sus elementos es separable sobre k. También decimos "K es separable sobre k ", o "K/k es separable". Si K/k es algebraica, pero no separable, decimos que K es una *extensión inseparable* de k.

Teorema 1.3.3. *Sean $k \subseteq L \subseteq K$ campos tales que, K/k es separable. Entonces L/k y K/L son separables.*

Demostración. L/k es separable ya que $L \subseteq K$ y los elementos de K son separables sobre k.
Para mostrar que K/L es separable, sea $a \in K$. Por ser a separable sobre k, tenemos que es raíz simple de $Irr(a, k)$, pero $k[x] \subseteq L[x]$, entonces $Irr(a, k)$ es un polinomio en $L[x]$ que tiene a a como raíz, así $Irr(a, L)$ divide a $Irr(a, k)$, y por lo tanto a es raíz simple de $Irr(a, L)$. ■

Definición 1.3.4. *Un campo k es llamado perfecto si no tiene extensiones inseparables.*

Como veremos, el estudio de campos perfectos se reduce a los campos de característica distinta de cero, ya que toda extensión algebraica de un campo de característica cero es separable.

Supongamos que $cark = p$ y consideremos el mapeo de k en sí mismo dado por $a \to a^p$. Es claro que $(ab)^p = a^p b^p$, y también tenemos que $(a + b)^p = a^p + b^p$. Esto último es porque:

$$(a + b)^p = a^p + b^p + \sum_{n=1}^{p-1} (\tfrac{p}{n}) a^n b^{p-n}.$$

Si $1 \leq n \leq p - 1$, el coeficiente binomial $(\frac{p}{n})$ es divisible por p y por lo que todos estos términos en la suma son cero. Así el mapeo en cuestión es un homomorfismo del campo k en sí mismo. Ya que cada homomorfismo de un campo en otro es un monomorfismo o el trivial, y debido a que $e^p = e$, este mapeo debe ser un monomorfismo de k es sí mismo. La imagen de este monomorfismo es el subcampo de k dado por:

$$k^p = \{a^p | a \in k\}.$$

Note que si $a \in k$, entonces a tiene a lo más una raíz p-ésima en cualquier extensión de k ya que si $b^p = c^p = a$, entonces $b = c$, así que k^p consiste de los elementos de k que tienen una raíz p-ésima.

Teorema 1.3.5. *El campo k es perfecto si y sólo si, la $car k = 0$ o $car k = p$ y $k^p = k$.*

Demostración. Supongamos que la $car k = 0$. Sea K una extensión algebraica de k, $a \in K$, y $p(x) = Irr(a, k)$. Entonces $p'(x) \neq 0$ y $p'(x) \in k[x]$ tiene grado menor al de $p(x)$. Por lo tanto $p(x)$ no divide a $p'(x)$, por lo que del Teorema 1.1.16 se sigue que $p'(a) \neq 0$. Así a es separable sobre k y ya que a fue arbitrario, entonces K/k es separable.

Ahora supongamos que $car k = p$ y $k^p = k$ y sean K, a y $p(x)$ como arriba. Supongamos que a no es separable sobre k. Ya que $p'(a) = 0$ y puesto que si $p'(x) \neq 0$, entonces $grad(p'(x)) < grad(p(x))$, tenemos por el Teorema 1.1.16 que debe ser $p'(x) = 0$. Sea bx^m un término típico de $p(x)$. Entonces $mbx^{m-1} = 0$ y por lo tanto debemos tener que $b = 0$ o m es divisible por p. Así $p(x)$ es de la forma:

$$p(x) = \sum_{r=0}^{n} a_r x^{pr}.$$

Ya que $k^p = k$, cada a_r tiene una única raíz p-ésima en k. Sea $b_r \in k$ tal que $b_r^p = a_r$ para $r = 0, 1, 2, \ldots, n$. Entonces

$$p(x) = \sum_{r=0}^{n} a_r x^{pr} = \sum_{r=0}^{n} b_r^p x^{pr} = (\sum_{r=0}^{n} b_r x^r)^p$$

donde

$$\sum_{r=0}^{n} b_r x^r \in k[x]$$

Pero esto contradice el hecho de que $p(x)$ es irreducible en $k[x]$. Así K/k debe ser separable y por lo tanto se tiene que k es perfecto.
Inversamente, supongamos que $car k = p$ y que k es perfecto. Mostraremos que $k^p = k$. Sea $a \in k$ y consideremos el polinomio $x^p - a \in k[x]$.
Si este polinomio tiene una raíz $b \in k$ entonces $a = b^p \in k^p$.

Supongamos que $x^p - a$ no tiene una raíz en k y sea $p(x)$ uno de sus factores irreducibles mónicos no constantes en $k[x]$. Consideremos la extensión $k(b)$ donde $p(b) = 0$. En $k(b)[x]$ tenemos que $x^p - a = x^p - b^p = (x - b)^p$ y ya que $p(x)$ divide a este polinomio, tenemos que $p(x) = (x - b)^m$ para algún $m \leq p$.
Si $m = 1$, entonces $x - b \in k[x]$ y así $b \in k$, lo cual no es cierto. Si $m > 1$, entonces b no es raíz simple de $p(x)$ y ya que $p(x) = Irr(b, k)$, $k(b)$ no es separable sobre k. Esto contradice el hecho de que k es perfecto. Por lo tanto se debe tener que $a \in k^p$ para todo $a \in k$, que es, $k^p = k$. ■

Corolario 1.3.6. *Cada campo finito es perfecto.*

Puesto que cualquier campo de característica cero es perfecto, como dijimos con anterioridad reducimos nuestro estudio a campos de característica p, así que en lo que resta de esta sección, supondremos que k es un campo de característica p y K/k es algebraica y finita.

Definición 1.3.7. *Sea $a \in K$ y sea $p(x) = Irr(a, k)$. Decimos que a es puramente inseparable sobre k, si $p(x) = (x - a)^m$ para alguna m.*

Es claro que todos los elementos de k son puramente inseparables sobre k, ya que si $a \in k$, entonces su polinomio irreducible es de la forma $x - a$.

Teorema 1.3.8. *Sea $a \in K$ puramente inseparable sobre k y $p(x) = Irr(a, k)$. Entonces existe un entero $e \geq 0$ tal que $grad(p(x)) = p^e$. Además e es el mínimo número natural tal que $a^{p^e} \in k$, es decir $a^{p^e} \in k$ y $a^{p^f} \notin k$ si $0 \leq f < e$.*

Demostración. Sea $a \in K$ y sea $grad(p(x)) = s = mp^e$, donde $p \nmid m$. Entonces $p(x) = (x - a)^{mp^e} = (x^{p^e} - a^{p^e})^m \in k[x]$, y de aquí se tiene que $ma^{p^e} \in k$, y como $p \nmid m$, entonces $a^{p^e} \in k$. Dado que $p(x)$ es irreducible, debe ser $m = 1$, y así $p(x) = x^{p^e} - a^{p^e} = (x - a)^{p^e}$, por lo que $grad(p(x)) = p^e$ y $a^{p^e} \in k$
Sea $0 \leq f < e$. Supongamos que $a^{p^f} \in k$ y sea $f(x) = x^{p^f} - a^{p^f} \in k[x]$ como $f(a) = 0$, entonces $p(x) \mid f(x)$ lo que es una contradicción.

$$\therefore a^{p^f} \notin k.$$

■

Definición 1.3.9. *Una extensión K de k es puramente inseparable sobre k si K es extensión finita de k y cada elemento de K es puramente inseparable sobre k.*

Corolario 1.3.10. *Si K es una extensión puramente inseparable de k, entonces $[K : k]$ es una potencia de p.*

Demostración. Como K/k es finita, como vimos en la prueba de la Proposición 1.1.22, a K lo podemos obtener por un número finito de extensiones simples sucesivas, es decir,

$$k_0 = k,\ k_1 = k(a_1),\ k_2 = k_1(a_2),\ \ldots,\ K = k_n = k_{n-1}(a_n)$$

Si mostramos que para todo $m = 2, \ldots, n$, a_m es puramente inseparable sobre k_{m-1}, tendremos es resultado deseado, puesto que por el Teorema 1.3.8, si esto pasa, el grado del $Irr(a_m, k_{m-1}) = p^e$, para algún entero $e \geq 0$, y como cada extensión $k_{i-1}(a_i)/ki - 1$, para $1 = 1, \ldots n$ es simple, sabemos por el Teorema 1.1.18, que el grado de la extensión es el grado del polinomio irreducible, y así por el Teorema 1.1.5 tendremos que el grado de la extensión K/k es una potencia de p.
Entonces solo probemos que $a_m$es puramente inseparable sobre k_{m-1} para todo $m = 2, \ldots, n$. Sean $p(x) = Irr(a_m, k)$ y $q(x) = Irr(a_m, k_{m-1})$. Entonces $q(x)|p(x)$ y ya que $p(x)$ es una potencia de $x - a_m$, necesariamente $q(x)$ también lo es. ■

Teorema 1.3.11. *Sea $a \in k$ tal que $a \notin k^p$. Entonces para cada entero $e \geq 0$, el polinomio $f(x) = (x^{p^e} - a)$ es irreducible en $k[x]$.*

Demostración. Sea $p(x)$ un factor irreducible mónico, no constante de $f(x)$ in $k[x]$ y sea $K = k(b)$, donde $p(b) = 0$. De esta manera $a = b^{p^e}$ y así, en $K[x]$, tenemos que $f(x) = (x - b)^{p^e}$. Si $q(x)$ es cualquier factor irreducible, mónico no constante de $f(x)$ in $k[x]$, entonces $q(x)$ es una potencia de $x - b$ y así $q(b) = 0$. Por lo tanto $p(x)$ divide a $q(x)$ por el Teorema 1.1.16, y entonces $q(x) = p(x)$. Esto significa que $f(x)$ es una potencia de $p(x)$, digamos, $f(x) = p(x)^m$. Ya que el grado de $f(x)$ es p^e , entonces el grado de $p(x)$ y m deben ser potencias de p, así que $f(x) = p(x)^{p^r}$ para algún entero $r \geq 0$. Sea c el término constante de $p(x)$ y recordemos que $c \in k$ ya que $p(x) \in k[x]$. Entonces $a = (\pm c)^{p^r}$. Si $r > 0$ tendríamos que $a \in k^p$,

lo cual no puede ser por hipótesis, así $r = 0$ y $f(x) = p(x)$ es irreducible en $k[x]$. ■

Corolario 1.3.12. *Si $a \in K$ y si existe un entero $e \geqslant 0$ tal que $a^{p^e} \in k$ entonces a es puramente inseparable sobre k.*

Corolario 1.3.13. *Un elemento $a \in K$ es separable y puramente inseparable sobre k si y sólo si $a \in k$.*

Sea L un campo arbitrario y sean M y N subcampos de L. El *compuesto* de M y N (en L) es la intersección de todos los subcampos de L, los cuales contienen a M y a L, Este es el subcampo más pequeño de L que contiene a ambos y será denotado por MN. Claramente tenemos que $MN = M(N) = N(M)$. Teniendo esta definición daremos algunos resultados sobre extensiones separables.

Teorema 1.3.14. *Si K/k es una extensión separable y si $car k = p$, entonces $kK^p = K$ (esto es cierto aún cuando $[K : k]$ es infinito). Si la extensión K/k es finita y $kK^p = K$, entonces K/k es separable.*

Corolario 1.3.15. *Si K/k una extensión y $a \in K$ es separable sobre k,entonces $k(a) = k(a^p)$ y $k(a)/k$ es separable. Si $k(a) = k(a^p)$, entonces a es separable sobre k.*

Demostración. Supongamos que $a \in K$ es separable sobre k. Sabemos que $k(a^p) \subseteq k(a)$. Mostremos que $k(a) \subseteq k(a^p)$, pero como $k \subseteq k(a^p)$, sólo tenemos que verificar que $a \in k(a^p)$. Como a es separable sobre k, entonces a es separable y puramente inseparable sobre $k(a^p)$, por lo tanto por el Corolario 1.3.13 $a \in k(a^p)$ y así $k(a) = k(a^p)$. De esto se sigue que $kk(a)^p = kk^p(a^p) = k(a^p) = k(a)$, y por el Teorema 1.3.14 $k(a)$ es separable sobre k. ■

Corolario 1.3.16. *Si L es una extensión finita separable de k y K es una extensión finita separable de L entonces K es separable sobre k.*

Demostración. Por hipótesis tenemos que $kL^p = L$ y $LK^p = K$. Por lo tanto $K = LK^p = kL^pK^p \subseteq kK^p$ y así $K = kK^p$, y entonces por el Teorema 1.3.14 K/k es separable. ■

Corolario 1.3.17. *Si $a_1, \ldots, a_n$ son elementos de K, los cuales son separables sobre k, entonces $k(a_1, \ldots, a_n)$ es separable sobre k.*

Demostración. Sean

$$k_1 = k(a_1),\ \ldots,\ k_n = k(a_1, \ldots, a_n) = k_{n-1}(a_n).$$

Haremos la demostración por inducción sobre n.
Así por el Corolario 1.3.15, k_1/k es separable. Supongamos que $i > 1$, y k_{i-1}/k es separable, probaremos que k_i/k es separable. Ya que a_i es separable sobre k, este es separable sobre k_{i-1}, entonces por el Corolario 1.3.15, k_i/k_{i-1} es separable y por lo tanto k_i/k es separable por el Corolario 1.3.16. ■

Observación 1.3.18. *El resultado del Corolario 1.3.16 es válido aún cuando los grados de las extensiones son infinitos. Supongamos que k, L y K son como en dicho Corolario, sin asumir algo acerca de las dimensiones, si $a \in K$, sean $b_0, b_1, \ldots, b_r$ los coeficientes de $Irr(a, L)$. Sea $L' = k(b_0, b_1, \ldots, b_r)$ por el Corolario 1.3.17, L' es separable sobre k. Además $Irr(a, L') = Irr(a, L)$ y así a es separable sobre sobre L'. Por el Corolario 1.3.15, $k(a)/L'$ es separable y por el Corolario 1.3.16 , $k(a)/k$ es separable. Entonces a es separable sobre k y ya que a es un elemento arbitrario de K, se sigue que K/k es separable.*

Corolario 1.3.19. *Si K es una extensión arbitraria de k, entonces*

$$K_s = \{a \in K : a \ \ separable \ \ sobre \ \ k\}$$

es un subcampo de K y $k \subseteq K_s$. Este campo es llamado la cerradura separable de k en K.

Sean K una extensión arbitraria de k, $a \in K$ algebraico sobre k, y $p(x) = Irr(a, k)$. Si a no es separable sobre k, entonces $p'(x) = 0$ y así $p(x) \in k[x^p]$, es decir, $p(x) = p_1(x^p)$, donde $p_1(x) \in k[x]$. El polinomio $p_1(x)$ es ciertamente irreducible en $k[x]$ y ,de hecho, $p_1(x) = Irr(a^p, k)$. Ahora, nuevamente a^p es separable sobre k o $p_1(x) = p_2(x^p)$, donde $p_2(x) \in k[x]$, en tal caso $p(x) = p_2(x^{p^2})$. Podemos continuar de esta manera hasta llegar a un polinomio $p_e(x) \in k[x]$, tal que $p(x) = p_e(x^{p^e})$, $p_e(x) =$

$Irr(a^{p^e}, k)$, y $p_e(x) \notin k[x^p]$. Entonces a^{p^e} es separable sobre k y e es el entero mas pequeño no negativo, para lo cual esto es cierto. Concluyendo, si $a \in K$ es algebraico sobre k entonces existe $e \in \mathbb{Z}, e \geqslant 0$ tal que a^{p^e} es separable sobre k. Por lo tanto tenemos el siguiente resultado:

Teorema 1.3.20. *Sea K una extensión algebraica arbitraria de k. Entonces K puede ser obtenida por una extensión separable, seguida de una extensión puramente inseparable.*

Si K/k es algebraica entonces K/K_s es puramente inseparable por lo visto antes del Teorema inmediato anterior. El grado $[K_s : k]$ es llamado el *grado de separabilidad* de K/k y es denotado por $[K : k]_s$. El grado $[K : K_s]$ es llamado el *grado de inseparabilidad* de K/k y es denotado por $[K : k]_i$. Si $[K : k]_i$ es finito, se sigue del Corolario 1.3.10 que este es una potencia de p, la característica de k. Por lo tanto tenemos:

Teorema 1.3.21. *Si K es una extensión finita de k y si $[K : k]$ no es divisible por p, entonces K/k es separable.*

Sea $f(x) \in k[x]$ irreducible de grado n. Sea e el entero no negativo determinado por $f(x) \in k[x^{p^e}]$, pero $f(x) \notin k[x^{p^{e+1}}]$. Sea $n = n_0 p^e$, n_0 es llamado el *grado reducido* de $f(x)$ y p^e el *grado de inseparabilidad* de $f(x)$.

Teorema 1.3.22. *Sea $f(x) \in k[x]$ un polinomio irreducible de grado reducido n_0 y grado de inseparabilidad p^e. Sea a una raíz de $f(x)$ y $k(a)/k$ una extensión simple. Entonces*

$$[k(a) : k]_s = n_o \text{ y } [k(a) : k]_i = p^e.$$

Demostración. Por definición de grado de inseparabilidad de $f(x)$ sabemos que a^{p^e} es separable sobre k y $gr(Irr(a^{p^e}, k)) = n_0$. Por lo tanto $[k(a^{p^e}) : k] = n_0$ y $[k(a) : k(a^{p^e})] = p^e$.
Ya que $k(a^{p^e})/k$ es separable, tenemos que $k(a^{p^e}) \subseteq k(a)_s$.
Sea $b \in k(a)_s$. Entonces b es separable sobre k y así este es separable sobre $k(a^{p^e})$ por el Teorema 1.3.3. Además, b es también puramente inseparable sobre $k(a^{p^e})$. Por lo tanto por el Corolario 1.3.13, $b \in k(a^{p^e})$, así tenemos que $k(a^{p^e}) = k(a)_s$, de lo cual se sigue que $[k(a) : k]_s = n_0$ y ya que $[k(a) : k] = [k(a) : k]_s[k(a) : k]_i = n_0[k(a) : k]_i$ y $[k(a) : k] = gr(f(x)) = n_0 p^e$, tenemos que $[k(a) : k]_i = p^e$ ∎

1.4. Extensiones Normales

Si K es una extensión de k y si un polinomio $f(x) \in k[x]$ se puede factorizar en factores lineales en $K[x]$, entonces diremos que $f(x)$ se descompone en $K[x]$. Es decir, si $f(x)$ se descompone en $K[x]$ tenemos que

$$f(x) = c(x - a_1) \cdots (x - a_n)$$

donde $a_1, \ldots, a_n \in K$.Ahora veamos la multiplicidad de las raíces de $f(x)$, es decir, veamos cuantas veces aparece cada factor lineal en esta factorización de $f(x)$, suponiendo que $f(x)$ es un polinomio mónico e irreducible en $k[x]$.

Teorema 1.4.1. *Sea $f(x) \in k[x]$ un polinomio mónico e irreducible y sea K una extensión de k, tal que $f(x)$ se descompone en $K[x]$. Si $cark = 0$ entonces cada raíz es simple, es decir, cada factor lineal de $f(x)$ en $K[x]$ aparece sólo una vez en la descomposición. Si $cark = p$ y si p^e es el grado de inseparabilidad de $f(x)$, entonces cada raíz de $f(x)$ tiene multiplicidad p^e, es decir, cada factor lineal de $f(x)$ en $K[x]$ aparece exactamente p^e veces en la descomposición.*

Demostración. Si $cark = 0$ el resultado se sigue del hecho de que k no tiene extensiones inseparables. Supongamos que $cark = p$. Tenemos que $f(x) \in k[x^{p^e}]$, pero $f(x) \notin k[x^{p^{e+1}}]$. Sean $f(x) = g(x^{p^e})$ donde $g(x) \in k[x]$ y $x - a$ un factor lineal de $f(x)$ en $K[x]$, entonces $g(a^{p^e}) = 0$ y ya que $g(x) \notin k[x^p]$, a^{p^e} es raíz simple de $g(x)$. Sea $g(x) = (x - a^{p^e})h(x)$, donde $h(a^{p^e}) \neq 0$. Entonces $f(x) = (x^{p^e} - a^{p^e})h(x^{p^e}) = (x - a)^{p^e} h_1(x)$ donde $h_1(x) = h(x^{p^e})$ y así $h_1(a) \neq 0$. ■

Definición 1.4.2. *Sea k un campo y $f(x) \in k[x]$. Una extensión K de k se llama un campo de descomposición de $f(x)$ sobre k, si*

1. *$f(x)$ se descompone en $K[x]$.*

2. *Si L es otra extensión de k, donde $f(x)$ se descompone en $L[x]$ y $L \subseteq K$, entonces $L = K$*
   Las condiciones anteriores son equivalentes a:

3. $K = k(\alpha_1, ..., \alpha_n)$*, donde las* $\alpha_1, \ldots, \alpha_n$ *son las raíces de* $f(x)$*.*

Con esta Definición a la mano, del Corolario 1.1.26 se sigue que:

Proposición 1.4.3. *Si* k *es un campo y* $f(x) \in k[x]$ *es un polinomio de grado* ≥ 1*, entonces existe un campo de descomposición* K/k *de* $f(x)$*, y más aún,* $[K : k] \leq n!$ *donde* $n = gr(f(x))$*.*

Lema 1.4.4. *Sean* $\phi : k \to k'$ *un isomorfismo de campos y* $f(x) \in k[x]$ *un polinomio. Sea* K *un campo de descomposición de* $f(x)$ *sobre* k*, y sea* K' *una extensión de* k' *tal que* $\phi(f(x)) \in k'[x]$ *se factoriza (en factores lineales) en* $K'[x]$*. Entonces, existe un monomorfismo* $\psi : K \to K'$ *tal que* $\psi|_k = \phi$*.*

Demostración. Construiremos el morfismo $\psi : K \to K'$ por inducción sobre $n = gr(f)$.
Como K es el campo de descomposición de $f(x)$ sobre k, entonces en $K[x]$ tenemos que :

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)...(1)$$

donde c es una constante.
Si $m(x) = Irr(\alpha_1, k)$ entonces $m(x)$ es un factor irreducible (en $k[x]$) de $f(x)$ por el Teorema 1.1.16, y como el isomorfismo $\phi : k \to k'$ induce un isomorfismo de anillos $\phi : k[x] \to k'[x]$ de manera natural, entonces $\phi(m(x))|\phi(f(x))$ en $k'[x]$, y además $\phi(m(x))$ es irreducible en $k'[x]$.
Ahora, por hipótesis $\phi(f(x))$ se descompone en $K'[x]$, y como $\phi(m(x))$ es un factor de $\phi(f(x))$ entonces $\phi(m(x))$ también se descompone en $K'[x]$,

$$\phi(m(x)) = (x - \beta_1) \cdots (x - \beta_r),$$

donde $\beta_i \in K'$, $i = 1, \ldots, r$. Notemos que $\phi(m(x))$ es mónico porque $m(x)$ lo es. Ahora como $\phi(m(x))$ es irreducible en $k'[x]$, entonces $\phi(m(x)) = Irr(\beta_i, k')$, para cada $1 \leq i \leq r$.
En particular, para β_1, estamos en la situación

$$\phi : k \to k'$$

isomorfismo de campos donde $\phi(Irr(\alpha_1, k)) = Irr(\beta_1, k')$ y así por el Teorema 1.2.3 existe un isomorfismo

$$\psi_1 : k(\alpha_1) \to k'(\beta_1)$$

tal que $\psi_1|_k = \phi$ y $\psi_1(\alpha_1) = \beta_1$.

Por otra parte,como K es el campo de descomposición de $f(x)$ sobre k, entonces K es el campo de descomposición $g(x) = f(x)/(x - \alpha_1)$ sobre $k(\alpha_1)$. Finalmente, como $gr(g) = n-1 < gr(f)$, por hipótesis de inducción existe un monomorfismo

$$\psi : K \to K'$$

tal que $\psi|_{k(\alpha_1)} = \psi_1$.
y además como $\psi_1|_k = \phi$, entonces $\psi|_k = \phi$. ■

Teorema 1.4.5. *Sea $\phi : k \to k'$ un isomorfismo de campos y $f(x) \in k[x]$ un polinomio. Sea K un campo de descomposición de $f(x)$ sobre k y sea K' un campo de descomposición de $\phi(f(x))$ sobre k'. Entonces existe un isomorfismo $\psi : K \to K'$ tal que $\psi|_k = \phi$.*

Demostración. Tenemos por el lema inmediato anterior que existe un monomorfismo $\psi : K \to K'$ tal que $\psi|_k = \phi$. Sólo falta mostrar que ψ es suprayectiva. Claramente $\psi(K)$ es un campo de descomposición de $\psi(f(x)) = \phi(f(x))$ sobre k', y como $\psi(K) \subseteq K'$, entonces $\psi(K) = K'$ por la definición de campo de descomposición. Entonces ψ es suprayectiva. ■

Corolario 1.4.6. *(**Unicidad del campo de descomposición**) Sea k un campo y $f(x) \in k[x]$ un polinomio. Si K y K' son campos de descomposición de $f(x)$ sobre k, entonces existe un isomorfismo $\psi : K \to K'$ tal que $\psi|_k = id$.*

Definición 1.4.7. *Una extensión K de k es una extensión normal si esta es algebraica sobre k y si cada polinomio irreducible en $k[x]$, el cual tiene una raíz en K, se factoriza en $K[x]$. También decimos que K es normal sobre k o que K/k es normal.*

Teorema 1.4.8. *Una extensión K/k es normal y finita si y sólo si K es el campo de descomposición de algún polinomio $f(x)$ en $k[x]$.*

Demostración. Supongamos que K/k es finita y normal. Entonces $K = k(a_1, \ldots, a_n)$ con $a_i \in K$, $i = 1, \ldots, n$ algebraicos sobre k y sean $m_i(x) = Irr(a_i, k)$. Ya que K/k es normal, cada $m_i(x)$ se descompone en $K[x]$. Por lo tanto $f(x) = m_1(x) \cdots m_n(x)$ se descompone en $K[x]$, y K es obtenida por adjuntar las raíces de $f(x)$ a k. Por lo tanto K es el campo de descomposición de $f(x)$ sobre k.
Ahora supongamos que K es el campo de descomposición de un polinomio $f(x) \in k[x]$. Entonces $[K : k] \leq n!$ donde $n = gr(f(x))$ por el Corolario 1.1.26 y así la extensión K/k es finita.
Probaremos que K/k es normal. Para esto, sea $g(x) \in k[x]$ cualquier polinomio irreducible que tiene una raíz $\alpha_1 \in K$. Queremos ver que K contiene a las otras raíces de $g(x)$. Sea α_2 cualquier otra raíz de $g(x)$. Queremos probar que $\alpha_2 \in K$,o bien queremos probar que $K(\alpha_2) = K$, es decir, que $[K(\alpha_2) : K] = 1$. Ahora, como $\alpha_1 \in K$, entonces $K(\alpha_1) = K$ y así $[K(\alpha_1) : K] = 1$.
Basta probar entonces que

$$[K(\alpha_1) : K] = [K(\alpha_2) : K]$$

Sea $M \supseteq K$ campo de descomposición de $f(x) \cdot g(x)$ sobre k. Así, en particular $\alpha_1, \alpha_2 \in M$. Ahora observemos que:

$$[K(\alpha_1) : K][K : k] = [K(\alpha_1) : k(\alpha_1)][k(\alpha_1) : k]...(1)$$

y

$$[K(\alpha_2) : K][K : k] = [K(\alpha_2) : k(\alpha_2)][k(\alpha_2) : k]...(2)$$

donde por el Teorema 1.2.4 $k(\alpha_1)$ y $k(\alpha_2)$ son isomorfos por ser α_1 y α_2 raíces del mismo irreducible $g(x) \in k(x)$, y así $Irr(\alpha_1, k) = Irr(\alpha_2, k)$, y en consecuencia, por el Teorema 1.2.4 existe un isomorfismo $\phi : k(\alpha_1) \to k(\alpha_2)$ que deja fijo a k y $\phi(\alpha_1) = \alpha_2$. Y así:

$$[k(\alpha_1) : k] = [k(\alpha_2) : k]...(3)$$

Ahora, como $K(\alpha_j)$ es campo de descomposición de $f(x)$ sobre $k(\alpha_j)$ para $j = 1, 2$, por el Teorema 1.4.5 existe un isomorfismo $\psi : K(\alpha_1) \to K(\alpha_2)$ tal que $\psi|_{k(\alpha_1)} = \phi$, y así, en particular

$$[K(\alpha_1) : k(\alpha_1)] = [K(\alpha_2) : k(\alpha_2)]...(4)$$

Sustituyendo (3) y (4) en (1)y (2), se tiene que:

$$[K(\alpha_1) : K] = [K(\alpha_2) : K],$$

■

Teorema 1.4.9. *Sea K una extensión normal finita de k y sean F y L campos entre k y K k-isomorfos . Entonces cada k-isomorfismo de F en L puede ser extendido a un k-automorfismo de K.*

Teorema 1.4.10. *Sea K una extensión finita de k. Entonces existe una extensión normal finita F de k, tal que $K \subseteq F$ y la cual es la extensión normal mas pequeña en el sentido que si L es una extensión normal de k la cual contiene a K, entonces existe un K-monomorfismo de F en L.*

Demostración. Sea $K = k(a_1, \ldots, a_n)$ y sean, para cada $i = 1, ..., n$, $f_i(x) = Irr(a_i, k)$ y $f(x) = f_1(x) \cdots f_n(x)$. Entonces $f(x) \in k[x]$. Sea F un campo de descomposición de $f(x)$ sobre K y sea F_1 el subcampo de F obtenido adjuntando todas las raíces de $f(x)$ en F a k. Entonces $K \subseteq F_1$ y así $F_1 = F$. De esta manera F es un campo de descomposición de $f(x)$ sobre k y, por el Teorema 1.4.8, F/k es normal finita.
Ahora supongamos que L es una extensión normal de k, la cual contiene a K. Para $i = 1 \ldots, n$, $f_i(x)$ tiene una raíz en L, digamos a_i, y por lo tanto se descompone en $L[x]$, por lo que $f(x)$ se descompone en $L[x]$. Entonces L contiene un campo de descomposición de $f(x)$ sobre K el cual por el Corolario 1.4.6 es K-isomorfo a F. ■

Lema 1.4.11. *Sea K/k una extensión finita. Entonces K/k es normal si y sólo si para cualquier extensión L de K tal que L/k es normal: se tiene que todo monomorfismo $\tau : K \to L$ que deja fijo a k es de hecho un k-automorfismo $\tau : K \to K$.*

Demostración. Supongamos que K/k es normal y sea L extensión de K tal que L/k es normal y $\tau : K \to L$ un monomorfismo tal que $\tau|_k = id$. Probaremos que $\tau(K) = K$.
Sea $\alpha \in K$ y sea $p(x) = Irr(\alpha, k) \in k[x]$. Entonces,

$$0 = p(\alpha) = \tau(p(\alpha)) = p(\tau(\alpha)),$$

ya que $p(x) \in k[x]$.
Así, $\tau(\alpha) \in L$ es otra raíz de $p(x)$. Pero como K/k es normal y $p(x) \in k[x]$ es irreducible con $\alpha \in K$ una raíz de $p(x)$, entonces $\tau(\alpha) \in K$. Por lo tanto

$$\tau(K) \subseteq K$$

Además, como $\tau : K \to \tau(K) \subseteq K$ es una función lineal e inyectiva entre k-espacios vectoriales de dimensión finita, entonces de

$$[K : k] = [\tau(K) : k] < \infty \text{ y } \tau(K) \subseteq K$$

con $\tau(K)$ k-subespacio de K, tenemos que $\tau(K) = K$.

Ahora supongamos que $p(x) \in k[x]$ es un polinomio irreducible tal que tiene una raíz $\alpha \in K$ y sea L extensión de k tal que L/k normal y $K \subseteq L$, la cual sabemos que existe por el teorema anterior. Como $\alpha \in K \subseteq L$ y L/k es normal, entonces $p(x)$ se descompone en L. Si $\beta \in L$ es una raíz cualquiera de $p(x)$, entonces por Teorema 1.2.4 existe un k-isomorfismo

$$\tilde{\sigma} : k(\alpha) \to k(\beta)$$

tal que $\tilde{\sigma}(\alpha) = \beta$. Como L/k es normal y finita, entonces por el Teorema 1.4.8, L es el campo de descomposición de algún polinomio $f(x) \in k[x]$. Así, ciertamente, L es el campo de descomposición de $f(x)$ considerado como polinomio en $k(\alpha)[x]$ ó $k(\beta)[x]$. Por el Lema 1.4.4 , existe un monomorfismo $\sigma : L \to L$ tal que $\sigma|_{k(\alpha)} = \tilde{\sigma}$ y así $\sigma(\alpha) = \beta$. Pero $\alpha \in K$, y así

$$\beta = \sigma(\alpha) = \sigma|_{K(\alpha)}(\alpha),$$

y como $\sigma|_K : K \to L$ es un monomorfismo tal que $(\sigma|_K)|_k = id$, por hipótesis se debe tener que $\sigma|_K(K) = K$, es decir, $\beta = (\sigma|_{K(\alpha)})(\alpha) \in K$, esto es , todas las raíces de $p(x)$ están en K, y así concluimos que K/k es normal. ■

Teorema 1.4.12. *Sean K una extensión finita de un campo k y L una extensión normal de k tal que $k \subseteq K \subseteq L$. Sea n_0 el grado de separabilidad de K/k. Entonces existen exactamente n_0 distintos k-monomorfismos de K en subcampos de L*

Corolario 1.4.13. *Si K es una extensión normal finita de K, entonces $o(G(K/k)) = [K : k]_s$*

Teorema 1.4.14. *Sea K una extensión normal finita de k. Sea $a \in K$ y supongamos que a es fijado por cada elemento de $G(K/k)$. Entonces a es puramente inseparable sobre k.*

Demostración. Debemos mostrar que a es la única raíz de $p(x) = Irr(a, k)$ en K: ya que como K/k es normal, $p(x)$ se descompone en $K[x]$.
Sea b otra raíz de $p(x)$ en K. Por el Teorema 1.2.4 existe un k-isomorfismo de $k(a)$ en $k(b)$, tal que manda a en b. Por el Teorema 1.4.9 este k-isomorfismo se puede extender a un k-automorfismo de K, pero por hipótesis a es fijado por cada k-automorfismo de K, por lo tanto $a = b$. ■

Antes de enunciar nuestra última proposición para extensiones normales necesitamos dar una definición y un resultado, que nos serán útiles en la proposición.

Definición 1.4.15. *Un campo k es algebraicamente cerrado, si no tiene extensiones algebraicas propias. Un campo K es llamado una cerradura algebraica de un campo k, si K es extensión algebraica de k y K es algebraicamente cerrado.*

Teorema 1.4.16. *Cada campo k tiene una cerradura algebraica y cualesquiera dos cerraduras algebraicas de k son $k-$isomorfas.*

Proposición 1.4.17. *Si K es una extensión algebraica sobre k, entonces las siguientes afirmaciones son equivalentes:*
1. El campo K es normal sobre k.
2. Si M es una cerradura algebraica de K y si $\tau : K \to M$ es un k-homomorfismo, entonces $\tau(K) = K$.
3. Si $k \subseteq L \subseteq K \subseteq N$ son campos y si $\sigma : L \to N$ es un k- homomorfismo, entonces $\sigma(L) \subseteq K$ y existe $\tau \in G(K/k)$ con $\tau|_L = \sigma$.

1.5. Extensiones de Galois

En esta sección presentamos el teorema que relaciona los conceptos de normalidad y separabilidad de una extensión K/k con la condición de que k sea el campo fijo de $G(K/k)$, recordando que, en general, el campo fijo

de $G(K/k)$ es un campo el cual contiene a k, y no necesariamente es igual a k.

Antes de empezar recordemos algunos hechos de las secciones anteriores:

Sea K es una extensión normal finita de k, si F es el campo fijo de $G(K/k)$, en el Teorema 1.4.14 mostramos que F/k es puramente inseparable. Note que $G(K/F) = G(K/k)$ y así, por el Teorema 1.2.11, $[K : F] = o(G(K/F))$. Además por el Corolario 1.4.13 , $[K : F]_s = o(G(K/F))$. Por lo tanto, $[K : F]_s = [K : F]$, lo cual implica que K/F es separable. Note que $[K : F] = o(G(K/k)) = [K : k]_s$, y así $[F : k] = [K : k]_i$.

Definición 1.5.1. *Una extensión algebraica K de k es llamada una extensión de Galois de k si el campo fijo de $G(K/k)$ es k. En este caso, $G(K/k)$ es llamado el grupo de Galois de la extensión K/k.*

Sea k un campo y sea K una extensión normal y separable de k. Recordemos que esto significa que K/k es algebraica, que cada $a \in K$ es raíz simple de $Irr(a, k)$, y que cada polinomio irreducible en $k[x]$, el cual tiene un raíz en K, se descompone en $K[x]$.

Teorema 1.5.2. *Sea K una extensión finita de k, entonces K es una extensión de Galois si y sólo si K es normal y separable.*

Demostración. Sea K una extensión finita de Galois de k y sea $G(K/k) = \{\sigma_1, \ldots, \sigma_n\}$, que sabemos es un grupo finito, por el Corolario 1.2.8.

Sea $a \in K$ tal que $a \notin k$, y sean $a_1 = a, a_2, \ldots, a_r$ las distintas imágenes de a bajo los σ_1. Ya que $G(K/k)$ es un grupo, si aplicamos uno de sus elementos, digamos σ_i, al elemento $a_j = \sigma_j(a)$, obtenemos

$$\sigma_i(a_j) = \sigma_i\sigma_j(a) = \sigma_h(a),$$

donde $\sigma_h = \sigma_i\sigma_j$. De esta manera los elementos de $G(K/k)$ permutan a los elementos $a_1, \ldots, a_r$ de K en sí mismos. Por lo tanto cada coeficiente de $f(x) = (x - a_1)\cdots(x - a_r)$, pertenece al campo fijo de $G(K/k) = k$. Sea $g(x)$ un factor irreducible de $f(x)$ en $k[x]$ tal que, digamos, $g(a_i) = 0$. Si $a_i = \sigma_i(a)$ y $a_j = \sigma_j(a)$, entonces $a_j = \sigma_j\sigma_i^{-1}(a_i)$, así que $g(a_j) = 0$. Así cada raíz de $f(x)$ es raíz de $g(x)$. Esto implica que $f(x)$ es irreducible en $k[x]$. Hemos mostrado que cada $a \in K$ es una raíz simple de $Irr(a, k)$

y que $Irr(a,k)$ se descompone en $K[x]$. Así K/k es normal y separable.
Inversamente, supongamos que K/k es finita, normal y separable. Sea F el campo fijo de $G(K/k)$. Entonces $[F:k] = [K:k]_i = 1$ y $F = k$ por lo visto al principio de la sección. ■

Proposición 1.5.3. *Supongamos que K/k es una extensión normal y separable y sea σ un k-monomorfismo de K en sí mismo. Entonces σ es un k-automorfismo de K.*

Demostración. Sea $a \in K$ y sea $f(x) = Irr(a,k)$. Ya que $f(x)$ tiene una raíz en K, a saber "a", este se factoriza en $K[x]$, por ser K extensión normal de k. Por lo tanto existe un campo de descomposición L de $f(x)$ tal que $k \subseteq L \subseteq K$: L es extensión normal y finita de k y $a \in L$. Sabemos que $k \subseteq \sigma(L) \subseteq L$ y que $[\sigma(L):k] = [L:k]$ y así $\sigma(L) = L$.
Por lo tanto existe $b \in L$ tal que $\sigma(b) = a$. ■

Proposición 1.5.4. *Sean K/k normal y separable y L extensión de k tal que $k \subseteq L \subseteq K$ y además sea σ un k-monomorfismo de L en K. Entonces existe un k-automorfismo τ de K tal que $\tau(a) = \sigma(a)$ para todo $a \in L$. Esto es, cada k-monomorfismo de L en K es la restricción de un k-automorfismo de K.*

Demostración. Sea
$\mathbb{F} = \{(F,\rho) | L \subseteq F \subseteq K \ \ \rho : F \to K \ un \ k-monomorfismo \ tal \ que \ \rho(a) = \sigma(a) \ \ \forall a \in L\}$
Para $(F_1,\rho_1),(F_2,\rho_2) \in \mathbb{F}$ definimos:
$(F_1,\rho_1) \leq (F_2,\rho_2)$ si y sólo si $F_1 \subseteq F_2$ y $\rho_2(a) = \rho_1(a)$ para todo $a \in F_1$
$\mathbb{F}$ es no vacío ya que $(L,\sigma) \in \mathbb{F}$ y no es difícil demostrar que $\leq$ es un orden parcial en $\mathbb{F}$. Mostraremos que $\mathbb{F}$ tiene un maximal usando el Lema de Zorn.
Si C es una cadena en $\mathbb{F}$, sea $N = \bigcup_{(F,\rho)\in C} F$.
Es claro que N es un campo intermedio entre L y K y sea $\phi : N \to K$ definido como sigue:
Dado $x \in N$, se tiene que $x \in F$, para algún $(F,\psi) \in C$. Definimos $\phi(x) = \psi(x)$.
ϕ esta bien definida, puesto que: si $x \in F$ y $x \in F'$ con $(F',\zeta),(F,\psi) \in C$, entonces, por ser C cadena:

$$(F', \zeta) \leq (F, \psi) \text{ o } (F, \psi) \leq (F', \zeta)$$

y en cualquiera de los dos casos $\zeta(x) = \psi(x)$.
$(N, \phi) \in \mathbb{F}$, ya que si $a \in L$, entonces $\phi(a) = \sigma(a)$. Por lo tanto por el Lema de Zorn $\mathbb{F}$ tiene un maximal (F', ρ'). Afirmamos que $F' = K$.
Supongamos que existe $a \in K$ tal que $a \notin F'$. Entonces $Irr(a, k)$ se descompone en $K[x]$ y tenemos $Irr(a, k) = f(x)g(x)$, donde $f(x) = Irr(a, F')$ y $g(x) \in F'[x]$. Entonces

$$Irr(a, k) = (\rho' f)(x)(\rho' g)(x)$$

y así $(\rho' f)(x)$ se descompone en $K[x]$.
Sea a_1 una raíz de $(\rho' f)(x)$ en K. Entonces existe un isomorfismo

$$\rho'' : F'(a) \to (\rho'(F'))(a_1)$$

tal que $\rho''(a) = a_1$ y $\rho''(b) = \rho'(b) \ \ \forall \ \ b \in F'$ Así $(F'(a), \rho'') \in C$ y es estrictamente mas grande que (F', ρ'), lo cual es una contradicción.
Entonces $F' = K$ y por la proposición anterior ρ' es un k-automorfismo de K y, así, es el τ deseado. ■

Ahora damos la generalización del Teorema 1.5.2, es decir, demostramos que el Teorema se cumple aún cuando la extensión no sea de grado finito.

Teorema 1.5.5. *Una extensión K de k es una extensión de Galois si y sólo si K es una extensión normal y separable de k.*

Demostración. Primero supongamos que K/k es normal y separable.
Demostremos que K/k es de Galois.
Sabemos que $k \subseteq F(G(K/k))$. Sea $a \in F(G(K/k))$, el campo fijo de $G(K/k)$. Como en la prueba de la Proposición 1.5.3 existe una extensión normal finita L de k con $k \subseteq L \subseteq K$ y $a \in L$.
Sea $\sigma \in G(L/k)$. Por la Proposición 1.5.4 existe un elemento $\tau \in G(K/k)$ tal que $\tau(b) = \sigma(b) \ \ \forall \ \ b \in L$. En particular $\tau(a) = \sigma(a) = a$ y así a está en el campo fijo de $G(L/k)$. Pero L es una extensión finita normal y separable, y por el Teorema 1.5.2, L es extensión de Galois, es decir, el campo fijo de $G(L/k)$ es k, y por lo tanto $a \in k$.
Ahora supongamos que K es una extensión de Galois, entonces esta es algebraica. Sea $a \in K$ y sea $f(x) = Irr(a, k)$. Sean $a = a_1, a_2, \ldots, a_n$ las

distintas imágenes de a bajo los k-automorfismos de K. Entonces $f(a_i) = 0$ para $i = 1, \ldots, n$ y así si $g(x) = (x - a_1) \cdots (x - a_n)$ vemos que $g(x)|f(x)$ en $K[x]$. Sin embargo, cada coeficiente de $g(x)$ es fijado por cada elemento de $G(K/k)$ por lo que $g(x) \in k[x]$. Pero ya que $g(x)$ divide a $f(x)$ en $k[x]$ y ya que $f(x)$ es mónico e irreducible en $k[x]$, se sigue que $f(x) = g(x)$.
Por lo tanto a es separable sobre k y concluimos que K/k es separable.
Si consideramos a $f(x)$ como el múltiplo constante mónico de un polinomio arbitrario irreducible no constante en $k[x]$, el cual tiene una raíz en K, vemos que tales polinomios se descomponen en $K[x]$. Por lo tanto K/k es normal. ■

1.6. El teorema del elemento primitivo

En esta sección determinamos bajo qué condiciones una extensión finita K de k es simple, es decir, $K = K(a)$ para algún $a \in K$. Para que podamos enunciar y demostrar este teorema necesitamos tener un resultado para campos finitos, así que comenzamos la sección dando este resultado.

Sea K un campo finito. Ya que el campo primo de un campo de característica cero es infinito, K debe ser de característica un primo, digamos que $car k = p$. Podemos suponer que el campo primo de K es de hecho el campo de clases residuales de enteros modulo p, el cual es denotado por $\mathbb{Z}_p$ (Teorema 1.1.10). Como K tiene sólo un número finito de elementos es ciertamente una extensión finita de $\mathbb{Z}_p$.
Sea $[K : \mathbb{Z}_p] = n$ y sea $\{a_1, ..., a_n\}$ una base de K sobre $\mathbb{Z}_p$. Entonces K consiste de todas las expresiones de la forma

$$c_1a_1 + c_2a_2 + \cdots + c_na_n, \text{ donde } c_1, ..., c_n \in \mathbb{Z}_p.$$

Así K tiene exactamente p^n elementos.
Sean $b_1, ..., b_{p^n}$ todos los elementos de K y sea $h = p^n - 1$.
El grupo multiplicativo de K es un grupo finito de orden h y así $b_i^h = 1$ para toda $b_i \neq 0$ y así $b_i^{p^n} = b_i$ en K para todo $i = 1, ..., p^n$ (incluyendo $b_i = 0$). Entonces el polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$ y teniendo en cuenta que, por otro lado, tiene a lo más p^n raíces se concluye que, K es el campo de descomposición, sobre su campo primo, de $x^{p^n} - x$. Por lo tanto hemos probado:

Teorema 1.6.1. *Si K es un campo finito de característica p y si K tiene grado n sobre su campo primo, entonces K tiene p^n elementos. Cualesquiera dos campos que tienen p^n elementos son isomorfos: si ellos contienen a $\mathbb{Z}_p$, entonces son $\mathbb{Z}_p-$isomorfos.*

Denotaremos a un campo que tenga p^n elementos por K_{p^n}.

Teorema 1.6.2. *El grupo multiplicativo de un campo finito es cíclico.*

Demostración. Sean K_{p^n} y $h = p^n - 1 = q_1^{r_1} \cdots q_m^{r_m}$, donde los q_i son primos distintos dos a dos. El grupo multiplicativo de K_{p^n} tiene orden h y por lo tanto nuestra tarea es encontrar un elemento de orden h en este grupo.
Si $h_i = h/q_i$, ya que $h_i < h$ existe un elemento $0 \neq b_i \in K_{p^n}$, el cual no es una raíz de $x^{h_i} - 1$.
Para cada $i = 1, \ldots, m$, sea $a_i = b_i^{h/q_i^{r_i}}$ y $a = a_1 \cdots a_m$. Tenemos $a_i^{q_i^{r_i}} = b_i^h = 1$ y de esta manera el orden de a_i divide a $q_i^{r_i}$. Si $a_i^{q_i^{r_i-1}} = 1$, entonces $b_i^{h/q_i} = 1$ lo cual es una contradicción por la condición que cumple b_i. Por lo tanto el orden de a_i es exactamente $q_i^{r_i}$.
Ya que $a^h = 1$, el orden de a divide a h.
Supongamos que este orden no es h, entonces existe algún primo divisor de h, digamos q_1, tal que $q_1^{r_1}$ no divide al orden de a.
Entonces tenemos que $1 = a^{h/q_1} = a_1^{h/q_1} a_2^{h/q_1} \cdots a_m^{h/q_1}$. Ya que $q_i^{r_i}$ divide a $\frac{h}{q_1}$ para $i = 2, ..., m$, tenemos que $a_i^{h/q_1} = 1$ para $i = 2, ..., m$, entonces $a_1^{h/q_1} = 1$. Esto implica que $q_1^{r_1}$, el orden de a_1, divide a h/q_1, lo cual es falso, por la forma que tiene h. Así a tiene orden h y nuestra tarea esta completa. ■

Sea K una extensión algebraica de k. Un elemento $a \in K$ es llamado un *elemento primitivo* de K (con respecto a k) si $K = k(a)$.

Teorema 1.6.3. *Una extensión finita K/k es simple, si y sólo si tiene un número finito de campos intermedios.*

Demostración. Si $K = k(a)$, sea $f(x) = Irr(a, k) \in k[x]$, y sea M cualquier campo intermedio. Sea $g(x) = Irr(a, M) \in M[x]$. Adjuntando los coeficientes de $g(x)$ a k se obtiene otro campo intermedio M' entre k y M.

Entonces, $g(x) \in M'[x]$ y claramente es irreducible sobre M' ya que lo es sobre M. Se sigue que $g = Irr(a, M')$. Ahora , como $K = k(a)$ entonces $K = M(a)$ y $K = M'(a)$ también, y así por el Teorema 1.1.18 tenemos que

$$[K : M] = gr(Irr(a, M)) = gr(g(x)) = gr(Irr(a, M')) = [K : M'],$$

y como $M' \subseteq M$, entonces $M = M'$.
Por lo tanto, el campo intermedio M está unívocamente determinado por el polinomio $g(x) = Irr(a, M)$, y como $g(x)|Irr(a, k) = f(x)$ y $f(x)$ es mónico, sólo hay un número finito de posibilidades para $g(x)$, es decir, sólo existe un número finito de campos intermedios M entre K y k.

Ahora supongamos que sólo existe un número finito de campos intermedios entre k y K.

Caso 1. Si k es un campo finito, como K/k es una extensión finita, entonces K también es un campo finito, y así por el Teorema 1.6.2, $K^* = K - 0$ es un grupo cíclico, digamos generado por $a \in K$, y por lo tanto $K = k(a)$.
Caso 2. Si k es un campo infinito; para cada $a \in K$, $k(a)$, es un campo intermedio entre k y K:
como K/k es finita, entonces $[k(a) : k]$ es finito. Sea $a \in K$ tal que $[k(a) : k]$ es *máximo*, tal extensión existe ya que K/k es finita. Mostraremos que $K = k(a)$. En efecto, sea $b \in K$ y consideremos los siguientes campos intermedios entre $k(a)$ y K:

$$k(a + rb) \text{ con } r \in k.$$

Como k es infinito, hay una infinidad de tales $r \in k$, pero como por hipótesis sólo existe un número finito de campos intermedios entre k y K, entonces existen $r_1 \neq r_2$ en k tales que

$$k(a + r_1b) = k(a + r_2b).$$

Ahora,

$$(r_1 - r_2)b = (a + r_1b) - (a + r_2b) \in k(a + r_1b) = k(a + r_2b),$$

y como

$$0 \neq r_1 - r_2 \in k \subseteq k(a + r_1b) = k(a + r_2b)$$

entonces $b \in k(a + r_1b) = k(a + r_2b)$, y así

$$a = (a + r_1 b) - r_1 b \in k(a + r_1 b) = k(a + r_2 b),$$

es decir $k(a, b) \subseteq k(a + r_1 b)$, y como claramente $k(a + r_1 b) \subseteq k(a, b)$, entonces

$$k(a, b) = k(a + r_1 b),$$

es decir, la extensión $k(a, b)/k$ es simple, y como $k(a) \subseteq k(a, b)$, entonces por la maximalidad de $[k(a) : k]$ se sigue que

$$[k(a, b) : k] = [k(a) : k]$$

y por la tanto $k(a) = k(a, b)$, y así $b \in k(a)$, es decir $K = k(a)$. ■

Teorema 1.6.4. *(**Teorema del elemento primitivo**) Si K/k es una extensión finita y separable, entonces es simple.*

Demostración. Mostraremos que si K es una extensión finita separable de k, entonces existe sólo un número finito de campos entre k y K y así por el teorema anterior esta será una extensión simple.

Por el Teorema 1.4.10 existe una extensión normal finita más pequeña F de k tal que $k \subseteq K \subseteq F$. Se sigue de la demostración del Teorema 1.4.10 que F es separable sobre k, esto es por como se construyo F y por que K/k es separable. Consideremos el grupo $G(F/k)$: por el Corolario 1.4.13 este es un grupo finito de orden $[F : k]$.
Sea L un campo entre k y F. El grupo $G(F/L)$ es un subgrupo de $G(F/k)$. Sea M otro campo entre k y F con $M \neq L$. Supongamos sin pérdida de generalidad que existe un elemento $a \in M$ tal que $a \notin L$. Ya que F es separable sobre L existe un elemento $\sigma \in G(F/L)$ tal que $\sigma(a) \neq a$. Esto muestra que $G(F/L) \neq G(F/M)$ y de esta manera existe una correspondencia uno a uno $L \to G(F/L)$ del conjunto de todos los campos entre k y F en el conjunto de todos los subgrupos de $G(F/k)$. Como $G(F/k)$ tiene sólo un número finito de subgrupos, existe únicamente un número finito de campos entre k y F. Dado que cualquier campo entre k y K está también entre k y F, existe sólo un número finito de campos entre k y K.

■

Corolario 1.6.5. *Si $car k = 0$ y K/k es finita, entonces es simple.*

Capítulo 2

Grupos Topológicos

En este capítulo presentaremos una breve recopilación de los principales resultados de Topología general y no daremos las demostraciones de todos los resultados, ya que la mayoría de estos temas se estudian en un curso básico de Topología.

2.1. Espacios Topológicos

Definición 2.1.1. *Una estructura topológica o topología en un conjunto X es una estructura dada por un conjunto τ de subconjuntos de X que satisfacen las siguientes propiedades:*

1. *$X \in \tau$ y $\emptyset \in \tau$*
2. *Si $U, V \in \tau$, entonces $U \cap V \in \tau$,*
3. *Si $\{U_i\}_{i \in I}$ es una colección de subconjuntos de X tal que cada $U_i \in \tau$ para toda $i \in I$, entonces $\bigcup_{i \in I} U_i \in \tau$.*

Definición 2.1.2. *Un espacio topológico es un conjunto con una estructura topológica, y será denotado por (X, τ).*

Los conjuntos de τ son llamados conjuntos abiertos de la estructura topológica definida por τ en X.

Ejemplo 2.1.3. *Sea X un conjunto. Entonces la familia de todos los subconjuntos de X forman una topología en X. Esta topología consistente de todos los subconjuntos de X es llamada la topología discreta en X. En esta topología todos los conjuntos son abiertos.*

Ejemplo 2.1.4. *Si X es cualquier conjunto, entonces la colección $\{X, \emptyset\}$ forman una topología en X. Esta topología es llamada la topología trivial o topología indiscreta en X. En esta topología los únicos conjuntos abiertos son X y $\emptyset$.*

En un espacio topológico (X, τ) diremos que un subconjunto C de X es *cerrado* si $X - C$ es abierto. Evidentemente en cualquier topología τ sobre X, $\emptyset$ y X son ambos, abiertos y cerrados.

Proposición 2.1.5. *Sea (X, τ) un espacio topológico. Entonces los conjuntos cerrados de una topología satisfacen las siguientes propiedades:*

1. *X y $\emptyset$ son conjuntos cerrados.*
2. *Si A y B son conjuntos cerrados, entonces $A \cup B$ es cerrado.*
3. *Si $\{A_i\}$ es una colección de conjuntos cerrados, entonces $\bigcap_i A_i$ es cerrado.*

Proposición 2.1.6. *Sea X cualquier conjunto, y supongamos que F es una familia de subconjuntos de X tales que:*

1. *X y $\emptyset$ están en F.*
2. *Si A y B están en F, entonces $A \cup B$ es un miembro de F.*
3. *Si $\{A_i\}$ es una colección de miembros de F, entonces $\bigcap_i A_i$ es un miembro de F.*

Si ahora definimos que un subconjunto U de X es abierto si y sólo si $U = X - C$, donde C es algún elemento de F, entonces el conjunto τ de conjuntos abiertos así formados, es una topología en X, la cual tiene a F como el conjunto de subconjuntos cerrados de X.

Ahora daremos otros métodos para determinar una topología en un conjunto dado.

Definición 2.1.7. *Sea (X, τ) un espacio topológico, una colección B de subconjuntos abiertos de X, es decir, $B \subseteq \tau$, es una base para la topología τ si cada conjunto abierto $G \in \tau$ es una unión de elementos de B. A cada elemento de B se le llama abierto básico.*

Proposición 2.1.8. *Supongamos que (X, τ) es un espacio topológico y que B es una base para τ. Entonces la intersección de cualesquiera dos miembros de B es la unión de miembros de B, y el mismo X es la unión de miembros de B.*

Ahora nos preguntamos, cuándo una colección de subconjuntos de un conjunto X es una base para una topología en X. La siguiente proposición responde esta pregunta.

Proposición 2.1.9. *Sea X un conjunto. Supongamos que B es una familia de subconjuntos de X tal que:*

1. *X es la unión de miembros de B, es decir, para todo $x \in X$ existe $U \in B$ tal que $x \in U$;*

2. *La intersección de cualesquiera dos miembros de B es la unión de miembros de B, es decir, para cualesquiera $U_1, U_2 \in B$ y todo punto $x \in U_1 \cap U_2$ existe $U \in B$ tal que $x \in U \subseteq U_1 \cap U_2$.*

Definimos $\tau = \{U \subset X | U \text{ es la union de miembros de } B\}$. Entonces τ es una topología en X y B es una base para τ. (La topología τ para la cual, B es una base es, de hecho, única)

Ejemplo 2.1.10. *Sean X y Y espacios topológicos. Entonces al producto $X \times Y$ podemos dar una topología de la siguiente forma. Definimos a un subconjunto de $X \times Y$ como abierto si es una unión de conjuntos de la forma $U \times V$, donde U es un subconjunto abierto de X y V es un subconjunto abierto de Y; esto es, la colección C de estos subconjuntos es una base para la topología. Es fácil verificar que esta colección satisface las condiciones para ser una base. Si $(x, y) \in (U \times V) \cap (U' \times V')$, entonces $(U \cap U') \times (V \cap V') = (U \times V) \cap (U' \times V')$ es un conjunto abierto básico que contiene a (x, y). Esta topología en $X \times Y$ es llamada la topología producto.*

Ejemplo 2.1.11. *Sea I un conjunto, y sea $\{X_i\}_{i\in I}$ una colección de espacios topológicos. Podemos generalizar la construcción anterior para definir la topología en $\prod_i X_i$. Si I es infinito, entonces necesitamos un paso extra en la definición. Consideremos el conjunto S de todos los subconjuntos de $\prod_i X_i$ de las forma $\prod_i U_i$, donde U_i es abierto en X_i y $U_i = X_i$ para todos, excepto un número finito de i. Si I es no finito, entonces sea C la colección de todos los conjuntos que son intersecciones finitas de elementos de S. Así C forma una base para la topología en $\prod_i X_i$. Llamaremos a esta la topología producto en $\prod_i X_i$.*

Definición 2.1.12. *Sea (X, τ) un espacio topológico y $A \subseteq X$.*
Una vecindad de A es cualquier subconjunto de X el cual contiene un conjunto abierto que contiene a A. Las vecindades de un subconjunto $\{x\}$ (consistente de un sólo punto) son también llamadas vecindades del punto x.

Definición 2.1.13. *Una familia $B(x)$ de vecindades de x es una base local en x en el espacio topológico (X, τ), si para toda vecindad V de x existe $U \in B(x)$ tal que $x \in U \subseteq V$.*

Como un resultado inmediato tenemos:

Proposición 2.1.14. *Un conjunto es vecindad de cada uno de sus puntos si y sólo si este es abierto.*

Definición 2.1.15. *Supongamos que (X, τ) es un espacio topológico, y supongamos que para cada punto $x \in X$ existe una colección η_x de conjuntos abiertos, con las siguientes propiedades:*

1. *$\eta_x \neq \emptyset$.*
2. *$x \in N$ para cada $N \in \eta_x$.*
3. *Si $N_1, N_2 \in \eta_x$, entonces existe $N_3 \in \eta_x$ tal que $N_3 \subseteq N_1 \cap N_2$.*
4. *Dado $N \in \eta_x$ y cualquier $y \in N$, existe $N' \in \eta_y$ tal que $N' \subseteq N$.*
5. *Un subconjunto U de X es abierto si y sólo si para cada cada $x \in U$, existe $N \in \eta_x$ tal que $N \subseteq U$.*

Entonces la colección de η_x (uno por cada $x \in X$) es llamado un sistema fundamental de vecindades abiertas para τ.

Definición 2.1.16. *Sea $A \subseteq X$, donde (X, τ) es un espacio topológico.*

- *La cerradura de A, denotada por $\bar{A}$, es la intersección de todos los conjuntos cerrados que contienen a A.*
- *El interior de A, denotado por A^0, es la unión de todos los conjuntos abiertos los cuales están contenidos en A.*
- *La frontera de A, denotada por $Fr(A)$ es el conjunto*

$$\{x | \text{cada abierto el cual contiene a } x \text{ contiene puntos de } A \text{ y de } X - A\}$$

El conjunto que es de nuestro interés es la cerradura de un conjunto,así que daremos unos resultados relacionados a este concepto.

Proposición 2.1.17. *Sea (X, τ) un espacio topológico, y sea $A \subseteq X$.*

1. *Si C es cualquier conjunto cerrado que contiene a A, entonces $\bar{A} \subseteq C$.*
2. *Si U es un conjunto abierto con $U \cap \bar{A} \neq \emptyset$, entonces $U \cap A \neq \emptyset$.*

Una consecuencia de esta proposición es que un elemento $x \in X$ está en la cerradura de un subconjunto A, si para cualquier abierto U tal que $x \in U$, tenemos que $U \cap A \neq \emptyset$. Esta es una forma útil para determinar cuándo un elemento está en $\bar{A}$.

Definición 2.1.18. *Si X y Y son espacios topológicos, entonces la función $f : X \to Y$ es continua si $f^{-1}(V)$ es abierto en X para cualquier conjunto abierto V en Y.*

Proposición 2.1.19. *Una función f de un espacio topológico (X, τ) en un espacio (Y, τ') es continua si y sólo si dado cualquier $f(x) \in Y$ y cualquier vecindad V de $f(x)$, existe una vecindad U de x tal que*

$$f(U) \subseteq V.$$

Sea X un espacio topológico, y sea R una relación de equivalencia en X, entonces R determina una partición de X en clases de equivalencia. Sea X^* el conjunto de clases de equivalencia, y para $x \in X$ denotemos la clase de equivalencia de x por $\bar{x}$. Tenemos una función natural suprayectiva

$$\begin{aligned} \pi : X &\to X^* \\ \pi(x) &= \bar{x} \end{aligned}$$

Definimos la *topología cociente* en X^* como sigue: Un subconjunto Y de X^* es abierto si $\pi^{-1}(Y)$ es abierto en X. Esto es, la topología cociente τ^* en X^* es $\tau^* = \{Y \subseteq X^* | \pi^{-1}(Y) \in \tau\}$. Obsérvese que según la definición de la topología cociente, la función π definida arriba es continua.

Definición 2.1.20. *Una función continua f de un espacio topológico (X, τ) en un espacio (Y, τ') es cerrada (abierta) si para todo subconjunto cerrado (abierto) $A \subseteq X$ su imagen $f(A)$ es cerrada (abierta) en Y.*

Si una función f de un conjunto X en un conjunto Y es biyectiva, entonces f^{-1} es una función de Y a X. Si X y Y son además espacios topológicos y si f es continua, no necesariamente f^{-1} es continua. Así tenemos la siguiente definición.

Definición 2.1.21. *Sea f una función de un espacio topológico (X, τ) en un espacio (Y, τ'). La función f es un homeomorfismo si es biyectiva, continua y f^{-1} es también continua.*
Si existe un homeomorfismo entre los espacios (X, τ) y (Y, τ'), decimos que X y Y son homeomorfos.

Proposición 2.1.22. *Sea f una función biyectiva de un espacio (X, τ) en un espacio (Y, τ). Entonces las siguientes afirmaciones son equivalentes:*

1. *f es un homeomorfismo.*

2. *Un subconjunto U de Y es abierto si y sólo si $f^{-1}(U)$ es abierto en X.*

3. *Un subconjunto F de Y es cerrado si y sólo si $f^{-1}(F)$ es cerrado en X.*

4. *Si B es una base para τ, entonces $f(B) = \{f(C)|C \in B\}$ es una base para τ'.*

2.2. Filtros

Recordemos primero que:

Definición 2.2.1. *Una sucesión $\{x_n|n \in \mathbb{N}\}$ de puntos de un espacio topológico X converge a un punto $x \in X$ si para toda vecindad V de x existe $m \in \mathbb{N}$ tal que $x_k \in V$ para toda $k \geq m$.*

Existe una aproximación alternativa al concepto de convergencia en un espacio topológico en general, a través de la noción de filtro. Introducimos la noción de filtros y estudiamos algunas de sus propiedades básicas.

Definición 2.2.2. *Sea X un conjunto. Un filtro en X es un conjunto F de subconjuntos de X los cuales tienen las siguientes propiedades:*

1. *$F \neq \emptyset$.*

2. *$\emptyset \notin F$*

3. *Si $A \in F$ y $A \subseteq B$, entonces $B \in F$.*

4. *Cada intersección finita de conjuntos de F pertenece a F.*

Si (X, τ) es un espacio topológico y F es un filtro en X, decimos que F *converge* a x, o que x es un *punto límite* de F denotado por $F \to x$, si cada vecindad de x es un miembro de F. Decimos que $x \in X$ es un *punto de adherencia* de un filtro F si cada vecindad de x interseca a cada miembro de F. Es decir, $F \to x$ si y sólo si dada cualquier vecindad U de x, $U \in F$ y x es punto de adherencia de F si y sólo si dada cualquier vecindad U de x, y cualquier $A \in F$, debe ser $U \cap A \neq \emptyset$.

Ejemplo 2.2.3. *Si $X \neq \emptyset$ el conjunto de todos los subconjuntos de X es un filtro en X.*

Ejemplo 2.2.4. *Si X es cualquier conjunto y Y es cualquier subconjunto no vacío de X, entonces la familia F de todos los subconjuntos de X, los cuales contienen a Y es un filtro en X.*

Sean (X, τ) un espacio topológico, $x \in X$ y $T(X, x)$ la familia de todas las vecindades de x, si $T^*(X, x)$ es la familia de todos los subconjuntos A de X tal que A contiene una vecindad de x, entonces $T^*(X, x)$ es un filtro en X, llamado el *filtro vecindad* de x. Además, ya que $T(X, x) \subseteq T^*(X, x)$,

$$T^*(X, x) \to x.$$

Ejemplo 2.2.5. *Sea X un conjunto y sea D una colección no vacía de subconjuntos no vacíos de X con la propiedad que si B y B' están en D, entonces existe $B'' \in D$ tal que $B'' \subseteq B \cap B'$. Sea*

$$F = \{A \subseteq X | A \supseteq B \ \ para \ \ algun \ \ B \in D\}$$

Entonces F es un filtro en X. Decimos que F es un filtro generado por D y que D es una base del filtro F.

Es decir, una familia no vacía de subconjuntos D de un conjunto X es una *base del filtro* si $\emptyset \notin D$ y para toda pareja $B, B' \in D$ existe $B'' \in D$ tal que $B'' \subseteq B \cap B'$.

Proposición 2.2.6. *Supongamos que F es un filtro en un espacio topológico (X, τ). Entonces x es un punto límite de F si y sólo si existe en filtro F' tal que $F \subseteq F'$ y $F' \to x$*

Definición 2.2.7. *Dados dos filtros F y F' en el mismo conjunto X, decimos que F' es mas fino que F, si $F \subseteq F'$. Si también $F \neq F'$, entonces F' es estrictamente mas fino que F*

Definición 2.2.8. *Un ultrafiltro en un conjunto X es un filtro F tal que no existe filtro en X el cual sea estrictamente mas fino que F. Es decir un filtro F es un ultrafiltro en X si dado cualquier filtro F' mas fino que F, entonces $F = F'$.*

En otras palabras un ultrafiltro es un elemento maximal en el conjunto parcialmente ordenado de todos los filtros.

Ejemplo 2.2.9. *Sea X cualquier conjunto y sea $x \in X$. Entonces la familia de todos los subconjuntos de X los cuales contienen a x forman un ultrafiltro F en X. Ya que si F' es cualquier filtro mas fino que F y $A' \in F'$, entonces o, $x \in A'$ o $x \notin A'$. Ahora si $x \in A'$, entonces $A' \in F$. Si $x \notin A'$; entonces $x \in X - A'$; por lo tanto $X - A' \in F \subseteq F'$. Pero, entonces*

$$A' \cap (X - A') = \emptyset \in F',$$

lo cual contradice el hecho de que cada miembro de F' es no vacío. Por lo tanto x es un elemento de cada miembro de F'; así $F' \subseteq F$, y por lo tanto

$$F = F'$$

Proposición 2.2.10. *Una condición necesaria y suficiente para que un filtro F en un conjunto X sea un ultrafiltro es que dado cualquier subconjunto A de X debe tenerse que*

$$A \in F \quad o \quad X - A \in F.$$

Proposición 2.2.11. *Si X es cualquier conjunto, entonces cada filtro F en X está contenido en un ultrafiltro.*

Proposición 2.2.12. *Sea F un ultrafiltro en un conjunto X. Si A y B son dos subconjuntos de X tal que $A \cup B \in F$, entonces $A \in F$ o $B \in F$.*

Corolario 2.2.13. *Si la unión de una sucesión finita $(A_i)_{1 \leq i \leq n}$ de subconjuntos de X pertenece a un ultrafiltro F, entonces al menos uno de los subconjuntos A_i pertenece a F.*

Proposición 2.2.14. *Si F es un ultrafiltro en un espacio topológico (X, τ) y x es un punto de adherencia de F, entonces $F \to x$.*

2.3. Propiedades Topológicas

Hay varias propiedades topológicas que necesitamos discutir.

Definición 2.3.1. *Sea X un espacio topólógico. Decimos que X es un espacio Hausdorff si para cualesquiera dos puntos distintos $x, y \in X$, existen conjuntos abiertos, ajenos U y V en X, con $x \in U$ y $y \in V$*

Teniendo esta definición y recordando la noción de filtros, tenemos el siguiente resultado:

Teorema 2.3.2. *Sea (X, τ) un espacio topológico, X es un espacio Hausdorff si y sólo si cada filtro convergente en X, tiene un único punto límite.*

Ejemplo 2.3.3. *Sea τ la topología en la recta real $\mathbb{R}$ donde los conjuntos abiertos son uniones de los intervalos $(a, b]$, entonces $(\mathbb{R}, \tau)$ es Hausdorff, ya que si tomamos $a, b \in \mathbb{R}$ con $a \neq b$, digamos $a < b$, y escogemos $U = (a-1, a]$ y $V = (a, b]$. Entonces*

$$U, V \in \tau,\ a \in U,\ b \in V \text{ y } U \cap V = \emptyset$$

Así $(\mathbb{R}, \tau)$ es Hausdorff.

Definición 2.3.4. *Si X es un espacio topológico, una cubierta abierta de X es una colección de conjuntos abiertos cuya unión es X. Si $\{U_i\}$ es una cubierta abierta de X, una subcubierta finita es un subconjunto finito de la colección, cuya unión es también X.*

Ejemplo 2.3.5. *Sea X un conjunto con la topología discreta. Entonces $\{\{x\} | x \in X\}$ es una cubierta abierta de X. Si X tiene la topología trivial, entonces las únicas cubiertas abiertas de X son $\{X, \emptyset\}$ y $\{X\}$.*

Ejemplo 2.3.6. *Sea $\mathbb{N}$ el conjunto de enteros positivos con la topología determinada como sigue, llamamos a un subconjunto U de $\mathbb{N}$ abierto si U contiene a todos, excepto un número finito de elementos de $\mathbb{N}$. Sea $\{U_i\}$, $i \in I$ cualquier cubierta abierta de $\mathbb{N}$. Tomemos cualquier elemento U_i. Entonces U_i contiene a todos excepto un número finito de enteros positivos; digamos en U_i no están los elementos $n_1, \ldots n_p$. Ya que $\{U_i\}$, $i \in I$, es una cubierta abierta, cada elemento de $\mathbb{N}$ está en al menos uno de los U_i, y por lo tanto existen a lo más otros p miembros de $\{U_i\}$, $i \in I$, digamos $U_{i_1}, \ldots U_{i_p}$, tal que:*

$$\mathbb{N} = U_i \cup U_{i_1} \cup \cdots \cup U_{i_p}.$$

Así $\{U_i, U_{i_1}, \ldots U_{i_p}\}$ es una subcubierta abierta finita de $\{U_i\}$, $i \in I$. Por lo tanto vemos que cada cubierta abierta de $\mathbb{N}$ (con la topología definida) tiene una subcubierta finita.

Definición 2.3.7. *Un espacio topológico X se dice que es cuasi-compacto si este satisface el siguiente axioma:*
$*$) *Cada filtro en X tiene al menos un punto de adherencia.*
Un espacio topológico X es compacto si es cuasi-compacto y Hausdorff.

Damos 3 axiomas, cada uno de los cuales es equivalente al axioma $*$):
i) Cada ultrafiltro en X es convergente.
ii) Cada familia de subconjuntos cerrados de X cuya intersección es vacía, contiene una subfamilia finita, cuya intersección es vacía.
iii) Cada cubierta abierta de X contiene una cubierta abierta finita de X.

En el Ejemplo 2.3.5, demostramos que $\mathbb{N}$ con la topología dada es compacto.

Como resultado inmediato tenemos:

Proposición 2.3.8. *Sean X y Y espacios topológicos y $f : X \to Y$ una función continua. Si A es un subconjunto compacto de X, entonces su imagen $f[A]$ es un subconjunto compacto de Y.*

Entre las propiedades mas significativas de los espacios compactos se encuentran las siguientes:

Proposición 2.3.9. *Sean X y Y espacios topológicos con X compacto. Entonces*

1. *Todo subespacio compacto de un espacio Hausdorff es cerrado.*
2. *Si existe una función continua suprayectiva $f : X \to Y$, donde Y es Hausdorff, entonces Y es compacto.*
3. *Toda función continua de un espacio compacto sobre un espacio Hausdorff es cerrada.*
4. *Y es compacto si y sólo si todo filtro en Y tiene un punto de adherencia.*

Observación 2.3.10. *Sea $\{X_i\}$ una colección de espacios topológicos compactos. Entonces el producto $\prod_i X_i$ es compacto en la topología producto. Este hecho no trivial es conocido como el Teorema de Tychonoff.*

Definición 2.3.11. *Un espacio topológico es llamado conexo si no es la unión de dos conjuntos abiertos ajenos, no vacíos.*

Una definición equivalente es obtenida reemplazando las palabras çonjunto abierto "por çonjunto cerrado ". X es *conexo* si y sólo si los únicos subconjuntos de X los cuales son abiertos y cerrados son el vacío y el espacio total X.
Si X es conexo y si A, B son subconjuntos no vacíos y abiertos tal que $A \cup B = X$, entonces $A \cap B \neq \emptyset$.

En el otro extremo tenemos:

Definición 2.3.12. *Un espacio topológico es llamado totalmente disconexo si los únicos subconjuntos conexos de X son los conjuntos unitarios.*

Un espacio con la topología discreta es totalmente disconexo.

2.4. Grupos Topológicos

Ahora los objetos de nuestro estudio son los grupos topológicos,

Definición 2.4.1. *Un grupo topológico es un grupo G con una topología τ, tal que satisface:*

(GT_I) La función $g_1 : G \times G \to G$ dado por $g_1(x, y) = x \cdot y$ es continua.
(GT_{II}) La función $g_2 : G \to G$ dado por $g_2(x) = x^{-1}$ es continua, donde x^{-1} es el inverso de x.
Donde $G \times G$ está dotado de la topología producto.

Si A y B son subconjuntos del grupo G, definimos $A^{-1} = \{x^{-1} | x \in A\}$ y $A \cdot B = \{a \cdot b | a \in A, b \in B\}$.

Una estructura de grupo y una topología en un conjunto G se dice que son compatibles si satisfacen (GT_I) y (GT_{II}).

Ejemplo 2.4.2. *La topología discreta en un grupo G es compatible con la estructura de grupo. Un grupo topológico cuya topología es la discreta es llamado un grupo discreto.*

Sea G un grupo topológico. Con la definición de continuidad de funciones en espacios topológicos vemos que si $N(x)$ es la familia de vecindades de un punto $x \in G$, podemos describir las condiciones de la definición anterior como sigue: si x y y son elementos de G, para cada vecindad U de xy, es decir, $U \in N(xy)$ existen vecindades $V \in N(x)$ y $W \in N(y)$ tales que $V \cdot W \subseteq U$; y para cada $U \in N(x^{-1})$ existe $V \in N(x)$ tal que $V^{-1} \subseteq U$.

Definición 2.4.3. *Sea G un grupo topológico y $g \in G$*

1. *La función $\psi_g : G \to G$ definida por $\psi_g(x) = xg$ es llamada traslación derecha por g.*

2. *La función $\sigma_g : G \to G$ definida por $\sigma_g(x) = gx$ es llamada traslación izquierda por g*

3. *La función $f : G \to G$ definida por $f(x) = x^{-1}$ es llamada inversión.*

Teorema 2.4.4. *Sea G un grupo topológico. Si $g \in G$ es un elemento fijo arbitrario, entonces las funciones ψ_g,σ_g y f, son homeomorfismos.*

Demostración. Primero mostraremos que f es un homeomorfismo. Como G es un grupo topológico, entonces $f(x) = x^{-1}$ es continua. Ahora, f es inyectiva puesto que si $f(x) = f(y)$ entonces $x^{-1} = y^{-1}$, y así $x = y$.
Además si $a \in G$, entonces $f(a^{-1}) = a$, por lo que f es suprayectiva, y también sabemos que la inversa de f es ella misma, así f es un homeomorfismo.

Ahora, solo probaremos que ψ_g, la traslación derecha por g, es homeomorfismo, ya que el caso izquierdo es similar.
Como G es grupo topológico, que ψ_g es continua es consecuencia de (GT_I).

Para ver que ψ_g es inyectiva, supongamos que $\psi_g(a) = \psi_g(b)$, entonces $ag = bg$, así que $a = b$.
ψ_g es suprayectiva, ya que si $b \in G$; entonces $\psi_g(bg^{-1}) = b$.
Ahora, la inversa de ψ_g es $\psi_{g^{-1}}$, ya que $\psi_{g^{-1}}(\psi_g(a)) = \psi_{g^{-1}}(ag) = agg^{-1} = a$, y $\psi_{g^{-1}}$ es continua, por lo que ψ_g es un homeomorfismo. ■

Definición 2.4.5. *Sean G y G' grupos topológicos. Una función biyectiva $f : G \to G'$ es un isomorfismo topológico si f y f^{-1} son homomorfismos continuos. Si $G = G'$, el isomorfismo f se llama automorfismo topológico.*

Teorema 2.4.6. *Si G es un grupo topológico y $a \in G$ está fijo, entonces la función $g(x) = axa^{-1}$ (la conjugación por a) es un automorfismo topológico.*

Demostración. Primero observemos que $g(x) = \sigma_a(\psi_{a^{-1}}(x))$, donde σ_a y $\psi_{a^{-1}}$ se han definido en la Definición 2.4.3. Así, tenemos que g es un homeomorfismo por ser la composición de dos homeomorfismos. Además g es un homomorfismo ya que $g(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = g(x)g(y)$. ■

Si G es un grupo abeliano, vemos que los automorfismos definidos en el teorema anterior son la identidad.

Lema 2.4.7. *Sea G un grupo topológico, y sea N_e una base local para la identidad e del grupo. Entonces las familias $\{xU|x \in G, U \in N_e\}$ y $\{Ux|x \in G, U \in N_e\}$, son bases para la topología del grupo G.*

Demostración. Veamos que $\{xU|x \in G, U \in N_e\}$ es una base para la topología en G. En forma similar se prueba que $\{Ux|x \in G, U \in N_e\}$ es base.
Sea W un conjunto abierto no vacío en G y $a \in W$. Como la función $f(x) = a^{-1}x$ es un homeomorfismo, transforma el abierto W en el abierto $a^{-1}W$ y además $e \in a^{-1}W$. Como N_e es una base local para e, existe $U \in N_e$ tal que $e \in U \subseteq a^{-1}W$. Así

$$a \in aU \subseteq aa^{-1}W = W,$$

lo cual muestra que $\{xU|x \in G, U \in N_e\}$ es una base del grupo topológico G. ■

El lema siguiente proporciona una base local para la identidad formada por vecindades tales que $V^{-1} = V$. Estas vecindades reciben el nombre de *simétricas*.

Lema 2.4.8. *Si G es un grupo topológico y $U \in N_e$, entonces existe $V \in N_e$ tal que $V^{-1} = V \subseteq U$. Por lo tanto, las vecindades simétricas de la identidad e constituyen una base local para e.*

Demostración. Sea $U \in N_e$ y $f(x) = x^{-1}$, f es un homeomorfismo por el Teorema 2.4.4 y por lo tanto $f(U) = U^{-1}$ es abierto y $e \in U^{-1}$. Así $V = U \cap U^{-1}$ es abierto y $V^{-1} = V$ con $e \in V \subseteq U$. ■

Teorema 2.4.9. *Sean G un grupo topológico, $a \in G$ y A, B, O, M subconjuntos de G. Entonces:*

1. *Si O es abierto, los conjuntos aO, Oa, O^{-1}, MO y OM son abiertos.*
2. *Si A es cerrado, aA, Aa,A^{-1} son conjuntos cerrados.*
3. *Si A y B son compactos, también lo son AB y A^{-1}.*

Demostración. 1) Sabemos por el Teorema 2.4.4 que $\psi_a(x) = xa$, $\sigma_a(x) = ax$ y $f(x) = x^{-1}$ son homeomorfismos. Por lo tanto si O es abierto, $\psi_a(O) = aO$, $\sigma_a(O) = Oa$ y $f(O) = O^{-1}$ también son abiertos. Ahora observemos que:

$$MO = \bigcup\{mO | m \in M\},$$

y

$$OM = \bigcup\{Om | m \in M\}.$$

Así OM y MO son abiertos, por ser ambos unión de abiertos.
2) Se prueba de forma similar a (1)
3) Como $g_1 : G \times G \to G$, dada por $g_1(a, b) = ab$ es una función continua y además $A \times B$ es compacto en $G \times G$, tenemos por la Proposición 2.3.8 que $g_1(A \times B) = AB$ es compacto. Y de manera similar, dado que la función $f : G \to G$ dada por $f(x) = x^{-1}$ es continua, tenemos por la Proposición 2.3.8 que $f(A) = A^{-1}$ es compacto. ■

Teorema 2.4.10. *Sea G un grupo topológico Hausdorff. Existe una base local $\mathbb{V}$ para e tal que cumple las siguientes condiciones:*

1. *$\cap\mathbb{V} = \{e\}$;*
2. *si U, V son dos elementos arbitrarios de $\mathbb{V}$, entonces existe $W \in \mathbb{V}$ tal que $W \subseteq U \cap V$;*
3. *para cada $U \in \mathbb{V}$ existe $V \in \mathbb{V}$ tal que $VV^{-1} \subseteq U$;*
4. *para cada $U \in \mathbb{V}$ y para cada $x \in U$ existe $V \in V$ con $xV \subseteq U$;*
5. *para cada $U \in \mathbb{V}$ y $a \in G$ existe $W \in \mathbb{V}$ con $aWa^{-1} \subseteq U$.*

Recíprocamente, si tenemos un grupo G y una familia V no vacía de subconjuntos de G que contienen a e, tales que se satisfacen las condiciones (1) *a* (5) *para V, entonces cada una de las familias $\{xU|U \in \mathbb{V}, x \in G\}$ y $\{Ux|U \in \mathbb{V}, x \in G\}$ es base para una topología de grupo τ para G. Además, $\mathbb{V}$ es una base local para e en (G, τ).*

La demostración de este resultado la podemos consultar en la referencia $[Or]$.

Ahora teniendo la noción de filtro, dada en la Sección 2.2, enunciaremos los resultados anteriores con este concepto.

Sea B el filtro vecindad del elemento identidad e en un grupo topológico G, y sea a cualquier otro elemento de G. Por el Teorema 2.4.4 se sigue que el filtro vecindad de a es la familia aB de conjuntos aV, donde $V \in B$ y también la familia Ba de conjuntos Va. Así conocemos el filtro vecindad de cualquier punto de un grupo topológico tan pronto como conocemos el filtro vecindad del *elemento identidad* e del grupo.

Teniendo en cuenta que las funciones g_1 y g_2, de la Definición 2.4.1 de grupo topológico, son continuas, en particular para $x = y = e$ y del Lema 2.4.8 obtenemos:

(GV_I) Dado cualquier $U \in B$ existe $V \in B$ tal que $VV \subseteq U$.

(GV_{II}) Dado cualquier $U \in B$, tenemos que $U^{-1} \in B$.

Cada filtro B en G el cual satisface las dos propiedades anteriores, también satisface:

(GV_a) Dado cualquier $U \in B$, existe $V \in B$ tal que $VV^{-1} \subseteq U$.

Finalmente, ya que $g(x) = axa^{-1}$ es un homeomorfismo el cual deja fijo a e, B tiene la siguiente propiedad:

(GV_{III}) Para todo $a \in G$ y todo $V \in B$, tenemos $aVa^{-1} \in B$.

Estas tres propiedades de un filtro B son características, es decir:

Proposición 2.4.11. *Sea G un grupo y sea B un filtro en G, el cual satisface los axiomas (GV_I), (GV_{II}) y (GV_{III}). Entonces existe una única topología en G, compatible con la estructura de grupo de G, para la cual B es el filtro vecindad del elemento identidad e. Para esta topología el filtro vecindad de cualquier punto $a \in G$ es el filtro aB y también el filtro Ba.*

Un método común para definir una topología compatible con la estructura de grupo G consiste en dar un filtro que satisfaga los axiomas (GV_I),

(GV_{II}) y (GV_{III}).

Las condiciones correspondientes para cuando B es *base de un filtro*, son las siguientes:
(GV'_I) Dado cualquier $U \in B$ existe $V \in B$ tal que $VV \subseteq U$.
(GV'_{II}) Dado cualquier $U \in B$, existe $V \in B$ tal que $V^{-1} \subseteq U$.

(GV'_{III}) Para todo $a \in G$ y para cualquier $U \in B$, existe $V \in B$ tal que $V \subseteq aUa^{-1}$.

Observación 2.4.12. *Si G es conmutativo, tenemos que $xAx^{-1} = A$ para cada subconjunto A de G y para cada $x \in G$, y por lo tanto (GV_{III}) (respectivamente (GV'_{III})) se satisface automáticamente para cada filtro (respectivamente base de un filtro)en G. Por otro lado, si G no es abeliano, entonces (GV_{III}) no es consecuencia de (GV_I) y (GV_{II}).*

Si G es un grupo conmutativo, escrito *aditivamente*, los axiomas los cuales caracterizan al filtro B de vecindades para dar origen a una topología compatible con la estructura de grupo de G son los siguientes:
(GA_I) Dado cualquier $U \in B$, existe $V \in B$ tal que $V + V \subseteq U$
(GA_{II}) Dado cualquier $U \in B$, tenemos que $-U \in B$

Proposición 2.4.13. *Un grupo topológico G es Hausdorff si y sólo si el conjunto $\{e\}$ es cerrado.*

Corolario 2.4.14. *Un grupo topológico es Hausdorff si y sólo si la intersección de las vecindades de e consiste únicamente del punto e.*

Ejemplo 2.4.15. *Definición de una topología en un grupo por medio de un conjunto de subgrupos:*
Si B es base de un filtro en un grupo G, formado por subgrupos de G, entonces vemos inmediatamente que B satisface los axiomas (GV'_I) y (GV'_{II}), ya que $HH^{-1} = H$ para cualquier subgrupo H de G. Por lo tanto el conjunto B será un sistema fundamental de vecindades de e en la topología compatible con la estructura de grupo G, si B satisface (GV_{III}). Esto será en particular el caso en que todos los subgrupos en B sean normales, por lo tanto , siempre si G es conmutativo. La topología así definida es Hausdorff por el Corolario 2.4.14, si y sólo si la intersección de todos los subgrupos de B consiste sólo de e. Los casos mas interesantes son aquellos en los cuales

el subgrupo $\{e\}$ no está en B (en otro caso la topología definida por B es la topología discreta): si $\{e\} \notin B$, la topología definida por B es Hausdorff sólo si B es un conjunto infinito.

Capítulo 3

Extensiones infinitas de Galois

En este capítulo estudiamos extensiones de Galois infinitas y probaremos un análogo al Teorema Fundamental de la Teoría de Galois para extensiones infinitas. La idea principal es asignar una topología al grupo de Galois de una extensión de Galois de dimensión infinita y entonces usar esta topología para determinar cuáles subgrupos del grupo de Galois son grupos de Galois de extensiones intermedias.

3.1. Topología de Krull

La idea de la Teoría de Galois es asociar a una extensión de campos K/k, un grupo y viceversa, es decir, queremos ver que cada subgrupo del grupo de Galois tiene la forma $G(K/F)$, para $k \subseteq F \subseteq K$. Pero necesitamos información acerca de $G(K/k)$, de hecho la forma adecuada para examinar a este grupo es asignándole una topología.

Sea K una extensión de Galois (Definición 1.5.1) de k y sean:
$\mathbb{G} = G(K/k)$
$\mathbb{I} = \{F|\ \ k \subseteq F \subseteq K,\ \ [F:k] < \infty,\ F/k\ \ de\ \ Galois\}$
$\mathbb{N} = \{N \subseteq \mathbb{G}|\ \ N = G(K/F), para\ \ algun\ \ F \in \mathbb{I}\}$

Nótese que los $N \in \mathbb{N}$ son subgrupos de $\mathbb{G}$.
Comenzamos probando unas cuantas propiedades simples de los conjuntos $\mathbb{I}$ y $\mathbb{N}$.

Lema 3.1.1. *Si $\alpha_1, \alpha_2, \ldots \alpha_n \in K$, entonces existe $F \in \mathbb{I}$ con $\alpha_i \in F$ para todo i.*

Demostración. Sea $F \subseteq K$ el campo de descomposición de los polinomios irreducibles de los α_i sobre k. Entonces, como cada α_i es separable sobre k, el campo F es normal por el Teorema 1.4.8 y por la Definición 1.4.2, $F = k(\alpha_1, \alpha_2, \ldots \alpha_n)$ y como cada α_i es separable sobre k, entonces por el corolario 1.3.17 F separable sobre k, por lo tanto F es extensión de Galois de k por el Teorema 1.5.5 y como hay un número finito de α_i, tenemos que $[F : k] < \infty$, y por lo tanto $F \in \mathbb{I}$. ■

Lema 3.1.2. *Sea $N \in \mathbb{N}$ y sea $N = G(K/E)$, con $E \in \mathbb{I}$. Entonces E es el campo fijo de N y $N \lhd \mathbb{G}$. Además $\mathbb{G}/N \cong G(E/k)$ y así $|\mathbb{G}/N| = |G(E/k)| = [E : k] < \infty$.*

Demostración. i) Mostramos primero que E es el campo fijo de N.
Ya que K/k es normal y separable, el campo K/E también es normal y separable, así K/E es de Galois. Por lo tanto E es el campo fijo de N.

ii) Ahora demostramos que N es normal en G.
Sea $\sigma \in G(K/k)$ y $\tau \in N = G(K/E)$.
Si $a \in E$, entonces cada conjugado de a está en E, ya que E/k es normal. En particular $\sigma(a) \in E$. Entonces:

$$\sigma^{-1}\tau\sigma(a) = \sigma^{-1}\tau(\sigma(a)) = \sigma^{-1}(\sigma(a)) = a$$

Como $a \in E$ fue arbitraria, entonces $\sigma^{-1}\tau\sigma \in N = G(K/E)$. Así $N \lhd G$

iii) Por último probaremos que $\mathbb{G}/N \cong G(E/k)$.
Sea $\phi : \mathbb{G} \to G(E/k)$ dado por:

$$\phi(\tau) = \tau|_E$$

y obsérvese que, como E/k es normal y finita, entonces por el Lema 1.4.11 se sigue que $\tau|_E$ es en efecto un k-automorfismo de E, es decir, $\tau|_E \in G(E/k)$.
Claramente ϕ es un homomorfismo de grupos.
Probaremos que ϕ es suprayectivo con núcleo $G(K/E)$.

1. ϕ es suprayectivo.
   Sea $\sigma \in G(E/k)$

σ es un k-monomorfismo de E en K y por la Proposición 1.5.4, σ es la restricción de un k-automorfismo de K, es decir, existe $\delta \in G(K/k)$ tal que $\delta|_E = \sigma$.

2. Finalmente:
   Para toda $\sigma \in G(K/k)$ se tiene que: $\sigma|_E = id_E$ si y sólo si $\sigma \in G(K/E)$, por lo tanto $nuc(\phi) = G(K/E)$.

■

Lema 3.1.3. $\bigcap_{N\in\mathbb{N}} N = \{id\}$. *Además* $\bigcap_{N\in\mathbb{N}} \sigma N = \{\sigma\}$ *para todo* $\sigma \in G$.

Demostración. Sea $\tau \in \bigcap_{N\in\mathbb{N}} N$ y sea $a \in K$, por el Lema 3.1.1 existe $E \in \mathbb{I}$ con $a \in E$. Sea $N = G(K/E) \in \mathbb{N}$. El automorfismo τ fija a E, ya que $\tau \in N$, así $\tau(a) = a$ y como a fue arbitrario, $\tau = id$. Por lo tanto $\bigcap_{N\in\mathbb{N}} N = \{id\}$.
Para la segunda afirmación, si $\tau \in \sigma N$ para todo $N \in \mathbb{N}$, entonces $\sigma^{-1}\tau \in N$ para todo N, así $\sigma^{-1}\tau = id$ por la primera parte, esto nos lleva a que $\tau = \sigma$ y así $\bigcap_{N\in\mathbb{N}} \sigma N = \{\sigma\}$.

■

Lema 3.1.4. *Sean* $N_1, N_2 \in \mathbb{N}$. *Entonces* $N_1 \cap N_2 \in \mathbb{N}$.

Demostración. Sean $N_i = G(K/E_i)$, con $E_i \in \mathbb{I}$, $i = 1, 2$. Cada E_i es extensión finita de Galois de k, es decir, cada $E_i/k, i = 1, 2$ es finita, normal y separable. Mostraremos que $E_1E_2 \in \mathbb{I}$, probando que E_1E_2/k es finita normal y separable, así E_1E_2/k será extensión de Galois por el Teorema 1.5.2

1. E_1E_2/k es finita.
   Como E_1/k y E_2/k son extensiones finitas, tenemos por la Proposición 1.1.22,que existe un número finito de elementos $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n \in K$ tales que:

$$E_1 = k(a_1, \ldots, a_m) \text{ y } E_2 = k(b_1, \ldots, b_n)$$

   y así $E_1E_2 = k(a_1, \ldots, a_m, b_1, \ldots, b_n)$ y por lo tanto E_1E_2/k es finita.

2. E_1E_2/k es normal.
   Por el Lema 1.4.11 es suficiente probar que para cualquier k-monomorfismo σ de E_1E_2 en una extensión normal F de E_1E_2 se tiene que $\sigma(E_1E_2) = E_1E_2$. Pero

$$\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2) = E_1E_2$$

   ya que E_1 y E_2 son extensiones normales de k.

3. E_1E_2/k es separable.
   Como $E_1E_2 = k(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n)$ y además cada $a_i, b_j \in K$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, es separable sobre k, puesto que E_1/k y E_2/k son separables, entonces por el Corolario 1.3.17, E_1E_2 es separable sobre k.

Por lo tanto E_1E_2/k es extensión de Galois y así $E_1E_2 \in \mathbb{I}$
Además: $G(K/E_1E_2) = N_1 \cap N_2$, ya que
$\sigma \in N_1 \cap N_2$
si y sólo si $\sigma|_{E_1} = id$ y $\sigma|_{E_2} = id$
si y sólo si $E_1 \subseteq F(\{\sigma\})$ y $E_2 \subseteq F(\{\sigma\})$,
si y sólo si $E_1E_2 \subseteq F(\{\sigma\})$
($F(\{\sigma\})$ es el campo fijo de $\{\sigma\}$ definido en 1.2.10, que aunque el campo fijo se definió para un subconjunto de un grupo de automorfismos, la definición de $F(\sigma)$ es la misma).
Esta última condición es cierta si y sólo si
$\sigma \in G(K/E_1E_2)$
Así $N_1 \cap N_2 = G(K/E_1E_2) \in \mathbb{N}$ ■

Ahora definimos una topología en el grupo de Galois $\mathbb{G}$, la cual será compatible con la estructura de grupo.

Definición 3.1.5. *La topología de Krull en $\mathbb{G}$ está definida como sigue: Un subconjunto X de $\mathbb{G}$ es abierto si $X = \emptyset$ ó si $X = \bigcup_i \sigma_i N_i$ para algunos $\sigma_i \in \mathbb{G}$ y $N_i \in \mathbb{N}$.*

De la definición, es claro que $\emptyset$ y $\mathbb{G} \in \mathbb{N}$ son abiertos y que la unión de conjuntos abiertos son abiertos. Mostramos que tenemos una topología en

$\mathbb{G}$ y para ello basta ver que la intersección de dos conjuntos abiertos es un conjunto abierto.
Es suficiente mostrar que $\tau_1 N_1 \cap \tau_2 N_2$ es abierto para cualesquiera $N_1, N_2 \in \mathbb{N}$ y $\tau_1, \tau_2 \in \mathbb{G}$. Si $\sigma \in \tau_1 N_1 \cap \tau_2 N_2$, entonces $\sigma = \tau_1 \rho$, $\rho \in N_1 = G(K/F_1)$ y $\sigma = \tau_2 \delta$, $\delta \in N_2 = G(K/F_2)$, entonces $\sigma\rho^{-1} = \tau_1$ y $\sigma\delta^{-1} = \tau_2$.

Sea $\gamma \in \tau_1 N_1 \cap \tau_2 N_2$ entonces de manera similar $\gamma = \tau_1\rho' = \tau_2\delta'$, $\rho' \in N_1$, $\delta' \in N_2$
sustituyendo a τ_1 y a τ_2, tenemos:
$\gamma = \sigma\rho^{-1}\rho' = \sigma\delta^{-1}\delta'$ con $\rho^{-1}\rho' \in N_1$ y $\delta^{-1}\delta' \in N_2$ y así $\gamma \in \sigma N_1 \cap \sigma N_2$ y como σ es un k-isomorfismo tenemos que:

$$\tau_1 N_1 \cap \tau_2 N_2 = \sigma N_1 \cap \sigma N_2 = \sigma(N_1 \cap N_2)$$

y $\sigma(N_1 \cap N_2)$ es abierto, ya que $N_1 \cap N_2 \in \mathbb{N}$ por el Lema 3.1.4.

Damos algunas propiedades de la Topología de Krull.
Ya que cada conjunto abierto no vacío de $\mathbb{G}$ es una unión de clases de subgrupos que pertenecen a $\mathbb{N}$, el conjunto:

$$\{\sigma N| \ \ \sigma \in \mathbb{G}, \ \ N \in \mathbb{N}\}$$

es una base para la Topología de Krull. Así el elemento identidad de $\mathbb{G}$ tiene como conjunto de vecindades a $\{N|N \in \mathbb{N}\}$, y $\sigma \in \mathbb{G}$ tiene como conjunto de vecindades a $\{\sigma N|N \in \mathbb{N}\}$.

Observación 3.1.6. *Si K es una extensión finita de k, por lo dicho en el párrafo anterior cada elemento σ de $\mathbb{G}$ tiene una vecindad la cual consiste únicamente de σ. En este caso $\mathbb{G}$ tiene la topología discreta.*

Observación 3.1.7. *Note que si $N \in \mathbb{N}, N = G(K/E)$ para algún $E \in \mathbb{I}$. Si $\sigma \in \mathbb{G}$, entonces:*

$$\sigma G(K/E)\sigma^{-1} = G(K/\sigma(E))$$

ya que si $\delta \in \sigma G(K/E)\sigma^{-1}$, $\delta = \sigma\tau\sigma^{-1}$ donde $\tau|_E = id$ y si $b \in \sigma(E)$, entonces:
$\delta(b) = \delta(\sigma(c))$, $c \in E$
$= \sigma\tau\sigma^{-1}(\sigma(c))$
$= \sigma\tau(c)$

$= \sigma(c) = b$
y así $\delta \in G(K/\sigma(E)$
Ahora si $\gamma \in G(K/\sigma(E))$, *tenemos que* $\gamma(\sigma(b)) = \sigma(b)$ *para todo* $b \in E$ *y por lo tanto tenemos que* $\sigma^{-1}\gamma(\sigma(b)) = b$ *para* $b \in E$, *y así* $\sigma^{-1}\gamma\sigma \in G(K/E)$, *y de aquí* $\gamma = \sigma(\sigma^{-1}\gamma\sigma)\sigma^{-1} \in \sigma G(K/E)\sigma^{-1}$.

Así que para $G(K/E) \in \mathbb{N}$ *se tiene:*

$$G(K/E)\sigma = \sigma(\sigma^{-1}G(K/E)\sigma) = \sigma G(K/\sigma^{-1}(E))$$

Concluimos entonces que $\{\sigma N|\sigma \in \mathbb{G}, N \in \mathbb{N}\} = \{N\sigma|\sigma \in \mathbb{G}, N \in \mathbb{N}\}$. *Esto es, al definir la topología de Krull, podemos tomar clases izquierdas, clases derechas o ambas, izquierdas y derechas.*

Proposición 3.1.8. *Bajo la topología de Krull,* $\mathbb{G}$ *es un grupo topológico.*

Demostración. Por la Definición 2.4.1 debemos mostrar que las funciones:

$$\begin{array}{c} g_1 : \mathbb{G} \times \mathbb{G} \to \mathbb{G} \\ g_1(x, y) = xy \end{array}$$

y

$$\begin{array}{c} g_2 : \mathbb{G} \to \mathbb{G} \\ g_2(x) = x^{-1} \end{array}$$

son continuas. Para g_1 tenemos que si $\sigma\tau N$ es una vecindad de $\sigma\tau$, entonces

$$g_1^{-1}(\sigma\tau N) \supseteq (\sigma(\tau N\tau^{-1})) \times (\tau N),$$

(recordemos que $N \lhd \mathbb{G}$, por lo que $\tau N\tau^{-1} = N$) es una vecindad de $\sigma\tau$ en $\mathbb{G} \times \mathbb{G}$.
Y para g_2 tenemos que si $\sigma^{-1}N$ es una vecindad de σ^{-1}, entonces

$$g_2^{-1}(\sigma^{-1}N) = N^{-1}\sigma = N\sigma,$$

es una vecindad de σ en $\mathbb{G}$. ■

Lema 3.1.9. *Cada conjunto abierto básico* σN *en* $\mathbb{G}$ *es también cerrado.*

Demostración. Sea $\tau \notin \sigma N$, es decir, $\tau \in \mathbb{G} - \sigma N$, entonces $\emptyset = \tau N \cap \sigma N$ (ya que N es subgrupo de $\mathbb{G}$), es decir,

$$\tau N \subseteq \mathbb{G} - \sigma N$$

En otras palabras, el complemento de σN contiene una vecindad de cada uno de sus puntos, así es un conjunto abierto, y por lo tanto σN es cerrado. ■

El siguiente Teorema describe las propiedades topológicas de $\mathbb{G}$.

Teorema 3.1.10. *Como espacio topológico, $\mathbb{G}$ es Hausdorff, compacto y totalmente disconexo.*

Demostración. i) $\mathbb{G}$ es totalmente disconexo.
Si $X \subseteq \mathbb{G}$ y $\sigma, \tau \in X$ con $\sigma \neq \tau$, sea σN una vecindad abierta de σ tal que $\tau \notin \sigma N$ (la existencia de N se sigue del Lema 3.1.3). Entonces:

$$X = (\sigma N \cap X) \cup ((\mathbb{G} - \sigma N) \cap X)$$

es una unión de abiertos ajenos no vacíos en X, así X es no conexo y como X es cualquier subconjunto de $\mathbb{G}$, entonces $\mathbb{G}$ es totalmente disconexo.

ii) $\mathbb{G}$ es Hausdorff
Sea $\sigma \in \mathbb{G}$. El Lema 3.1.3 muestra que $\{\sigma\} = \bigcap_{N \in \mathbb{N}} \sigma N$. Si $\tau \neq \sigma$, entonces existe $N \in \mathbb{N}$ tal que $\tau \notin \sigma N$. Cada σN es una vecindad abierta de σ, pero también es cerrado, por el Lema 3.1.9 y así σN y $\mathbb{G} - \sigma N$ son abiertos disjuntos con $\sigma \in \sigma N$ y $\tau \in \mathbb{G} - \sigma N$ y por lo tanto $\mathbb{G}$ es Hausdorff.

iii) $\mathbb{G}$ es Compacto.
Finalmente veremos que $\mathbb{G}$ es compacto, mostrando que cada cada ultrafiltro en $\mathbb{G}$ converge, por la equivalencia *i)* dada en la Definición 2.3.7.
Sea $\mathbb{U}$ un ultrafiltro en $\mathbb{G}$. Entonces, si $S_1 \ldots, S_r$ son subconjuntos de $\mathbb{G}$ y $S_1 \cup \ldots \cup S_r \in \mathbb{U}$, se sigue que $S_i \in \mathbb{U}$ para algún i, por el Corolario 2.2.13.

Sea $a \in K$ y sea $H = G(K/k(a))$.
Por el Lema 3.1.2 se tiene que H tiene índice finito en $\mathbb{G}$. Si $\tau_1 H, \ldots, \tau_s H$, son las distintas clases izquierdas de H en $\mathbb{G}$, tenemos:

$$\mathbb{G} = \tau_1 H \cup \ldots \cup \tau_s H \in \mathbb{U} \text{ y así } \tau_i H \in \mathbb{U}, \text{ para algún } i.$$

Si $i \neq j$ entonces $\tau_j H \cap \tau_i H = \emptyset$ y así $\tau_j H \notin \mathbb{U}$.
Ahora definamos $\sigma(a) = \tau_i(a)$.
Como vemos $\sigma(a)$ esta definida a partir de la extensión simple $k(a)$, para ver que está bien definida mostraremos que $\sigma(a)$ puede, en realidad, ser definido de una forma similar usando cualquier extensión finita de k en K, la cual contiene a a.
Supongamos que $a \in L$ donde $k \subseteq L \subseteq K$ y $[L : k]$ es finito. Sea $H' = G(K/L)$, por el argumento usado arriba, existe exactamente una clase izquierda $\tau' H'$ de H' en $\mathbb{G}$ tal que $\tau' H' \in \mathbb{U}$. Note que $H' \subseteq H$.
Ya que $\tau' H$ y $\tau' H'$ pertenecen a $\mathbb{U}$, $\tau_i H \cap \tau' H' \neq \emptyset$, si $\rho \in \tau_i H \cap \tau' H'$, entonces $\rho^{-1}\tau' \in H' \subseteq H$ y $\tau_i^{-1}\rho \in H$ y así $\tau_i^{-1}\tau' = (\tau_i^{-1}\rho)(\rho^{-1}\tau') \in H$.
Entonces $\tau' H = \tau_i H$ y $\tau' H' \subseteq \tau_i H$.
Por lo tanto $\tau'(a) = \tau_i(a) = \sigma(a)$.
Ahora, ya que dos elementos arbitrarios de K pertenecen a alguna extensión finita de k en K, σ manda sumas en sumas y productos en productos. Puesto que $\sigma(1) = 1$, σ es un monomorfismo de K en sí mismo, y por la Proposición 1.5.3, $\sigma \in \mathbb{G}$.
Probaremos que el ultrafiltro $\mathbb{U}$ converge a σ, mostrando que cada vecindad de σ está en $\mathbb{U}$. Para esto, es suficiente mostrar que para $H \in \mathbb{N}$, tenemos $\sigma H \in \mathbb{U}$.
Sea $H = G(K/F) \in \mathbb{N}$. Entonces $[F(a) : k] < \infty$ y sea $H' = G(K/F(a))$. Se tiene que $H' \subseteq H$ y por la forma en la cual σ esta determinada tenemos $\sigma H' \subseteq \sigma H$ y así $\sigma H \in \mathbb{U}$. ■

La siguiente es otra demostración de que $\mathbb{G}$ es compacto:

Sea $P = \prod_{N \in \mathbb{N}} \mathbb{G}/N$, el producto directo de los grupos finitos $\mathbb{G}/N$. Damos una topología en P, dando a cada $\mathbb{G}/N$ la topología discreta, y entonces a P, la topología producto. Note que cada $\mathbb{G}/N$ es Hausdorff y compacto, así P es Hausdorff, y por el teorema de Tychonoff, P es compacto.
Existe un homomorfismo natural de grupos:

$$f : \mathbb{G} \to P$$
$$f(\sigma) = (\sigma N)_{N \in \mathbb{N}}$$

Mostraremos que f es un homeomorfismo de $\mathbb{G}$ sobre $Im(f)$ y que esta imagen es un subconjunto cerrado de P. Ya que P es compacto y Hausdorff,

esto mostrará que $Im(f)$ es compacto, por lo tanto $\mathbb{G}$ será compacto, ya que $\mathbb{G}$ es homeomorfo a $Im(f)$.
Sea f como arriba. El núcleo de f consiste de aquellos $\sigma \in \mathbb{G}$ con $(\sigma N)_{N\in}\mathbb{N} = (N)_{N\in\mathbb{N}}$. Por lo tanto, si $\sigma \in nuc(f)$, entonces $\sigma \in \bigcap_{N\in\mathbb{N}} N = \{id\}$; esto es por el Lema 3.1.3. Así f es inyectiva.
Sea $\pi_N : P \to \mathbb{G}/N$ la proyección en la N-componente. Entonces

$$\pi_N(f(\sigma)) = \sigma N \text{ para todo } \sigma \in \mathbb{G}$$

Los conjuntos unitarios τN forman una base para la topología discreta en $\mathbb{G}/N$, así por la definición de la topología producto, cada conjunto abierto en P es una unión de una intersección finita de conjuntos de la forma $\pi_N^{-1}(\tau N)$ para varios $\tau \in \mathbb{G}$ y $N \in \mathbb{N}$. Para mostrar que f es continua es suficiente mostrar que $f^{-1}(\pi_N^{-1}(\tau N))$ es abierto en $\mathbb{G}$ para cualquier τN, pero esta preimagen es justamente τN, el cual es abierto, así f es continuo. Además, $f(\tau N) = \pi_N^{-1}(\tau N) \cap Im(f)$ es abierto en $Im(f)$, así f^{-1}es también continua. Por lo tanto f es un homeomorfismo de $\mathbb{G}$ en $Im(f)$.
Resta mostrar que la $Im(f)$ es cerrado en P. Al verificar que $Im(f)$ es cerrado en P, identificaremos a $\mathbb{G}/N$ con el grupo isomorfo $G(E_N/k)$, donde E_N denota el campo fijo de N. Este isomorfismo es del Lema 3.1.2. Esto equivale a identificar la clase τN con $\tau|_{E_N}$. Con esta identificación, para $\rho \in P$ el elemento $\pi_N(\rho)$ es un automorfismo de E_N. Note que para $\tau \in \mathbb{G}$ tenemos $\pi_N(f(\tau)) = \tau|_{E_N}$. Sea

$$C = \{\rho \in P | para \;\; cada \;\; N, M \in \mathbb{N}, \pi_N(\rho)|_{E_N \cap E_M} = \pi_M(\rho)|_{E_N \cap E_M}\}$$

Afirmamos que $C = Im(f)$. Ahora, $Im(f) \subseteq C$ ya que

$$\pi_N(f(\tau))|_{E_N} = \tau|_{E_N} \text{ para cualquier } \tau \in \mathbb{G}$$

Para mostrar que $C \subseteq Im(f)$, sea $\rho \in C$. Definimos $\tau : K \to K$ como sigue:
Para $a \in K$, elegimos cualquier $E_N \in \mathbb{I}$, con $a \in E_N$,lo que es posible por el Lema 3.1.1, y definimos $\tau(a) = \pi_N(\rho)(a)$. La condición que $\rho \in C$ muestra que este es un mapeo bien definido. Para ver que τ es un homomorfismo de anillos, si $a, b \in K$, sea $E_N \in \mathbb{I}$ con $a, b \in E_N$. Entonces $\tau|_{E_N} = \pi_N(\rho)$ es un homomorfismo de anillos, así:

$$\tau(a+b) = \tau(a) + \tau(b) \quad \text{y} \quad \tau(ab) = \tau(a)\tau(b)$$

El mapeo τ es una biyección ya que podemos construir τ^{-1} usando ρ^{-1}. Es claro que τ deja fijo a k, y así $\tau \in \mathbb{G}$.
Ahora, como $\tau|_{E_N} = \pi_N(\rho)$ vemos que $f(\tau) = \rho$. Así $C = Im(f)$.
Para mostrar que C es cerrado en P, tomemos cualquier $\rho \in P - C$, Entonces existen $M, N \in \mathbb{N}$ con

$$\pi_N(\rho)|_{E_N \cap E_M} \neq \pi_M(\rho)|_{E_N \cap E_M}.$$

Así $\pi_N^{-1}(\pi_N(\rho)) \cap \pi_M^{-1}(\pi_M(\rho))$ es un subconjunto abierto de P que contiene a ρ ajeno a C. Por lo tanto $P - C$ es abierto y así, $C = Im(f)$ es cerrado.

3.2. Extensiones infinitas de Galois

Sea K una extensión de Galois de k y sea $\mathbb{G} = G(K/k)$. Sea H un subgrupo de $\mathbb{G}$ y denotemos a la cerradura de H por $\overline{H}$

Proposición 3.2.1. *Si L es el campo fijo de H, entonces $G(K/L) = \overline{H}$.*

Demostración. Sean $\sigma \in \overline{H}$, $a \in L$ y $H' = G(K/k(a))$.
Como $\sigma H'$ es un abierto tal que $\sigma \in \sigma H'$ tenemos que $H \cap \sigma H' \neq \emptyset$. Sea $\tau \in H \cap \sigma H'$. Entonces:
$\tau(b) = b$ para todo $b \in L$ y $\sigma^{-1}\tau(c) = c$ para todo $c \in k(a)$.
Por lo tanto $\sigma(a) = \tau(a) = a$, así que σ deja fijo a cada elemento de L. Por lo tanto $\sigma \in G(K/L)$.
Ahora sea $\sigma \in G(K/L)$.
Para mostrar que $\sigma \in \overline{H}$, debemos mostrar que para cada $H' \in \mathbb{N}$, $H \cap \sigma H' \neq \emptyset$.

Ya que el campo fijo de H' es una extensión finita separable de k, es de la forma $k(a)$ para algún $a \in K$, esto es por el Teorema del elemento primitivo.

Sea $F \subseteq K$ extensión normal finita de L tal que $a \in F$.
Si $\rho \in H$, entonces $\rho|_F$ es un L- automorfismo de F y pertenece a $G(F/L)$.
Se sigue que todos los elementos de $G(F/L)$ se obtienen de la misma forma,

ya que L es exactamente el campo fijo de H. La restricción de σ a F es algún elemento de $G(F/L)$ y existe un elemento $\tau \in H$ tal que $\sigma(b) = \tau(b)$ para todo $b \in F$. En particular, $\sigma(a) = \tau(a)$ y por lo tanto $\sigma^{-1}\tau$ fija a cada elemento de $k(a)$, es decir, $\sigma^{-1}\tau \in H'$. Entonces $\tau \in H \cap \sigma H'$. ■

Teorema 3.2.2. *Sea K una extensión de Galois de k. Entonces existe una correspondencia uno a uno entre los subgrupos cerrados de $G(K/k)$ y los campos L tales que $k \subseteq L \subseteq K$.*
Esta correspondencia es $L \leftrightarrow G(K/L)$.

Demostración. Definimos un mapeo del conjunto de subgrupos cerrados de $\mathbb{G}$ en el conjunto de todos los campos L, con $k \subseteq L \subseteq K$ como sigue:

$$\phi : \{H \leq \mathbb{G} | H \ \ cerrado \ \ en \ \ \mathbb{G}\} \rightarrow \{L \leq K | k \subseteq L \subseteq K\}$$
$$\phi(H) = F(H)$$

donde $F(H)$ denota el campo fijo de H.
Probaremos que ϕ es biyectiva.
i) ϕ es inyectiva.
Sean H_1, H_2, subgrupos cerrados de $\mathbb{G}$, tal que $\phi(H_1) = \phi(H_2)$
Entonces $F(H_1) = F(H_2)$, y por la Proposición 3.2.1:

$$H_1 = \overline{H}_1 = G(K/F(H_1)) = G(K/F(H_2)) = \overline{H}_2 = H_2$$

Por lo tanto el mapeo es inyectivo.

ii) ϕ es suprayectiva.
Sea $k \subseteq L \subseteq K$ y sea $H = G(K/L)$. Sea $F(H)$ el campo fijo de H. Probaremos que $F(H) = L$, es decir, probaremos que el campo fijo de $G(K/L)$ es justamente L. Se sigue de la Proposición 3.2.1 que $G(K/F(H))$ es un subgrupo cerrado de $\mathbb{G}$.
Ya que $L \subseteq F(G(K/L)) = F(H)$, sólo tenemos que probar que $F(H) = F(G(K/L)) \subseteq L$, para ello mostraremos que si $a \notin L$, entonces $\sigma(a) \neq a$ para algún $\sigma \in G(K/L)$.
Sea L' una extensión normal finita de L en K tal que $a \in L'$. Ya que $a \notin L$ existe un L-automorfismo τ de L' tal que $\tau(a) \neq a$. Por la Proposición 1.5.4 existe un L-automorfismo σ de K tal que $\sigma(b) = \tau(b)$ para todo $b \in L'$. Entonces $\sigma \in G(K/L)$ y $\sigma(a) \neq a$. ■

Como lo mencionamos en la Observación 3.1.6 para cuando K/k es finita, la topología de Krull definida en $G(K/k)$ es la topología discreta, es decir, todos los subgrupos de $G(K/k)$ son cerrados y para este caso en particular tenemos:

Teorema 3.2.3. *Sea K una extensión finita de Galois. Entonces existe una correspondencia uno a uno entre los campos L tal que $k \subseteq L \subseteq K$ y los subgrupos de $G(K/k)$. Esta correspondencia está dada por*

$$L \leftrightarrow G(K/L).$$

Si $k \subseteq L \subseteq K$, entonces L es extensión de Galois de k si y sólo si $G(K/L)$ es un subgrupo normal de $G(K/k)$. En este caso

$$G(L/k) \cong G(K/k)/G(K/L).$$

Para finalizar este trabajo damos un ejemplo donde tenemos una extensión infinita $K/\mathbb{Q}$ donde la correspondencia entre subgrupos del grupo de Galois $G(K/\mathbb{Q})$ y las extensiones intermedias no es biyectiva, de hecho en el ejemplo veremos que por un lado hay un número no numerable de subgrupos de $G(K/\mathbb{Q})$ y por otro sólo un número numerable de campos intermedios entre $\mathbb{Q}$ y K.
Sea C la cerradura algebraica del campo $\mathbb{Q}$ de los números racionales y sea K el compuesto de todas las extensiones cuadráticas de $\mathbb{Q}$ en C. No existe dificultad en mostrar que $K = \mathbb{Q}(S)$, donde $S = \{\sqrt{p} : p = -1 \ o \ p \ es \ primo\}$.
Sea $G(K/\mathbb{Q})$ el grupo de automorfismos de K que dejan fijo a los elementos de $\mathbb{Q}$
Para cualquier $\sigma \in G(K/\mathbb{Q})$ y cualquier $\sqrt{p} \in S$, $\sigma(\sqrt{p})$ debe ser una raíz de $x^2 - p$, así que $\sigma(\sqrt{p}) = \sqrt{p}$ o $\sigma(\sqrt{p}) = -\sqrt{p}$, por lo que en cualquiera de los dos casos $\sigma^2 = id_K$. Entonces cada elemento de $G(K/\mathbb{Q})$ es de orden 2, por lo que podemos considerar a $G(K/\mathbb{Q})$ como un $\mathbb{Z}_2$-espacio vectorial y como tal tendrá una base B. Para cada subconjunto T de S, existe $\sigma \in G(K/\mathbb{Q})$ tal que $\sigma(\sqrt{p}) = -\sqrt{p}$ para todo $\sqrt{p} \in T$ y $\sigma(\sqrt{p}) = \sqrt{p}$ para todo $\sqrt{p} \in S - T$. Denotemos por σ_T a este automorfismo. Por otro lado, cualquier $\sigma \in G(K/\mathbb{Q})$ determina un subconjunto T de S que es $T = \{\sqrt{p} | \sigma(\sqrt{p}) = -\sqrt{p}\}$. Así pues la función $\varphi : \wp(S) \to G(K/\mathbb{Q})$,con

$\wp(S)$ el conjunto potencia de S, es biyectiva y entonces tienen la misma cardinalidad. Pero S es numerable, así que $card(G(K/\mathbb{Q})) = 2^{\chi_0}$, donde χ_0 es la cardinalidad de los números naturales y por lo tanto $G(K/\mathbb{Q})$ es no numerable. Esto implica que B es no numerable, ya que si B lo fuera, puesto que cada elemento de $G(K/\mathbb{Q})$ es combinación lineal finita de elementos de B y teniendo en cuenta que el campo es $\mathbb{Z}_2$, cada elemento de $G(K/\mathbb{Q})$ determina un subconjunto finito de S, e inversamente cada subconjunto finito de S determina un único elemento de $G(K/\mathbb{Q})$, por lo que, debido a que la cardinalidad del conjunto de subconjuntos finitos de S coincide con la de S, tendríamos que $G(K/\mathbb{Q})$ es numerable, que ya hemos visto que no lo es.
Por otro lado, para cada $\tau \in B$, el subgrupo generado por $B - \{\tau\}$ es de índice dos en $G(K/\mathbb{Q})$. Entonces $G(K/\mathbb{Q})$ tiene un número no numerable de subgrupos de índice 2. Sin embargo es claro que sólo hay un número numerable de extensiones cuadráticas de $\mathbb{Q}$.

Conclusiones

El objetivo de este trabajo consistió en presentar la generalización del Teorema Fundamental de la Teoría de Galois para extensiones finitas. Esto consiste en caracterizar a los subgrupos del grupo de Galois de una extensión infinita de Galois correspondientes a un campo intermedio. Concretamente, los subgrupos de la forma $G(K/L)$, para un campo intermedio L ($k \subseteq L \subseteq K$) son precisamente los subgrupos cerrados de $G(K/k)$ respecto a cierta topología, la así llamada topología de Krull.
Para llegar a este importante resultado hicimos uso de varios conceptos y resultados de la Teoría de Galois para extensiones finitas, así como de Topología y conocimientos básicos de Grupos Topólogicos.

Bibliografía

[Mc] McCarthy, Paul J., *Algebraic Extensions of Fields*, University of Kansas, New York, 1966.

[Za] Zaldívar, Felipe, *Teoría de Galois*, Universidad Autónoma Metropolitana, México, 1996.

[We] Weintraub, Steven H., *Galois Theory*, Springer, New York, London, 2006.

[Mp] Morandi, Patrick, *Field and Galois Theory*, Springer, New York, 1996.

[Bu] Bourbaki, Nicolas, *Elements of mathematics, general topology*, Hermann, Paris, 1966.

[Or] Rendón, Oscar, *Grupos topológicos*, Universidad Autónoma Metropolitana, México, 1997.