Universidad Nacional Autónoma de México

Facultad de Ciencias

Teoría de Galois para extensiones infinitas

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemático

PRESENTA:

Victor Jesús Segundo Gutiérrez

TUTOR

Dr. Valente Santiago Vargas

CIUDAD UNIVERSITARIA, CD.MX. 2024

Índice general

Introducción

Todo lo que existe se desarrolla y establece relaciones con los demás objetos en más de una forma que se manifiesta en cambios mútuos, inflingiendo un cambio que siempre ocurre sin importar si somos o no sensibles de contemplar este complejo proceso.

La comunicación forma una parte fundamental de la relación entre las distintas especies de seres vivos. La interacción entre éstos se da en primera instancia para sobrevivir y en nuestro caso como humanidad una vez alcanzado cierto grado de desarrollo, para exteriorizar lo que se entiende sobre lo que acaece en la realidad y finalmente para transfigurar el mundo.

Los lenguajes se afilan con estos fines; entender, explicar y trastocar, en un ciclo repetitivo pero cada vez más novedoso sin ser conscientes que la realidad y el pensamiento se están modificando o las implicaciones que estos hechos puedan llegar a tener.

En los inicios de la humanidad se presentan situaciones que no se pueden resolver con un lenguaje convencional; es así que aparecen los primeros vestigios de la Aritmética, el Álgebra y una Geometría aparentemente independientes, que se concentran en resolver problemas de cantidades constantes y no variables. Debieron pasar varios siglos para que estas ideas coagularan y se plantearan métodos sistemáticos que permitieran un progreso en el pensamiento y poder plantear nuevos horizontes de alcances de las técnicas sin estar conscientes de los límites que planteaban sus herramientas. El progreso fue lento pero radical.

Las ideas fundamentales de Evariste Galois (1811-1832), de donde emergió la teoría de Galois como la conocemos hoy día, sucedieron en el siglo XIX, un siglo muy importante históricamente, donde el contexto del lenguaje matemático permitía resolver cuestiones del pasado que se establecian sólo como conjetura o que el contexto histórico o del lenguaje no permitía plantear cierto problema, toda época queda bien delímitada. Desde un punto de vista matemático y en

general científico, el retroceso de la Edad Media en estos campos había quedado medianamente superado entrado el siglo XVIII por los escasos pero grandes avances logrados un siglo atrás como por ejemplo la gestación e invención del cálculo. Sucedió que se toma ventaja de este conocimiento para dar lugar a una revolución industrial que determina una realidad muy compleja de la cual Galois es producto.

Es sabido que el siglo XIX fue una etapa de autocrítica para las matemáticas, al final de este siglo se desarrollaron, entre otras cosas, la Teoría de Grupos y Campos para lograr entender, entre otras cosas, lo que Galois quería decir en sus manuscritos, culminando una parte de la teoría en el Teorema Fundamental de Galois para extensiones finitas.

Los matemáticos de finales del siglo XIX no tardaron en cuestionar si la correspondencia de Galois que se plantea en el teorema fundamental se satisface en las extensiones de grado infinito. Fue en el año de 1901 cuando R. Dedekind proporcionó un ejemplo de una extensión de grado infinito donde dicha correspondencia falla. En 1928 W. Krull proporcionó, de forma novedosa, una topología al grupo de Galois de una extensión infinita para hallar a los subgrupos y campos intermedios que se corresponden de forma biyectiva. De esta forma se lograba la generalización de la teoría de Galois; más aún, la topología de Krull recupera la Teoría Clásica de Galois.
Todos estos progresos impulsaron aún más a la Teoría de Grupos Topológicos, los Grupos Profinitos y, más allá de la realidad o invención, la Teoría Inversa de Galois.

La Teoría de Galois es una nueva herramienta del lenguaje matemático, en primer lugar porque para su desarrollo requiere del desarrollo de conceptos matemáticos como función, simetría, grupo, extensión de campos, anillos y propiedades de éstos, topología y otros más que naturalmente no existían formalmente. En segundo lugar la Teoría de Galois establece la correspondencia entre dos categorías distintas; a una extensión se le asocia un grupo y hay una correspondencia entre los campos intermedios y ciertos subgrupos del grupo asociado, además hay una traducción de unas propiedades de campos a grupos y viceversa, lo cual es novedoso ya que después se encontraron más correspondencias de este tipo entre distintas clases de objetos matemáticos. La correspondencia de Galois es en cierto modo, piedra angular de las matemáticas modernas.

En los primeros dos capítulos del presente trabajo se desarrollan las ideas principales de Teoría de Grupos, Campos y Extensiones de Galois, necesarias para estudiar el teorema de Galois para extensiones finitas. En el tercer capítulo se exponen conceptos y resultados básicos de Grupos Topológicos, Límites inversos y grupos profinitos, indispensables para comprender el desarrollo del capítulo cuatro donde se construye la topología de Krull en el grupo de Galois

de una extensión ya sea finita o infinita. Finalmente, con esta herramienta se prueba que el grupo de Galois, dotado de la topología de Krull, es un grupo topológico y un grupo profinito. El capítulo cuatro termina con el teorema de Krull y en seguida el teorema de Galois para extensiones infinitas. Este trabajo cuenta con un apéndice de Topología donde se exponen todos los elementos de los que se habla en el capítulo tres y cuatro.

Capítulo 1

Preliminares

En este capítulo se exponen conceptos de teoría de grupos, anillos y campos que forman la médula espinal del desarrollo de la teoría de Galois que se expone en los capítulos sucesivos donde la teoría se verá impulsada por la introducción de un grupo asociado a una extensión de campos y una topología asociada a dicho grupo. Muchos resultados de esta sección son tomados de [8] y [20] en donde además pueden hallarse pruebas de lo que aquí no se desarrolla y en otros casos son resultados dejados como ejercicios al lector.

1.1. Grupos, anillos y campos

Definición 1.1 *Un* ***grupo*** *es un par* $(G, \star)$, *donde* G *es un conjunto distinto del vacío y* $\star$ *es una operación binaria sobre* G *que verifica las siguientes propiedades:*

a) $a \star (b \star c) = (a \star b) \star c$ *para todo* $a, b, c \in G$, *es decir,* $\star$ *es asociativa.*

b) Existe $e \in G$ *tal que* $a \star e = e \star a$ *para todo* $a \in G$.

c) Para todo $a \in G$, *existe* $y \in G$ *tal que* $a \star y = y \star a = e$.

Observación 1.2 *Se puede demostrar que en un grupo* $(G, \star)$ *el elemento* $e \in G$ *del inciso b) y el elemento* $y \in G$ *del inciso c) de la definición 1.1 son únicos. Estos elementos se denominan, el* ***neutro*** *o* ***identidad*** *del grupo y el* ***inverso*** *de* a *en el grupo* G, *respectivamente, a este último lo abreviamos por* a^{-1}.

Definición 1.3 *Un grupo* $(G, \star)$ *es* ***abeliano*** *si, para cualesquiera* $a, b \in G$, *se verifica que* $a \star b = b \star a$.
Diremos que un grupo $(G, \star)$ *es* ***no abeliano*** *si existen* $a, b \in G$ *tales que*

$a \star b \neq b \star a$.
Cuando trabajemos con un grupo abeliano, simbolizaremos a la operación del grupo con $+$, *al neutro del grupo como* 0 *y al inverso de* a *como* $-a$.

Observación 1.4 *En caso de no haber confusiones, a un grupo* $(G, \star)$ *lo abreviaremos simplemente con el símbolo* G, *y la operación entre los elementos de* G *se abreviará como* $a \star b = ab$. *También, en caso de haber más de un grupo, abreviaremos el elemento neutro de* G *como* 1_G.

Definición 1.5 *Sean* $(G, \star)$ *un grupo y* $\emptyset \neq H \subseteq G$. *Se dice que* H *es un* ***subgrupo*** *de* G, *si al restringir la operación de* G *a* H *obtenemos una operación que dota a* H *de una estructura de grupo.*

Observación 1.6 *En lo sucesivo, para indicar que* H *es un subgrupo de un grupo* G, *usaremos el símbolo* $H \leq G$.

Proposición 1.7 *Sean* G *un grupo y* $H \subseteq G$. *Entonces,* $H \leq G$ *si y solo si se satisface lo siguiente:*

a) Si e *es el neutro de* G, *entonces* $e \in H$.

b) Para cualesquiera $a, b \in H$ *se tiene que* $a \star b \in H$.

c) Si $a \in H$, *entonces* $a^{-1} \in H$.

Observación 1.8 *En la proposición 1.7, la condición de que* $e \in H$ *garantiza que* $H \neq \emptyset$.

Las condiciones que impone la proposición 1.7 pueden simplificarse en una sola que las involucre. Esto se muestra en la siguiente proposición.

Proposición 1.9 *Sean* G *un grupo y* $\emptyset \neq H \subseteq G$. *Entonces,* H *es un subgrupo de* G *si y solo, si para todo* $a, b \in H$, *se tiene que* $ab^{-1} \in H$.

Demostración. Se deja como ejercicio al lector. □

Ejemplo 1.10 *El lector puede probar que el siguiente conjunto, denominado el* ***centro de G****, es un subgrupo de* G :

$$Z(G) := \{a \in G : ax = xa \text{ para todo } x \in G\}.$$

En general, no todos los subconjuntos no vacíos de un grupo G son subgrupos. Sin embargo, dado un subconjunto $X \subseteq G$, podemos construir un subgrupo a partir de X. En el caso en que X conste de un único elemento podremos clasificar este tipo de grupos.

Definición 1.11 *Sean G un grupo y $X \subseteq G$. El* ***subgrupo generado por X*** *es el subgrupo de G más pequeño que contiene a X. A dicho subgrupo lo abreviaremos por $\langle X \rangle$ y queda descrito como:*

$$\langle X \rangle := \{x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} : \text{con } x_i \in X, e_i = \pm 1, \text{ para todo } i, \text{ y } n \in \mathbb{Z}^+\}.$$

En caso de $X = \emptyset$, se admite que $\langle X \rangle = \{e\}$, donde e es el neutro bajo la operación del grupo G.

Observación 1.12 *Para ver una construcción completa del subgrupo generado por un subconjunto no vacío X de un grupo G, se recomienda ver [20, págs, 22-23].*

Definición 1.13 *Sean G un grupo y $a \in G$. Se define el* ***subgrupo cíclico generado por a,*** *como el subconjunto de G que consta de todas las potencias de a, es decir:*

$$\langle a \rangle := \{a^n \in G : n \in \mathbb{Z}\}.$$

Además, se dice que G es un ***grupo cíclico*** *si existe $a \in G$ tal que $\langle a \rangle = G$.*

El lector puede probar fácilmente que, si G es un grupo cíclico, entonces G es abeliano. Esto nos dice que un grupo no abeliano no puede ser cíclico.

Más adelante definiremos un grupo $\mathbb{V}$ (vea ejemplo 1.17), que nos ayudará a probar que el recíproco de la afirmación anterior es falso.

Definición 1.14 *Sean G un grupo y $a \in G$. Se define el* ***orden de a*** *como la cardinalidad del subgrupo generado por a. El orden de $a \in G$ lo abreviaremos por el símbolo $|\langle a \rangle|$.*

Observación 1.15 *El lector puede probar que, dado un grupo G, el único elemento de orden 1 es la identidad de G.*

Definición 1.16 *Sea G un grupo. El* ***orden de G*** *está definido como el cardinal de G y será denotado por $|G|$.*

De igual forma se puede definir el ***orden de un subgrupo*** *H de G como el cardinal de H visto como grupo.*

Ejemplo 1.17 *En este ejemplo examinaremos un grupo muy importante que se verá involucrado en la teoría posterior.*
Consideremos un conjunto de cuatro elementos $\mathbb{V} = \{e, a, b, c\}$. Al ser un conjunto finito podemos dotarlo de una operación. De forma concreta sus productos y resultados se muestran en la siguiente tabla:

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Con esta operación $\star$, $\mathbb{V}$ se convierte en un grupo, el cual recibe el nombre de ***grupo de Klein****.*
Puede observarse que cada uno de los elementos de $\mathbb{V}$ es de orden 2, y que no es un grupo cíclico pero sí abeliano.

Definición 1.18 *Sean $(G,\star)$ y $(G',\bullet)$ dos grupos. Un* ***morfismo de grupos*** *entre ellos es una función $f : G \longrightarrow G'$ tal que, para todo $a, b \in G$, se tiene:*

$$f(a \star b) = f(a) \bullet f(b).$$

Observación 1.19 *Para simplificar la escritura en la definición de morfismo de grupos, escribiremos $f(ab) = f(a)f(b)$ para todo $a, b \in G$, entendiendo que la operación del lado izquierdo es en G y la operación del lado derecho es la operación en G'.*

Como veremos a continuación, si consideramos un morfismo entre dos grupos, digamos $f : G \longrightarrow G'$, este induce dos subgrupos, uno en G y otro en G', dichos subgrupos serán de mucha importancia en lo sucesivo ya que nos ayudarán a formar nuevos grupos.

Definición 1.20 *Sean G, G' dos grupos y $f : G \longrightarrow G'$ un morfismo de grupos. Se definen el* ***kernel de f*** *e* ***imagen de f****, como los siguientes subconjuntos de G y G', respectivamente:*

$$Ker(f) = \{a \in G : f(a) = 1_{G'}\},$$
$$Im(f) = \{f(a) : a \in G\}.$$

Observación 1.21 *El lector puede verificar que $Ker(f) \neq \emptyset$ y que además $Ker(f) \leq G$. De igual forma, se puede verificar que $Im(f)$ es un subgrupo de G'; más aún, si $H \leq G$, entonces $f(H) \leq G'$.*

Definición 1.22 *Sean G y G' grupos y $f : G \longrightarrow G'$ un morfismo de grupos. Diremos que:*

a) f es un ***monomorfismo*** *si para cualesquiera $x, y \in G$ tales que $f(x) = f(y)$, entonces $x = y$.*

b) f es un ***epimorfismo*** *si $Im(f) = G'$.*

*c) f es un **isomorfismo** de grupos si f es monomorfismo y epimorfismo. Este hecho será denotado por $G \simeq^f G'$.*

Observación 1.23 *Si $f : G \longrightarrow G'$ es un morfismo de grupos, el lector puede probar que f es un monomorfismo si y solo si $Ker(f) = \{1_G\}$.*

Definición 1.24 *Sean G un grupo, $H \leq G$ y $t \in G$. Definimos **una clase lateral izquierda de H en G** como el siguiente subconjunto de G:*

$$tH := \{th : h \in H\}.$$

*De forma similar se define una **clase lateral derecha de H en G** como:*

$$Ht = \{ht : h \in H\}.$$

*Al elemento $t \in G$ se le conoce como un **representante** de la clase lateral ya sea derecha o izquierda.*

Observación 1.25 *a) El lector puede probar que, si tomamos $t = e \in G$ en la definición 1.24 de clase lateral derecha entonces se tiene que $eH = He = H$, donde la igualdad es de conjuntos.*

b) Para cada $t \in G$ se puede crear la respectiva clase izquierda (o derecha), en cuyo caso tendremos el conjunto de clases:

$$\{tH : t \in G\}.$$

Intuitivamente, en este conjunto hay tantas clases izquierdas como elementos de G, sin embargo, hay elementos de G que determinan la misma clase lateral derecha o izquierda. Esto nos hace requerir de un criterio para determinar cuándo dos clases son iguales y es esto lo que motiva la siguiente proposición.

Proposición 1.26 *Sean G un grupo, $H \leq G$ y $t, t' \in G$. Entonces:*

$$Ht = Ht' \text{si y solo si } t \cdot (t')^{-1} \in H.$$

De igual forma, para las clases laterales izquierdas, el lector puede verificar que:

$$tH = t'H \text{ si y solo si } (t')^{-1}t \in H.$$

Demostración. La prueba de este hecho es una aplicación de la definición de clases derechas e izquierdas. □

Observación 1.27 *En lo sucesivo trabajaremos con clases laterales izquierdas, el lector puede enunciar resultados análogos para clases laterales derechas.*

Proposición 1.28 *Sean G un grupo, $H \leq G$ y $t, t' \in G$. Entonces se verifica que:*

$$tH = t'H \text{ o } tH \cap t'H = \emptyset.$$

Demostración. Nuevamente se deja como ejercicio al lector. □

El número de clases izquierdas será muy relevante en un futuro. En el caso finito, el teorema de Lagrange (vea teorema 1.34) nos ayudará a cuantificar este número.

Dados G un grupo y H un subgrupo, puede plantearse la cuestión sobre si hay más clases laterales izquierdas que derechas o viceversa. La siguiente proposición nos indica que estas nociones que parecieran diferir, de hecho coinciden.

Proposición 1.29 *Sean G un grupo y $H \leq G$. Hay una correspondencia biyectiva entre el conjunto de las clases laterales izquierdas y derechas.*

Demostración. Vea [20, teorema 2.10, pág. 25]. □

Definición 1.30 *Sean G un grupo y $H \leq G$. Se define el* ***índice de H en G*** *como la cardinalidad del conjunto de clases laterales izquierdas y será denotado por $[G : H]$.*

Proposición 1.31 *Sean G un grupo, H y N subgrupos de G tales que cumplen $N \leq H \leq G$. Entonces se satisface que $[G : N] = [G : H] \cdot [H : N]$. Por lo tanto, si $N \leq H$ y $[G : N] < \infty$, entonces $[G : H] \leq [G : N]$.*

Demostración. Para ver una prueba consulte [18, teorema 3.1, pág. 62.] □

Observación 1.32 *Si G es cualquier grupo, entonces $G = \bigcup_{g \in G} g\{e\}$. Si G es finito, entonces $[G : \{e\}] < \infty$.*

Observación 1.33 *Al tomar un grupo G y $H \leq G$, entonces H induce una relación de equivalencia en G que, de forma natural, se define como:*

$$\text{Si } t, t' \in G \text{ entonces } t \sim t' \text{ si y sólo si } t(t')^{-1} \in H.$$

Por lo tanto, si $t \in G$, con ayuda de la proposición 1.26 podemos describir su clase de quivalencia inducida por H de la siguiente forma:

$$[t]_\sim = \{t' \in G : t(t')^{-1} = h \in H\} = \{t' \in G : t = t'h \in t'H\} = t'H = tH.$$

Es decir, la partición inducida por la relación de equivalencia consta de las clases laterales izquierdas. Además, el número de elementos en la partición es $[G : H]$.

Al conjunto de todas las clases laterales izquierdas inducidas por un subgrupo de un grupo G lo denotaremos de la siguiente forma:

$$G/H = \{tH : t \in G\}.$$

De igual forma, un subgrupo H de un grupo G induce la siguiente correspondencia de forma natural:

$$\pi : G \longrightarrow G/H \ ,$$
$$t \overset{\pi}{\longmapsto} tH \ .$$

Si al conjunto de clases G/H pudiera dotársele de una operación, podríamos probar que π es efectivamente un morfismo de grupos, que $Ker(\pi) = H$ y que π es suprayectivo.
Sin embargo, en general no es posible dotar a G/H de una operación entre clases que esté bien definida, y es esta la razón de imponer la condición de normalidad (vea definición 1.41) para H que estudiaremos en lo sucesivo.

La prueba del siguiente teorema consta de aplicar la idea de la partición que induce H en G.

Teorema 1.34 (Lagrange) *Si G es un grupo finito y $H \leq G$, entonces $|H|$ divide a $|G|$ y $[G : H] = \frac{|G|}{|H|}$.*

Demostración. Vea [20, teorema 2.11, pág. 26]. □

El siguiente corolario se puede concluir tanto de la proposición 1.31 como del teorema de Lagrange (vea teorema 1.34).

Corolario 1.35 *Si G es un grupo finito y $H \leq G$, entonces $[G : H] < \infty$.*

Demostración. Ya que $|G|$ es finito y $H \leq G$, entonces $|H|$ es finito, por lo tanto, del teorema de Lagrange (vea teorema 1.34) se sigue que $[G : H] < \infty$. □

El teorema de Lagrange puede aplicarse, entre otras cosas, para identificar subgrupos de un grupo dado. Esta podría ser una de las principales cuestiones de la teoría de grupos: clasificar los grupos de cierto orden y para cada uno de ellos establecer la clasificación de sus subgrupos.

El converso del teorema de Lagrange surge como una cuestión natural, sin embargo resulta ser falso, es decir, no es del todo cierto que si d es un divisor del orden de un grupo finito G, entonces exista un subgrupo de G con orden d. Veremos que esto se verifica por lo menos en dos casos, cuando d es un primo o cuando G es un grupo cíclico y que el converso del teorema de Lagrange caracteriza a los grupos cíclicos finitos.

Proposición 1.36 *Sean G un grupo finito y $a \in G$. Entonces el orden de a divide al orden de G.*

Demostración. Es una consecuencia inmediata del teorema de Lagrange. □

El teorema de Lagrange también nos ayuda a reconocer a algunos grupos cíclicos según su orden, esto puede observarse en el siguiente resultado.

Proposición 1.37 *Sea G un grupo tal que $|G| = p$ con p un número primo, entonces G es cíclico.*

Demostración. Se deja como ejercicio para el lector. □

En el caso en el que G es un grupo cíclico y finito de orden mayor a 1, habrá un subgrupo para cada uno de los divisores de $|G|$, en particular se verifica el recíproco del teorema de Lagrange como muestra el siguiente resultado.

Proposición 1.38 *Sea G un grupo de orden finito $n \in \mathbb{Z}^+$. Entonces G es un grupo cíclico si y solo si, para cada divisor d de n, existe a lo más un subgrupo cíclico de G de orden d.*

Demostración. Vea [20, teorema 2.17, pág. 28]. □

Esto es lo más que diremos acerca de los grupos cíclicos, para más información sobre ello le recomendarmos ver [20, pág. 28] y una ingeniosa caracterización de los grupos cíclicos finitos que puede hallar en [17].

Proposición 1.39 (Cauchy) *Sean G un grupo finito y p un primo tal que p divide a $|G|$, entonces existe un elemento en G de orden p.*

Demostración. Vea [20, teorema 4.2, pág 74]. □

Corolario 1.40 *Sean G un grupo finito y p un primo tal que p divide a $|G|$, entonces existe un subgrupo de G de orden p.*

De entre toda la clase de subgrupos de un grupo G, existen unos subgrupos de particular interés que nos ayudan a formar o construir nuevos grupos, los introducimos a continuación y serán de suma importancia en el teorema fundamental de la teoría de Galois (vea teorema 2.75).

Definición 1.41 *Sean G un grupo y $H \leq G$. Se dice que H es un **subgrupo normal** de G si para todo $g \in G$ se tiene que:*

$$H = gHg^{-1}.$$

Equivalentemente, H es un subgrupo normal en G si toda clase izquierda de H en G es una clase derecha, es decir:

$$Hg = gH \text{ para todo } g \in G.$$

Usaremos el símbolo $H \trianglelefteq G$ para indicar que H es un subgrupo normal de G.

Observación 1.42 *Si para un grupo G y $H \leq G$ se verifica que $gHg^{-1} \leq H$ para todo $g \in G$, entonces se verifica que $g^{-1}Hg \leq H$ para todo $g \in G$ y viceversa.*

El lector podrá notar que la siguiente proposición es consecuencia de la definición de subgrupo normal.

Proposición 1.43 *Sean G un grupo, N y H subgrupos de G tales que*

$$N \trianglelefteq G \text{ y } N \subseteq H,$$

entonces $N \trianglelefteq H$.

Demostración. Se deja de ejercicio al lector. □

Ejemplo 1.44 *Note que si G es un grupo y $H \leq Z(G) \leq G$, entonces $H \trianglelefteq G$. Más aún, si G es un grupo abeliano, entonces todos sus subgrupos son normales.*

Observación 1.45 *El lector puede corroborar que el kernel de todo homomorfismo de grupos es un subgrupo normal del dominio.*

Definición 1.46 *Sean G un grupo, $g \in G$ y $H \leq G$. El **subgrupo conjugado** de H, determinado por g, es $gHg^{-1} \leq G$.*

En las siguientes proposiciones veremos que un subgrupo H de un grupo G es normal si contiene a todos sus subgrupos conjugados, y que la intersección de todos los conjugados de un subgrupo es un subgrupo normal en el grupo G.

Proposición 1.47 *Sean G un grupo y H un subgrupo de G. Entonces, H es normal en G si y solo si, para todo $g \in G$, se tiene $gHg^{-1} \leq H$.*

Demostración. Es claro que si H es normal, entonces contiene a todos sus conjugados. Para la otra implicación basta probar que para todo $g \in G$ se tiene $H \leq gHg^{-1}$, suponiendo que $gHg^{-1} \leq H$ para todo $g \in G$. Supongamos entonces que $gHg^{-1} \leq H$ para todo $g \in G$.

Sea $g \in G$, entonces para $h \in H$ se tiene:

$$h = ehe = g(g^{-1}hg)g^{-1} \in gHg^{-1}.$$

Esto ya que por la hipótesis $gHg^{-1} \leq H$ para todo $g \in G$, implica, por la observación 1.42, que $g^{-1}Hg \leq H$.
Así concluimos que $H = gHg^{-1}$ para todo $g \in G$, por lo que H es normal en G. □

Proposición 1.48 *Sean G un grupo y $H \leq G$. Entonces $\mathcal{H} = \bigcap_{a \in G} aHa^{-1} \trianglelefteq G$.*

Demostración. Sea $g \in G$ un elemento arbitrario, entonces:

$$g\mathcal{H}g^{-1} = g\left(\bigcap_{a \in G} aHa^{-1}\right)g^{-1} \subseteq \bigcap_{a \in G} gaH(ga)^{-1} \subseteq \mathcal{H}.$$

Ya que hemos probado que $\mathcal{H}$ contiene a todos sus subgrupos conjugados, entonces, de la proposición 1.47, se sigue que $\mathcal{H} \trianglelefteq G$. □

Si consideramos H y K dos subgrupos de un grupo G, el lector puede verificar que el conjunto $HK := \{hk : h \in H \text{ y } k \in K\}$ contiene al neutro en G (es decir que $HK \neq \emptyset$), pero no necesariamente es un subgrupo de G. Sin embargo, al pedir que K sea un subgrupo normal en G se tiene el siguiente resultado:

Proposición 1.49 *Sean G un grupo y $H, K \leq G$ tales que $K \trianglelefteq G$. Entonces $HK \leq G$.*

Demostración. Se deja la prueba al lector y se le sugiere usar la proposición 1.9. □

Proposición 1.50 *La intersección arbitraria de subgrupos normales de un grupo G es un subgrupo normal en G.*

Demostración. Se deja al lector. □

Proposición 1.51 *Sean G un grupo, H y K subgrupos normales de G. Entonces $HK = KH$.*

Demostración. Sea $\alpha \in HK$, entonces existen $h \in H$ y $k \in K$ tales que $\alpha = hk = ehk = k(k^{-1}hk)$. Como H es normal en G, entonces $k^{-1}hk = h' \in H$ y por lo tanto $\alpha = kh' \in KH$. De forma similar se prueba la otra contención, y de esta manera podemos concluir que $HK = KH$. □

Proposición 1.52 *Sean G un grupo y $H \leq G$ tal que $[G : H] = 2$. Entonces $H \trianglelefteq G$.*

Demostración. En efecto, si $[G : H] = 2$, entonces el conjunto de las clases laterales izquierdas es $\{H, tH\}$, para algún $t \in G \setminus H$.
Si tomamos $g \in G$, ya que H induce una partición en G, tenemos dos casos:

a) Si $g \in H$, es inmediato que si $h \in H$, entonces $ghg^{-1} \in H$, al ser un producto de elementos en H y porque H es cerrado bajo la operación de G.

b) Si $g \in tH$, entonces existe $k \in H$ tal que $g = tk$. Deberíamos probar que para todo $h \in H$, $ghg^{-1} \in H$. Supongamos que $ghg^{-1} \in tH$, por lo tanto existe $h' \in H$ tal que $ghg^{-1} = th'$, al sustituir el valor de g tenemos que:

$$tkhk^{-1}t^{-1} = th'.$$

Multiplicando por t^{-1} de ambos lados y despejando a t se sigue que :

$$t = (h')^{-1}khk^{-1} \in H.$$

Lo cual representa una contradicción a la hipótesis de que $t \in G \setminus H$. Y por lo tanto, debe verificarse que $ghg^{-1} \in H$.
En ambos casos se ha probado que, para todo $g \in G$, se tiene que $gHg^{-1} \subseteq H$. Ahora de la proposición 1.47 se sigue que H es normal en G. □

Si G es un grupo y $H \trianglelefteq G$, se puede verificar que la siguiente operación en el conjunto G/H está bien definida, es decir, que no depende de los representantes de las clases izquierdas:

$$\text{Sean } t, t' \in G, \text{ se define } tH \cdot t'H = tt'H.$$

Proposición 1.53 *Sean G un grupo y $H \trianglelefteq G$. Entonces el conjunto G/H es un grupo con la operación entre clases indicada arriba, y además se tiene que $|G/H| = [G : H]$.*

Demostración. Vea [20, teorema 2.21, pág. 32]. □

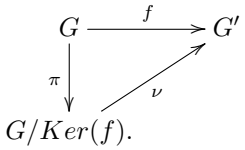
Definición 1.54 *Sean G un grupo y H un subgrupo normal de G. Al grupo G/H que se ha construido en la proposición 1.53, le llamaremos* ***grupo cociente.***

Observación 1.55 *De ahora en adelante, la notación G/H estará reservada exclusivamente para indicar que G/H es un grupo con la operación $\cdot$ admitiendo que H es normal en G.*

Proposición 1.56 (Primer Teorema de Isomorfismo) *Sean G, G' dos grupos y $f : G \longrightarrow G'$ un homomorfismo de grupos. Entonces, la siguiente función:*

$$\nu : G/Ker(f) \longrightarrow Im(f)$$
$$gKer(f) \longmapsto f(g)$$

es un isomorfismo de grupos, y es tal que el siguiente diagrama conmuta:



Es decir, $f = \nu \circ \pi$, donde π es el morfismo canónico introducido en la observación 1.33.

Demostración. Vea [20, teorema 2.24, pág. 35]. □

Proposición 1.57 (Segundo teorema de isomorfismo) *Sea N y H subgrupos de un grupo G, con N normal en G. Entonces $N \cap H \trianglelefteq H$ y además:*

$$H/H \cap N \simeq NH/N.$$

Demostración. Vea [20, teorema 2.26, pág. 34]. □

Proposición 1.58 (Tercer teorema de isomorfismo) *Sean G un grupo y $H, K \trianglelefteq G$ tales que $K \leq H \leq G$. Entonces H/K es un subgrupo normal de G/K y:*

$$G/H \simeq (G/K)/(H/K).$$

Demostración. Vea [20, teorema 2.27, pág. 37]. □

Teorema 1.59 (Teorema de la correspondencia biyectiva) *Sean G un grupo, K un subgrupo normal en G y $\pi : G \longrightarrow\!\!\!\!\!\rightarrow G/K$ la proyección canónica (vea observación 1.33). Entonces, el morfismo canónico π proporciona una correspondencia biyectiva entre todos los subgrupos de G que contienen a K y todos los subgrupos de G/K.*
Más aún, se satisface lo siguiente:

a) Si H, L son subgrupos de G, entonces:

$$K \leq H \leq L \leq G \text{ si y solo si } H/K \leq L/K \leq G/K.$$

Además: $[L : H] = [L/K : H/K]$.

b) Si H, L son subgrupos de G tales que $K \leq H \leq L$, entonces:

$$H \trianglelefteq L \text{ si y solo si } H/K \trianglelefteq L/K.$$

Además, del tercer teorema de isomorfismo (vea teorema 1.58), se sigue que:

$$(L/K)\,/\,(H/K) \simeq L/H.$$

Demostración. Para revisar una prueba de este importante teorema le recomendamos ver [20, teorema 2.28, pág. 38]. □

Definición 1.60 *Sea X un conjunto arbitrario no vacío. Una* ***permutación*** *de los elementos de X es una función biyectiva $f : X \longrightarrow X$. El conjunto de todas las permutaciones de X es abreviado por el símbolo S_X, es decir:*

$$S_X := \{ f : X \longrightarrow X \ : f \text{ es biyectiva}\}.$$

El conjunto S_X es un grupo con la operación composición de funciones. Más aÃºn, si $|X| < \infty$, entonces $|S_X| = |X|!$

Observación 1.61 *Para ver una construcción y detalles sobre las propiedades del grupo de permutaciones, vea [20, permutaciones, pág. 2].*

Teorema 1.62 (Cayley) *Todo grupo G es isomorfo a un subgrupo de $S_{|G|}$. En particular, si $|G| = n$, entonces G es isomorfo a un subgrupo de S_n.*

Demostración. [20, teorema 3.12, pág. 52]. □

Si todo grupo G tiene una representación en $S_{|G|}$, entonces podemos pensar que ya se conocen todos los grupos; de aquí surge la duda ¿por qué se trabaja con un grupo G arbitrario en lugar de buscar su representación en $S_{|G|}$ y trabajar con ello? La respuesta es que $S_{|G|}$ tiene un orden demasiado grande en comparación con $|G|$ y es complicado buscar su representación incluso cuando G es finito, además, la operación composición es algo de compleja manipulación dada la naturaleza de los elementos en $S_{|G|}$.
La siguiente definición y resultados serán utilizados al final del capítulo 2, donde daremos algunos ejemplos de polinomios que son solubles por radicales. Omitiremos la prueba de cada uno de estos resultados.

Definición 1.63 *Se dice que un grupo G es* ***soluble*** *si existe una cadena ascendente y finita de la siguiente forma:*

$$H_0 := \{e\} \subseteq H_1 \subseteq ... \subseteq H_{n-1} \subseteq H_n = G,$$

tal que para todo $i = 0, ..., n-1$, $H_i \trianglelefteq H_{i+1}$ y el cociente H_{i+1}/H_i es abeliano.

Proposición 1.64 *Sea G un grupo. Entonces se verifican las siguientes propiedades:*

a) Si G es soluble, entonces todo subgrupo de G es soluble.

b) Si $H \trianglelefteq G$ y G es soluble, entonces G/H es soluble.

c) Si $H \trianglelefteq G$ y tanto H como G/H son solubles, entonces G es soluble.

Demostración. Para ver una prueba vea [26, teorema 5.17, pág. 156]. □

Proposición 1.65 *Si G es un grupo finito tal que $|G| < 60$, entonces G es soluble.*

Demostración. Vea [20, ejercicio 5.21, pág. 107]. □

De la proposición anterior y del hecho de que $|S_n| = n!$, se obtiene el siguiente resultado.

Proposición 1.66 *Para todo $n \leq 4$, el grupo S_n es soluble.*

Proposición 1.67 *Para todo $5 \leq n, S_n$ no es soluble.*

Demostración. [26, corolario 5.19, pág. 158]. □

Proposición 1.68 *Si G es un grupo abeliano, entonces G es soluble.*

Demostración. Se deja de ejercicio al lector. □

El siguiente resultado tiene un enunciado simple que es el primer paso para intentar caracterizar a los grupos solubles respecto a su orden.

Teorema 1.69 *Todo grupo finito de orden impar es soluble.*

Demostración. Vea el artículo [10]. □

A continuación se enuncian los resultados más importantes sobre los teoremas de Sylow, que nos ayudan a identificar los sugbrupos de un grupo, y por tanto, nos permiten clasificar los grupos.

Teorema 1.70 *Sea p un primo. Si G es un grupo finito de orden $p^k m$ con $(p, m) = 1$, entonces todo $p-$subgrupo de Sylow P de G tiene orden p^k.*

Demostración. Vea [20, teorema 4.14, pág. 80]. □

Corolario 1.71 *Sean G un grupo finito y p un primo. Si p^k divide a $|G|$, entonces G contiene un subgrupo de orden p^k.*

Demostración. Vea [20, corolario 4.15, pág. 80]. □

Teorema 1.72 *Si G es un grupo finito de orden $p^n m$ con p un primo y $(p, m) = 1$, entonces G tiene un subgrupo de orden p^n.*

Demostración. Vea [20, Teorema 4.17, pág. 81]. □

1.1.1. Anillos

En esta sección empezamos exponiendo la noción de anillo la cual se obtiene a partir de un grupo abeliano que se le dota de una nueva operación llamada producto. Los anillos son un buen ejemplo de una estructura algebraica que se construye a partir de un objeto con *menos* estructura. Nosotros nos enfocaremos en exponer nociones tales como elementos unidad, asociados y elementos irreducibles en un anillo que dan lugar a factorizaciones de ciertos elementos del anillo en elementos más básicos. Estos conceptos dan lugar a una nueva clase de anillos llamados de factorización única que veremos en este capítulo con el fin de que todo este contenido tenga una aplicación en la sección 1.2, aquí estudiamos y damos ejemplosde los conceptos mencionados en el anillo de polinomios $R[x]$ asociado a un anillo R.

Definición 1.73 *Un* ***anillo conmutativo con 1*** *es una terna $(R, +, \cdot)$, donde R es un conjunto no vacío, $+$ y $\cdot$ son operaciones sobre R, que verifican las siguientes propiedades:*

a) $(R, +)$ *es un grupo abeliano.*

b) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *para todo* $a, b, c \in R$*, es decir, que la operación* $\cdot$ *es asociativa.*

c) Existe $1 \in R$ *tal que, para todo* $a \in R$ *se tiene* $a \cdot 1 = 1 \cdot a = a$.

d) $a \cdot b = b \cdot a$*, para todo* $a, b \in R$*. En este caso diremos que los elementos de R conmutan bajo el producto.*

e) $a \cdot (b + c) = a \cdot b + a \cdot c$*, para todo* $a, b, c \in R$*, es decir, la operación* $\cdot$ *se distribuye sobre la suma.*

Observación 1.74 *a) Las operaciones $+$ y $\cdot$ de un anillo conmutativo se denominan suma y producto de R respectivamente.*

b) Si $(R, +, \cdot)$ es un anillo conmutativo con 1, en general no es cierto que $(R, \cdot)$ es un grupo, ya que no necesariamente todo elemento de R posee un inverso multiplicativo. Sin embargo, al igual que en un grupo, puede probarse que el elemento 1 es único en R. A este último se le llama neutro para el producto de R.

c) Si $(R, +, \cdot)$ es un anillo conmutativo con 1, al neutro del grupo abeliano $(R, +)$ lo denotaremos como 0.

d) En caso de no haber confusión a un anillo conmutativo $(R, +, \cdot)$ lo escribiremos simplemente con R, la suma entre dos elementos a y b de R como $a + b$ y el producto de ellos como ab. En ocasiones, para enfatizar al elemento neutro para el producto de R lo escribiremos como 1_R.

Definición 1.75 *Sea R un anillo conmutativo con 1. Decimos que R es un* ***dominio entero*** *si, dados cualesquiera $a, b \in R$ tales que $a \cdot b = 0$, se tiene que $a = 0$ o $b = 0$.*

Observación 1.76 *En este trabajo solamente estudiaremos anillos conmutativos con 1, y para referirnos a ellos usaremos la denominación de anillo. Cuando se presente la situación, aclararemos si se pide la condición de que el anillo sea dominio entero.*

Definición 1.77 *Sean R un anillo y $S \subseteq R$ con $S \neq \emptyset$. Decimos que S es un* ***subanillo*** *de R si las restricciones de las operaciones $+$ y $\cdot$ de R a S son operaciones que hacen de S un anillo, y además $1_S = 1_R$.*

Proposición 1.78 *Sean R un anillo y $\{S_\alpha\}_{\alpha \in I}$ una familia de subanillos de R. Entonces $\bigcap_{\alpha \in I} S_\alpha$ es un subanillo de R.*

Demostración. La demostración se deja como ejercicio. □

Dado un anillo cualquiera, hay una variada clase de elementos que nos ayudan a obtener información sobre él. Un caso es la aglomeración de tales elementos en subconjuntos como los siguientes.

Definición 1.79 *Sean R un anillo e $\emptyset \neq I \subseteq R$. Llamamos a I un* ***ideal*** *de R si verifica las siguientes dos condiciones:*

a) $(I, +)$ es un subgrupo de $(R, +)$.

b) Para todo $a \in R$ y $b \in I$, se tiene que $ab \in I$.

La noción de ideal es importante pues nos permite construir el anillo cociente, como lo muestra la siguiente definición.

Definición 1.80 *Sean R un anillo e I un ideal. En el grupo cociente $R/I = \{a + I : a \in I\}$ se tienen dos operaciones bien definidas*

$$+ : R/I \times R/I \longrightarrow R/I, \qquad \cdot : R/I \times R/I \longrightarrow R/I,$$

dadas como siguen:

$$(a + I) + (b + I) := (a + b) + I \text{ y } (a + I) \cdot (b + I) := ab + I,$$

para todos $a + I, b + I \in R/I$. Estas dos operaciones dotan de estructura de anillo al grupo cociente R/I y a tal anillo lo llamaremos ***anillo cociente****.*

Observación 1.81 *El lector puede verificar fácilmente, usando el hecho que I es un ideal, que R/I es un anillo.*

Proposición 1.82 *Si R es un anillo e $\{I_i\}_{i\in I}$ es una familia de ideales de R, entonces $\bigcap_{i\in I} I_i$ es un ideal de R.*

Definición 1.83 *Sean R un anillo y $X \subseteq R$. El* ***ideal generado por*** *X, denotado por $\langle X\rangle$, se define como:*

$$\langle X\rangle = \bigcap\{I : I \text{ ideal de } R \text{ y } X \subseteq I\}.$$

Si X es un subconjunto finito de R, entonces $\langle X\rangle$ se llama ***el ideal finitamente generado por*** *X. Si $X = \{x_0\} \subseteq R$ e I es el ideal generado por X, entonces diremos que I es el* ***ideal principal generado por*** *x_0.*

Observación 1.84 *a) Si I es el ideal finitamente generado por el subconjunto $X = \{x_0, ..., x_n\}$, entonces todo elemento de I se puede escribir como una combinación lineal de elementos de X. Es decir, si $x \in I$, entonces existen $a_0, ..., a_n \in R$ tales que $x = a_0x_0 + ... + a_nx_n$. En este caso, abreviaremos a I como $I = \langle x_0, ..., x_n\rangle$.*

b) Si I es el ideal principal generado por $x_0 \in R$, por la anterior observación se sigue que si $x \in I$, entonces $x = ax_0$ para algún $a \in R$.

Definición 1.85 *Sea R un anillo. Se dice que R es un* ***dominio de ideales principales*** *si todo ideal de R es principal.*

Definición 1.86 *Sean R un anillo y $a, b \in R$. Decimos que* ***a divide a b*** *si existe $k \in R$ tal que $ak = b$. Este hecho lo abreviaremos como $a|b$.*

Observación 1.87 *Puede probarse que, si R es un dominio entero y además a y b son elementos de R tales que $a|b$, entonces el elemento k que existe tal que $ak = b$, es único con dicha propiedad. Dejamos la prueba de este hecho a nuestro lector.*

Definición 1.88 *Consideremos un anillo R.*

a) Un elemento $u \in R\backslash\{0\}$ se llama ***unidad*** *si existe $v \in R$ tal que $uv = 1$. Al subconjunto de unidades del anillo lo abreviaremos por $U(R)$ y si u es una unidad, entonces aquel $v \in R$ que existe tal que $u \cdot v = 1$ lo denotaremos por $v := u^{-1}$.*

b) Decimos que dos elementos $a, b \in R \setminus \{0\}$ son ***asociados*** *si existe $u \in U(R)$ tal que $a = bu$. En este caso también decimos que los elementos a y b difieren en una unidad.*

c) *Si R es un dominio entero, un elemento $a \in R \setminus (U(R) \cup \{0\})$ será llamado* ***irreducible*** *de R si siempre que $a = bc$, entonces $b \in U(R)$ o bien $c \in U(R)$.*

d) *Si R es un dominio entero, un elemento $a \in R \setminus \{0\}$ es* ***reducible*** *si no es irreducible.*

e) *Si R es un dominio entero, diremos que un elemento $p \in R \setminus \big(U(R) \cup \{0\}\big)$ es* ***primo*** *si, para cualesquiera $a, b \in R$ tales que $p|ab$, se tiene $p|a$ o $p|b$.*

Observación 1.89 *a) El conjunto $(U(R), \cdot, 1)$ constituye un grupo.*

b) *El lector puede probar fácilmente que si R es un dominio entero y $p \in R \setminus \{0\}$ es un elemento primo, entonces p es un irreducible de R.*

Si R es un dominio entero, en general no es cierto que todo elemento irreducible de R es primo, sin embargo, esto sí se satisface bajo la condición de que R es un dominio de factorización única.

Definición 1.90 *Un* ***dominio de factorización única*** *es un dominio entero R tal que todo elemento $a \in R \setminus (U(R) \cup \{0\})$ se factoriza de forma única, salvo asociados, como producto finito de elementos irreducibles, es decir, existen $q_1, ..., q_n \in R$ irreducibles tales que:*

$$a = q_1 \cdots q_n.$$

Y si $q'_1, ..., q'_m \in R$ son irreducibles tales que $a = q'_1 \cdots q'_m$, entonces $m = n$ y existen $u_1, ..., u_n \in U(R)$ y $\sigma \in S_n$ tales que para cada $i \in \{1, ..., n\}$ se tiene que $q_i = u_i q'_{\sigma(i)}$, es decir que q_i y $q'_{\sigma(i)}$ difieren en una unidad.

Proposición 1.91 *Sea R un dominio de factorización única. Tomemos un elemento $p \in R \setminus (U(R) \cup \{0\})$, entonces:*

$$p \text{ es primo en } R \text{ si y solo si } p \text{ es irreducible en } R.$$

Demostración. Vea [8, proposición 12, pág. 286]. □

Observación 1.92 *El ejemplo típico de dominio de factorización única es el anillo de los enteros $\mathbb{Z}$. En la sección 1.2 se construirá un anillo muy especial que será un dominio de factorización única y que será el objeto de estudio a lo largo de todo este texto. Al momento de llegar a esa sección ya no mencionaremos este hecho, sin embargo es una consecuencia inmediata a partir de resultados anteriores que se exponen en [8, corolario 5, pág. 300].*

El estudio de los anillos también abarca la comparación de las propiedades que tienen éstos mediante el siguiente concepto.

Definición 1.93 *Sean $(R, +_R, \cdot_R)$ y $(R', +_{R'}, \cdot_{R'})$ dos anillos. Un* ***morfismo de anillos*** *entre ellos es una función $f : R \longrightarrow R'$ tal que, para cualesquiera $a, b \in R$, se satisfacen las siguientes condiciones:*

a) $f(a +_R b) = f(a) +_{R'} f(b)$. *Es decir, que f es un morfismo de grupos abelianos.*

b) $f(a \cdot_R b) = f(a) \cdot_{R'} f(b)$.

c) $f(1_R) = 1_{R'}$.

Observación 1.94 *Para simplificar la notación de la definición 1.93, los incisos (a) y (b) los escribiremos, respectivamente, como:*

$$f(a + b) = f(a) + f(b) \text{ y } f(ab) = f(a)f(b),$$

sobreentendiendo que del lado izquierdo de cada igualdad tenemos operaciones en R y del lado derecho operaciones en R'.

Proposición 1.95 *Sea $f : R \longrightarrow R'$ un morfismo de anillos, entonces:*

a) El inciso c) de la definición 1.93, nos dice que todo morfismo de anillos conmutativos con 1 es distinto de cero.

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

c) $f(-a) = -f(a)$ *para todo* $a \in R$.

d) Si $u \in R$ es una unidad, entonces $f(u)$ es una unidad de R'.

e) Si $u \in R$ es una unidad, entonces $f(u^{-1}) = f(u)^{-1}$.

Proposición 1.96 *Sean R y R' dos anillos y $f : R \longrightarrow R'$ un morfismo entre ellos. Las siguientes propiedades se satisfacen:*

a) Si S es un subanillo de R, entonces $f(S)$ es un subanillo de R'.

b) Si I es un ideal de R', entonces $f^{-1}(I)$ es un ideal de R .

c) Si I es un ideal de R, entonces $f(I)$ es un ideal de $f(R)$.

Definición 1.97 *Sean R y R' dos anillos y $f : R \longrightarrow R'$ un morfismo entre ellos. Se define el* ***kernel*** *e* ***imagen*** *de f, respectivamente, como los siguientes conjuntos:*

$$Ker(f) = \{x \in R : f(x) = 0\},$$
$$Im(f) = \{f(a) \in R' : a \in R\}.$$

Observación 1.98 *Se deja como ejercicio al lector probar que $Ker(f)$ es un ideal propio de R, y que, $Im(f)$ es un subanillo de R'.*

Definición 1.99 *Sea $f : R \longrightarrow R'$ un morfismo entre los anillos R y R'.*

*a) Se dice que f es un **morfismo inyectivo** si, para cualesquiera $x, y \in R$ tales que $f(x) = f(y)$, se verifica $x = y$.*

*b) f es un **morfismo suprayectivo** si $Im(f) = R'$.*

*c) f es un **isomorfismo** si es un morfismo inyectivo y suprayectivo.*

Proposición 1.100 *Sea $f : R \longrightarrow R'$ un morfismo entre los anillos R y R'. Entonces, f es un morfismo inyectivo si y solo si $Ker(f) = \{0\}$.*

Demostración. La demostración se deja como ejercicio al lector. □

1.1.2. Campos

Definición 1.101 *Un conjunto K es un **campo** si K es un anillo tal que todos sus elementos distintos de cero son unidad, es decir, si para todo $a \in K \setminus \{0\}$, existe $a^{-1} \in K$ tal que $a \cdot a^{-1} = 1$.*

Observación 1.102 *Si K es un campo, entonces K es un dominio entero.*

Definición 1.103 *Sean K un campo y $\emptyset \neq K' \subseteq K$. Diremos que K' es un **subcampo de K** si es un subanillo de K y para todo $a \in K' \setminus \{0\}$, se tiene que $a^{-1} \in K'$.*

Observación 1.104 *a) Los ideales de un campo se corresponden con la definición 1.79 de ideales en un anillo.*

b) Si $\emptyset \neq I$ es un ideal de un campo K, entonces $I = \{0\}$ o bien $I = K$. Más aún, un anillo K es un campo si sus únicos ideales son K y $\{0\}$.

Definición 1.105 *Sean K y F dos campos. Un **morfismo de campos** entre ellos es un morfismo de anillos $f : F \longrightarrow K$ (vea definición 1.93).*

Observación 1.106 *a) Las nociones de **inyectividad**, **imagen** y **suprayectividad** para un morfismo de campos, coinciden con las nociones de inyectividad, imagen y suprayectividad de morfismo entre anillos, vea definición 1.99. Además, si un morfismo entre campos es inyectivo y suprayectivo, le llamaremos **isomorfismo***

b) Por el inciso a) de la observación 1.95, todo morfismo de campos es no cero; y por el inciso b) de la observación 1.104 tenemos que $Ker(f) = \{0\}$, es decir, todo morfismo entre campos es inyectivo.

Observación 1.107 *Sea $f : F \longrightarrow K$ un morfismo entre los campos F y K. Ya que f es un morfismo inyectivo entre dos campos, en este caso pensaremos a F como un sumergimiento dentro de K, esto es, consideraremos a F como un subcampo de K. En un futuro inmediato veremos la relevancia de este hecho al desarrollar la definición 1.139.*

Proposición 1.108 *Sean F, F' campos y $f : F \longrightarrow F'$ un morfismo de campos. Entonces $Im(f)$ es un subcampo de F' isomorfo a F.*

Demostración. Por el inciso a) de la proposición 1.96, tenemos que $Im(f)$ es un subanillo de F'.
Ahora tomemos $f(a) \in Im(f) \setminus \{0\}$. Por el inciso b) de la observación 1.106, f es inyectivo, entonces $a \in F \setminus \{0\}$, y al ser F un campo, existe $a^{-1} \in F$ tal que $a \cdot a^{-1} = 1_F$. Al aplicar f, junto con las propiedades de morfismo de campos (vea definición 1.93) y del inciso e) de la proposición 1.95 se sigue que, $1_{F'} = f(a)f(a^{-1}) = f(a) \cdot f(a)^{-1}$.
Por lo tanto $f(a)^{-1}$ es el inverso multiplicativo de $f(a)$, y así concluimos que $Im(f)$ es un subcampo de F'. □

Proposición 1.109 *Sean K un campo y $\{F_\alpha\}_{\alpha \in I}$ una familia de subcampos de K. Entonces $\bigcap_{\alpha \in I} F_\alpha$ es un subcampo de K.*

Demostración. La prueba se deja de ejercicio al lector. □

Definición 1.110 *Se define el **campo primo** de un campo K como la intersección de todos los subcampos de K.*

1.2. El anillo de polinomios

Seguramente el lector ya habrá tenido contacto con el anillo de polinomios a una edad temprana. Sin embargo, como es usual en matemáticas, dicho anillo puede construirse mediante un método muy interesante para otros fines, pero poco práctico al momento de estudiar las relaciones entre los elementos de este conjunto, no obstante, el método le da un fundamento a las consecuencias de tal construcción.

Nuestro estudio comenzará a partir de la definición de polinomio en un anillo R de una manera informal, así que, para el lector interesado en estudiar dos construcciones, vea [12, pág. 97] y [1, pág. 25].

Definición 1.111 *Sea R un anillo. Se define un **polinomio en variable x con coeficientes en R** como una expresión de la siguiente forma:*

$$f(x) := a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0,$$

donde $n \in \mathbb{N}$ y $a_i \in R$ para todo $i \in \{0, \cdots, n\}$. Decimos que a_i es el coeficiente de x_i en f para todo $i \in \{1, ..., n\}$.
*El **grado** de un polinomio f, denotado por $grad(f)$, es el mayor exponente con el cual aparece la variable x y cuyo coeficiente es distinto de cero, a tal coeficiente se le llama **coeficiente principal**. Los polinomios constantes no nulos, es decir, a los elementos del anillo no nulos tienen el grado igual a cero. Al término a_0 se le denomina **término independiente**. Al polinomio 0 no se le asocia grado, sin embargo, en caso de requerirlo se le asociará el grado $-\infty$ y es el único polinomio al cual se le asigna tal grado. Un polinomio es llamado **mónico** si su coeficiente principal a_n es igual a 1.*

***Notación:** Al conjunto de todos los polinomios en una variable con coeficientes en un anillo R lo denotaremos por el símbolo $R[x]$.*

Definición 1.112 *Sean R un anillo y $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{j=0}^{m} b_j x^j$ dos polinomios en $R[x]$. La **igualdad de polinomios** en una variable se define como:*

$$f(x) = g(x) \text{ si y solo si } m = n \text{ y } a_i = b_i \text{ para todo } i \in \{0, ..., n\}.$$

Definición 1.113 *Sea R un anillo. El conjunto de polinomios con coeficientes en R, es decir $R[x]$, es un anillo conmutativo con 1 con las operaciones de suma y producto definidas como sigue:*

Para $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$ dos polinomios cualesquiera en $R[x]$ y sin pérdida de generalidad supongamos que $n \leq m$, se define la suma y producto de f y g como sigue:

$$f + g := (a_0 + b_0) + (a_1 + b_1)x +, ..., +(a_n + b_n)x^n + b_{n+1}x^{n+1} + ... + b_m x^m,$$
$$f \cdot g := a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + ... + c_i x^i + ...$$

donde $c_i = \sum_{r+s=i} (a_r \cdot b_s)$, para $i \in \{0, ..., m + n\}$.

A $R[x]$ se le denomina **el anillo de polinomios en la variable x con coeficientes en R.**

Observación 1.114

a) Para cualquier anillo R, siempre podemos construir su anillo de polinomios. Para ver más sobre este hecho vea [1, pág. 26].

b) El polinomio cero, $\bar{0}(x) = 0$ es el neutro aditivo para $R[x]$ y el polinomio $\bar{1}(x) = 1_R$ es el neutro multiplicativo para $R[x]$.

c) Si los polinomios f y g se consideran como en la definición 1.113, entonces:

$grad(f+g) \leq max\{grad(f), grad(g)\}$ *y* $grad(f \cdot g) \leq grad(f) + grad(g)$.

Observación 1.115 *a) En la segunda desigualdad del inciso c) de la observación 1.114 se verifica la igualdad cuando el anillo R es un dominio entero, en particular un campo. Para ver una demostración del inciso c) vea [8, proposición 4, pág. 235].*

b) Notemos que todo elemento de R puede ser considerado como un polinomio constante en $R[x]$, este hecho formalmente significa que existe un morfismo inyectivo de anillos dado por:

$$R \overset{i}{\hookrightarrow} R[x],$$
$$a \longmapsto a\ .$$

La definición 1.113 puede generalizarse a un anillo de polinomios de varias variables de forma inductiva.

Definición 1.116 *Sea R un anillo y $n \in \mathbb{Z}^+$, se define* ***el anillo de polinomios en n variables****, denotado por $R[x_1, x_2, ..., x_n]$, como sigue:*

$$R[x_1, x_2, ..., x_n] := R[x_1, x_2, ..., x_{n-1}][x_n].$$

Es decir, $R[x_1, x_2, ..., x_n]$ es el anillo de polinomios en variable x_n con coeficientes en $R[x_1, ..., x_{n-1}]$.
Para tener más información acerca de los elementos en $R[x_1, ..., x_n]$ introduciremos los siguientes conceptos:
Un ***monomio*** *en $R[x_1, ..., x_n]$ es una expresión de la forma:*

$$ax_1^{d_1}x_2^{d_2}\cdots x_n^{d_n},$$

donde $a \in R$ y para cada $i \in \{1, ..., n\}$, se tiene que $d_i \in \mathbb{Z}^+ \cup \{0\}$ es el ***grado en la variable*** *x_i.*
El ***grado de un monomio****, denotado por d, se define como la suma de los grados de las variables, es decir:*

$$d = d_1 + d_2 + ... + d_n.$$

Los polinomios en $R[x_1, ..., x_n]$ se pueden observar de forma más precisa como sumas finitas de monomios en $R[x_1, ..., x_n]$ y el ***grado del polinomio*** *es el máximo grado de cada uno de sus monomios.*

En lo sucesivo, no enunciaremos de forma directa las propiedades para el anillo $R[x_1, ..., x_n]$, sino que estas quedarán enunciadas de forma implícita cuando enunciemos las propiedades que adquiere el anillo $R[x]$ en términos de las propiedades del anillo R.

Además de la relación que se establece en la observación 1.115, hay más relaciones que nos ayudan a indagar sobre las propiedades de $R[x]$ a partir de las propiedades de R.

Proposición 1.117 *Si R es un dominio entero, entonces $R[x]$ es un dominio entero.*

Demostración. Ver [11, teorema 2.10, pág. 35]. □

Proposición 1.118 *Sea R un dominio entero. Las unidades de $R[x]$ son exactamente las unidades del anillo R.*

Demostración. Le recomendarmos revisar [11, teorema 2.10, pág. 35]. □

Observación 1.119 *Si F es un campo, al ser F un domino entero, se sigue que las unidades de $F[x]$ son todos los elementos de F que no son cero.*

Hay una variada clase de propiedades que relacionan a los anillos R y $R[x]$, sin embargo quedan fuera de la discusión que aquí trataremos. Para ver más sobre tales propiedades vea [8, capítulo 8, pág. 270].

Si consideramos un campo K, obtenemos nuevas propiedades además de las ya mencionadas para $K[x]$ cuando hemos considerado a K en el caso particular de anillo.

Teorema 1.120 *Sean K un campo y $f, g \in K[x]$ con $g \neq 0$. Entonces existen $q(x), r(x) \in K[x]$, llamados cociente y residuo respectivamente, tales que verifican lo siguiente*

$$f(x) = q(x)g(x) + r(x), \quad con \quad r(x) = 0 \quad o \quad 0 \leq grad(r(x)) < grad(g(x)).$$

Demostración. Vea [8, teorema 3, pág. 299]. □

En este caso decimos que el anillo $K[x]$ posee un **algoritmo de la división** o que es un **dominio euclidiano**. Para ver más sobre esta clase especial de anillos vea [8, capítulo 8, pág. 270].

Observación 1.121 *Si en el teorema anterior 1.120, se llega a obtener que $r(x) = 0$, decimos que $g(x)$ **divide** a $f(x)$. Esto en relación a la definición 1.86.*

Teorema 1.122 *Si K es un campo, entonces $K[x]$ es un dominio de ideales principales.*

Demostración. Vea [8, proposición 1, pág. 273]. □

La observación 1.115 nos indica que existe un morfismo de R a $R[x]$ y la siguiente construcción nos da un morfismo entre $R[x]$ y R cuyo kernel será muy importante en desarrollos posteriores y motiva parte de la teoría.

Definición 1.123 *Sean R un anillo, $\alpha \in R$ y $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. Se define la **evaluación** de f en α como sigue:*

$$f(\alpha) := \sum_{i=0}^{n} a_i \alpha^i \in R.$$

Proposición 1.124 *Sean R un anillo y $\alpha \in R$. La siguiente asignación, llamada **evaluación en** α, es un morfismo de anillos:*

$$\begin{aligned} ev_\alpha : R[x] &\longrightarrow R, \\ f(x) &\longmapsto f(\alpha)\ . \end{aligned}$$

Más aún, si R es un campo, entonces el morfismo evaluación es un morfismo entre $R-$espacios vectoriales.

Demostración. La demostración se deja como ejercicio al lector. □

Observación 1.125 *Sean R un anillo y $\alpha \in R$ un elemento cualquiera. Entonces el kernel del morfismo evaluación en α es el conjunto:*

$$Ker(ev_\alpha) = \{f(x) \in R[x] : f(\alpha) = 0\}.$$

Es decir, $ker(ev_\alpha)$ es el ideal de todos los polinomios en $R[x]$ que se hacen cero al aplicarles α.

Definición 1.126 *Sean K un campo y $f(x) \in K[x]$ un polinomio no cero. Un elemento $\alpha \in K$ es una **raíz** o un **cero** de $f(x)$ si $f(\alpha) = 0$.*

Teorema 1.127 (Teorema del residuo) *Sean K un campo, $f(x) \in K[x]$ con $f(x) \neq 0$ y $\alpha \in K$. El residuo que se obtiene de dividir $f(x)$ por $x - \alpha$ es $f(\alpha)$. Más aún, α es una raíz de un polinomio $f(x) \in K[x]$ si y solo si $x - \alpha$ divide a $f(x)$.*

Demostración. Vea [11, teorema 2.18, pág. 40]. □

Definición 1.128 *Sean K un campo, $f(x) \in K[x] \setminus \{0\}$ y $m \in \mathbb{Z}^+$. Se dice que α es una raíz de $f(x)$ de **multiplicidad m**, con $1 \leq m$, si $(x - \alpha)^m$ divide a $f(x)$ pero $(x - \alpha)^{m+1} \not| f(x)$.*

*Si α es una raíz de $f(x)$ de multiplicidad $m = 1$, entonces diremos que α es una **raíz simple** de $f(x)$.*

Sean K un campo y $\alpha \in K$ una raíz de $f(x) \in K[x]$ con $grad(f(x)) = n \geq 1$. Del teorema 1.127 tenemos que $x-\alpha$ divide a $f(x)$, luego, existe $g(x) \in K[x]\backslash\{0\}$ tal que $f(x) = (x-\alpha)g(x)$. Por el inciso a) de la observación 1.115 tenemos que $grad(f(x)) = grad(x-\alpha) + grad(g(x)) = 1 + grad(g(x)) \geqslant 1$. En conclusión, cuando $f(x)$ posee una raíz en K, entonces se factoriza como el producto de dos polinomios de grado menor o igual a él.

Por otra parte, si consideramos el polinomio $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, al aplicar la fórmula general, se tiene que las raíces de este polinomio,$\sqrt{2}$ y $-\sqrt{2}$, no son elementos de $\mathbb{Q}$. Es decir, $f(x)$ no puede factorizarse como el producto de polinomios en $\mathbb{Q}[x]$ de grado menor. Esto motiva el desarrollo de la siguiente sección y la siguiente definición en relación a la definición 1.88 y proposición 1.118.

Observación 1.129 *Sea R un dominio entero, por la proposición 1.117 tenemos que $R[x]$ es un dominio entero. Luego, es posible hablar de* ***elementos irreducibles*** *en $R[x]$ en el sentido de la definición 1.88 (c). Sin embargo, esta definición no es muy adecuada para lo que queremos que sea irreducible en un anillo de polinomios. Por ejemplo, consideremos el anillo de polinomios $\mathbb{Z}[x]$ y $f(x) = 2x + 2 \in \mathbb{Z}[x]$. Entonces $f(x) = 2(x + 1)$ donde 2 y $x + 1$ no son unidades en $\mathbb{Z}[x]$; y por lo tanto $f(x) = 2x + 2$ no es irreducible en el sentido de la definición 1.88 (c). Sin embargo, $f(x)$ no se puede factorizar en dos polinomios de grado menor al de $f(x)$; y entonces $f(x)$ si sería irreducible en este sentido. Entonces tiene sentido hablar de la siguiente definición.*

Definición 1.130 *Sea R un dominio entero. Se dice que un polinomio $f(x) \in R[x] \setminus \{0\}$ es un polinomio* ***grado-irreducible*** *si:*

(a) $grad(f(x)) \geq 1$.

(b) Si $f(x) = g(x)h(x)$ *con* $g(x), h(x) \in R[x]$, *entonces* $grad(g(x)) = 0$ *o* $grad(h(x)) = 0$.

El ejemplo en la observación 1.129, muestra que en general la noción de irreducible y grado-irreducible en $R[x]$ no coincide. No obstante, la siguiente proposición nos dice que en el anillo de polinomios sobre un campo Ã©stas nociones sí coinciden.

Proposición 1.131 *Sea K un campo y $f(x) \in K[x] \setminus \{0\}$. Entonces $f(x)$ es irreducible en el sentido de la definición 1.88 (c) si y solo si $f(x)$ es grado-irreducible.*

Demostración. Sea deja como ejercicio al lector. □

Observación 1.132 *Gracias a la proposición 1.131, cuando estemos trabajando sobre $K[x]$ donde K es un campo, solo utilizaremos el adjetivo irreducible para referirnos a cualquiera de las dos definiciones.*

En las próximas secciones veremos que la existencia de los elementos irreducibles en $F[x]$, cuando F es un campo, restringen el universo de elementos que son objeto de estudio y lo clarifica mucho más. Uno de los resultados más sobresalientes es el que exponemos a continuación y clasifica a los elementos de $F[x]$ en reducibles o irreducibles.

Teorema 1.133 *Si F es un campo, entonces $F[x]$ es un dominio de ideales principales y un dominio de factorización única.*

Demostración. Una referencia al hecho de que $F[x]$ es un dominio de ideales principales se ha dado en el teorema 1.122. Una demostración de que $F[x]$ es un dominio de factorización única puede hallarse como una consecuencia inmediata de [8, teorema 14, pág. 287]. □

Puede haber distintos polinomios irreducibles sobre un campo F, por ejemplo, todo polinomio de grado 1 es irreducible. Si en $F[x]$ no hay más irreducibles que los polinomios de grado 1, entonces el campo adquiere propiedades muy interesantes, según veremos en las secciones posteriores 2.3 y 2.2. Por otro lado, el hecho de que en un anillo $F[x]$ haya elementos irreducibles, distintos a los de grado 1, permite introducir nuevos conceptos que progresivamente van construyendo campos donde dichos polinomios ya no son considerados irreducibles. Esto lo estudiaremos más a fondo en las siguientes secciones. El problema que intentamos resolver es ¿cómo identificar polinomios irreducibles sobre un anillo?

El criterio de Eisenstein es un método práctico que nos ayuda a determinar si cierto polinomio con coeficientes en $\mathbb{Z}$ es o no grado-irreducible, no solo en $\mathbb{Z}$ sino también en $\mathbb{Q}$. A continuación presentamos algunos de criterios que son de uso frecuente en la teoría.

Proposición 1.134 *Un polinomio $f(x) \in \mathbb{Z}[x]$ es grado-irreducible en $\mathbb{Z}[x]$ si y solo si $f(x+1)$ es grado-irreducible en $\mathbb{Z}[x]$.*

Demostración. Vea [26, ejemplo 1, pág. 36]. □

Proposición 1.135 (Lema de Gauss.) *Sea $f(x) \in \mathbb{Z}[x]$ un polinomio grado-irreducible, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.*

Demostración. Vea [26, teorema 1.49, pág. 34]. □

Proposición 1.136 (Criterio de Eisenstein.) *Sea $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. Si existe un primo $p \in \mathbb{Z}$ que satisface:*

a) $p | a_i$ para todo $i \in \{0, ..., n-1\}$ y $p \nmid a_n$,

b) $p^2 \nmid a_0$,

entonces f es irreducible en $\mathbb{Q}[x]$.

Demostración. Se puede ver una demostración en [11, teorema 2.27, pág. 46]. □

Hay una buena razón por la cual los elementos irreducibles de $F[x]$ son relevantes en el estudio, por ejemplo, si F es un campo, del teorema 1.133 se sigue que $F[x]$ es un dominio de factorización única, y de la proposición 1.91 se tiene que si $p(x)$ es un irreducible en $F[x]$, esto equivale a que sea primo en $F[x]$. Es decir, los elementos irreducibles de $F[x]$ poseen dos propiedades a la vez. Sin embargo esa no es la única característica ellos, de forma más general cuando F es un campo, hemos visto en el teorema 1.133 que $F[x]$ es dominio de ideales principales y de factorización única, por ello, al tomar un elemento irreducible $p(x) \in F[x]$, el paso al cociente en $F[x]$ módulo $\langle p(x)\rangle$, el anillo $F[x]/\langle p(x)\rangle$, adquiere nuevas propiedades que expondremos a continuación. Para esto, recordemos la siguiente definición.

Definición 1.137 *Sea R un anillo. Un ideal I de R es **maximal** si $I \neq R$ y cada vez que un ideal J satisfaga que $I \subseteq J \subseteq R$, entonces $J = I$ o $J = R$.*

Proposición 1.138 *Sean F un campo y $p(x) \in F[x]\setminus\{0\}$. Los siguientes enunciados son equivalentes:*

a) $p(x)$ es irreducible en $F[x]$.

b) $\langle p(x)\rangle$ es un ideal maximal de $F[x]$.

c) $F[x]/\langle p(x)\rangle$ es un campo.

Demostración. Para una prueba detallada puede ver [11, teorema 2.4, pág 29]. □

En la siguiente sección introduciremos la definición 1.152 que nos permitirá obtener una caracterización, vea proposición 1.159, para $F[x]/\langle p(x)\rangle$ cuando F es un campo y $p(x)$ es un elemento irreducible de $F[x]$.

1.3. Extensiones de campos

Definición 1.139 *Una **extensión de campos** de un campo F es un par (K, f) donde K es un campo y $f : F \longrightarrow K$ es un morfismo campos.*
El símbolo K/F lo usaremos para indicar que K es una extensión de campos de F.

Observación 1.140 *Sea $f : F \longrightarrow K$ una extensión de campos. Por la proposición 1.108, sabemos que existe un subcampo de K isomorfo a F. De esta forma, muchas veces cuando hablemos de una extensión K/F, sin pérdida de generalidad supondremos que $F \subseteq K$.*

Observación 1.141 *Sea K/F una extensión de campos de F. Entonces K es un F-espacio vectorial con el producto por escalares inducido por el morfismo $f : F \longrightarrow K$ de la siguiente forma: Si $a \in F$ y $b \in K$, entonces $a \bullet_F b := f(a) \cdot_K b \in K$.*

Definición 1.142 *Sea K/F una extensión de campos. Se define el **grado de la extensión**, denotada por $[K : F]$, como la dimensión de K como un F-espacio vectorial. Diremos que K/F es una **extensión finita** si $[K : F] < \infty$, y en caso contrario diremos que es una **extensión infinita**.*

Observación 1.143 *Notemos que si F es un campo, entonces $[F : F] = 1$. Esto ya que una base para F como F-espacio vectorial es $\{1\}$. Por simple que sea este hecho pronto nos permitirá probar un resultado que usaremos en las siguientes secciones.*
También notemos que si K/F es una extensión de campos, entonces $[K : F] \geq 1$.

La siguiente proposición es un ejemplo de una propiedad que tienen ciertos morfismos de campos, esta propiedad será estudiada con detalle en el capítulo 2.

Proposición 1.144 *Sean $K/\mathbb{Q}$, $K'/\mathbb{Q}$ extensiones de campo y $f : K \longrightarrow K'$ un morfismo de campos. Entonces, $f(q) = q$ para todo $q \in \mathbb{Q}$.*

Demostración. Por el inciso c) de la definición 1.93 se tiene que $f(1) = 1$. Ahora, notemos que si $n \in \mathbb{Z}^+$, entonces:

$$f(n) = f(\underbrace{1 + ... + 1}_{n-veces}) = \underbrace{f(1) + ... + f(1)}_{n-veces} = \underbrace{1 + ... + 1}_{n-veces} = n.$$

Luego, por lo anterior y la proposición 1.95 (c), se concluye que $f(n) = n$ para $n \leq 0$. Así, tenemos que $f(n) = n$ para todo $n \in \mathbb{Z}$.
Sea $\frac{p}{q} \in \mathbb{Q}$, entonces tenemos que:

$$f(\tfrac{p}{q}) = f(p) \cdot f(q^{-1}) = f(p) \cdot f(q)^{-1} = p \cdot q^{-1} = \tfrac{p}{q}$$

donde la segunda igualdad se satisface por el inciso e) de la proposición 1.95. Concluimos que para todo $q \in \mathbb{Q}, f(q) = q$. □

Este último resultado nos dice que todo morfismo de campos que tienen de campo base a $\mathbb{Q}$, *deja fijo a* $\mathbb{Q}$, es decir, f se comporta como la función identidad

al restringirlo a $\mathbb{Q}$. El inicio del siguiente capítulo tratará sobre el estudio de una clase similar de morfismos que pueden llegar a formar la estructura de grupo. Pensamos que esta proposición es un testigo de que tales morfismos existen.

Definición 1.145 *Sean K/F una extensión de campos y L un campo. Se dice que L es un* ***campo intermedio*** *de la extensión K/F si L es una extensión de campos de F tal que $F \subseteq L \subseteq K$.*

Proposición 1.146 *Sean F, K, L campos tales que $F \subseteq L \subseteq K$, entonces se tiene:*

$$[K : F] = [K : L] \cdot [L : F].$$

Demostración. Para ver una demostración puede consultar [8, teorema 14, pág. 523]. □

Observación 1.147 *Sean F, L y K campos de tal forma que $F \subseteq L \subseteq K$ y $[K : F] < \infty$. Entonces $[K : L]$ y $[L : F]$ son finitas.*

Observación 1.148 *Si K/F es una extensión de campos tal que $[K : F] = n$ y d es un divisor de n, podemos preguntarnos: ¿hay un campo intermedio L de K/F tal que $[K : L] = d$? En general esta afirmación es falsa. En el ejemplo 2.79 veremos una condición para que esto se satisfaga.*

Proposición 1.149 *Sean F, K, L campos tales que $F \subseteq L \subseteq K$.*

a) Si $[K : F] = [L : F] < \infty$, entonces $K = L$.

b) Si $[K : L] = [K : F] < \infty$, entonces $L = F$.

Demostración.

a) Ya que K y L son F espacios vectoriales de la misma dimensión y al ser L un subespacio vectorial de K, entonces se concluye que $K = L$.

b) De las hipótesis, de la proposición 1.146 y de la observación 1.147, se sigue:

$$[K : L] = [K : F] = [K : L] \cdot [L : F].$$

Podemos cancelar $[K : L]$ de los extremos, obteniendo que $1 = [F : F] = [L : F]$, y por el inciso a) de la proposición 1.149, se concluye que $L = F$.

□

Corolario 1.150 *Sea K/F una extensión de campos. Entonces $[K : F] = 1$ si y solo si $F = K$.*

Demostración. El regreso quedó probado en la observación 1.143 y la otra implicación es inmediata a partir del inciso a) de la proposición 1.149. □

Corolario 1.151 *Si K/F es una extensión de campos tal que $[K:F]=p$ con $p\in\mathbb{Z}^+$ un primo, entonces no hay campos intermedios distintos de K y F en la extensión K/F.*

Demostración. Suponga que existe un campo intemedio en la extensión K/F y use la proposición 1.146 y el corolario 1.150, se deja el resto de la prueba al lector. □

Definición 1.152 *Sean K/F una extensión de campos y $X\subseteq K$. Se define el **subanillo de K generado por F y X**, denotado por $F[X]$ (el **subcampo de K generado por F y X**, denotado por $F(X)$) como sigue:*

$$F[X]:=\bigcap\{R:R \text{ es subanillo de } K,\ X\subseteq R \text{ y } F\subseteq R\}, \tag{1.1}$$
$$F(X):=\bigcap\{L:L \text{ es un subcampo de } K,\ X\subseteq L \text{ y } F\subseteq L\}.$$

Observación 1.153 *a) Los subconjuntos de K de la ecuación 1.1, efectivamente son un subanillo y un subcampo de K, respectivamente, en virtud de las proposiciones 1.78 y 1.109.*

b) $F[X]$ es el menor subanillo de K que contiene a X y F. De igual forma, $F(X)$ es el menor subcampos de K que contiene a X y F.

c) $F(X)$ es una extensión de campos de F.

*d) Si X es un subconjunto finito, digamos $X=\{\alpha_1,...,\alpha_n\}$, entonces escribiremos: $F[X]=F[\alpha_1,...,\alpha_n]$ y $F(X)=F(\alpha_1,..,\alpha_n)$. Se dice que el campo $F(\alpha_1,...,\alpha_n)$ es **finitamente generado sobre** F.*

*e) Si $X=\{\alpha\}$ diremos que $F(\alpha)/F$ es una **extensión simple** de F.*

Dada una extensión de campos K/F podemos llegar a obtener nuevas extensiones de campo de F según la cantidad de elementos de K que no se encuentren en F. Los siguientes teoremas nos proporcionan información sobre cómo se observan los elementos en dichas extensiones.

Comenzaremos el desarrollo con las extensiones simples, luego las finitas y finalizaremos generando el resultado con extensiones arbitrarias.

Observación 1.154 *Sea K/F una extensión de campos. Dados $a,b\in K$ con $b\neq 0$ utilizaremos la notación $\frac{a}{b}$ para denotar al elemento $ab^{-1}\in K$.*

Proposición 1.155 *Sean K/F una extensión de campos y $\alpha\in K$. Entonces se tiene:*

$$F[\alpha] = Im(ev_\alpha) = \{f(\alpha) \in K : f(x) \in F[x]\},$$
$$F(\alpha) = \left\{ \tfrac{f(a)}{g(\alpha)} \in K : f(x), g(x) \in F[x] \text{ y } g \notin Ker(ev_\alpha) \right\}.$$

Más aún, $F(\alpha)$ es el campo de cocientes de $F[\alpha]$.

Demostración. Para una demostración detallada vea [14, proposición 1.8, pág. 5]. □

Proposición 1.156 *Sean K/F una extensión de campos de F y $\alpha_1, ..., \alpha_n \in K$, entonces:*

$$F[\alpha, ..., \alpha_n] = \{f(\alpha_1, ..., \alpha_n) : f \in F[x_1, ..., x_n]\},$$
$$F(\alpha, ..., \alpha_n) = \left\{ \tfrac{f(\alpha, ..., \alpha_n)}{g(\alpha_1, ..., \alpha_n)} : f, g \in F[x_1, ..., x_n] \text{ y } g(\alpha_1, ..., \alpha_n) \neq 0 \right\}.$$

Demostración. Vea [14, proposición 1.9, pág. 5]. □

Observación 1.157 *Hay una sutil diferencia entre el hecho de que K está finitamente generado como campo y que K sea un espacio vectorial de dimensión finita sobre F. Las distinciones quedan determinadas por la proposición 1.156 y la definición 1.142.*

Teorema 1.158 *Sean K/F una extensión de campos de F y $X \subseteq K$. La extensión de campos de F que se obtiene de adjuntar X a F es:*

$$F(X) = \bigcup \{F(\alpha_1, ..., \alpha_n) : \alpha_i \in X \text{ para todo } i\},$$

donde la unión corre sobre todos los subconjuntos finitos de X.

Demostración. Ver [14, teorema 1.10, pág. 6]. □

Posterior a la proposición 1.138 prometimos dar una expresión más flexible para la representación de $F[x]/\langle p(x)\rangle$ cuando F es un campo y $p(x)$ es un elemento irreducible en $F[x]$.

Proposición 1.159 *Sean K/F una extensión de campos, $p(x) \in F[x] \setminus F$ un polinomio irreducible y $\alpha \in K$ una raíz de $p(x)$, entonces*

$$F[x]/\langle p(x)\rangle \simeq F(\alpha). \tag{1.2}$$

Demostración. Por la descripción de los elementos de $F(\alpha)$ dada en la proposición 1.155, podemos definir la siguiente función:

$$\varphi : F[x] \longrightarrow F(\alpha), \tag{1.3}$$
$$f(x) \longmapsto f(\alpha).$$

El lector puede comprobar que φ es un morfismo de anillos.
Con ayuda del morfismo φ puede definirse otro morfismo:

$$\widetilde{\varphi} : F[x]/\langle p(x)\rangle \longrightarrow F(\alpha) \ , \tag{1.4}$$
$$\widetilde{\varphi}(f(x) + \langle p(x)\rangle) \longmapsto \varphi(f(x)) \ .$$

Ya que $p(x) \in F[x]$ irreducible, se sigue, del inciso c) de la proposición 1.138 que el dominio de $\widetilde{\varphi}$ es un campo. Usando el hecho de que φ es un morfismo de anillos, el lector puede corroborar que $\widetilde{\varphi}$ es un morfismo de campos y que está bien definido.
Ahora, consideremos $x + \langle p(x)\rangle$ y $a + \langle p(x)\rangle$ en $F[x]/\langle p(x)\rangle$ para cada $a \in F$, entonces:

$$\widetilde{\varphi}(x + \langle p(x)\rangle) = \varphi(x) = \alpha \in Im(\widetilde{\varphi}) \subseteq F(\alpha),$$
$$\widetilde{\varphi}(a + \langle p(x)\rangle) = \varphi(a) = a \in Im(\widetilde{\varphi}) \subseteq F(\alpha).$$

Por la proposición 1.108 se tiene que $Im(\widetilde{\varphi})$ es un subcampo de K que contiene a F y α. Ahora, por el inciso b) de la observación 1.153, $F(\alpha)$ es el menor de los campos intermedios de K que cumplen esta condición. Concluimos que, $F(\alpha) = Im(\widetilde{\varphi})$, es decir, $\widetilde{\varphi}$ es un morfismo de campos suprayectivo.
Además, por el inciso b) de la observación 1.106, se tiene que $\widetilde{\varphi}$ es inyectivo y por lo tanto $\widetilde{\varphi}$ es un isomorfismo. □

Observación 1.160 *A partir de la definición de φ en la ecuación 1.3, se sigue que si $a \in F$, entonces $\varphi(a) = a$, por lo tanto, la función $\widetilde{\varphi}$ y su inversa, vea ecuación 1.4, que logra el isomorfismo de la ecuación 1.2, también se comporta como la identidad al aplicarle elementos de F.*

La proposición 1.159 supone la hipótesis de la existencia de una extensión de campos de F que contiene una raíz del polinomio irreducible $p(x)$. En la proposición 2.28 de la sección 2.2, se probará la existencia de tal campo.

Proposición 1.161 *Sean F, F' campos y $\sigma : F \longrightarrow F'$ un morfismo de anillos. Entonces, σ induce el siguiente morfismo de anillos de polinomios:*

$$\widetilde{\sigma} : F[x] \longrightarrow F'[x] \ ,$$
$$f(x) = \sum_{i=0}^{n} a_i x^i \longmapsto \widetilde{\sigma}(f(x)) = \sum_{i=0}^{n} \sigma(a_i) x^i \ .$$

Y posee las siguientes propiedades:

a) Si σ es inyectivo (suprayectivo), entonces $\widetilde{\sigma}$ es inyectivo (suprayectivo).

b) Si σ es un isomorfismo de anillos, entonces $\widetilde{\sigma}$ también lo es.

c) Si σ es un isomorfismo y $p(x) \in F[x]$ es un irreducible sobre F (respectivamente $\langle p(x)\rangle$ es un ideal maximal), entonces $\widetilde{\sigma}(p(x))$ es irreducible sobre F' ($\langle\widetilde{\sigma}(p(x))\rangle$ es ideal maximal).

d) Si σ es un isomorfismo de anillos y $p(x)$ es un irreducible en F, la función γ definida como:

$$\gamma : F[x]/\langle p(x)\rangle \longrightarrow F'[x]/\langle\widetilde{\sigma}(p(x))\rangle \ ,$$
$$f(x) + \langle p(x)\rangle \longmapsto \widetilde{\sigma}(f(x)) + \langle\widetilde{\sigma}(p(x))\rangle.$$

es un isomorfismo de campos.

Demostración. La prueba la dejamos como ejercicio al lector. □

El inciso d) de la proposición 1.161 tiene una implicación importante que se verá en el lema 2.48. Aunque este último lema corresponde a un resultado posterior, el lector puede ir directo al resultado citado.

Dada una extensión K/F, las extensiones de campos de F generadas a partir de subconjuntos de K albergan ciertos elementos que son de interés para el anillo $F[x]$ que de forma general estudiaremos en las secciones 2.2 y 2.3, el concepto subyacente a éstos últimos es el que sigue.

Definición 1.162 *Sea K/F una extensión de campos. Un elemento $\alpha \in K$ se dice **algebraico** sobre F si existe $f(x) \in F[x] \setminus \{0\}$ tal que $f(\alpha) = 0$. Si no existe un polinomio no cero en $F[x]$ del que α sea raíz, diremos que α es **trascendente** sobre F.*
*Una extensión K/F se llama **algebraica sobre F** si todo elemento de K es algebraico sobre F.*

Observe que los elementos de una extensión de campos de un campo F quedan separados en algebraicos o trascendentes.

Proposición 1.163 *Sean K/F una extensión de campos y $\alpha \in K$ algebraico sobre F. Entonces existe un único polinomio mónico irreducible $p(x) \in F[x]$ tal que $p(\alpha) = 0$. Además, si $f(x) \in F[x]$ es tal que $f(\alpha) = 0$, entonces $p(x)|f(x)$ en $F[x]$.*

Demostración. Para la demostración vea [8, proposición 9, pág. 520]. □

Observación 1.164 *Sean K/F una extensión de campos y $\alpha \in K$ algebraico sobre F. Tenemos que el polinomio $p(x) \in F[x]$ que anula a α, construido en la proposición anterior, es de grado mínimo de entre los polinomios de $F[x]$ que anulan a α.*

Definición 1.165 *Sean K/F una extensión y $\alpha \in K$ algebraico sobre F. Definimos el **polinomio mínimo** de α con coeficientes en F como el único polinomio mónico e irreducible que anula a α construido en la proposición 1.163 y será denotado como* $\mathbf{min}(F, \alpha)$.

Observación 1.166 *Sea $\alpha \in K$ un elemento algebraico sobre un campo F.*

a) Puede probarse que $Ker(ev_\alpha) = \langle min(F, \alpha) \rangle$. Esto se verifica por el hecho de que F es un campo y por lo tanto $F[x]$ posee algoritmo de la división, y es un dominio de ideales principales según se ha visto en los teoremas 1.120 y 1.122.

La siguiente proposición resume algunas de las propiedades importantes del polinomio mínimo que ya se dijeron anteriormente, y también nos ayuda a calcular el grado de la extensión $F(\alpha)/F$.

Proposición 1.167 *Sean K/F una extensión y $\alpha \in K$ un elemento algebraico sobre F. Entonces:*

a) El polinomio $min(F, \alpha)$ es irreducible en $F[x]$.

b) Si $g(x) \in ker(ev_\alpha)$, entonces $min(F, \alpha) | g(x)$.

c) Si $n = grad(min(F, \alpha))$, el conjunto $\{1, \alpha, ..., \alpha^{n-1}\}$ es una base para $F(\alpha)$ como F-espacio vectorial, es decir:

$$[F(\alpha) : F] = grad(min(F, \alpha)).$$

Demostración. Para una demostración vea [14, proposición 1.15, pág. 7]. □

Observación 1.168 *a) Sean K/F una extensión, $\alpha \in K$ un elemento algebraico sobre F y $f(x) \in F[x]$ un irreducible tal que $f(\alpha) = 0$. Entonces, $k\ min(F, \alpha) = f(x)$, donde $k \in F$ es una constante única. La prueba de este hecho se basa en la observación 1.87. Esto implica que $\langle f \rangle = \langle min(F, \alpha) \rangle$. Además, observe que:*

$$grad(min(F, \alpha)) = grad(f(x)).$$

b) Consideremos las hipótesis de la proposición 1.159. Sabemos por el inciso a) de la observación 1.168 que $min(F, \alpha)$ genera el mismo ideal que $f(x)$, por lo tanto, en la proposición 1.159 se puede concluir que:

$$F[x]/\langle min(F,\alpha)\rangle \simeq F(\alpha).$$

c) Hasta este momento hemos tenido contacto con dos nociones de isomorfismo, entre campos y entre espacios vectoriales. En general, dichos conceptos no son equivalentes, en primer lugar porque involucran a objetos de distinta naturaleza, sin embargo, expondremos esta distinción con el siguiente ejemplo.

Consideremos la extensión de campos $\mathbb{R}/\mathbb{Q}$ *y sean* $\sqrt{2}, \sqrt{3} \in \mathbb{R}\setminus\mathbb{Q}$*, de esta forma, obtenemos dos extensiones* $\mathbb{Q}(\sqrt{2})$ *y* $\mathbb{Q}(\sqrt{3})$ *de* $\mathbb{Q}$*.*

Observemos que los polinomios x^2-2 *y* x^2-3 *son irreducibles por el criterio de Eisenstein (vea proposición 1.136), al usar los números primos 2 y 3 respectivamente, además, dichos polinomios son anulados por* $\sqrt{2}$ *y* $\sqrt{3}$ *respectivamente.*
De modo que, por el inciso c) de la proposición 1.167 obtenemos:

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

Es decir, hay un $\mathbb{Q}$*-isomorfismo de espacios vectoriales entre los campos* $\mathbb{Q}(\sqrt{2})$ *y* $\mathbb{Q}(\sqrt{3})$*.*

Ahora mostremos que estos dos campos no pueden ser isomorfos como campos, para ello consideremos un isomorfismo de campos entre ellos, digamos $f : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$ *. De la proposición 1.144 se tiene que, para todo* $q \in \mathbb{Q}$*,* $f(q) = q$*.*

Ya que $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$*, entonces, existen* $a, b \in \mathbb{Q}$ *tal que* $f(\sqrt{2}) = a + b\sqrt{3}$*, de esta forma se tiene:*

$$2 = f(2) = f(\sqrt{2}) \cdot f(\sqrt{2}) = (a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3}.$$

Por lo tanto, $2ab = 0$ *y así* $a = 0$ *o* $b = 0$*. Si* $a = 0$ *se sigue que* $|b| = \frac{\sqrt{2}}{\sqrt{3}} \in \mathbb{Q}$*, mientras que si* $b = 0$ *se sigue que* $a^2 = 2$*. Naturalmente ambos hechos son imposibles ya que* $\sqrt{2}$ *y* $\sqrt{3}$ *no son racionales.*

De este modo se tiene que los campos $\mathbb{Q}(\sqrt{2})$ *y* $\mathbb{Q}(\sqrt{3})$ *son isomorfos como* $\mathbb{Q}$*-espacios vectoriales pero no como campos.*

Si K/F es una extensión y $\alpha \in K$ es un elemento algebraico, sabemos que, existe el polinomio mínimo de α sobre F. Tomemos otro polinomio $f(x) \in F[x]\setminus\{0\}$ que se anula en α y es de grado n, el siguiente resultado nos dice la cota máxima de raíces que puede tener $f(x)$ ya sea en F o en cualquier extensión de F.

Proposición 1.169 *Sean F un campo, $f(x) \in F[x] \setminus \{0\}$ un polinomio tal que $1 \leq grad(f(x)) = n$. Entonces, el número de raíces de $f(x)$ en cualquier extensión de campos de F, contadas con sus respectivas multiplicidades, es menor o igual a n. Más aún, si $\alpha_1, ..., \alpha_m$ son todas las raíces de $f(x)$ que están en una extensión K de F, con multiplicidades $\beta_1, ..., \beta_m$ respectivamente, entonces existe $g(x) \in K[x] \setminus \{0\}$ tal que $g(x)$ no posee raíces en K y se tiene:*

$$f(x) = (x - \alpha_1)^{\beta_1} \cdots (x - \alpha_m)^{\beta_m} \cdot g(x).$$

Demostración. Le recomendamos ver [26, teorema 2.10, pág. 53]. □

Proposición 1.170 *Si la extensión de campos K/F es finita, entonces es algebraica y finitamente generada.*

Demostración. Supongamos que $[K : F] = n$ con n un número natural y sea $\alpha \in K$. El conjunto $\{1, ..., \alpha^{n-1}, \alpha^n\}$ es linealmente dependiente por lo que existen $a_0, ..., a_n \in F$ no todos cero tal que se satisface:

$$a_0\alpha^0 + ... + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0.$$

Es decir, α anula al siguiente polinomio:

$$f(x) = \sum_{i=0}^{n} a_i x^i \in F[x] \setminus \{0\}.$$

Concluimos que la extensión K/F es algebraica.

Por otro lado, si $\{\alpha_1, ..., \alpha_n\}$ es una base para K como F espacio vectorial, y $\beta \in K$ es un elemento arbitrario, se sigue que existen $a_1, ..., a_n \in F$ tales que $\beta = a_1\alpha_1 + \cdots + a_n\alpha_n$. Si consideramos el polinomio $f(x_1, ..., x_n) = a_1x_1 + \cdots + a_nx_n \in F[x_1, ..., x_n]$, es claro que $f(\alpha_1, ..., \alpha_n) = \beta$. De esta forma $\beta \in F(\alpha_1, ..., \alpha_n)$ (vea proposición 1.156); y así $K \subseteq F(\alpha_1, ..., \alpha_n)$. Además, es claro que $F(\alpha_1, ..., \alpha_n) \subseteq K$, por lo que concluimos que $K = F(\alpha_1, ..., \alpha_n)$. □

En las proposiciones 1.138 y 1.159 hemos caracterizado al anillo $F[x]/\langle p(x)\rangle$ cuando consideramos que $p(x)$ es un polinomio irreducible y α es una raíz de $p(x)$ en alguna extensión de campos de F y sería excelente obtener una mejor descripción para $F(\alpha)$, además de la obtenida en la proposición 1.155. El siguiente resultado nos ayuda a obtener dicha caracterización.

Proposición 1.171 *Sean K/F una extensión de campos y $p(x) \in F[x] \setminus \{0\}$ un polinomio irreducible no constante de grado n y $\alpha \in K$ una raíz de $p(x)$. Entonces:*

$$F(\alpha) = \left\{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1} \in K : a_0, ..., a_{n-1} \in F\right\}. \quad (1.5)$$

Demostración. Es clara la siguiente contención:

$$\left\{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1} \in K : a_0, ..., a_{n-1} \in F\right\} \subseteq F(\alpha).$$

Por otra parte, del inciso a) de la observación 1.168 se tiene que $grad(p(x)) = grad(min(F, \alpha))$ y por el inciso c) de la proposición 1.167 se sigue:

$$[F(\alpha) : F] = grad(min(F, \alpha)) = n,$$

y que el conjunto $\{1, \alpha, ..., \alpha^{n-1}\} \subseteq F(\alpha)$ es una base para $F(\alpha)$ como F-espacio vectorial, es decir, si $\beta \in F(\alpha)$, entonces existen únicos $b_0, b_1, ..., b_{n-1} \in F$ tales que $\beta = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}$ lo cual se traduce en que:

$$\beta \in \left\{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1} \in K : a_0, ..., a_{n-1} \in F\right\}.$$

Por lo tanto concluimos la igualdad de la ecuación 1.5. □

Para plantear un uso de los resultados previos podemos considerar el siguiente ejemplo donde calculamos la dimensión de una extensión de campos sobre $\mathbb{Q}$, para ello primero exponemos una proposición que se usa en nuestro ejemplo.

Proposición 1.172 *Sean $F/\mathbb{Q}$ una extensión de campos y $f(x) \in F[x] \setminus \{0\}$ un polinomio mónico tal que $grad(f(x)) = 2$. Si las raíces de $f(x)$ no están en F, entonces $f(x)$ es irreducible sobre F.*

Demostración. Supongamos que $f(x) \in F[x]$ se reduce en F, es decir que existen $g(x), k(x) \in F[x] \setminus \{0\}$ tales que $f(x) = g(x) \cdot k(x)$.
Del inciso c) de la observación 1.114, sin pérdida de generalidad se sigue que $grad(g(x)) = 1$ o bien que $grad(g(x)) = 2$.
Si $grad(g(x)) = 1$ al ser $f(x)$ un polinomio mónico se tiene que $g(x) = ax + \alpha = a \cdot \left(x + \frac{\alpha}{a}\right)$ con $a \neq 0$ (pues en caso contrario $g(x)$ no es de grado 1), de la proposición 1.127 se sigue que, $-\frac{\alpha}{a} \in F$ es una raíz de $f(x)$, lo cual no puede ocurrir ya que por hipótesis se tiene que $f(x)$ no tiene raíces en F.
Por lo tanto, $grad(g(x)) = 2$ y así, $k(x)$ es constante, lo cual implica que $f(x)$ no puede factorizarse como el producto de dos polinomios de grado menor a él, esto significa que $f(x)$ es irreducible sobre F. □

Ejemplo 1.173 *Calculemos la dimensión de la extensión $\mathbb{Q}(\sqrt[4]{2}, \sqrt{3})/\mathbb{Q}$.*
Para ello, observemos que tenemos la siguientes extensiones de $\mathbb{Q}$:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, \sqrt{3}).$$

La contención $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ es propia ya que si $\sqrt[4]{2} \in \mathbb{Q}$, entonces el cuadrado de dicho elemento también sería racional, y asi $\sqrt{2} \in \mathbb{Q}$, lo cual es falso.
Además, por el criterio de Eisenstein (vea proposición 1.136) usando el primo

$p = 2$, se tiene que $x^4 - 2$ es irreducible sobre $\mathbb{Q}$. Ahora, del inciso a) de la observación 1.168 se tiene que:

$$min(\mathbb{Q}, \sqrt[4]{2}) = x^4 - 2.$$

Y de esta forma por el inciso c) de la proposición 1.167 concluimos que:

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

Por otra parte, de la proposición 1.171 el conjunto $\left\{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\right\}$ es una base para $\mathbb{Q}\left(\sqrt[4]{2}\right)$ como $\mathbb{Q}$-espacio vectorial.
Supongamos que $\sqrt{3} \in \mathbb{Q}\left(\sqrt[4]{2}\right)$, se sigue que existen escalares únicos a, b, c y $d \in \mathbb{Q}$ tal que:

$$\sqrt{3} = a + b\sqrt[4]{2} + c\sqrt{2} + d\left(\sqrt[4]{2}\right)^3,$$

elevando al cuadrado de ambos lados e igualando a cero se tiene:

$$\left(-3 + a^2 + 4bd + 2c^2\right) + 2(ab + 2cd)\sqrt[4]{2} + (2ac + b^2 + 2d^2)\sqrt{2} + 2(ad + bc)(\sqrt[4]{2})^3 = 0.$$

Ya que $\left\{1, \sqrt[4]{2}, \sqrt{2}, \left(\sqrt[4]{2}\right)^3\right\}$ es linealmente independiente, entonces:

$$a^2 + 4bd + 2c^2 = 3, ab + 2cd = 0, 2ac + b^2 + 2d^2 = 0 \text{ y } ad + bc = 0. \tag{1.6}$$

Supongamos que $b = 0$, las ecuaciones anteriores se convierten en:

$$a^2 + 2c^2 = 3, 2cd = 0, 2(ac + d^2) = 0 \text{ y } ad = 0.$$

Si $c = 0$, entonces de la primera ecuación se tiene que $a \in \mathbb{Q}$ tal que $a^2 = 3 \in \mathbb{Q}$, lo cual no puede ocurrir, por lo que $c \neq 0$, de este hecho junto con la segunda ecuación se concluye que $d = 0$ y en este caso la tercera ecuación se convierte en $2ac = 0$ y como $c \neq 0$, entonces $a = 0$, así que de la primera ecuación obtenemos que c es una racional no cero tal que $c^2 = \frac{3}{2}$, lo cual nuevamente es imposible ya que ni $\sqrt{2}$ ni $\sqrt{3}$ son racionales.
Por lo tanto debe ocurrir que $b \neq 0$.
Consideremos las ecuaciones 1.6. De la segunda de estas ecuaciones se sigue que $a = -\frac{2cd}{b}$, sustituyendo este valor en la cuarta ecuación, multiplicando por b y manipulando un poco la expresión llegamos a:

$$c\left(b - \sqrt{2}d\right)\left(b + \sqrt{2}d\right) = 0$$

Examinemos cada posible caso:
Si $c = 0$ entonces las ecuaciones 1.6 se convierten en:

$$a^2 + 4bd = 3, ab = 0, b^2 + 2d^2 = 0 \text{ y } ad = 0,$$

notemos que en la tercera ecuación, ya que tenemos la suma de los cuadrados de dos números igual a cero, entonces $b = 0 = d$*, pero por hipótesis esto es imposible ya que* $b \neq 0$*. Por lo tanto concluimos que* $c \neq 0$*.*
Ahora, notemos que los casos $b - \sqrt{2}d = 0$ *y* $b + \sqrt{2}d = 0$ *no pueden pasar ya que* b *y* d *son números racionales y* $\sqrt{2}$ *es irracional.*
Ya que se están excluyendo cada una de las posibilidades para los valores de b *y por lo tanto para los valores de* a, c *y* d *concluimos que* $\sqrt{3}$ *no se puede expresar como combinación lineal de* $\left\{1, \sqrt[4]{2}, \sqrt{2}, \left(\sqrt[4]{2}\right)^3\right\}$*, en otras palabras,* $\sqrt{3} \notin \mathbb{Q}(\sqrt[4]{2})$*.*
Y de esta forma tenemos obtenemos las extensiones propias:

$$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt[4]{2}) \subsetneq \mathbb{Q}(\sqrt[4]{2}, \sqrt{3}).$$

Observemos que $\sqrt{3}$ *anula al polinomio* $x^2 - 3 \in \mathbb{Q}(\sqrt[4]{2})$*. De la proposición 1.172 se sigue que este polinomio es irreducible sobre* $\mathbb{Q}(\sqrt[4]{2})$*, pues sus raíces,* $\sqrt{3}$ *y* $-\sqrt{3}$ *no son elementos de* $\mathbb{Q}(\sqrt[4]{2})$*. Del inciso a) de la observación 1.168 se sigue que:*

$$min(\mathbb{Q}(\sqrt[4]{2}), \sqrt{3}) = x^2 - 3.$$

Del inciso c) de la proposición 1.167 concluimos lo siguiente:

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

Ahora, por la proposición 1.146 se sigue:

$$[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}\sqrt[4]{2} : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Esto es, la dimensión de $\mathbb{Q}\left(\sqrt[4]{2}, \sqrt{3}\right)$ *como* $\mathbb{Q}$*-espacio vectorial es* 8*.*

Si K es una extensión de F y $X \subseteq K$ donde X consta de más de un elemento, en general es complicado obtener una descripción para $F(X)$ similar a la obtenida en la proposición 1.171, sin embargo, la mejor descripción que podemos tener de $F(X)$ es la dada en el teorema 1.158. Los siguientes resultados nos ayudan a obtener información acerca de la dimensión de $F(X)$ sobre F cuando $|X| < \infty$ y los elementos de X son algebraicos, esto en términos de la dimensión de las extensiones simples de F que pueden obtenerse a partir de los elementos de X.

Proposición 1.174 *Sean* K/F *una extensión y* $\{\alpha_1, ..., \alpha_n\}$ *un subconjunto de* K *de elementos algebraicos sobre* F*, entonces* $F(\alpha_1, ..., \alpha_n)$ *es una extensión finita de* F *y además:*

$$\left[F\left(\alpha_1, ..., \alpha_n\right) : F\right] \leqslant \prod_{i=1}^{n} \left[F\left(\alpha_i\right) : F\right].$$

Demostración. Para detalles sobre la prueba vea [14, proposición 1.21, pág. 10]. □

Corolario 1.175 *Sean K/F una extensión de campos y $\alpha \in K$. Se verifica que α es algebraico sobre F si y solo si $[F(\alpha) : F] < \infty$. Más aún, K/F es una extensión algebraica si $[K : F] < \infty$.*

Demostración. Si $\alpha \in K$ es algebraico sobre F, existe el polinomio $min(F, \alpha) \in F[x]$ que es anulado por α, por el inciso c) de la proposición 1.167 obtenemos que $[F(\alpha) : F] < \infty$.

Por otro lado, si $[F(\alpha) : F] < \infty$, por la proposición 1.170 se sigue que $F(\alpha)$ es una extensión algebraica sobre F, en particular $\alpha \in K$ es algebraico sobre F.

El segundo enunciado de este corolario se probó en la proposición 1.170. □

Corolario 1.176 *Sean K/F una extensión y $\beta \in K$ un elemento trascendente sobre F, entonces $[F(\beta) : F]$ es infinita.*

Demostración. Procedamos por contradicción, es decir, supongamos que la dimensión $[F(\beta) : F] < \infty$, luego, por el corolario 1.175, β es algebraico sobre F, contradiciendo a la hipótesis. □

Observación 1.177 *En general, al tomar una extensión K/F algebraica, no se puede concluir que esta extensión sea una extensión finita esto se mostrará con el planteamiento de un ejemplo dado en la proposición 2.41 la cual usará un hecho no trivial. El lector interesado puede ir directo a ese apartado.*

Ejemplo 1.178 *Una base para $\mathbb{C}$ como $\mathbb{R}$ espacio vectorial es $\{1, i\} \subseteq \mathbb{C}$ y, por lo tanto, $[\mathbb{C} : \mathbb{R}] = 2$. De esta forma, la extensión $\mathbb{C}/\mathbb{R}$ es algebraica, esto en virtud del corolario 1.175.*

Con el objetivo de mostrar la importancia de los resultados previos, exponemos de forma detallada las demostraciones de las siguientes dos proposiciones.

Proposición 1.179 *Sean K/F una extensión de campos y $X \subseteq K$ tal que todo elemento de X es algebraico sobre F, entonces $F(X)$ es una extensión algebraica sobre F. Más aún, si $|X| < \infty$, entonces $[F(X) : F] < \infty$.*

Demostración.

Sean $X \subseteq K$ como en las hipótesis y $\alpha \in F(X)$. Del teorema 1.158 se sigue que existe $\{a_1, ..., a_n\} \subseteq X$ tal que $\alpha \in F(a_1, ..., a_n)$ y ya que todos los elementos de X son algebraicos sobre F, se sigue de la proposición 1.174 que $F(a_1, ..., a_n)$ es una extensión finita de F y de la proposición 1.170 se sigue que dicha extensión es algebraica sobre F y por lo tanto $\alpha \in F(a_1, ..., a_n) \subseteq F(X)$ es algebraico sobre F. Concluimos que la extensión $F(X)/F$ es algebraica.

Probemos la segunda afirmación.
Si $|X| < \infty$, entonces $X = \{\alpha_1, ..., \alpha_n\}$ es un subconjunto de K de elementos algebraicos sobre F y por el corolario 1.175 se sigue que, para cada $i \in \{1, .., n\}$, $[F(\alpha_i) : F] < \infty$.
Finalmente, por la proposición 1.174 se obtiene que $[F(X) : F] < \infty$. □

Proposición 1.180 *Sean F, K, L campos tales que $F \subseteq L \subseteq K$. Si las extensiones L/F y K/L son algebraicas, entonces K/F es una extensión algebraica. Más aún, si K/F es algebraica, entonces K/L y L/F son extensiones algebraicas.*

Demostración. Sea $\alpha \in K$. Como K es algebraica sobre L, existe un polinomio $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in L[x]$ tal que $f(\alpha) = 0$.
Ahora, como la extensión L/F es algebraica, entonces $\{a_0, ..., a_{n-1}\} \subseteq L$ es un subconjunto finito de elementos algebraicos de sobre F, y de la proposición 1.179 se obtiene que $[F(a_0, ..., a_{n-1}) : F] < \infty$.

Sea $L_0 = F(a_0, ..., a_{n-1})$, como $\alpha \in K$ es algebraico sobre L_0, entonces $L_0(\alpha)$ es un subcampo de K y a la vez una extensión finita y algebraica sobre L_0, esto por el corolario 1.175.

De esta forma tenemos que $F \subseteq L_0 \subseteq L_0(\alpha)$ y por la proposición 1.146 obtenemos:

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

Como $F \subseteq F(\alpha) \subseteq L_0(\alpha)$, por observación 1.147 concluimos que $[F(\alpha) : F] < \infty$ y así, por el corolario 1.175, se concluye que α es algebraico sobre F.
La segunda parte de esta proposición queda como ejercicio para el lector. □

Capítulo 2

Teoría Clásica de Galois

Este capítulo inicia con una extensión de campos K/F y su asociación a un grupo, el grupo de Galois $G = Gal(K/F)$; veremos que el teorema 2.14 plantea una relación entre los campos intermedios de K/F y ciertos subgrupos de G. Lo subsecuente es desarrollar conceptos de extensiones normales y separables (vea las secciones 2.4 y 2.5 respectivamente) con el fin de dar una caracterización de las extensiones finitas de Galois (vea la proposición 2.66) y una generalización en la proposición 2.67, que dan lugar a una correspondencia biyectiva en el teorema 2.14. Todas las secciones de este capítulo decantan en el teorema fundamental de la teoría de Galois para extensiones finitas (vea teorema 2.75) donde se extraen más relaciones entre K/F y G. Este capítulo concluye con una sección de aplicaciones de este importante teorema.

Muchos de los resultados de este capítulo son extraídos de [14] y en varios de ellos no se ofrece una demostración pues el objetivo es enunciar el teorema fundamental de la teoría de Galois para extensiones finitas, no demostrarlo. Sin embargo, en tales casos sólo se proporciona una referencia de dónde puede hallarse una demostracón. Todos los resultados que aquí se ofrecen son indispensables para desarrollar el capítulo 4.

2.1. El Grupo de Galois

Definición 2.1 *Sea K un campo. El conjunto de todos los* ***automorfismos*** *de K se define como:*

$$Aut(K) := \left\{ \tau : K \longrightarrow K \ : \tau \text{ es un automorfismo} \right\}$$

Definición 2.2 *Sean K y L extensiones de un campo F y $\tau : K \longrightarrow L$ un morfismo de campos. Se dice que τ es un* ***morfismo que deja fijo a*** *F, o de*

forma equivalente, que τ es un ***F-homomorfismo*** *si para todo $x \in F, \tau(x) = x$, es decir, $\tau|_F = id_F$.*

Observación 2.3 *Sean K/F y L/F extensiones de campos y $\tau : K \longrightarrow L$ un morfismo que deja fijo a F. Se verifica lo siguiente:*

a) Ya que τ es un morfismo de campos, entonces τ es inyectivo.

b) τ es un morfismo de F-espacios vectoriales.

c) Si $[K : F] = [L : F] < \infty$, entonces τ es isomorfismo de F-espacios vectoriales entre K y L. Además, es un isomorfismo de campos.

Proposición 2.4 *Sean K/F y L/F dos extensiones de campos, $\tau : K \longrightarrow L$ un F-homomorfismo, $\alpha \in K$ algebraico sobre F y $f(x) \in F[x] \setminus \{0\}$ un polinomio que es anulado por α. Entonces $f(\tau(\alpha)) = 0$. Más aún, $min(F, \alpha) = min(F, \tau(\alpha))$.*

Demostración. Vea [14, lema 2.3, pág. 17]. □

Al considerar una extensión de campos K/F se puede aglomerar a todos los F-automorfismos de K en K en el siguiente conjunto:

$$Gal\big(K/F\big) = \big\{\tau \in Aut(K) : \tau|_F = id_F\big\} \tag{2.1}$$

El lector puede probar que al conjunto $Gal(K/F)$ se le puede dotar de la operación composición entre morfismos y que dicha operación le provee la estructura de grupo, este grupo es el objeto de estudio en la teoría de Galois moderna.

Definición 2.5 *El* ***grupo de Galois de una extensión*** *K/F se define como:*

$$\big(Gal\,(K/F)\,, \circ\big),$$

donde $\circ$ es la operación composición de funciones.

Proposición 2.6 *Sean K/F una extensión, $\emptyset \neq X \subsetneq K$ tal que $K = F(X)$ y $\sigma, \tau \in Gal\big(K/F\big)$. Entonces, $\sigma|_X = \tau|_X$ si y solo si $\tau = \sigma$.*

Demostración. Para ver una demostración vea [14, lema 2.2, pág. 16]. □

Observación 2.7 *Por la contrapositiva de este enunciado se obtiene:*

$$\tau \neq \sigma \text{ si y solo si } \sigma|_X \neq \tau|_X.$$

Con la proposición 2.6 se conjetura que el cardinal del grupo $Gal(K/F)$ depende del cardinal de X, es decir, que depende de la posibilidad de definir morfismos distintos de $Gal(K/F)$ que son isomorfismos de K en K que permutan a los elementos de X, cuando $K = F(X)$. Esto es de interés ya que quisiéramos establecer una relación del grupo de Galois con otros grupos conocidos, un progreso sobre dicha relación es el siguiente.

Proposición 2.8 *Si K/F una extensión finita, entonces $Gal(K/F)$ es un grupo finito.*

Demostración. Ver [14, corolario 2.4, pág. 17]. □

Ya que sabemos que el grupo de Galois es finito cuando la extensión es finita un primer objetivo sería acotar este número entre valores conocidos, digamos por $[K : F]$, esto se verá en la proposición 2.16.

Proposición 2.9 *Sean F, K, L campos tales que $F \subseteq L \subseteq K$. Al tomar el grupo de Galois se tiene que $Gal(K/L)$ es un subgrupo de $Gal(K/F)$.*

Demostración. Primero observemos que si $\tau \in Gal(K/L)$, entonces para todo $a \in L$ se tiene que $\tau(a) = a$. En particular $\tau(a) = a$ para todo $a \in F$ ya que $F \subseteq L$. Con este argumento se ha probado que $Gal(K/L) \subseteq Gal(K/F)$.
Tomemos el morfismo identidad del grupo $Gal(K/F)$, $id_K : K \longrightarrow K$, que fija a todos los elementos de K y como $L \subseteq K$, en particular, id_K fija a los elementos de L, y de esta forma $id_K \in Gal(K/L)$.
Ahora tomemos $\sigma, \tau \in Gal(K/L)$ y $a \in L$. Entonces $\sigma \circ \tau : K \longrightarrow K$ y también se satisface que:

$$(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a.$$

Por lo tanto $\sigma \circ \tau \in Gal(K/L)$.
Finalmente, sean $\sigma \in Gal(K/L)$ y $a \in L$, entonces $\sigma(a) = a$. Al aplicar $\sigma^{-1} \in Gal(K/F)$ a esta igualdad se tiene que:

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

Por lo tanto $\sigma^{-1} \in Gal(K/L)$. Esto prueba que $Gal(K/L)$ es un subgrupo de $Gal(K/F)$. □

Como vemos, este último resultado establece una relación entre los campos intermedios y los subgrupos del grupo de Galois asociados a la extensión. En el teorema 2.14 veremos que podemos obtener una relación en el sentido inverso y lo lograremos relacionando a los subgrupos de $Gal(K/F)$ con campos intermedios de la extensión que posean ciertas características.

Definición 2.10 *Sean K un campo y $S \subseteq Aut(K)$. El* ***campo fijo*** *determinado por S es el siguiente subconjunto de K:*

$$K^S = \{a \in K : \sigma(a) = a, \text{ para todo } \sigma \in S\}.$$

Observación 2.11 *Se deja el lector probar que K^S es un subcampo de K.*

Proposición 2.12 *Sean K/F una extesión de campos y $S \subseteq Gal(K/F)$, entonces K^S es un campo intermedio de la extensión K/F, esto es:*

$$F \subseteq K^S \subseteq K.$$

Demostración. Notemos que S consta de automorfismos de K que dejan fijo al campo F, es decir, que para todo $a \in F$ y para todo $\sigma \in S$, se tiene que $\sigma(a) = a$. Por lo tanto, $F \subseteq K^S$. □

En el siguiente lema se proporcionan resultados sobre el comportamiento de la acción que realiza la operación tomar el campo fijo, de la definición 2.10.

Lema 2.13 *Consideremos K un campo.*

a) Si E_1, E_2 son subcampos de K tales que $E_2 \subseteq E_1$, entonces

$$Gal(K/E_1) \subseteq Gal(K/E_2).$$

b) Si L es subcampo de K, entonces $L \subseteq K^{Gal(K/L)}$.

c) Si $S_1 \subseteq S_2 \subseteq Aut(K)$, entonces $K^{S_2} \subseteq K^{S_1}$.

d) Si $S \subseteq Aut(K)$, entonces $S \subseteq Gal(K/K^S)$.

e) Si $S \subseteq Aut(K)$, entonces $K^S = K^{Gal(K/K^S)}$.

f) Si L es un subcampo de K, entonces $Gal(K/L) = Gal\big(K/K^{Gal(K/L)}\big)$.

Demostración. Para ver una demostración detallada puede consultar [14, lema 2.9, pág. 18]. □

La proposición 2.12 y el lema 2.13 nos permiten construir una relación entre los subgrupos de $Gal(K/F)$ de la forma $Gal(K/L)$ con $F \subseteq L \subseteq K$ y el conjunto de los campos intermedios de K/F de la forma K^S para algún $S \subseteq Gal(K/L)$.

Teorema 2.14 *Sea K/F una extensión de campos. Consideremos los siguientes conjuntos:*

$$G := \{Gal(K/L) \subseteq Gal(K/F) : F \subseteq L \subseteq K\},$$
$$\pounds := \{K^S : \text{ para algún } S \subseteq Aut(K) \text{ y } F \subseteq K^S \subseteq K\}.$$

Las funciones definidas como sigue:

$$\begin{aligned} \Phi : G &\longrightarrow \pounds \\ Gal(K/L) &\longmapsto K^{Gal(K/L)} , \end{aligned}$$

$$\Psi : \mathcal{L} \longmapsto G$$
$$K^S \longmapsto Gal(K/K^S)\ ,$$

satisfacen las siguientes propiedades:

a) Ψ *es biyectiva e invierte inclusiones.*

b) Φ *es inversa de* Ψ*.*

Demostración.

a) El inciso a) del lema 2.13 nos dice que Ψ invierte inclusiones.

Primero demostraremos que Ψ es inyectiva.

Sean $K^S, K^{S'} \in \mathcal{L}$ tales que $\Psi(K^S) = \Psi(K^{S'})$. Por la definición de Ψ se sigue que $Gal(K/K^S) = Gal(K/K^{S'})$. Del inciso d) del lema 2.13 se sabe:

$$S \subseteq Gal(K/K^S),$$
$$\text{y } S' \subseteq Gal(K/K^{S'}).$$

Aplicando el inciso c) y e) del lema 2.13 llegamos a lo siguiente ya que $Gal(K/K^S) = Gal(K/K^{S'})$:

$$K^{S'} = K^{Gal(K/K^{S'})} \subseteq K^S$$
$$K^S = K^{Gal(K/K^S)} \subseteq K^{S'}.$$

Concluimos que $K^S = K^{S'}$, obteniendo la inyectividad de Ψ.

La suprayectividad de Ψ se satisface por el inciso f) del lema 2.13. Por lo tanto, Ψ determina una correspondencia biyectiva.

b) Para verificar que Φ es inversa de Ψ, tomemos K^S con $S \subseteq Aut(K)$ y $Gal(K/L)$ con L un campo intermedio en la extensión K/F. Al aplicar las respectivas composiciones, obtenemos:

$$\begin{aligned}\big(\Psi \circ \Phi\big)\big(Gal(K/L)\big) &= \Psi\big(\Phi(Gal(K/L))\big)\\ &= \Psi(K^{(Gal(K/L))})\\ &= Gal\big(K/K^{\left(Gal(K/L)\right)}\big)\\ &= Gal(K/L). \quad \text{Por inciso f) del lema 2.13.}\end{aligned}$$

Ahora desarrollamos la composición de $\Phi \circ \Psi$ como sigue:

$$\begin{aligned}(\Phi \circ \Psi)(K^S) &= \Phi(\Psi(K^S)) \\ &= \Phi(Gal(K/K^S)) \\ &= K^{(Gal(K/K^S)} \\ &= K^S. \quad \text{Por e) de lema 2.13.}\end{aligned}$$

□

Observe que para concluir que la composición de ambas funciones sea la identidad son indispensables los incisos *e*) y *f*) del lema 2.13.

Observación 2.15 *El teorema 2.14 proporciona una correspondencia biyectiva entre los subgrupos del grupo de Galois de la forma $Gal(K/L)$ con L un campo intermedio de la extensión K/F y los campos fijos de K/F que provienen de subconjuntos del grupo $Gal(K/F)$, sin embargo éstos no son todos los subgrupos de $Gal(K/F)$ ni todos los campos intermedios. Al no obtener una correspondencia biyectiva entre todos los subgrupos de $Gal(K/F)$ y los campos intermedios de K/F, lo que queremos es indagar acerca de cuáles condiciones hay que imponer para que se tenga una biyección entre todos los subgrupos de Galois y los campos intermedios de la extensión.*

El teorema de Galois, vea teorema 2.75, nos proporcionará condiciones necesarias para que dicha correspondencia biyectiva ocurra, un caso particular donde se verifica esta correspondencia es el siguiente: si K/F es una extensión de campos y cualquier campo intermedio de la extensión es de la forma $L = K^S$ con $S \subseteq Aut(K)$, entonces por el teorema 2.14 y el inciso e) del lema 2.13 obtendríamos una correspondencia biyectiva entre todos los campos intermedios de K/F y los subgrupos de $Gal(K/F)$.

En lo sucesivo indagaremos más sobre esta observación, y de hecho, las extensiones que son el objeto de estudio a lo largo de este trabajo serán las extensiones de campo que cumplan esta condición añadiendo algunas otras que estudiaremos en las siguientes dos secciones 2.4 y 2.5.

Si consideramos K/F una extensión finita de campos, sabemos, por la proposición 2.8, que $Gal(K/F)$ es un grupo finito, sin embargo este enunciado no nos ofrece un poco más de información sobre si el grupo de Galois asociado a la extensión excede el cardinal de cierto campo o número conocido.

Proposición 2.16 *Sea K/F una extensión finita, entonces se verifica que*

$$|Gal(K/F)| \leqslant [K : F] < \infty. \tag{2.2}$$

Demostración. Vea [14, proposición 2.13, pág. 20]. □

De forma natural surge la cuestión sobre bajo qué condiciones de la extensión K/F se verifica la igualdad o la desigualdad estricta en la ecuación 2.2 de la proposición 2.16, la respuesta, como es de esperarse, no es del todo trivial.

Proposición 2.17 *Sean K un campo y $G \leq Aut(K)$ con $|G| < \infty$. Si consideremos la extensión K/K^G, entonces:*

$$|G| = [K : K^G] \text{ y } G = Gal(K/K^G).$$

Demostración. Para ver la demostración de este hecho le recomendamos ver [14, proposición 2.14, pág. 21]. □

Definición 2.18 *Sea K/F una extensión algebraica de campos. Se dice que **K es de Galois sobre F**, o simplemente que K/F es de Galois, si se verifica que $F = K^{Gal(K/F)}$.*

Observación 2.19 *La definición de una extensión algebraica de Galois (vea definición 2.18) no implica finitud o infinitud. Esto es, una extensión algebraica de Galois puede ser finita o infinita.*

Si consideramos K un campo y $S \subseteq Aut(K)$, por el inciso e) del lema 2.13 se sigue que K es de Galois sobre K^S. Ese hecho nos muestra que las extensiones de Galois efectivamente existen, de hecho, las extensiones finitas de Galois quedan caracterizadas de la siguiente forma.

Teorema 2.20 *Si K/F es una extensión finita, se satisface:*

$$K/F \text{ es de Galois si y solo si } |Gal(K/F)| = [K : F] < \infty.$$

Demostración. Supongamos que K/F es una extensión finita de Galois, es decir, que $F = K^{Gal(K/F)}$. Como $Gal(K/F) \subseteq Aut(K)$, se sigue de la proposición 2.8 que $|Gal(K/F)| < \infty$, y por la proposición 2.17 obtenemos:

$$|Gal(K/F)| = [K : K^{Gal(K/F)}] = [K : F].$$

Por otra parte, supongamos que $|Gal(K/F)| = [K : F] < \infty$. De la proposición 2.17 se sigue :

$$[K : K^{Gal(K/F)}] = |Gal(K/F)| = [K : F].$$

Por la proposición 2.12 se tiene que $F \subseteq K^{Gal(K/F)}$, y así, del inciso b) de la proposición 1.149 obtenemos:

$$F = K^{Gal(K/F)}.$$

Concluimos que la extensión K/F es de Galois. □

El teorema 2.20 establece una relación entre la dimensión de la extensión y el orden del grupo de Galois. Cuando la extensión K/F dada en las hipótesis es simple (vea observación 1.153), naturalmente el criterio sigue siendo válido, sin embargo las extensiones simples se pueden caracterizar de una forma ligeramente distinta.
En general no todas las extensiones son simples, sin embargo algunas extensiones pueden reducirse a ser simples, esto se verá en el teorema 2.84.

Corolario 2.21 *Sean K/F una extensión y $\alpha \in K$ un algebraico sobre F. Entonces, se cumple que $|Gal(F(\alpha)/F)|$ es igual al número de raíces distintas de $min(F,\alpha) \in F[x]$ en $F(\alpha)$.*

Demostración. Vea [14, corolario 2.17, pág 22]. □

Corolario 2.22 *Sean K/F una extensión de campos de F y $\alpha \in K$ un elemento algebraico sobre F tal que $n = grad(min(F,\alpha))$ entonces:*

$F(\alpha)/F$ es de Galois si y solo si $min(F,\alpha)$ tiene n raíces distintas en $F(\alpha)$.

Demostración. Si $F(\alpha)/F$ es de Galois, entonces por el teorema 2.20 y el inciso c) de la proposición 1.167 tenemos que:

$$|Gal(F(\alpha)/F)| = [F(\alpha) : F] = grad(min(F,\alpha)) = n.$$

Luego, por el corolario 2.21 tenemos que $min(F,\alpha)$ tiene n raíces distintas en $F(\alpha)$.
El regreso es inmediato a partir del corolario 2.21 y del inciso c) de la proposición 1.167, se deja como ejercicio al lector. □

Observación 2.23 *De los resultados anteriores se sigue que si K/F es una extensión de campos y $\alpha \in K$ es algebraico sobre F de tal forma que la extensión $F(\alpha)/F$ es de Galois, entonces $min(F,\alpha)$ se descompone sobre $F(\alpha)$ en factores lineales distintos. Es decir, una extensión simple $F(\alpha)/F$ no es de Galois si $min(F,\alpha)$ no se descompone como el producto de factores lineales sobre $F(\alpha)$ o si tiene una raíz con multiplicidad mayor a 1, esto en virtud de los dos resultados anteriores. La condición de que $min(F,\alpha)$ no tenga raíces repetidas nos permitirá reclasificar a las extensiones y caracterizar aquellas donde un polinomio se descompone sin tener raíces repetidas.*

Ejemplo 2.24 *a) Consideremos la extensión de campos $\mathbb{Q}(\omega)/\mathbb{Q}$, donde $\omega = e^{\frac{2\pi i}{3}}$. Usando la proposición 1.134 y el criterio de Eisenstein (vea proposición 1.136) con $p = 3$, puede probarse que $min(\mathbb{Q},\omega) = x^2 + x + 1$.*

Además, la otra raíz de este polinomio es $\omega^2 \in \mathbb{Q}(\omega)$.
Es decir, $\mathbb{Q}(\omega)$ *contiene dos raíces distintas de* $min(\mathbb{Q}, \omega)$. *Por el corolario 2.22 tenemos que* $\mathbb{Q}(\omega)/\mathbb{Q}$ *es de Galois.*

b) *Ahora tomemos la extensión de campos* $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$. *Usando el criterio de Eisenstein, (vea proposición 1.136) con el primo* $p = 2$ *puede probarse que* $min(\mathbb{Q}, \sqrt[4]{2}) = x^4 - 2$. *Además,* $-\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ *es otra raíz de* $min(\mathbb{Q}, \sqrt[4]{2})$ *y las otras dos raíces son complejas.*

Por el corolario 2.21 concluimos que:

$$|Gal(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})| = 2.$$

Por el inciso c) de la proposición 1.167 se tiene que $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ *y del teorema 2.20 se concluye que la extensión* $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ *no es de Galois.*

c) *Probaremos que la extensión* $\mathbb{Q}(\sqrt{5}, \sqrt{7})/\mathbb{Q}$ *es de Galois para hacerlo usaremos el teorema 2.20. Primero notemos que*

$$\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7}). \tag{2.3}$$

Es claro que $\mathbb{Q}(\sqrt{5} + \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{5}, \sqrt{7})$.
Para probar la otra contención de la ecuación 2.3 tomemos $a = \sqrt{5} + \sqrt{7} \in \mathbb{Q}(\sqrt{5} + \sqrt{7})$, *entonces* $a - \sqrt{7} = \sqrt{5}$, *luego,* $a^2 - 2a\sqrt{7} + 7 = 5$. *Al despejar a* $\sqrt{7}$ *tenemos:*

$$\sqrt{7} = \frac{a^2 + 2}{2a} \in \mathbb{Q}(\sqrt{5} + \sqrt{7}).$$

De forma similar se puede probar que $\sqrt{5} \in \mathbb{Q}(\sqrt{5} + \sqrt{7})$. *Concluimos que* $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{5} + \sqrt{7})$, *y por lo tanto, se satisface la ecuación 2.3.*

Consideremos la extensión intermedia $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$, *que es de grado 2, esto ya que al usar el criterio de Eisenstein (vea proposición 1.136) con el primo* $p = 5$ *puede probarse que* $min(\mathbb{Q}, \sqrt{5}) = x^2 - 5$.

Por otro lado, por contradicción puede probarse que $\sqrt{7} \notin \mathbb{Q}(\sqrt{5})$, *esto usando el hecho de que* $\sqrt{5} \notin \mathbb{Q}$. *Además, notemos que* $\sqrt{7}$ *anula al polinomio* $x^2 - 7 \in \mathbb{Q}(\sqrt{5})[x]$ *que es mónico e irreducible (ya que sus raíces no están en* $\mathbb{Q}(\sqrt{5})$*). De la proposición 1.172 se sigue que* $x^2 - 7$ *es el polinomio mínimo sobre* $\mathbb{Q}(\sqrt{5})$, *por lo tanto,* $\sqrt{7}$ *es algebraico sobre* $\mathbb{Q}(\sqrt{5})$. *Del inciso c) de la proposición 1.167 se sigue:*

$$[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})] = 2.$$

Ya que $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{5}) \subsetneq \mathbb{Q}(\sqrt{5}, \sqrt{7})$, *se sigue, de la proposición 1.146:*

$$[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Observemos que $-\sqrt{5}, \sqrt{5} \in \mathbb{Q}(\sqrt{5})$, *y ambos son raíces distintas de* x^2-5, *del corolario 2.21 se sigue que* $|Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q})| = 2$, *de forma similar se puede concluir que* $|Gal(\mathbb{Q}(\sqrt{7})/\mathbb{Q})| = 2$.

Para calcular $Gal(\mathbb{Q}(\sqrt{5}, \sqrt{7})/\mathbb{Q})$ *bastaría hallar el polinomio mínimo irreducible de grado 4 con coeficientes en* $\mathbb{Q}$ *que sea anulado por* $\sqrt{5}+\sqrt{7}$ *para conocer la forma en que los automorfismos van a permutar las raíces de ese polinomio mínimo. Sin embargo no procederemos de este modo y lo haremos calculando los elementos de* $Gal\big(\mathbb{Q}(\sqrt{5}, \sqrt{7})/\mathbb{Q}\big)$ *como sigue:*

Sean $\sigma \in Gal\big(\mathbb{Q}(\sqrt{5}, \sqrt{7})/\mathbb{Q}\big)$ *y* $\sqrt{5} \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$. *De la proposición 2.4 se sigue que* $\sigma(\sqrt{5})$ *es una raíz de* $x^2 - 5$ *y por lo tanto:*

$$\sigma(\sqrt{5}) = \sqrt{5} \text{ o } \sigma(\sqrt{5}) = -\sqrt{5}.$$

De la misma forma, usando el polinomio $x^2 - 7$ *y su raíz* $\sqrt{7} \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$ *tenemos que:*

$$\sigma(\sqrt{7}) = \sqrt{7} \text{ o } \sigma(\sqrt{7}) = -\sqrt{7}.$$

por lo tanto, tenemos las siguientes 4 posibilidades para los elementos de $Gal\left(\mathbb{Q}(\sqrt{5}, \sqrt{7})/\mathbb{Q}\right)$.

$$id: \begin{cases} 1 \longmapsto 1 \\ \sqrt{5} \longmapsto \sqrt{5} \\ -\sqrt{5} \longmapsto -\sqrt{5} \\ \sqrt{7} \longmapsto \sqrt{7} \\ -\sqrt{7} \longmapsto -\sqrt{7} \end{cases} \qquad \tau: \begin{cases} 1 \longmapsto 1 \\ \sqrt{5} \longmapsto -\sqrt{5} \\ -\sqrt{5} \longmapsto \sqrt{5} \\ \sqrt{7} \longmapsto \sqrt{7} \\ -\sqrt{7} \longmapsto -\sqrt{7} \end{cases}$$

$$\sigma: \begin{cases} 1 \longmapsto 1 \\ \sqrt{5} \longmapsto \sqrt{5} \\ -\sqrt{5} \longmapsto -\sqrt{5} \\ \sqrt{7} \longmapsto -\sqrt{7} \\ -\sqrt{7} \longmapsto \sqrt{7} \end{cases} \qquad \sigma \circ \tau: \begin{cases} 1 \longmapsto 1 \\ \sqrt{5} \longmapsto -\sqrt{5} \\ -\sqrt{5} \longmapsto \sqrt{5} \\ \sqrt{7} \longmapsto -\sqrt{7} \\ -\sqrt{7} \longmapsto \sqrt{7} \end{cases}$$

Basta mostrar que efectivamente cada una de estas correspondencias determina un elemento en $Gal\left(\mathbb{Q}(\sqrt{5}, \sqrt{7})/\mathbb{Q}\right)$.

Probaremos que $\sigma \circ \tau$ *es un elemento del grupo de Galois, para ello construiremos extensiones de morfismos como sigue:*

Definamos el siguiente morfismo:

$$\gamma : \mathbb{Q}(\sqrt{5}) \longrightarrow \mathbb{Q}(\sqrt{5})$$
$$a + b\sqrt{5} \longmapsto a - b\sqrt{5}\ ,$$

y es tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{5}) & \xrightarrow{\gamma} & \mathbb{Q}(\sqrt{5}) \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i} \\ \mathbb{Q} & \xrightarrow{id_{\mathbb{Q}}} & \mathbb{Q} \end{array}$$

Se deja como ejercicio al lector probar que γ *es un elemento de* $Aut\big(\mathbb{Q}(\sqrt{5})\big)$. *Más aún,* $\gamma|_{\mathbb{Q}} = id_{\mathbb{Q}}$, *y por lo tanto,* $\gamma \in Gal\left(\mathbb{Q}\left(\sqrt{5}\right)/\mathbb{Q}\right)$.

Extendamos γ *a* $\widetilde{\gamma} = \sigma \circ \tau$ *de la siguiente forma: para cualesquiera elementos* $\alpha, \beta \in \mathbb{Q}(\sqrt{5})$

$$\begin{aligned} \widetilde{\gamma} : \mathbb{Q}(\sqrt{5}, \sqrt{7}) &\longrightarrow \mathbb{Q}(\sqrt{5}, \sqrt{7}) \\ \alpha + \beta\sqrt{7} &\longmapsto \gamma(\alpha) - \gamma(\beta)\sqrt{7}\ . \end{aligned}$$

El objetivo es probar que $\widetilde{\gamma}$ *es un automorfismo, para ello probemos primero que es un morfismo de campos.*

Sean $\alpha+\beta\sqrt{7}$ *y* $\alpha'+\beta'\sqrt{7} \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$ *con* $\alpha, \beta, \alpha', \beta' \in \mathbb{Q}\big(\sqrt{5}\big)$, *entonces:*

$$\begin{aligned} &\widetilde{\gamma}\big(\alpha + \beta\sqrt{7}) + (\alpha' + \beta'\sqrt{7})\big) \\ &= \widetilde{\gamma}\big(\alpha + \alpha' + (\beta + \beta')\sqrt{7}\big) \\ &= \gamma(\alpha + \alpha') - \gamma(\beta + \beta')\sqrt{7} \quad \textit{por definición de } \widetilde{\gamma} \\ &= \gamma(\alpha) + \gamma(\alpha') - (\gamma(\beta) + \gamma(\beta'))\sqrt{7} \quad \textit{ya que } \gamma \textit{ es morfismo de campos} \\ &= \gamma(\alpha) - \gamma(\beta)\sqrt{7} + (\gamma(\alpha') - \gamma(\beta')\sqrt{7}) \\ &= \widetilde{\gamma}(\alpha + \beta\sqrt{7}) + \widetilde{\gamma}(\alpha' + \beta'\sqrt{7}). \end{aligned}$$

Ahora verifiquemos que $\widetilde{\gamma}$ *abre el producto de cualesquiera dos elementos de* $\mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right)$ *así como los hemos citado arriba. La prueba se sigue a partir de las propiedades de morfismo de campos de* γ.

$$\begin{aligned} &\widetilde{\gamma}\left((\alpha + \beta\sqrt{7}) \cdot (\alpha' + \beta'\sqrt{7})\right) = \\ &= \widetilde{\gamma}\left((\alpha\alpha' + 7\beta\beta') + (\alpha\beta' + \alpha'\beta)\sqrt{7}\right) \textit{ por def. de producto en } \mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right) \\ &= \gamma\left(\alpha\alpha' + 7\beta\beta'\right) - \gamma\left(\alpha\beta' + \alpha'\beta\right)\sqrt{7} \textit{ por def. de } \widetilde{\gamma} \\ &= (\gamma(\alpha) \cdot \gamma(\alpha') + 7\gamma(\beta)\gamma(\beta')) - (\gamma(\alpha) \cdot \gamma(\beta') + \gamma(\alpha') \cdot \gamma(\beta))\sqrt{7} \\ &= \left(\gamma(\alpha) - \gamma(\beta)\sqrt{7}\right) \cdot \left(\gamma(\alpha') - \gamma(\beta')\sqrt{7}\right) \\ &= \widetilde{\gamma}\left(\alpha + \beta\sqrt{7}\right) \cdot \widetilde{\gamma}\left(\alpha' + \beta'\sqrt{7}\right). \end{aligned}$$

Concluimos que $\widetilde{\gamma}$ es un morfismo de campos, y por lo tanto, $\widetilde{\gamma}$ es un morfismo de campos inyectivo, esto por el inciso b) de la observación 1.106.

Por la forma en la que se ha definido $\widetilde{\gamma}$ se tiene que $\widetilde{\gamma}|_{\mathbb{Q}} = id_{\mathbb{Q}}$, es decir, que es un $\mathbb{Q}$-morfismo. Además, $\widetilde{\gamma}|_{\mathbb{Q}(\sqrt{5})} = \gamma$.

El siguiente diagrama conmutativo ilustra nuestra situación:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{5},\sqrt{7}) & \xrightarrow{\widetilde{\gamma}} & \mathbb{Q}(\sqrt{5},\sqrt{7}) \\ \uparrow i & & \uparrow i \\ \mathbb{Q}(\sqrt{5}) & \xrightarrow{\gamma} & \mathbb{Q}(\sqrt{5}) \end{array}$$

Ahora probaremos que $\widetilde{\gamma}$ es suprayectivo:

Sea $\alpha + \beta\sqrt{7} \in \mathbb{Q}(\sqrt{5}+\sqrt{7})$ con $\alpha, \beta \in \mathbb{Q}(\sqrt{5})$. Ya que el morfismo $\gamma : \mathbb{Q}(\sqrt{5}) \longrightarrow \mathbb{Q}(\sqrt{5})$ es suprayectivo, se sigue que existen $\alpha', \beta' \in \mathbb{Q}(\sqrt{5})$ tal que:

$$\gamma(\alpha') = \alpha \text{ y } \gamma(\beta') = \beta.$$

Consideremos $\alpha' - \beta'\sqrt{7} \in \mathbb{Q}(\sqrt{5},\sqrt{7})$. Por propiedades de morfismo de γ y considerando que $\widetilde{\gamma}|_{\mathbb{Q}} = id_{\mathbb{Q}}$ y que $\widetilde{\gamma}|_{\mathbb{Q}(\sqrt{5})} = \gamma$ se sigue:

$$\widetilde{\gamma}\left(\alpha' - \beta'\sqrt{7}\right) = \gamma(\alpha') + \gamma(\beta')\sqrt{7} = \alpha + \beta\sqrt{7}.$$

Por lo tanto, $\widetilde{\gamma}$ es suprayectivo. Luego, $\widetilde{\gamma}$ es un automorfismo que satisface:

$$\widetilde{\gamma}(1) = 1, \widetilde{\gamma}(\sqrt{5}) = -\sqrt{5}, \widetilde{\gamma}(-\sqrt{5}) = \sqrt{5}, \widetilde{\gamma}(\sqrt{7}) = -\sqrt{7} \text{ y } \widetilde{\gamma}(-\sqrt{7}) = \sqrt{7}.$$

De este modo tenemos, $\widetilde{\gamma} \in Gal\left(\mathbb{Q}(\sqrt{5},\sqrt{7})/\mathbb{Q}\right)$.

El lector puede probar, usando una construcción similar, que los morfismos σ, τ son elementos de $Gal\left(\mathbb{Q}(\sqrt{5},\sqrt{7})/\mathbb{Q}\right)$.
Concluimos que:

$$|Gal(\mathbb{Q}(\sqrt{5}+\sqrt{7}/\mathbb{Q})| = [\mathbb{Q}(\sqrt{5},\sqrt{7}) : \mathbb{Q}] = 4.$$

Por lo tanto, $\mathbb{Q}(\sqrt{5},\sqrt{7})/\mathbb{Q}$ es una extensión de Galois.

Observación 2.25 *En el inciso c) del ejemplo 2.24 se ha probado la igualdad $\mathbb{Q}\left(\sqrt{5},\sqrt{7}\right) = \mathbb{Q}\left(\sqrt{5}+\sqrt{7}\right)$, es decir, que dicha extensión de $\mathbb{Q}$ es simple. En el ejemplo 1.173 puede intentar probarse, que la extensión $\mathbb{Q}\left(\sqrt{3},\sqrt[4]{2}\right)$ es simple y lo que naturalmente se intuye es intentar probar que:*

$$\mathbb{Q}\left(\sqrt{3},\sqrt[4]{2}\right) = \mathbb{Q}\left(\sqrt{3}+\sqrt[4]{2}\right), \tag{2.4}$$

y al hacerlo, siguendo la idea del ejercicio c) de 2.24, no se obtienen argumentos para pensar que efectivamente la ecuación 2.4 es verdadera y en ese caso resta preguntarnos ¿Cuál es el elemento que genera a esta extensión de $\mathbb{Q}$?

Una de las cualidades que comparten las extensiones sobre $\mathbb{Q}$, $\mathbb{Q}\left(\sqrt{3}, \sqrt[4]{2}\right)/\mathbb{Q}$ y $\mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right)/\mathbb{Q}$, es que ambas son finitas. En el teorema del elemento primitivo (vea teorema 2.84) mostraremos que toda extensión finita sobre $\mathbb{Q}$ es simple.

2.2. Campos de descomposición

Definición 2.26 *Sean K una extensión de campos de F y $f(x) \in F[x]\setminus\{0\}$ con $grad(f) = n$. Decimos que f se **descompone** sobre K si $f(x) = a\prod_{i=1}^{n}(x-\alpha_i)$ con $\alpha_i \in K$ para todo $i \in \{1, ..., n\}$ y $a \in F$.*

Dicho de otra forma, un polinomio f se descompone sobre K si este último contiene todas las raíces de f.

Ejemplo 2.27 *a) Tomemos el polinomio $f(x) = x^2+1 \in \mathbb{R}[x]$. Cuyas raíces son $i, -i \in \mathbb{C}\setminus\mathbb{R}$. Es decir, el polinomio $f(x) = x^2+1$ se descompone sobre $\mathbb{C}$.*

b) $\mathbb{Q}(\omega)$ donde $\omega = e^{\frac{2\pi i}{3}}$, es el campo de descomposición de $x^2+x+1 \in \mathbb{Q}[x]$ ya que ω y ω^2 son sus dos raíces y ambos son elementos de esta extensión de $\mathbb{Q}$.

A partir del ejemplo 2.27 surge el interrogante sobre si siempre es posible obtener un campo de descomposición de un polinomio o polinomios dados en $F[x]$ para cualquier campo F. La siguiente proposición nos brinda información sobre esto.

Proposición 2.28 *Sean F un campo fijo, $n \in \mathbb{Z}^+$ y $f(x) \in F[x]\setminus\{0\}$ con $grad(f) = n$. Entonces, existe una extensión de campos K de F tal que K tiene una raíz de $f(x)$ y $[K : F] \leq n$.*

Demostración. Vea [14, teorema 3.3, pág. 28]. □

Corolario 2.29 *Sean F un campo y $f(x) \in F[x]\setminus\{0\}$ un polinomio de grado $n \in \mathbb{Z}^+$. Entonces, existe una extensión de campos K de F tal que $f(x)$ se descompone sobre K y $[K : F] \leq n!$.*

Demostración. Vea [14, teorema 3.3, pág. 28]. □

Definición 2.30 *Sean K/F una extensión de campos y $f(x) \in F[x]\setminus\{0\}$.*

*a) Se dice que K es un **campo de descomposición** de f sobre F si f se descompone sobre K y $K = F(\alpha_1, ..., \alpha_n)$(vea definición 1.152), donde para todo $i \in \{1, ..., n\}$ se tiene $\alpha_i \in K$ es raíz de $f(x)$.*

b) Sea $S = \{f_i(x)\}_{i\in I} \subsetneq F[x]$ una familia de polinomios no constantes de $F[x]$. Decimos que K es un ***campo de descomposición para*** *S si cada polinomio de S se descompone sobre K y $K = F(X)$ (en el sentido del teorema 1.158), donde X es el conjunto de raíces de los elementos de S.*

Observación 2.31 *En lo sucesivo, al invocar a un subconjunto S de $F[x]$ se entenderá que es un subconjunto no vacío de polinomios no constantes de $F[x]$.*

El siguiente resultado nos dice que existen los campos de descomposición de subconjuntos finitos de polinomios no constantes de $F[x]$.

Corolario 2.32 *Si $S = \{f_1, ..., f_n\}$ es un subconjunto finito de $F[x]$, entonces existe un campo de descomposición para S.*

Demostración. Sea S un conjunto como en las hipótesis y consideremos el polinomio $f = f_1 \cdot \cdots \cdot f_n \in F[x]$, por el corolario 2.29 se sigue que existe K una extensión de campos de F tal que $f(x)$ se descompone sobre K. Naturalmente, ya que K contiene a todas las raíces de $f(x)$, contiene también a cada una de las raíces de f_i para cada $i \in \{1, ..., n\}$. Sea $X \subseteq K$ el conjunto de todas las raíces de f en K, luego, $F(X) \subseteq K$ es un campo de descomposición para todos los polinomios de S. □

Dado un campo fijo F, por el momento nada sabemos sobre si existe un campo de descomposición de subconjuntos arbitrariamente grandes de polinomios no constantes de $F[x]$ y en caso de que tales campos existan, falta resolver si son únicos.

2.3. Cerraduras algebraicas

En la sección anterior se ha probado la existencia de campos de descomposición para subconjuntos finitos (vea corolario 2.32) de polinomios pero nada se ha dicho de la existencia de campos de descomposición de subconjuntos infinitos de polinomios incluyendo a todos los polinomios de un campo dado. En esta sección presentaremos a los campos de descomposición para subconjuntos infinitos de polinomios y daremos una referencia de una prueba de su existencia que se basa en el axioma de elección.

Proposición 2.33 *Sea K un campo. Los siguientes enunciados son equivalentes:*

a) No hay extensiones algebraicas de K mas que K mismo.

b) No hay extensiones finitas de K mas que K mismo.

c) Si L es una extensión de campos de K, entonces

$$K = \{a \in L : a \text{ es algebraico sobre } K\}.$$

d) Todo polinomio $f(x) \in K[x] \setminus \{0\}$ se descompone sobre K.

e) Todo polinomio $f(x) \in K[x] \setminus \{0\}$ posee una raíz en K.

Demostración. Vea [14, lema 3.10, pág. 30]. □

Definición 2.34 *Se dice que un campo K es algebraicamente cerrado si satisface alguno de los enunciados de la proposición 2.33.*

Ejemplo 2.35 *La muestra por excelencia de la existencia de campos algebraicamente cerrados es la del campo de los números complejos $\mathbb{C}$. La demostración es el Teorema Fundamental del Álgebra (vea teorema 2.86).*

Definición 2.36 *Sea F un campo. Una **cerradura algebraica de F** es una extensión K/F que satisface:*

a) K/F es algebraica sobre F.

b) K es algebraicamente cerrado.

Ejemplo 2.37 *De los ejemplos 1.178 y 2.35 se sigue que la extensión $\mathbb{C}/\mathbb{R}$ es algebraica y, por lo tanto, el campo $\mathbb{C}$ es una cerradura algebraica de $\mathbb{R}$.*

Definición 2.38 *Sean K/F una extensión de campos. Al siguiente conjunto:*

$$\overline{F} := \{a \in K : \ a \text{ es algebraico sobre } F\},$$

*se le denomina una **cerradura algebraica de F en K.***

Proposición 2.39 *Sea K/F una extensión. Entonces $\overline{F}$ es un campo y es la mayor extensión algebraica de F contenida en K.*

Demostración. Para ver una demostración le recomendamos ver [14, corolario 1.26, pág. 11]. □

Ejemplo 2.40 *Ya que $\mathbb{C}$ es una cerradura algebraica de $\mathbb{R}$, entonces $\mathbb{C}$ contiene una cerradura algebraica para cada uno de sus subcampos.*

Proposición 2.41 *Sea $\mathbb{A} \subseteq \mathbb{C}$ una cerradura algebraica de $\mathbb{Q}$ en $\mathbb{C}$, entonces $[\mathbb{A} : \mathbb{Q}]$ es infinita.*

Demostración. Notemos que si p es un número primo, entonces $\sqrt{p} \in \mathbb{C} \setminus \mathbb{Q}$ y además este elemento anula al polinomio:

$$x^2 - p \in \mathbb{Q}[x].$$

Más aún, este polinomio es irreducible por el criterio de Eisenstein (vea proposición 1.136). De esta forma, para cada p número primo se tiene que $\sqrt{p} \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$. Por lo tanto, se tiene:

$$\left\{\sqrt{p} \in \mathbb{C} : p \text{ es primo}\right\} \subseteq \mathbb{A}. \tag{2.5}$$

Sabemos, gracias a Euclides, que hay una cantidad infinita de números primos, por lo tanto, de la ecuación 2.5 se sigue que hay una cantidad infinita de elementos algebraicos sobre $\mathbb{Q}$ que, además, son linealmente independientes sobre $\mathbb{Q}$. De esta forma, concluimos que:

$$[\mathbb{A} : \mathbb{Q}] \text{ es infinita.}$$

□

La proposición 2.41 supone, de forma intuitiva, que los subconjuntos finitos de $\{\sqrt{p} : p \text{ es primo}\}$ son linealmente independientes sobre $\mathbb{Q}$, sin embargo, la prueba de este hecho, que es abarcado por un caso más general, no es del todo trivial.

Proposición 2.42 *Sean $n_1, ..., n_k$ distintos enteros libres de cuadrados y tomemos $a_1, ..., a_k \in \mathbb{Z} \setminus \{0\}$, entonces la suma $a_1\sqrt{n_1} + ... + a_k\sqrt{n_k}$ no es cero.*

Demostración. Para ver una prueba de este hecho revise [3]. □

La definición 2.38 supone la existencia de una extensión de campos K/F y de K extrae elementos algebraicos para consolidar la cerradura algebraica de F en dicha extensión. Sin embargo, podría ocurrir que los elementos de K no son necesariamente todas las raíces de los polinomios irreducibles sobre F, en otras palabras, que la extensión podría quedarse "pequeña", por así decir, para llegar a ser una cerradura algebraica de F y, por lo tanto, necesitaríamos una extensión de K de la cual extraer la totalidad de los elementos que anulan a todos los polinomios irreducibles sobre F.
El siguiente teorema afirma que hay una cerradura algebraica para cualquier campo. Este hecho depende de una sólida construcción usando el axioma de elección.

Teorema 2.43 *Existe una cerradura algebraica para cualquier campo.*

Demostración. Vea [14, teorema 3.14, pág. 32]. □

Corolario 2.44 *Sea F un campo. Entonces existe un campo algebraicamente cerrado que contiene a F.*

Demostración. Por el teorema 2.43, existe una cerradura algebraica de F y por definición 2.36 ésta es algebraicamente cerrada. □

Sea K una cerradura algebraica de F. Ya que K es un campo algebraicamente cerrado, se sigue, del inciso d) de la proposición 2.33 que K posee todas las raíces de cada polinomio en $K[x]$. Consideremos $S \subseteq F[x]$ un subconjunto arbitrario y $X \subseteq K$ el conjunto de raíces de los polinomios en S, entonces $F(X)$ es un campo de descomposición para S y además $F(X) \subseteq K$. Es decir, tenemos el siguiente corolario:

Corolario 2.45 *Sean K/F una cerradura algebraica de F y $S \subseteq F[x]$. Entonces K contiene un campo de descomposición de S.*

Corolario 2.46 *Sea K un campo. Un campo de descomposición del conjunto de todos los polinomios no constantes en $K[x]$ es una cerradura algebraica de K.*

Demostración. Es inmediato a partir del corolario 2.45, se deja al lector. □

Corolario 2.47 *Sea K una cerradura algebraica de F. Entonces, todo polinomio irreducible en $F[x]$ se descompone sobre K.*

Demostración. Es inmediato a partir del inciso d) de la proposición 2.33. □

Por el teorema 2.43 sabemos que existen las cerraduras algebraicas de un campo fijo F, se abre el interrogante, ¿dichas cerraduras son únicas? Una pregunta similar se puede plantear respecto a los campos de descomposicion de un polinomio o de un subconjunto de polinomios. Los siguientes resultados nos permitirán concluir que las cerraduras algebraicas de un campo F, son únicas salvo isomorfismo y lo mismo ocurrirá con los campos de descomposición de un subconjunto dado de polinomios de $F[x]$.
Recordemos la construcción hecha en la proposición 1.161 donde si F y F' son dos campos y $\sigma : F \longrightarrow F'$ es un morfismo de campos, entonces σ induce un morfismo entre los anillos $\widetilde{\sigma} : F[x] \longrightarrow F'[x]$. En el siguiente teorema nos referiremos a $\widetilde{\sigma}$ como el morfismo que extiende a σ según se menciona en el apartado citado.

Lema 2.48 *Sean F, F' campos, $\sigma : F \longrightarrow F'$ un isomorfismo de campos, $p(x) \in F[x] \setminus F$ un polinomio irreducible sobre F y $\alpha \in K$ una raíz de $p[x]$, donde K es una extensión de F. Sea $\alpha' \in K'$ una raíz de $\widetilde{\sigma}(p(x)) \in F'[x]$, donde K' es una extensión de campos de F'. Entonces existe un isomorfismo de campos $\tau : F(\alpha) \longrightarrow F(\alpha')$ tal que $\tau|_F = \sigma$ y satisface que $\tau(\alpha) = \alpha'$. Más aún, puede probarse que τ es único con estas propiedades.*

Demostración. Ya que $p(x)$ es un polinomio irreducible, se sigue, de la proposición 1.138, que $F[x]/\langle p(x)\rangle$ es un campo y $\langle p(x)\rangle$ es un ideal maximal de $F[x]$, además de la proposición 1.159 se obtiene el siguiente isomorfismo

$$\begin{aligned}\varphi : F[x]/\langle p(x)\rangle &\longrightarrow F(\alpha)\ ,\\ f(x)+\langle p(x)\rangle &\longmapsto f(\alpha)\ .\end{aligned}$$

Ahora, como el ideal $\langle p(x)\rangle$ es maximal de $F[x]$, por el inciso c) de la proposición 1.161 se tiene que el ideal $\langle \widetilde{\sigma}(p(x))\rangle$ es maximal de $F'[x]$ y por la proposición 1.159 tenemos el siguiente isomorfismo:

$$\begin{aligned}\varphi' : F'[x]/\langle \widetilde{\sigma}(p(x)\rangle &\longrightarrow F'(\alpha')\\ g(x)+\langle \widetilde{\sigma}(p(x))\rangle &\longmapsto g(\alpha')\ .\end{aligned}$$

Ahora, por el inciso d) de la proposición 1.161, se obtiene un isomorfismo γ definido de la siguiente forma:

$$\begin{aligned}\gamma : F[x]/\langle p(x)\rangle &\longrightarrow F'[x]/\langle \widetilde{\sigma}(p(x)\rangle\ ,\\ f(x)+\langle p(x)\rangle &\longmapsto \widetilde{\sigma}(f(x))+\langle \widetilde{\sigma}(p(x))\rangle\ .\end{aligned}$$

Luego, obtenemos el siguiente diagrama:

$$F(\alpha) \xrightarrow{\varphi^{-1}} F[x]/\langle p(x)\rangle \xrightarrow{\gamma} F'[x]/\langle \widetilde{\sigma}(p(x)\rangle \xrightarrow{\varphi'} F'(\alpha')\ .$$
$$\varphi'\circ\gamma\circ\varphi^{-1}$$

Tomemos $a \in F$, entonces:

$$\begin{aligned}(\varphi'\circ\gamma\circ\varphi^{-1})(a) &= (\varphi'\circ\gamma)(\varphi^{-1}(a))\\ &= (\varphi'\circ\gamma)(a) \quad \text{Por a) de la observación 1.160.}\\ &= \varphi'(\gamma(a))\\ &= \varphi'(\sigma(a)+\langle\widetilde{\sigma}(p(x))\rangle)\\ &= \sigma(a).\end{aligned}$$

Además, se puede observar lo siguiente a partir de las definiciones de los morfismos:

$$\alpha \xmapsto{\varphi^{-1}} x+\langle p(x)\rangle \xmapsto{\gamma} x+\langle\widetilde{\sigma}(p(x))\rangle \xmapsto{\varphi'} \alpha'.$$
$$\varphi'\circ\gamma\circ\varphi^{-1}$$

Sea $\tau := \varphi' \circ \gamma \circ \varphi^{-1}$. Ya que τ es una composición de isomorfismos de campos, entonces τ es un isomorfismo que satisface $\tau|_F = \sigma$ y $\tau(\alpha) = \alpha'$. Concluimos que:

$$F(\alpha) \simeq F'(\alpha').$$

Ahora probaremos que el isomorfismo $\tau : F(\alpha) \longrightarrow F(\alpha')$ es único con las propiedades mencionadas, para ello supongamos que existe otro isomorfismo $\widetilde{\tau} : F(\alpha) \longrightarrow F'(\alpha')$ tal que $\widetilde{\tau}|_F = \sigma$ y $\widetilde{\tau}(\alpha) = \alpha'$

Ya que $\alpha \in K$ es algebraico sobre F, por el corolario 1.175 se sigue que la extensión simple $F(\alpha)/F$ es algebraica y finita. Sea $n = grad(p(x))$ y por la proposición 1.167 (c) tomemos el conjunto $\{1, \alpha, ..., \alpha^{n-1}\}$ como una base para $F(\alpha)$ como $F-$espacio vectorial y sea $\widehat{x} \in F(\alpha)$, por lo tanto existen $a_0, ..., a_{n-1} \in F$ tales que:

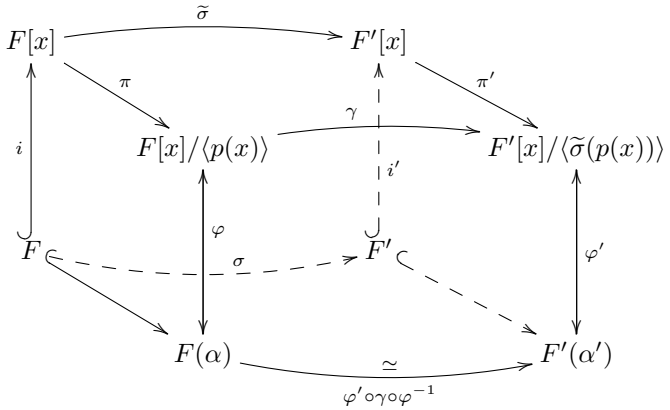
$$\widehat{x} = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1}.$$

Entonces:

$$\begin{aligned}
\widetilde{\tau}(\widehat{x}) &= \widetilde{\tau}(a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1}) \\
&= \sum_{i=0}^{n-1} \widetilde{\tau}(a_i\alpha^i) \\
&= \sum_{i=0}^{n-1} \widetilde{\tau}(a_i)(\alpha')^i \quad \text{esto ya que } \widetilde{\tau}(\alpha) = \alpha' \\
&= \sum_{i=0}^{n-1} \sigma(a_i)(\alpha')^i \quad \text{pues } \widetilde{\tau}|_F = \sigma \\
&= \sum_{i=0}^{n-1} \tau(a_i)\tau(\alpha^i) \quad \text{ya que } \tau|_F = \sigma \text{ y } \tau(\alpha) = \alpha' \\
&= \sum_{i=0}^{n-1} \tau(a_i\alpha^i) \\
&= \tau(\sum_{i=0}^{n-1} a_i\alpha^i) \\
&= \tau(\widehat{x}).
\end{aligned}$$

Concluimos que $\tau = \widetilde{\tau}$ y por lo tanto, τ es único con las propiedades que hemos enunciado. □

A continuación exponemos un diagrama que simplifica el proceso de la demostración y establece claramente las relaciones entre los campos que se han invocado.



Proposición 2.49 *Sean K/F, K'/F' extensiones de campos y $\sigma : F \longrightarrow F'$ un isomorfismo de campos. Supongamos que K es un campo de descomposición de $\{f_i\}_{i\in I} \subseteq F[x]$ y que $\tau : K \longrightarrow K'$ es un homomorfismo de campos tal que $\tau|_F = \sigma$. Entonces $\tau(K)$ es un campo de descomposición para el conjunto $\{\widetilde{\sigma}(f_i)\}_{i\in I} \subseteq F'[x]$.*

Demostración. Ver [14, lema 3.18, pág. 33]. □

Proposición 2.50 *Sean F, F' campos, $\sigma : F \longrightarrow F'$ un isomorfismo de campos, $f(x) \in F[x]$ un polinomio no constante y K un campo de descomposición para $f(x)$ sobre F y sea K' un campo de descomposición para $\widetilde{\sigma}(f(x))$ sobre F'. Entonces existe un único isomorfismo $\tau : K \longrightarrow K'$ tal que $\tau|_F = \sigma$. Más aún, si $\alpha \in K$ es algebraico sobre F y α' es una raíz de $\widetilde{\sigma}(min(F,\alpha))$, entonces el morfismo τ puede elegirse de tal forma que $\tau(\alpha) = \alpha'$.*

Demostración. Ver [14, teorema 3.19, pág. 34]. □

Teorema 2.51 *Sean F, F' campos y $\sigma : F \longrightarrow F'$ un isomorfismo de campos, $S = \{f_i(x)\}_{i\in I} \subseteq F[x] \setminus \{0\}$ y $S' = \{\widetilde{\sigma}(f_i(x))\}_{i\in I} \subseteq F'[x]$. Además, sea K el campo de descomposición de S sobre F y K' el campo de descomposición de S' sobre F'. Entonces, existe un único isomorfismo $\tau : K \longrightarrow K'$ tal que $\tau|_F = \sigma$. Más aun, τ puede elegirse de tal forma que si $\alpha \in K$ y $\alpha' \in K'$ es una raíz cualquiera de $\widetilde{\sigma}(min(F,\alpha))$, entonces $\tau(\alpha) = \alpha'$.*

Demostración. Vea [14, teorema 3.20, pág. 34]. □

2.4. Extensiones normales

La sección 2.2 inició con la búsqueda de una extensión de campos de un campo F para el cual un polinomio no constante sobre $F[x]$ se pudiera escribir

como el producto de factores irreducibles de grado 1, con ayuda de eso se probó que siempre se puede extender el resultado para una cantidad finita de polinomios sobre un campo dado y también se dió solución cuando se considera una cantidad arbitraria de polinomios, el problema de descomponer esos polinomios se puede resolver por el teorema 2.43.

En esta breve sección consideraremos las extensiones de un campo arbitrario F que se quedan, por así decir, a medio camino de ser cerraduras algebraicas, es decir que son subcampos de la cerradura algebraica de F y que cumplen la misma condición pero sólo para una algunos subconjuntos de $F[x]$.

Definición 2.52 *Se dice que una extensión de campos K/F es **normal** si existe $S \subseteq F[x] \setminus F$ tal que K es campo de descomposición de S.*

Observación 2.53 *a) Note que no hay restricción para la cantidad de polinomios no constantes que puede albergar S.*

b) Sean F,K, L campos tales que, $F \subseteq L \subseteq K$ con K/F normal, entonces K/L es normal. En general no es posible concluir que L/F es normal ya que no hay información suficiente para afirmar que L posee todas las raíces de un polinomio en $F[x]$ que se descompone sobre K. En el inciso c) del teorema fundamental de Galois (vea teorema 2.75) se examinará una condición para que la extensión intermedia L/F sea normal.

c) La definición de normalidad de una extensión tiene sentido tanto para extensiones finitas como infinitas.

Proposición 2.54 *Toda extensión de campos de grado 2 es normal.*

Demostración. Sea K/F una extensión tal que $[K : F] = 2$.
Sea $\alpha \in K \setminus F$. Ya que la extensión es finita entonces es algebraica, esto por la proposición 1.170, así, α es algebraico sobre F y es tal que $K = F(\alpha)$ ya que la dimensión de K como F-espacio vectorial es 2.
Por otra parte, del inciso c) de la proposición 1.167 se verifica que el grado de $min(F, \alpha)$ es 2. Ya que α es una raíz de este polinomio, de la proposición 1.127 se sigue que $x - \alpha | min(F, \alpha)$ en $K[x]$, por lo tanto, existe $g(x) \in K[x]$ tal que:

$$min(F, \alpha) = (x - \alpha) \cdot g(x).$$

Del inciso a) de la observación 1.115 se tiene que $grad(g(x)) = 1$, es decir, que $min(F, \alpha)$ se factoriza linealmente sobre K. De esta forma, concluimos que K es normal sobre F. □

Existe una relación estrecha entre extensiones de campos de grado dos y la proposición 1.52. El teorema fundamental de Galois (teorema 2.75) explicará más sobre esta relación entre normalidad de grupos y normalidad de extensiones.

Proposición 2.55 *Sea K/F una extensión algebraica. Los siguientes enunciados son equivalentes:*

a) K/F es una extensión normal.

b) Si M es la cerradura algebraica de K y si $\tau : K \longrightarrow M$ es un F-homomorfismo, entonces $\tau(K) = K$.

c) Sean F, K, L y N campos tales que $F \subseteq L \subseteq K \subseteq N$ y $\sigma : L \longrightarrow N$ un F-homomorfismo. Entonces $\sigma(L) \subseteq K$ y además, existe $\tau \in Gal(K/F)$ tal que $\tau|_L = \sigma$.

d) Si $p(x) \in F[x] \setminus \{0\}$ es cualquier polinomio irreducible tal que $p(x)$ tiene una raíz en K, entonces K contiene un campo de descomposición para $p(x)$.

Demostración. Para una demostración le recomendamos revisar [14, proposición 3.28, pág. 36]. □

2.5. Extensiones separables

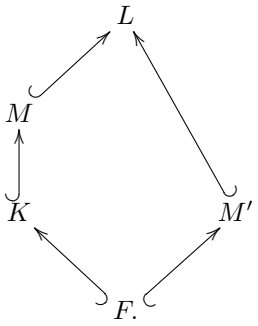
Definición 2.56 *Sean F un campo y $p(x) \in F[x] \setminus \{0\}$ un polinomio irreducible sobre F. Se dice que $p(x)$ es **separable sobre** F si $p(x)$ no tiene raíces repetidas en cualquier campo de descomposición. En otro caso diremos que $p(x)$ es **inseparable**.*
*Un polinomio $f(x) \in F[x]$ se dice que es separable si cada factor irreducible de $f(x)$ en $F[x]$ es separable sobre F y en otro caso diremos que es **inseparable.***

Observación 2.57 *Sea $f(x) \in F[x]$ un polinomio y K un campo de descomposición de $f(x)$, si $f(x)$ no tiene raíces repetidas en K entonces $f(x)$ no tiene raíces repetidas en cualquier extensión L/K.*

Demostración. Tenemos la factorización de $f(x)$ en $K[x]$ de la siguiente manera: $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ con $a \in K$, $\alpha_i \in K$ para todo $i = 1, \cdots, n$ y $\alpha_i \neq \alpha_j$ si $i \neq j$. Sea $f(x) = a(x-\beta_1)\ldots(x-\beta_n)$ la factorización de $f(x)$ en $L[x]$. Como $K[x] \subseteq L[x]$, tenemos que los polinomios $x - \alpha_i \in L[x]$ y como $L[x]$ es de factorización única, después de reordenar podemos suponer que $x - \alpha_i = x - \beta_i \in L[x]$ para todo $i = 1, \cdots, n$ y así tenemos que en la factorizacíon de $f(x)$ en $L[x]$ no tiene raíces repetidas. □

Lema 2.58 *Sea K/F una extensión de campos y $f(x) \in F[x]$. Si $f(x)$ es separable sobre F, entonces $f(x)$ es separable sobre K.*

Demostración. Sea $p(x) \in K[X]$ un factor irreducible (podemos suponer que es mónico) de $f(x)$ visto como polinomio en $K[x]$. Sea L la cerradura algebraica de K y $M \subseteq L$ un campo de descomposición de $p(x) \in K[X]$ (vea corolario 2.45). Sea $\alpha \in M$ una raíz de $p(x)$, como $p(x) \in K[X]$ es irreducible mónico y $p(\alpha) = 0$, tenemos que $p(x) = min(K, \alpha)$.
Por otro lado, como $p(x)|f(x)$ en $K[x]$ (pues $p(x)$ es factor de $f(x)$), tenemos que $f(\alpha) = 0$ y así α es algebraico sobre F ya que $f(x) \in F[x]$. Por lo tanto, existe $min(F, \alpha) \in F[x]$ y además $min(F, \alpha)|f(x)$ en $F[x]$ por la propiedad de los polinomios mínimos. Sea M'/F una extensión tal que M' es un campo de descomposición de $min(F, \alpha)$. Como $F \subseteq K \subseteq L$ entonces $min(F, \alpha)$ se factoriza linealmente en L y así podemos suponer que $M' \subseteq L$. Tenemos el siguiente diagrama de inclusiones de campos:



Como $f(x)$ es separable sobre F y $min(F, \alpha)$ es un factor irreducible de $f(x) \in F[x]$, tenemos que $min(F, \alpha)$ no tiene raíces repetidas en M'. Luego por la observación 2.57 tenemos que:

$$(*) : min(F, \alpha) \text{ no tiene raíces repetidas en } L.$$

Ahora bien, como $min(F, \alpha)$ también está en $K[X]$, tenemos por la propiedad del polinomio mínimo que $min(K, \alpha) \mid min(F, \alpha)$ en $K[x]$. Es decir, tenemos siguiente factorización en $K[x]$:

$$min(F, \alpha) = min(K, \alpha) \cdot g(x),$$

con $g(x) \in K[x]$. Ahora, si $p(x) = min(K, \alpha)$ tuviera raíces repetidas en M, entonces $min(F, \alpha)$ tendría raíces repetidas en M y por lo tanto $min(F, \alpha)$ tendría raíces repetidas en L, lo cual contradice la afirmación $(*)$ de arriba. Por lo tanto, $p(x)$ no tiene raíces repetidas en M, probándose que $p(x)$ es separable sobre K y por lo tanto $f(x)$ es separable sobre K. □

Como hemos visto en la definición 2.56, el concepto de separabilidad se refiere, en primer lugar, a los polinomios irreducibles de $F[x]$ cuando F es un

campo y luego es posible extender la definición a cualquier polinomio en $F[x]$, esto en virtud del teorema 1.133 pues se obtiene que $F[x]$ es un dominio de factorización única y de esta forma podemos hablar de la separabilidad de un polinomio no cero en términos de la separabilidad de sus factores irreducibles en $F[x]$. Es posible extender la definición de separabilidad para elementos de una extensión de campos de F y luego sobre la separabilidad de extensiones como veremos a continuación.

Definición 2.59 *Sean K/F una extensión de campos y $\alpha \in K$ un elemento algebraico sobre F. Se dice que α **es separable sobre F** si el polinomio $min(F, \alpha)$ es separable sobre F.*

Definición 2.60 *Una extensión algebraica K/F es una **extensión separable** si todo elemento $\alpha \in K$ es separable sobre F. En cualquier otro caso la extensión K/F se dice **inseparable**.*

A continuación exponemos algunas propiedades sobre la separabilidad de polinomios.

Proposición 2.61 *Sean F un campo y $f(x), g(x) \in F[x]$. Entonces se satisfacen las siguientes condiciones:*

a) Si $f(x)$ no tiene raíces repetidas en cualquier campo de descomposición entonces $f(x)$ es separable sobre F.

b) Si $g(x)|f(x)$ y $f(x)$ es separable sobre F, entonces $g(x)$ es separable sobre F.

c) El producto de cualquier familia finita de polinomos separables sobre F es separable sobre F.

Demostración. Para una demostración vea [14, Lema 4.3, pág. 40]. □

Proposición 2.62 *Sean F, L y K campos tales que $F \subseteq L \subseteq K$. Si K/F es separable, entonces las extensiones intermedias L/F y K/L son separables.*

Demostración. Se deja como ejercicio al lector. □

Es importante notar que en la proposición 2.62 no se involucra la finitud o infinitud sobre la extensión K/F.

Proposición 2.63 *Si F es un campo de característica 0, entonces todo polinomio no cero en $F[x]$ es separable.*

Demostración. Vea [19, Lema 4.4, pág. 201]. □

Proposición 2.64 *Sea K/F una extensión de campos finita tal que K es el campo de descomposición de un polinomio separable sobre F, entonces:*

$$|Gal(K/F)| = [K : F] < \infty.$$

Demostración. Para una demostración vea [21, teorema 56, pág. 60]. □

Corolario 2.65 *Si K/F es una extensión finita y K es el campo de descomposición de un polinomio separable sobre F, entonces K/F es de Galois.*

Demostración. La prueba es inmediata a partir de la proposición 2.64 y del teorema 2.20. □

El teorema 2.20 nos proporcionó dos formas equivalentes para probar que una extensión finita es de Galois, el siguiente resultado establece relaciones equivalentes para extensiones normales y separables con las extensiones de Galois. Es la caracterización más importante que tendremos sobre las extensiones finitas de Galois.

Proposición 2.66 *Sea K/F una extensión finita. Los siguientes enunciados son equivalentes:*

a) K es el campo de descomposición de un polinomio separable sobre $F[x]$.

b) K/F es de Galois.

c) Existe $G \leq Aut(K)$ tal que $|G| < \infty$ y $F = K^G$.

d) K/F es normal y separable.

Demostración.

a) $\implies$ b) Esta implicación se ha probado en el corolario 2.65.

b) $\implies$ c) Ya que K/F es una extensión finita, entonces, si consideramos $G = Gal(K/F) \subseteq Aut(K)$, por la proposición 2.16 se tiene que $|G| < \infty$ y como la extensión K/F de Galois se concluye que $F = K^{Gal(K/F)}$.

c) $\implies$ d)

Primero probaremos la separabilidad de la extensión K/F, para ello tomemos $\alpha \in K$.

Por hipótesis, existe $G = \{\sigma_i\}_{i=0}^{n-1} \subseteq Aut(K)$ tal que $|G| = n < \infty$ y $F = K^G$, entonces consideremos:

$$A = \{\sigma_i(\alpha) \in K : \sigma_i \in G \text{ y } 0 \leq i \leq n-1\}.$$

Al ser G un grupo finito, entonces A debe ser finito y como los automorfismos de G pueden llegar a coincidir en la evaluación en α, entonces en A hay una cantidad menor o igual que n de elementos distintos. Sea $X = \{\sigma_0(\alpha) = id_K(\alpha), \sigma_1(\alpha), \sigma_2(\alpha), ..., \sigma_s(\alpha)\} \subseteq K$ el conjunto de los distintos elementos de A con $0 \leq s \leq n-1$.

Veamos que los elementos de G permutan a los elementos de X. Sean $\sigma_i \in G$ y $\sigma_j(\alpha) \in X$, entonces:

$$\sigma_i\left(\sigma_j(\alpha)\right) = \sigma_i \circ \sigma_j(\alpha) = \sigma_k\left(\alpha\right),$$

para algún $\sigma_k \in G$ y esto pasa ya que G es un grupo bajo la composición. Ya que $A = \{\sigma_i(\alpha) \in K : 0 \leq i \leq n-1\}$ y X consta de todos los elementos distintos de A, tenemos que $\sigma_k(\alpha) \in X$. Ahora, sean $\sigma_i \in G$ y $\sigma_j(\alpha), \sigma_{j'}(\alpha) \in X$ tales que $\sigma_i(\sigma_j(\alpha)) = \sigma_i(\sigma_{j'}(\alpha))$. Como $G \leq Aut(K)$ tenemos que σ_i es inyectiva y así concluimos que $\sigma_j(\alpha) = \sigma_{j'}(\alpha)$. Por lo tanto $\sigma_i|_X : X \longrightarrow X$ es inyectiva; y como X es finito concluimos que $\sigma_i|_X$ es una biyección. Es decir, $\sigma_i|_X$ permuta los elementos de X.
Ahora para cada $0 \leq i \leq n-1$ consideremos las siguientes extensiones para cada $\sigma_i \in G$, $\widetilde{\sigma_i} : K[x] \longrightarrow K[x]$ así como en la proposición 1.161 y tomemos el polinomio:

$$p(x) = (x-\alpha) \cdot (x-\sigma_1(\alpha)) \cdots (x-\sigma_s(\alpha)) \in K[x]. \tag{2.6}$$

Por lo que hemos dicho previamente, obtenemos que:

$$\widetilde{\sigma_i}(p(x)) = (x-\sigma_i(\alpha)) \cdot (x-\sigma_i(\sigma_1(\alpha))) \cdots (x-\sigma_i(\sigma_s(\alpha))) = p(x), \tag{2.7}$$

esto ya que los $\sigma_i \in G$ permutan a los elementos de X.

Ahora, los coeficientes de $p(x)$ quedan fijos bajo la acción de σ_i, esto ya que al desarrollar el producto de la ecuación 2.7 se obtiene una expresión similar a la siguiente en su forma general:

$$p(x) = x^{s+1} + a_s x^s + \cdots + a_0 \text{ con } a_i \in K$$

entonces, por definición de $\widetilde{\sigma_i} : K[x] \longrightarrow K[x]$ se sigue:

$$\widetilde{\sigma}_i\left(p(x)\right) = x^{s+1} + \sigma_i(a_s)x^s + \cdots + \sigma_i(a_1)x + \sigma_i(a_0) = p(x),$$

y por igualdad de polinomios se tiene que: $\sigma_i(a_j) = a_j$, esto para todo $j \in \{0, ..., s\}$ es decir, los coeficientes de $p(x)$ son elementos de $K^G = F$ y por lo tanto $p(x) \in F[x]$.

Observemos que, por construcción, $p(x)$ tiene todas sus raíces distintas, además se tiene que $p(\alpha) = 0$ y al ser $\alpha \in K$ algebraico sobre F se tiene por el inciso b) de la proposición 1.167 que $min(F, \alpha) | p(x)$ en $F[x]$.

Ahora, tomemos $g(x) \in F[x]\backslash\{0\}$ un polinomio cualquiera tal que $g(\alpha) = 0$ y notemos que para cada $\sigma_i \in G$ con $i \in \{0, ..., n-1\}$ se tiene que:

$$g(\sigma_i(\alpha)) = \sigma_i(g(\alpha)) = \sigma_i(0) = 0,$$

y esto es así ya que los coeficientes de $g(x)$ son elementos de $F = K^G$ y σ_i los deja fijos. En particular, para cada $i \in \{0, ..., s\}$, $\sigma_i(\alpha)$ son raíces distintas de $g(x)$ y ahora, a partir de la proposición 1.169, en $K[x]$ se tiene que:

$$p(x) = (x - \alpha) \cdots (x - \sigma_s(\alpha)) | g(x). \tag{2.8}$$

Ya que la ecuación 2.8 se verifica para cualquier polinomio $g(x)$ no cero en $F[x]$ que se anule al aplicarle α, entonces puede pensarse, en particular a $g(x) = min(F, \alpha)$ y por lo tanto $p(x)|min(F, \alpha)$ en $K[x]$.
Sin embargo, como $p(x)$ y $min(F, \alpha)$ pertenecen a $F[x]$, se tiene por el algoritmo de la división en $F[x]$ que $p(x)$ divide a $min(F, \alpha)$ en $F[x]$ esto ya que $F[x] \subseteq K[x]$ y $p(x)$ divide a $min(F, \alpha)$ en $K[x]$.
Al ser $min(F, \alpha)$ irreducible en $F[x]$, y ya que se tiene $min(F, \alpha)|p(x)$ y $p(x)|min(F, \alpha)$ en $F[x]$, tenemos que existe $k \in F$ tal que $min(F, \alpha) = k \cdot p(x)$, y como $p(x)$ y $min(F, \alpha)$ son ambos mónicos, entonces $k = 1$ y por lo tanto $p(x) = min(F, \alpha) \in F[x]$ es un polinomio que no tiene raíces repetidas. Es decir, $\alpha \in K$ es un elemento separable sobre F. Concluimos que la extensión K/F es una extensión separable.

De la construcción anterior se puede concluir que si $\alpha \in K$ es algebraico sobre F, entonces $min(F, \alpha) = p(x)$, donde $p(x)$ es el polinomio que se ha construido en la ecuación 2.6.

Ahora probaremos que la extensión K/F es normal usando la equivalencia de normalidad que se ha dado en el inciso d) de la proposición 2.55.

Sea $f(x) \in F[x] \setminus \{0\}$ irreducible sobre F tal que $\alpha \in K$ es una raíz de $f(x)$. Ya que la extensión K/F es finita, de la proposición 1.175 se sigue que α es algebraico sobre F. Construyamos el polinomio $p(x)$ asociado a α, similarmente a como se ha hecho en ecuación 2.6. Entonces tenemos que en $F[x]$ se verifica:

$$p(x)|f(x).$$

Y por lo tanto existe $k(x) \in F[x] \setminus \{0\}$ tal que $f(x) = p(x) \cdot k(x)$ y al ser $f(x)$ un polinomio irreducible entonces $k(x)$ tiene que ser una constante.

Observemos que por construcción de $p(x)$ (vea ecuación 2.6) se tiene $grad(p(x)) = s + 1$ y todas las raíces de $p(x)$ son los elementos de X y $|X| = s + 1$, por lo tanto $p(x)$ descompone linealmente en K y por ende

tenemos que $f(x)$ también se descompone linealmente en K, es decir, K contiene un campo de descomposición de $f(x)$.

Concluimos que la extensión K/F es normal y separable.

d) $\Longrightarrow$ a)

Ya que por hipótesis tenemos que la extensión K/F es finita, normal y separable, entonces, sea $\{\alpha_0 = 1, \alpha_1, ..., \alpha_n\} \subseteq K$ una F-base de K formada por elementos algebraicos y separables. Tomemos la familia de polinomios mínimos y separables asociados a cada α_i:

$$\{min(F, \alpha_i) \in F[x] : 1 \leq 0 \leq n\} \subseteq F[x] \setminus \{0\}.$$

Ya que cada uno de estos polinomios irreducibles $min(F, \alpha_i)$ tiene una raíz $\alpha_i \in K$ y la extensión K/F es normal sobre F, entonces por el inciso d) de la proposición 2.55 se sigue que $min(F, \alpha_i)$ se descompone como el producto de factores lineales en $K[x]$ y cada uno de los factores son distintos ya que la extensión K/F es separable.

Consideremos el siguiente polinomio, que es producto de polinomios separables:

$$f(x) = \prod_{i=1}^{n} min(F, \alpha_i) \in F[x].$$

Por el inciso c) de la proposición 2.61 tenemos que el polinomio $f(x)$ es separable, además se cumple que K es el campo de descomposición para $f(x)$.

Concluimos que K es el campo de descomposición para $f(x)$, que es un polinomio separable.

□

La proposición 2.66 se puede formular nuevamente, a términos más generales, si se intercambia la condición sobre finitud de la extensión por la condición de ser una extensión algebraica, así como lo muestra la siguiente proposición.

Proposición 2.67 *Sea K/F una extensión algebraica. Entonces, los siguientes enunciados son equivalentes:*

a) La extensión K/F es de Galois.

b) K/F es una extensión normal y separable.

c) K es el campo de descomposición de un conjunto de polinomios separables sobre F.

Demostración. Para una demostración de este hecho, vea [14, teorema 4.9, pág. 42]. □

Corolario 2.68 *Sea K/F una extensión finita y separable. Entonces K está contenida en una extensión de Galois sobre F.*

Demostración. Ya que la extensión K/F es finita, entonces, por el corolario 1.175 sea $\{\alpha_1, ..., \alpha_n\} \subseteq K$ una base de elementos algebraicos para K como F-espacio vectorial, en particular, $K = F(\alpha_1, ..., \alpha_n)$. Ahora, sea $min(F, \alpha_i) \in F[x] \setminus \{0\}$ el polinomio mínimo para cada α_i con $i \in \{1, \ldots, n\}$ y consideremos el polinomio:

$$f(x) = \prod_{i=1}^{n} min(F, \alpha_i) \in F[x].$$

Notemos que $f(x)$ es separable ya que es un producto de polinomios separables, esto por el inciso c) de la proposición 2.61.

Ahora, por el corolario 2.29, existe M un campo de descomposición para $f(x) \in F[x]$ y además, $[M : F] < \infty$. Ya que M contiene al conjunto $\{\alpha_1, \ldots, \alpha_n\}$ y a F entonces obtenemos la siguiente relación:

$$F \subseteq K \subseteq M.$$

De esta forma podemos concluir, usando la equivalencia dada en el inciso d) de la proposición 2.66, que M/F es una extensión de Galois, esto ya que M es el campo de descomposición de un polinomio separable sobre F. Por lo tanto, K está contenida en una extensión de Galois sobre F. □

Corolario 2.69 *Si K/F es una extensión de campos, entonces F/F es una extensión de Galois.*

Demostración. Primero notemos que F/F es una extensión de grado 1 (vea corolario 1.150), y es normal ya que para todo $\alpha \in F$, se tiene que F es el campo de descomposición de $x - \alpha$ que es un polinomio de grado uno, y posee raíces distintas. De esta forma, concluimos que F/F es una extensión algebraica, normal y separable. El resultado se sigue de la proposición 2.67. □

Corolario 2.70 *Sean F, L, K campos tales que $F \subseteq L \subseteq K$ con K/F una extensión algebraica. Si K/F es de Galois, entonces K/L es una extensión de Galois.*

Demostración. Primero notemos que, por la proposición 1.180, K/L es una extensión algebraica. Por otra parte, del inciso b) de la proposición 2.67, se obtiene que K/F es una extensión normal y separable. Ahora, del inciso b) de la observación 2.53 y de la proposición 2.62 se sigue, respectivamente, que K/L

es una extensión normal y separable. Finalmente, de la proposición 2.67, se sigue que K/L es una extensión de Galois. □

Observación 2.71 *Observe que en la prueba del corolario 2.70 no se ha involucrado la finitud o infinitud de la extensión K/F, es ésta la razón que este corolario sea válido para extensiones finitas e infinitas.*

Proposición 2.72 *Sea K/F una extensión algebraica y sean L_1/F y L_2/F extensiones de campos tal que $L_1 \subseteq K$ y $L_2 \subseteq K$. Si L_1/F y L_2/F son extensiones de Galois, entonces $(L_1 \cap L_2)/F$ es una extensión de Galois. Además, si L_1/F o L_2/F son extensiones finitas, entonces $L_1 \cap L_2/F$ es una extensión finita.*

Demostración. Consideremos las extensiones de campos $F \subseteq L_1 \cap L_2 \subseteq K$, por proposición 1.180 tenemos que $L_1 \cap L_2/F$ es una extensión algebraica.
Ahora, sea $f(x) \in F[x]$ un polinomio irreducible con $n = \text{grad}(f(x))$ y tal que $f(x)$ tiene una raíz $a \in L_1 \cap L_2$. Como L_1/F es de Galois, en particular es normal (ver proposición 2.67) y como $a \in L_1$ tenemos que L_1 contiene a un campo de descomposición de $f(x)$ y así concluimos que las n raíces de $f(x)$ están en L_1 (ver proposición 2.55 (d)), similarmente tenemos que las n raíces de $f(x)$ están en L_2 y por lo tanto $L_1 \cap L_2$ tiene las n raíces de $f(x)$. Por lo tanto, $L_1 \cap L_2$ contiene a un campo de descomposición de $f(x)$. Luego por proposición 2.55 (d), tenemos que $L_1 \cap L_2/F$ es una extensión normal de F. Como L_1/F es de Galois, tenemos que L_1/F es separable (ver proposición 2.67). Luego, como $F \subseteq L_1 \cap L_2 \subseteq L_1$, concluimos por proposición 2.62 que $L_1 \cap L_2/F$ es una extensión separable y así por proposición 2.67 tenemos que $L_1 \cap L_2/F$ es una extensión de Galois. La segunda afirmación se sigue de la proposición 1.146. □

En la sección 1.3 hemos visto que, dada una extensión K/F y $\alpha \in K$ un elemento algebraico sobre F, hay un campo intermedio de K/F tal que $F \subseteq F(\alpha) \subseteq K$, y de hecho tenemos distintos resultados que nos hablan de la dimensión de $F(\alpha)/K$ además la descripción de los elementos en $F(\alpha)$. Esto puede hallarse en las proposiciones 1.167 y 1.171.
Dados dos campos intermedios de una extensión K/F, no necesariamente debería ocurrir que ellos se comparen respecto a la contención, sin embargo, veremos que se puede construir un campo intermedio de la extensión K/F que los contenga. El propósito de esta breve sección es describir a ese campo, llamado *el composite.*

Definición 2.73 *Sean L_1/F, L_2/F extensiones de campos de F contenidas en una extensión en común K. Se define el* ***composite*** *de L_1 y L_2 como el campo generado por L_1 y L_2 y es denotado por $L_1L_2 = L_1(L_2) = L_2(L_1)$ (vea teorema 1.158).*

En otras palabras, el composite de L_1 y L_2 es el menor de los subcampos de K que son extensiones de F y que contiene a L_1 y a L_2.

En la siguiente proposición enunciamos algunas de las propiedades relativas a finitud, algebraicidad, separabilidad y normalidad asociados al composite de dos campos.

Proposición 2.74 *Sean K un campo y L_1/F L_2/F dos extensiones de campo tal que $L_1 \subseteq K$ y $L_2 \subseteq K$, entonces:*

a) Si $L_1 = F(\alpha_1, \ldots, \alpha_n)$ y $L_2 = F(\beta_1, \ldots, \beta_m)$, entonces:

$$L_1L_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m).$$

b) L_1/F y L_2/F son extensiones finitas si y solo si L_1L_2/F es finita.

c) L_1/F y L_2/F son algebraicas si y solo si L_1L_2/F es algebraica.

d) $[L_1L_2 : F] \leq [L_1 : F] \cdot [L_2 : F]$. Si $([L_1 : F], [L_2 : F]) = 1$, entonces la igualdad se verifica.

e) Si L_1/F y L_2/F son normales, entonces L_1L_2/F es normal.

f) Si L_1/F y L_2/F son separables, entonces L_1L_2/F es separable.

g) Si L_1/F y L_2/F son extensiones de Galois, entonces la extensión L_1L_2/F es de Galois.

Demostración. Se deja de ejercicio al lector. □

2.6. Teorema fundamental de la teoría de Galois

En el teorema 2.14 vimos que es posible establecer una correspondencia biyectiva que invierte inclusiones entre ciertos campos intermedios de una extensión dada y subgrupos selectos del grupo de Galois asociados a dicha extensión. En este apartado se establece que una condición para que se elimine la restricción para la biyección es que la extensión K/F sea finita y de Galois y así, la biyección se satisface entre todos los campos intermedios y todos los subgrupos del grupo de Galois asociados a la extensión. Además, si a la extensión K/F se le pide ser de Galois, resulta más fructífero el teorema 2.14.

En lo sucesivo, si K/F es una extensión, se define $\mathcal{L}$ como la colección de todos los campos intermedios de la extensión K/F.

Teorema 2.75 (Teorema fundamental de Galois) *Sea K/F una extensión de Galois finita y consideremos las siguientes dos funciones:*

$$\Psi : \pounds \longrightarrow \{H : H \leq Gal(K/F)\} ,$$
$$L \longmapsto Gal(K/L) .$$

$$\Phi : \{H : H \leq Gal(K/F)\} \longrightarrow \pounds ,$$
$$H \longmapsto K^H .$$

Entonces, Ψ y Φ determinan una correspondencia biyectiva que invierte inclusiones.
Más aún, si $L \in \pounds$ se corresponde con $H \leq Gal(K/F)$ bajo la correspondencia de Ψ y Φ , entonces se tiene que:

a) $[K : L] = |H|$.

b) $[L : F] = [Gal(K/F) : H]$.

c) $H \trianglelefteq Gal(K/F)$ *si y solo si* L/F *es una extensión de Galois.*

d) Si se satisface el inciso c), entonces $Gal(K/F)/H \cong Gal(L/F)$.

Demostración. Exponer una prueba de este importante resultado nos desvía de nuestra trayectoria, es por ello que le recomendamos ver [14, teorema 5.1, pág 51]. □

2.7. Algunas aplicaciones del Teorema Fundamental de la teoría de Galois

En esta sección se proveen distintas aplicaciones del Teorema fundamental de la teoría de Galois para extensiones finitas, algunas de ellas resuelven problemas fundamentales de las teorías de campos y grupos.

Ejemplo 2.76 *Si K/F es una extensión finita de Galois tal que $Gal(K/F)$ es un grupo abeliano, entonces todo campo intermedio L de la extensión K/F es de Galois sobre F. Supongamos que L se corresponde con H bajo Ψ. Luego, H es un subgrupo normal de $Gal(K/F)$ y por el inciso c) del Teorema fundamental de la teoría de Galois (vea teorema 2.75), se obtiene que L/F es de Galois.*

Ejemplo 2.77 *Si K/F es una extensión finita de Galois, entonces sólo hay una cantidad finita de campos intermedios en dicha extensión. Esto ya que, por el teorema 2.20, sabemos que $|Gal(K/F)| = [K : F] < \infty$. Por lo tanto, el grupo $Gal(K/F)$ sólo posee una cantidad finita de subgrupos que están en correspondencia biyectiva con los campos intermedios de K/F, esto por el Teorema fundamental de la teoría de Galois (vea teorema 2.75).*

Ejemplo 2.78 *Lo que haremos en este ejemplo es obtener la retícula de campos intermedios y subgrupos del grupo de Galois asociados a una extensión de $\mathbb{Q}$, probaremos que dicha extensión es de Galois y describiremos las propiedades de los campos asignados bajo la correspondencia de las funciones Φ y Ψ definidas en el teorema 2.75.*
Consideremos el polinomio mónico $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ y obtengamos un campo de descomposición para $f(x)$.
Sea $z = x^2$, al hacer esta sustitución obtenemos el polinomio $g(z) = z^2 - z - 2$ de segundo grado cuyas soluciones son:

$$z = 2 \text{ y } z = -1.$$

Esto significa que las raíces de f son $x = \pm\sqrt{2}$ y $x = \pm\sqrt{-1} = \pm i$. Además, ya que las 4 raíces de f son distintas, se sigue que f es un polinomio separable sobre $\mathbb{Q}$.
Notemos que el campo $\mathbb{Q}(\sqrt{2}, i)$ es un campo de descomposición para $f(x)$.
Para probar que $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ es una extensión de Galois, basta ver que es una extensión finita, esto en virtud de la proposición 2.66.
Consideremos la siguiente extensión de campos:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i). \tag{2.9}$$

Primero notemos que $x^2 - 2$ es mónico, además es irreducible en $\mathbb{Q}$ gracias al criterio de Eisenstein (vea proposición 1.136) usando el primo $p = 2$. De esta forma obtenemos que $min(\mathbb{Q}, \sqrt{2}) = x^2 - 2$, y a partir del inciso c) de la proposición 1.167 se sigue que:

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = grad(min(\mathbb{Q}, \sqrt{2})) = 2.$$

Por lo tanto, la extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es normal y separable, de la proposición 2.66 se sigue que esta es una extensión finita de Galois.
Por otro lado, calculemos el grado de $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(\sqrt{2})$.
Consideremos el siguiente polinomio mónico de grado dos, $x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$, cuyas raíces son $\pm i \notin \mathbb{Q}(\sqrt{2})$. Por lo tanto $x^2 + 1$ es irreducible en $\mathbb{Q}(\sqrt{2})[x]$ al usar el criterio de la proposición 1.172.
De este modo, por el inciso c) de la proposición 1.167, nuevamente obtenemos que $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$.
Al aplicar la proposición 1.146 en la ecuación 2.9 se sigue:

$$[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},i):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\cdot 2 = 4 < \infty.$$

Por lo tanto, tenemos que $\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}$ *es una extensión finita y de la proposición 2.66 se sigue que es una extensión de Galois. Ahora, de la proposición 2.64 se sigue:*

$$|Gal(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2},i):\mathbb{Q}] = 4.$$

Bien, pues ahora obtengamos los elementos del grupo de Galois para esta extensión.
Naturalmente, un elemento del grupo de Galois de $\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}$ *es el automorfismo identidad* $id_{\mathbb{Q}(\sqrt{2},i)}$ *que se comporta enviando cada elemento en sí mismo, este se obtiene de un proceso de extender el morfismo identidad en* $\mathbb{Q}$ *a un automorfismo identidad del campo* $\mathbb{Q}(\sqrt{2})$ *y posteriormente al campo* $\mathbb{Q}(\sqrt{2},i)$*. El siguiente diagrama ilustra esta extensión.*

$$\begin{array}{ccc}
\mathbb{Q}(\sqrt{2})(i) & \xrightarrow{id_{\mathbb{Q}(\sqrt{2},i)}} & \mathbb{Q}(\sqrt{2})(i) \\
\uparrow{\scriptstyle \tilde{i}} & & \uparrow{\scriptstyle \tilde{i}} \\
\mathbb{Q}(\sqrt{2}) & \xrightarrow{id_{\mathbb{Q}(\sqrt{2})}} & \mathbb{Q}(\sqrt{2}) \\
\uparrow{\scriptstyle i} & & \uparrow{\scriptstyle i} \\
\mathbb{Q} & \xrightarrow{id_{\mathbb{Q}}} & \mathbb{Q}
\end{array}$$

Ya que la extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *es de Galois, por el teorema 2.20 se sigue que el grupo de Galois asociado a esta extensión posee 2 elementos. Uno de esos automorfismos es la identidad en* $\mathbb{Q}$ *y el otro es el automorfismo conjugación que permuta a* $\sqrt{2}$ *con* $-\sqrt{2}$*:*

$$\begin{aligned}
\sigma : \mathbb{Q}(\sqrt{2}) &\longrightarrow \mathbb{Q}(\sqrt{2}) \ , \\
a + b\sqrt{2} &\longmapsto a - b\sqrt{2} \ .
\end{aligned} \tag{2.10}$$

Además el $\mathbb{Q}$*-automorfismo* σ *es de orden 2.*
Ahora extendamos nuevamente el automorfismo σ *a un automorfismo en la extensión* $\mathbb{Q}(\sqrt{2},i)$*, esto se lleva a cabo como sigue: para cualesquiera* $\alpha,\beta \in \mathbb{Q}(\sqrt{2})$*,*

$$\begin{aligned}
\tilde{\sigma} : \mathbb{Q}(\sqrt{2},i) &\longrightarrow \mathbb{Q}(\sqrt{2},i), \\
\alpha + \beta i &\longmapsto \sigma(\alpha) + \sigma(\beta)i
\end{aligned}$$

Observemos que por construcción de $\tilde{\sigma}$ *se tiene que* $\tilde{\sigma}|_{\mathbb{Q}} = id_{\mathbb{Q}}$*.*
De igual forma a como se hizo en el inciso c) del ejemplo 2.24 se prueba que $\tilde{\sigma}$ *es un automorfismo. Por construcción de* $\tilde{\sigma}$ *se satisface lo siguiente:*

$$\begin{array}{ccc} \tilde{\sigma}(1)=1 & \tilde{\sigma}(\sqrt{2})=-\sqrt{2} & \tilde{\sigma}(-\sqrt{2})=\sqrt{2} \\ \tilde{\sigma}(i)=i & \tilde{\sigma}(-i)=-i & \tilde{\sigma}(\sqrt{2}i)=-\sqrt{2}i \\ & \tilde{\sigma}(-\sqrt{2}i)=\sqrt{2}i. & \end{array}$$

Concluimos que $\tilde{\sigma} \in Gal(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$ *y debido a que* σ *es de orden* 2, *se sigue que* $\tilde{\sigma}$ *es de orden 2, pues:*

$$(\tilde{\sigma}\circ\tilde{\sigma})(\alpha+\beta i)=\tilde{\sigma}(\tilde{\sigma}(\alpha+\beta i))=\tilde{\sigma}(\sigma(\alpha)+\sigma(\beta)i)=\sigma^2(\alpha)+\sigma^2(\beta)i=\alpha+\beta i.$$

El siguiente diagrama ilustra la construcción de $\tilde{\sigma}$*:*

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2})(i) & \xrightarrow{\tilde{\sigma}} & \mathbb{Q}(\sqrt{2})(i) \\ \uparrow{\scriptstyle \tilde{i}} & & \uparrow{\scriptstyle \tilde{i}} \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow{\sigma} & \mathbb{Q}(\sqrt{2}) \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle i} \\ \mathbb{Q} & \xrightarrow{id_{\mathbb{Q}}} & \mathbb{Q} \end{array}$$

Partiendo de nueva cuenta del morfismo σ *de la ecuación 2.10, podemos construir otro elemento del grupo de Galois de la extensión* $\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}$ *como se ve a continuación. Para cualesquiera* $\alpha,\beta \in \mathbb{Q}(\sqrt{2})$,

$$\begin{aligned} \widehat{\sigma} : \mathbb{Q}(\sqrt{2},i) &\longrightarrow \mathbb{Q}(\sqrt{2},i) \\ \alpha+\beta i &\longmapsto \sigma(\alpha)-\sigma(\beta)i\ . \end{aligned}$$

De forma similar a como se hizo con $\tilde{\sigma}$, *concluimos que* $\widehat{\sigma}$ *es un* $\mathbb{Q}$*-automorfismo y es tal que:*

$$\begin{array}{ccc} \widehat{\sigma}(1)=1 & \widehat{\sigma}(\sqrt{2})=-\sqrt{2} & \widehat{\sigma}(-\sqrt{2})=\sqrt{2} \\ \widehat{\sigma}(i)=-i & \widehat{\sigma}(-i)=i & \widehat{\sigma}(\sqrt{2}i)=\sqrt{2}i \\ & \widehat{\sigma}(-\sqrt{2}i)=-\sqrt{2}i. & \end{array}$$

De esta forma, $\widehat{\sigma} \in Gal\big(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}\big)$.
Como $Gal(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$ *es un grupo bajo la operación composición, entonces* $\tilde{\sigma}\circ\widehat{\sigma} \in Gal(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$. *Si* $\alpha,\beta \in \mathbb{Q}(\sqrt{2})$ *entonces, al realizar las composiciones adecuadas, el* $\mathbb{Q}$*-automorfismo* $\tilde{\sigma}\circ\widehat{\sigma}$ *queda definido por:*

$$(\widetilde{\sigma}\circ\widehat{\sigma})(\alpha+\beta i) := \alpha-\beta i.$$

Además, por construcción el morfismo $\tilde{\sigma}\circ\widehat{\sigma}$ *se tiene:*

$$\begin{array}{ccc} (\widetilde{\sigma}\circ\widehat{\sigma})(1)=1 & (\widetilde{\sigma}\circ\widehat{\sigma})(\sqrt{2})=\sqrt{2} & (\widetilde{\sigma}\circ\widehat{\sigma})(-\sqrt{2})=-\sqrt{2}, \\ (\widetilde{\sigma}\circ\widehat{\sigma})(i)=-i & (\widetilde{\sigma}\circ\widehat{\sigma})(-i)=i & (\widetilde{\sigma}\circ\widehat{\sigma})(\sqrt{2}i)=-\sqrt{2}i \\ & y\ (\widetilde{\sigma}\circ\widehat{\sigma})(-\sqrt{2}i)=\sqrt{2}i. & \end{array}$$

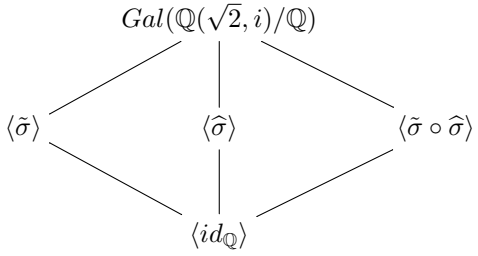
Más aún, usando la proposición 2.6, se puede probar que $\tilde{\sigma} \circ \widehat{\sigma} = \widehat{\sigma} \circ \tilde{\sigma}$ *y que éste es un elemento de orden* 2*. Por lo tanto,* $Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ *es abeliano, y así, todos sus subgrupos son normales en él. De esta forma:*

$$Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) = \{id, \tilde{\sigma}, \widehat{\sigma}, \tilde{\sigma} \circ \widehat{\sigma}\}.$$

Ahora, como $Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ *posee 4 elementos y 3 de ellos son de orden 2, entonces este grupo no es cíclico. Se concluye que:*

$$Gal\big(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}\big) \simeq \mathbb{V} = \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Podemos construir la retícula de los subgrupos cíclicos de orden 2 del grupo de Galois:



Al tener los elementos del grupo de Galois asociados a nuestra extensión podemos asignarles los respectivos campos fijos bajo la función Φ *del teorema 2.75, en este caso lo haremos considerando la acción de cada elemento generador de cada subgrupo.*

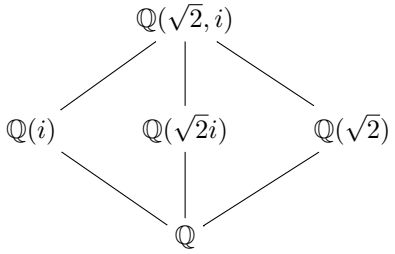
$$\langle\tilde{\sigma}\rangle \xrightarrow{\Phi} \mathbb{Q}(i).$$

$$\langle\widehat{\sigma}\rangle \xrightarrow{\Phi} \mathbb{Q}(\sqrt{2}i).$$

$$\langle\tilde{\sigma} \circ \widehat{\sigma}\rangle \xrightarrow{\Phi} \mathbb{Q}(\sqrt{2}).$$

$$\langle id_{\mathbb{Q}}\rangle \xrightarrow{\Phi} \mathbb{Q}.$$

Por lo tanto, la retícula de subcampos intermedios asociados a la extensión $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ *es la siguiente:*



(2.11)

Para finalizar notemos que, con ayuda del inciso c) del teorema 2.75, podemos describir las extensiones normales sobre $\mathbb{Q}$; como $Gal(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$ es un grupo abeliano, entonces todos sus subgrupos son normales en él, luego, los campos asociados a cada uno de los subgrupos son normales sobre $\mathbb{Q}$, de esta forma, cada una de las extensiones de $\mathbb{Q}$ que aparecen en el diagrama 2.11 son extensiones normales de $\mathbb{Q}$.

Con ayuda del teorema fundamental de la teoría de Galois podemos resolver la cuestión que se ha planteado en la observación 1.148 sobre la existencia de campos intermedios en una extensión finita K/F cuya dimensión sea un divisor de $[K:F]$.

Ejemplo 2.79 *Sean K/F una extensión de Galois tal que $[K:F]=n$ y p un entero primo tal que p divide a n. Entonces, existe un campo L tal que $F \subseteq L \subseteq K$ con $[K:L]$=p.*

En efecto, ya que K/F es una extensión de Galois, del teorema 2.20 se sigue que:

$$|Gal(K/F)| = [K:F] = n.$$

Si p es un divisor de $|Gal(K/F)|$, del corolario 1.40 tenemos que existe un subgrupo $H \leq Gal(K/F)$ tal que $|H| = p$.
Ahora, ya que la extensión K/F es de Galois, se sigue, del teorema fundamental de la teoría de Galois (vea teorema 2.75), que H se corresponde con el campo intermedio K^H de K/F. Finalmente, por el inciso a) del teorema 2.75, se tiene que:

$$[K:K^H] = |H| = p.$$

Y concluimos lo que se deseaba.

En un material más extenso sobre teoría de grupos se construye el grupo de permutaciones de n elementos como sigue: sean X un conjunto con $|X| = n$ y $S_n = \left\{ \sigma : X \longrightarrow X : \sigma \text{ es biyección} \right\}$ con la operación composición. Este

grupo S_n posee orden $n!$ y entre los hechos importantes de este grupo es que contiene un subgrupo $\mathbb{A}_n = \{\sigma \in S_n : \sigma \text{ es par},\}$ llamado **grupo alternante** de S_n y tiene orden $|\mathbb{A}_n| = \frac{n!}{2}$.

En el caso particular cuando $n = 4$ el grupo alternante $\mathbb{A}_4$ se caracteriza por poseer un subgrupo isomorfo al grupo $\mathbb{V}$ (vea ejemplo 1.17) y este es el único subgrupo normal de $\mathbb{A}_4$. Además, $\mathbb{A}_4$ posee tres subgrupos de orden 2, 4 subgrupos de orden 3 y $\mathbb{A}_4$ es un grupo que no posee un subgrupo de orden 6. Para más detalles sobre $\mathbb{A}_4$ vea [8, Transposiciones y el grupo alternante, pág 106] y de igual forma [8, figura 8, pág. 111].

Ejemplo 2.80 *Sea K/F una extensión finita de Galois con $Gal(K/F) = \mathbb{A}_4$. Veamos que no existe un campo intermedio L de K/F tal que $[L : F] = 2$.*
Supongamos que existe un campo intermedio L de K/F con las características mencionadas en el enunciado. De la proposición 1.146 y del hecho de que la extensión K/F es de Galois se sigue que:

$$12 = |Gal(K/F)| = [K : F] = [K : L] \cdot [L : F] = [K : L] \cdot 2.$$

Por lo tanto, $[K : L] = 6$. Además, del corolario 2.70, se sigue que K/L es de Galois y por el teorema 2.20 se obtiene $|Gal(K/L)| = 6$.
Es decir, $Gal(K/F)$ contiene un subgrupo de orden 6, pero $\mathbb{A}_4$ no contiene subgrupos de orden 6. Concluimos que el campo intermedio L de K/F no puede existir.

En el siguiente ejemplo se describe el subgrupo de Galois asociado a una extensión de grado un número primo.

Ejemplo 2.81 *Si K/F es de Galois y $[K : F] = p$ con $p \in \mathbb{Z}$ un primo, del teorema 2.20 se sigue que:*

$$|Gal(K/F)| = p.$$

Por lo tanto, de la proposición 1.37, concluimos que $Gal(K/F)$ es un grupo cíclico de orden p, y así, $Gal(K/F) \cong \mathbb{Z}/p\mathbb{Z}$.

Ejemplo 2.82 *Hallemos todos los campos intermedios de una extensión de Galois K/F tal que $\mathcal{G} = Gal(K/F) \cong \mathbb{Z}_{pq}$ con p, q primos distintos.*
Como $|\mathcal{G}| = pq$ y $(p, q) = 1$, del corolario 1.71 se sigue que existen subgrupos H y N de $\mathcal{G}$ que satisfacen:

$$|H| = p \text{ y } |N| = q.$$

Ya que $\mathbb{Z}_{pq}$ es cíclico de orden pq, usando la proposición 1.38 tenemos que H y N son los únicos subgrupos no triviales de $\mathcal{G}$.

Como la extensión K/F es de Galois, usando la correspondencia biyectiva del teorema 2.75 tenemos que H se corresponde con K^H y N con K^N.
Del inciso a) del teorema 2.75 obtenemos:

$$[K : K^H] = |H| = p \text{ y,}$$
$$[K : K^N] = |N| = q.$$

Por lo tanto, K^H y K^N son los únicos campos intermedios de K/F.

Ejemplo 2.83 *Sean p, q enteros primos distintos y K/F una extensión de Galois tal que $Gal(K/F) \cong \mathbb{Z}_{p^2q}$. Hallemos tres campos intermedios L_1, L_2 y L_3 de K/F que cumplan:*

$$[L_1 : F] = p^2, [L_2 : F] = p, [L_3 : F] = q. \tag{2.12}$$

Ya que q es un primo y divide a $|Gal(K/F)| = p^2q$, del corolario 1.71 se sigue que existe un subgrupo H_1 de $Gal(K/F)$ tal que $|H_1| = q$. Bajo la correspondencia biyectiva del teorema 2.75 se tiene que H_1 se corresponde con K^{H_1}.
Por otra parte, del inciso b) del teorema 2.75 y del teorema 1.34 se sigue que:

$$[K^{H_1} : F] = [Gal(K/F) : H_1] = \frac{p^2q}{q} = p^2.$$

De esta forma, se cumple la primera parte de la ecuación 2.12.
El corolario 1.71, nos permite garantizar subgrupos H_2 y H_3 de $Gal(K/F)$ tal que $|H_2| = p^2$ y $|H_3| = p$. Razonando con estos subgrupos así como lo hemos hecho previamente con H_1 podemos concluir que se satisface la ecuación 2.12.

La observación 2.25 y el ejemplo 2.24 inciso c) nos hacían pensar que toda extensión sobre $\mathbb{Q}$ es simple. Ahora estamos listos para probar esta conjetura de forma más general en el siguiente teorema.

Teorema 2.84 (Teorema del Elemento Primitivo) *Sea K/F una extensión finita. Entonces K/F es simple si y solo si K/F posee una cantidad finita de campos intermedios.*

Demostración. [14, teorema 5.6, pág. 55]. □

Corolario 2.85 *Si K/F es una extensión finita y separable, entonces $K = F(\alpha)$ para algún $\alpha \in K$.*

Demostración. [14, corolario 5.7, pág. 56]. □

Teorema 2.86 (Teorema Fundamental del Álgebra) *El campo $\mathbb{C}$ es algebraicamente cerrado.*

Demostración. [14, teorema 5.15 , pág. 59]. □

Ejemplo 2.87 *Si $F/\mathbb{Q}$ es una extensión finita de $\mathbb{Q}$ contenida en $\mathbb{C}$, entonces F no puede ser algebraicamente cerrado.*

Consideremos $\mathbb{A}$ la cerradura algebraica de $\mathbb{Q}$ en $\mathbb{C}$. Por la proposición 2.41 sabemos que $[\mathbb{A} : \mathbb{Q}] = \infty$. Por otro lado, ya que $F/\mathbb{Q}$ es finita, del corolario 1.175 se sigue que $F/\mathbb{Q}$ es algebraica. Ahora, de la proposición 2.39 se tiene que $F \subseteq \mathbb{A}$ y de hecho, $F \neq \mathbb{A}$. Luego, existe un elemento $\beta \in \mathbb{A} \setminus F$ y podemos tomar la siguiente cadena de campos: $\mathbb{Q} \subseteq F \subseteq F(\beta) \subseteq \mathbb{A}$. Notemos que β es algebraico sobre $\mathbb{Q}$ y por lo tanto, es algebraico sobre F. Del corolario 1.175 se sigue que $[F(\beta) : F] < \infty$. Por lo tanto $F(\beta)$ es una extensión finita de F que no es F. Luego, por el inciso b) de la proposición 2.33 concluimos que F no es un campo algebraicamente cerrado.

La médula espinal del desarrollo de la Teoría de Galois se basa en determinar las condiciones bajo las cuales las raíces de un polinomio pueden expresarse en términos de sus coeficientes usando operaciones elementales y radicales. A los polinomios cuyas raíces pueden expresarse de esta forma se les denomina **solubles por radicales**. El último aliento de Galois fue suficiente para dar respuesta a esta cuestión y determinar un criterio que relaciona campos con grupos en vista del desarrollo de la teoría.

Teorema 2.88 (Galois) *Sean F un campo de característica 0, $f(x) \in F[x] \setminus \{0\}$ y K un campo de descomposición para $f(x)$. Entonces $f(x)$ es soluble por radicales si y solo si $Gal(K/F)$ es un grupo soluble (vea definición 1.63).*

Demostración. La prueba de este hecho requiere algunos desarrollos y resultados previos, mismos que pueden ser consultados en [14, teorema 16.10, pág. 150]. □

Ejemplo 2.89 *Si F es un campo de característica cero y K/F es una extensión tal que $Gal(K/F)$ es abeliano, de la proposición 1.68 se sigue que el grupo $Gal(K/F)$ es soluble, por lo que, del teorema 2.88, todo polinomio $f(x) \in F[x]$ que tenga por campo de descomposición a K, es soluble por radicales.*

Ejemplo 2.90 *Si F es de característica cero y K/F es una extensión tal que el grupo $Gal(K/F)$ es de orden impar, del teorema 1.69 se sigue que $Gal(K/F)$ es un grupo soluble. Por lo tanto, todo polinomio no cero en $F[x]$ que tenga campo de descomposición K, es soluble por radicales en virtud del teorema 2.88.*

Ejemplo 2.91 *Si F es un campo de característica cero y $f(x) \in F[x] \setminus \{0\}$ es tal que $grad(f(x)) \leq 4$, entonces $f(x)$ es soluble por radicales. Esto ya que por el corolario 2.29 existe una extensión K de F tal que es campo de descomposición para $f(x)$ y $[K : F] \leq 4!$ y por la proposición 2.16 se sigue que $|Gal(K/F)| \leq$*

$4! = 24 < 60$. Así, de la proposición 1.65 se sigue que $Gal(K/F)$ es un grupo soluble. Ahora, por el teorema 2.88 concluimos que $f(x)$ es soluble por radicales. Es decir, que todo polinomio de grado menor o igual a 4 es soluble por radicales.

Sin embargo, para polinomios de grado mayor o igual a 5 se puede hallar un polinomio que no sea soluble por radicales como muestra el siguiente resultado.

Ejemplo 2.92 (Abel-Ruffini) *El polinomio $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ no es soluble por radicales. La teoría que se requiere para mostrar esto puede hallarse en [26, ejemplo 5.6, pág. 164]. Lo anterior es un caso particular de un hecho más general atribuido a Abel y Ruffini: Si $n \in \mathbb{Z}^+$ es tal que $n \geq 5$, entonces, el polinomio de grado n, $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ con coeficientes en un campo F en general no es soluble por radicales. Es decir, en general no puede hallarse una fórmula para determinar las raíces de un polinomio de grado mayor que o igual a 5. Una prueba de esta afirmación puede encontrarse en [19, teorema 4.27, pág. 216].*

Capítulo 3

Intermezzo

En el desarrollo de este capítulo abodaremos conceptos y resultados que desplegarán su fuerza en el capítulo 4. En la primera sección de este capítulo daremos una introducción a los grupos topológicos y sus principales propiedades. En la segunda sección se introducen los límites inversos y de igual forma propiedades básicas. Luego, en esta misma sección se introducen los grupos pro-$\mathcal{C}$ y de forma particular los grupos profinitos que tienen relación directa con los límites inversos y grupos topológicos y se estudian propiedades. Todos estos conceptos toman forma en el capítulo 4 para probar que el grupo de Galois, con la topología de Krull, es un grupo topológico y más aún, un grupo profinito Hausdorff, compacto y totalmente disconexo (vea corolario 4.22).

3.1. Grupos Topológicos

En esta sección desarrollamos elementos básicos de grupos topológicos. Los resultados que exponemos son extraídos principalmente de [25]. Todos los resultados que aquí se incluyen se demuestran a detalle.

El contenido de esta sección será usado tanto en la sección 3.3 como en el capítulo 4; en este último se construye la topología de Krull en el grupo de Galois de una extensión y se prueba que con esta topología dicho grupo resulta ser un grupo topológico Hausdorff, compacto y totalmente disconexo (vea corolario 4.22). Finalmente, todo lo desarrollado en esta sección nos permitirá establecer el teorema fundamental de Galois para extensiones infinitas 4.24.

Definición 3.1 *Un* ***grupo topológico*** *es una terna $(G, \cdot, \tau)$ tal que $(G, \cdot)$ es un grupo y (G, τ) es un espacio topológico, de tal forma que la siguiente función es continua:*

$$\begin{aligned} \zeta : G \times G &\longrightarrow G \,, \\ (x, y) &\longmapsto x \cdot y^{-1} \end{aligned}$$

Usando el hecho de que la composición de funciones continuas es nuevamente una función continua, podemos obtener una propiedad para la operación ζ en un grupo topológico, misma que nos ayudará a obtener una sencilla caracterización de los grupos topológicos.

Lema 3.2 *Sea $(G, \cdot, \tau)$ un grupo topológico. Si consideramos las siguientes dos funciones:*

$$\begin{aligned} \star : G \times G &\longrightarrow G \qquad y \qquad (\_)^{-1} : G \longrightarrow G \\ \star(x, y) &\longmapsto x \cdot y \qquad\qquad x \longmapsto x^{-1} \,, \end{aligned}$$

entonces $\star$ es continua y suprayectiva. Además, la función $(\_)^{-1}$ es un homeomorfismo.
Por otro lado, si $(G, \cdot)$ es un grupo y (G, τ) es un espacio topológico de tal forma que $\star$ es continua y $(\_)^{-1}$ es un homeomorfismo, entonces $(G, \cdot, \tau)$ es un grupo topológico.

Demostración. Se deja como ejercicio al lector. □

En caso de no haber confusiones, cuando $(G, \cdot, \tau)$ sea un grupo topológico, lo abreviaremos simplemente por G; además la operación $\cdot$ en G se abreviará simplemente por $x \cdot y = xy$.

Ejemplo 3.3

a) Un grupo G dotado con la topología discreta es un grupo topológico.

b) Sea $(V, \|\cdot\|)$ un espacio vectorial normado. Entonces $(V, +)$ es un grupo topológico con la topología inducida por la norma $\|\cdot\|$.

c) $(\mathbb{R}, +)$ con la topología inducida por la métrica euclideana es un grupo topológico.

d) Un caso particular del inciso b) es que $(\mathbb{R}^n, \|\cdot\|)$ es un grupo topológico, donde $\|\cdot\|$ es la norma euclideana.

Como un caso general de los anteriores dos incisos, en la proposición 3.20 probaremos que la propiedad de grupo topológico se preserva bajo el producto topológico.

Cuando un conjunto posee una topología, es natural preguntarse sobre la naturaleza de los subconjuntos que son abiertos, y por lo tanto de los subconjuntos cerrados; así mismo, nos preguntamos sobre las propiedades internas del espacio que le proporcionan estructura. El siguiente resultado nos proporciona información sobre los grupos topológicos.

Definición 3.4 *Sean G un grupo topológico y H un subconjunto de G. Se dice que H es un* ***subgrupo abierto*** *de G si H es un subgrupo de G y es un subconjunto abierto de G.*

Si H es un subgrupo de un grupo topológico G, entonces H es un espacio topológico con la topología de subespacio inducida por G, esto debido a que la operación $\zeta|_H : H \times H \longrightarrow H$ está bien definida al ser H un subgrupo de G, además, dicha función es continua ya que es la restricción de la función continua ζ. De esta forma, hemos probado la siguiente proposición.

Proposición 3.5 *Sean G un grupo topológico y $H \leq G$. Entonces H es un grupo topológico con la topología de subgrupo inducida por G.*

A continuación, enlistamos algunas propiedades básicas sobre grupos topológicos que usaremos en un futuro, no sin antes considerar la siguiente definición.

Definición 3.6 *Sean G un grupo y H, K subconjuntos no vacíos de G. Se definen los siguientes subconjuntos de G :*

$$HK = \{h \cdot k : h \in H \text{ y } k \in K\},$$
$$H^{-1} = \left\{h^{-1} : h \in H\right\}.$$

En el caso en que $K = \{g\}$ para algún $g \in G$, el conjunto $H \cdot \{g\}$ será abreviado como Hg. De igual forma, $\{g\} \cdot H$ será abreviado como gH.

Observación 3.7 *Si G es un grupo y H, K son subconjuntos no vacíos de G, entonces $(HK)^{-1} = K^{-1}H^{-1}$. Además, si $H \subseteq K$, se sigue que $H^{-1} \subseteq K^{-1}$.*

Proposición 3.8 *Para un grupo topológico G se verifican las siguientes propiedades:*

a) Para todo $g \in G$ las siguientes dos funciones son homeomorfismos:

$$\upsilon_g : G \longrightarrow G, \quad x \longmapsto xg \qquad \text{y} \qquad {}_g\upsilon : G \longrightarrow G, \quad x \longmapsto gx.$$

b) Si H es un subconjunto abierto (respectivamente cerrado) de G, se tiene que, para todo $g \in G$, los conjuntos gH y Hg son subconjuntos abiertos de G (resp. subconjuntos cerrados de G).

c) Todo subgrupo abierto de G es cerrado. Además, si H es un subgrupo cerrado de G tal que $[G : H] < \infty$, entonces H es un subgrupo abierto de G.

d) Si G es compacto, todo subgrupo abierto de G tiene índice finito en G.

e) Si H es un subgrupo de G y U es un subconjunto abierto no vacío de G tal que $U \subseteq H$, entonces H es un subgrupo abierto de G.

Demostración.

a) Sea $g \in G$ un elemento arbitrario. Consideremos la función constante $\lambda_{g^{-1}} : G \longrightarrow G$ dada por $x \longmapsto g^{-1}$ y el siguiente diagrama:

$$\begin{array}{ccccc} G & \xrightarrow{(id_G, \lambda_{g^{-1}})} & G \times G & \xrightarrow{\zeta} & G \\ & \searrow^{\upsilon_g} & & \nearrow & \\ x & \longmapsto & (x, g^{-1}) & \longmapsto & xg \end{array}$$

donde $\upsilon_g = \zeta \circ (id_G, g^{-1})$ es una función continua al ser composición de funciones continuas.

Por otra parte, consideremos la función constante $\lambda_g : G \longrightarrow G$ dada por $x \longmapsto g$ y la función ϑ expuesta en el siguiente diagrama:

$$\begin{array}{ccccccc} & & \overset{\vartheta}{\frown} & & & & \\ G & & \xrightarrow{(id_G, \lambda_g)} & G \times G & \xrightarrow{\zeta} & G & \\ x & & \longmapsto & (x, g) & \longmapsto & xg^{-1} & \end{array}$$

donde $\vartheta = \zeta \circ (id_G, g))$ es una función continua, ya que es la composición de funciones continuas. Ahora, observemos que:

$$\begin{aligned} (\vartheta \circ \upsilon_g)(x) = \vartheta(\upsilon_g(x)) = \vartheta(xg) = (xg)g^{-1} = x, \\ \text{y } (\upsilon_g \circ \vartheta)(x) = \upsilon_g(\vartheta(x)) = \upsilon_g(xg^{-1}) = (xg^{-1})g = x. \end{aligned}$$

Concluimos que $\vartheta = \upsilon_g^{-1}$, por lo que υ_g es un homeomorfismo al poseer inversa continua.

De forma similar, el lector puede probar que ${}_g\upsilon$ es un homeomorfismo.

b) Por el inciso a) de la proposición 3.8, sabemos que las funciones υ_g y ${}_g\upsilon$ son homeomorfismos para cada $g \in G$. Por otro lado, por la proposición A.41, son morfismos abiertos.
Al ser H un abierto de G, se sigue que $\upsilon_g(H) = Hg$ y ${}_g\upsilon(H) = gH$ son subconjuntos abiertos en G.
De forma similar se puede concluir que, si H es un cerrado de G, se tiene que gH y Hg son cerrados de G.

c) Sea H un subgrupo abierto de G. Probaremos que el complemento de H en G es abierto.
Como H induce una partición del grupo G, según se ha visto en la observación 1.33, tenemos que $G = \bigcup_{g\in G} gH$ y por lo tanto:

$$G \setminus H = \bigcup_{g\in G\setminus H} gH. \tag{3.1}$$

Esta igualdad se verifica debido a que, si tomamos $\alpha \in G \setminus H$, y dado que $H \leq G$, entonces $e \in H$, además $\alpha = \alpha \cdot e \in \alpha H \subseteq \bigcup_{g\in G\setminus H} gH$.
Por otro lado, si $\alpha \in gH$ para algún $g \in G \setminus H$, entonces $\alpha = g \cdot h \in G$ para un $h \in H$, por lo que $\alpha h^{-1} = g \in G \setminus H$. Observe que si $\alpha \in H$, se sigue $\alpha h^{-1} \in H$, y así $g \in H$, lo cual es una contradicción. Por lo tanto, $\alpha \notin H$ y de esta forma se tiene $\alpha \in G \setminus H$.

En el inciso b) de la proposición 3.8 se ha probado que cada clase gH es abierta si H es un subgrupo abierto. De la ecuación 3.1 se sigue que $G \setminus H$ es abierto, pues es unión de abiertos. Concluimos así que H es un subgrupo cerrado de G.

Continuamos con la segunda parte de nuestro enunciado.

Tomemos H un subgrupo cerrado de G tal que $[G : H] < \infty$, esto implica que existen $\{g_1 = e, ..., g_n\} \subseteq G$ tales que:

$$G = \bigcup_{i=1}^{n} g_i H.$$

Por lo tanto, el complemento de H en G puede ser escrito como:

$$G \setminus H = \bigcup_{i=2}^{n} g_i H. \tag{3.2}$$

Por el inciso b) de la proposición 3.8, se tiene que la ecuación 3.2 es una unión finita de cerrados, obteniendo que $G \setminus H$ es cerrado y por lo tanto H es abierto.

d) Sea H un subgrupo abierto de G. De la observación 1.33, se sigue que H induce una partición de G de la siguiente forma:

$$G = \bigcup_{g\in G} gH. \tag{3.3}$$

Del inciso b) de la proposición 3.8, tenemos que cada clase lateral izquierda de H es abierta, por lo tanto, en la ecuación 3.3 tenemos una cubierta

abierta de G. Como G es un espacio topológico compacto, existe $\{g_1 = e, ..., g_n\} \subseteq G$ de tal forma que:

$$G = \bigcup_{i=1}^{n} g_i H.$$

Es decir, $[G : H] < \infty$.

e) Ya que U es un subconjunto abierto no vacío de G tal que $U \subseteq H$, entonces:

$$H = \bigcup_{h \in H} hU. \tag{3.4}$$

Esta igualdad se verifica debido a que por hipótesis $U \subseteq H$, por lo que, como H es cerrado bajo producto, se sigue que $hU \subseteq hH \subseteq H$, para cada $h \in H$. De esta forma, tenemos que $\bigcup_{h \in H} hU \subseteq H$.
Por otro lado, consideremos $h \in H$. Como $U \neq \emptyset$, entonces existe $\alpha \in U$. Ahora, ya que H es subgrupo, es cerrado bajo inversos y productos, por lo que $h\alpha^{-1} \in H$. De este modo, tenemos que:

$$h = (h\alpha^{-1})\alpha \in h\alpha^{-1}U \subseteq \bigcup_{h \in H} hU.$$

Por lo tanto, queda probada la igualdad de la ecuación 3.4.
Ahora, del inciso b) de la proposición 3.8 y de la ecuación 3.4, se sigue que H es la unión de clases abiertas. Por lo tanto, H es abierto de G.

□

Observación 3.9 *Notemos que para la prueba del inciso c) de la proposición 3.8, es necesaria la condición de que H sea un subgrupo de G y no se puede pedir solamente que H sea un subconjunto abierto de G.*

Proposición 3.10 *Sean G un grupo topológico y $H \leq G$. Entonces $\overline{H}$ es un subgrupo de G. Además, si $H \trianglelefteq G$, entonces $\overline{H} \trianglelefteq G$.*

Demostración. Primero demostraremos que $\overline{H}$ es un subgrupo de G. Para ello notemos que, como H es un subgrupo de G, se tiene que es cerrado bajo producto. De la definición de cerradura en un espacio topológico (vea definición A.11) se sigue que $HH \subseteq H \subseteq \overline{H}$. Así, para cada $h \in H$, se tiene que $hH \subseteq \overline{H}$, luego, $H \subseteq h^{-1}\overline{H}$. Ahora, del inciso b) de la proposición 3.8, tenemos que $h^{-1}\overline{H}$ es un cerrado en G. Al aplicar el operador cerradura a esta contención, obtenemos que $\overline{H} \subseteq h^{-1}\overline{H}$ y por lo tanto $h\overline{H} \subseteq \overline{H}$, es decir, $H\overline{H} \subseteq \overline{H}$.
Ahora sea $x_0 \in \overline{H}$. De la contención que hemos probado previamente, se sigue

que $Hx_0 \subseteq \overline{H}$, por lo tanto $H \subseteq \overline{H}x_0^{-1}$. Observemos que el conjunto de la derecha es un cerrado, por lo que, al aplicar el operador cerradura a esta contención, se obtiene que $\overline{H} \subseteq \overline{H}x_0^{-1}$. De esta forma llegamos a que $\overline{H}x_0 \subseteq \overline{H}$. Ya que x_0 fue un elemento arbitrario en $\overline{H}$, concluimos que $\overline{H} \cdot \overline{H} \subseteq \overline{H}$, esto es, $\overline{H}$ es cerrado bajo producto.
Probaremos que $\overline{H}$ es cerrado bajo inversos probando que $\overline{H}^{-1} = \overline{H}$. Ya que H es subgrupo de G, se tiene que H es cerrado bajo inversos, esto es $H^{-1} = H$. Ahora, como $H \subseteq \overline{H}$, de la observación 3.7, se sigue que al aplicar inversos a la última contención obtenemos $H = H^{-1} \subseteq \overline{H}^{-1}$. Como la función tomar inversos (vea lema 3.2) es un homeomorfismo, se sigue que $\overline{H}^{-1}$ es un cerrado de G. Por lo tanto, al aplicar cerraduras, se tiene $\overline{H} \subseteq \overline{H}^{-1}$. De esta última ecuación, al tomar inversos nuevamente, se sigue que $\overline{H}^{-1} \subseteq \overline{H}$. Concluimos que $\overline{H} = \overline{H}^{-1}$, es decir, $\overline{H}$ es cerrado bajo inversos.

Para la última parte, si $H \trianglelefteq G$, entonces, para todo $g \in G$, se tiene que $gHg^{-1} = H \subseteq \overline{H}$. Por lo tanto, $H \subseteq g^{-1}\overline{H}g$, además, el conjunto de la derecha es un cerrado en virtud del inciso b) de la proposición 3.8.
Así, al aplicar cerradura a ambos lados de la contención obtenemos que, para todo $g \in G$, $\overline{H} \subseteq g^{-1}\overline{H}g$. Esto implica que $g\overline{H}g^{-1} \subseteq \overline{H}$. Finalmente, de la proposición 1.47, se sigue que $\overline{H} \trianglelefteq G$. □

Proposición 3.11 *Sea G un grupo topológico. La topología en G coincide con la topología discreta si y solo si $\{e\}$ es un subgrupo abierto de G, donde e es la identidad de G.*

Demostración. Si suponemos que G es un espacio discreto, entonces todo subconjunto unitario es abierto, en particular, el subgrupo $\{e\}$ es abierto.
Por otro lado, supongamos que $\{e\}$ es un subgrupo abierto de G. Tomemos $g \in G$ un elemento arbitrario. Del inciso b) de la proposición 3.8, se sigue que $g \cdot \{e\} = \{g\}$ es abierto. El resultado se sigue del hecho de que todo abierto en G es unión de los conjuntos unitarios de sus elementos, que hemos probado son abiertos de G. □

Observación 3.12 *Si A, B son conjuntos, $U \subseteq B$ y $f : A \longrightarrow B$ es una función, entonces se satisface que:*

$$f(f^{-1}(U)) \subseteq U. \tag{3.5}$$

Consideremos ahora la función $\star$ del lema 3.2 y sea $U \subseteq G$ un abierto. Por ser $\star$ continua entonces $\star^{-1}(U) \subseteq G \times G$ es abierto en $G \times G$, considerado con la topología producto (vea definición A.51). Por lo tanto, existen $V, W \subseteq G$ abiertos tales que $\star^{-1}(U) = V \times W$. Ahora, de la ecuación 3.5, se sigue que:

$$\star(\star^{-1}(U)) = \star(V \times W) = VW \subseteq U. \tag{3.6}$$

Además, VW es abierto ya que:

$$VW = \bigcup_{v \in V} vW.$$

Y por el inciso b) de la proposición 3.8, tenemos que $vW \subseteq G$ es abierto de G. Así, VW es abierto de G al ser la unión de clases izquierdas abiertas. De la misma forma puede probarse que si $U_1, ..., U_n \subseteq G$ son abiertos entonces $U_1 \cdots U_n$ es abierto en G.
Un razonamiento similar puede aplicarse usando la función ζ de la definición 3.1 para probar que, si U es un abierto de G, entonces existen V y W abiertos de G tal que VW^{-1} es abierto de G y $VW^{-1} \subseteq U$.

Proposición 3.13 *a) Sean G un grupo topológico y $H \trianglelefteq G$. Entonces el grupo cociente G/H es un grupo topológico con la topología cociente. Además, la función $\pi : G \longrightarrow G/H$ definida como $g \longmapsto gH$, es abierta.*

b) Si G es un grupo topológico Hausdorff y compacto y H, K son subgrupos cerrados de G, entonces HK es un subconjunto cerrado de G.

c) Sean G un grupo topológico compacto, Y un subconjunto cerrado de G y $\{X_i\}_{i \in I}$ una familia de cerrados de G que satisface la siguiente propiedad:

$$\text{Para cualesquiera } \alpha, \beta \in I \text{ existe } \lambda \in I \text{ tal que } X_\lambda \subseteq X_\alpha \cap X_\beta. \quad (3.7)$$

Entonces, se satisface que:

$$\left(\bigcap_{i \in I} X_i \right) Y = \bigcap_{i \in I} X_i Y. \quad (3.8)$$

d) G es Hausdorff si y solo si $\{e\}$ es un cerrado de G. Más aún, si G es totalmente disconexo, entonces G es Hausdorff. Se sigue que si $H \trianglelefteq G$, entonces G/H es Hausdorff si y solo si H es cerrado en G.

Demostración.

a) Primero veremos que la función $\pi : G \longrightarrow G/H$ es abierta.
Sea U abierto de G, probaremos que $\pi(U)$ es abierto en G/H.
Por la definición de topología cociente (vea definición A.42), basta ver que $\pi^{-1}(\pi(U))$ es abierto en G.

Afirmamos que:

$$\pi^{-1}(\pi(U)) = UH. \quad (3.9)$$

En efecto, si $x \in UH$, entonces $x = uh$ con $u \in U$ y $h \in H$. Al aplicar el morfismo π se tiene que, $\pi(x) = xH = uhH = uH \in \{uH : u \in U\} = \pi(U)$. Por lo tanto, $x \in \pi^{-1}(\pi(U))$.

Por otro lado, tomemos $z \in \pi^{-1}(\pi(U))$. Esto implica que $\pi(z) \in \pi(U)$, es decir, $zH = u'H$ para algún $u' \in U$. De la proposición 1.26, se tiene que $(u')^{-1}z = h \in H$. Por lo tanto, $z = u'h \in UH$.

Concluimos la igualdad en la ecuación 3.9.

Finalmente, notemos que $UH = \bigcup_{h \in H} Uh$. Del inciso b) de la proposición 3.8, se sigue que, para todo $h \in H$, Uh es abierto en G, por lo que UH es abierto en G. Concluimos que $\pi(U)$ es abierto en virtud de la definición A.42. De esta forma, el morfismo π es abierto.

Ya que el cociente G/H es un espacio topológico con la topología cociente, para probar que es un grupo topológico basta probar que la siguiente función es continua:

$$\Lambda : G/H \times G/H \longrightarrow G/H \ ,$$
$$(gH, g'H) \longmapsto g(g')^{-1}H \ .$$

Sea U un subconjunto abierto de G/H. Probaremos que $\Lambda^{-1}(U)$ es un abierto de $G/H \times G/H$, lo haremos probando que es vecindad para cada uno de sus puntos. Sea $(gH, kH) \in \Lambda^{-1}(U)$, al aplicar Λ se obtiene $gk^{-1}H \in U$, por lo que $gk^{-1} \in \pi^{-1}(U)$, que es un subconjunto abierto de G ya que π es continua. Por lo tanto, $(g, k) \in \zeta^{-1}(\pi^{-1}(U))$, donde ζ es la función de la definición 3.1; y al ser este último un conjunto abierto ya que ζ es una función continua, se sigue de la proposición A.7, que existen W_1, W_2 abiertos de G tales que $(g, k) \in W_1 \times W_2 \subseteq \zeta^{-1}(\pi^{-1}(U))$. Al aplicar ζ y de la observación 3.12, obtenemos:

$$gk^{-1} \in W_1 \cdot W_2^{-1} \subseteq \zeta(\zeta^{-1}(\pi^{-1}(U))) \subseteq \pi^{-1}(U).$$

Por lo tanto,

$$\pi(W_1 \cdot W_2^{-1}) \subseteq U. \tag{3.10}$$

Por otro lado, ya que W_1, W_2 son abiertos en G y π es abierta, de la definición de topología producto (vea definición A.51), se tiene que $\pi(W_1) \times \pi(W_2)$ es abierto de $G/H \times G/H$. Además, se afirma que:

$$(gH, kH) \in \pi(W_1) \times \pi(W_2) \subseteq \Lambda^{-1}(U). \tag{3.11}$$

La contención en la ecuación 3.11 se verifica en virtud de que, si tomamos $(\alpha H, \beta H) \in \pi(W_1) \times \pi(W_2)$ con $\alpha \in W_1$ y $\beta \in W_2$, al aplicarles el morfismo Λ y usando la ecuación 3.10, se sigue:

$$\alpha\beta^{-1}H \in \pi\left(W_1 \cdot W_2^{-1}\right) \subseteq U.$$

Finalmente, de la ecuación 3.11, se concluye que $\Lambda^{-1}(U)$ es vecindad para cada uno de sus puntos, y de la proposición A.7, se tiene que $\Lambda^{-1}(U)$ es un abierto de $G/H \times G/H$. Así, se obtiene que Λ es continua.

b) Ya que G es un grupo topológico compacto y H y K son subgrupos cerrados de G, de la proposición A.59 obtenemos que H y K son compactos de G. De la proposición A.62, se sigue que $H \times K$ es compacto y cerrado en $G \times G$. Ahora, por el lema 3.2, tenemos que la función $\star$ es continua, por lo que, de acuerdo al inciso e) de la proposición A.39, se tiene que $\star|_{H\times K}$ es continua y de la proposición A.63 se sigue que $\star(H, K) = HK$ es compacto en G. Finalmente, como G es un espacio Hausdorff, de la proposición A.61 se sigue que HK es cerrado de G.

c) Primero observemos que, si $\{X_i\}_{i\in I}$ es una familia de cerrados en G que cumplen la propiedad de la ecuación 3.7, entonces también se cumple que para cualquier cantidad finita de elementos $\alpha_1, ..., \alpha_n \in I$, existe $\lambda \in I$ tal que:

$$X_\lambda \subseteq \bigcap_{i=1}^{n} X_{\alpha_i}. \tag{3.12}$$

Notemos que para todo $i \in I$ se tiene que $\bigcap_{i\in I} X_i \subseteq X_i$. De esta forma, para todo $i \in I$ se verifica la siguiente ecuación:

$$\left(\bigcap_{i\in I} X_i\right) Y \subseteq X_i Y. \tag{3.13}$$

Por lo tanto, de la ecuación 3.13 concluimos una de las contenciones que deseamos:

$$\left(\bigcap_{i\in I} X_i\right) Y \subseteq \bigcap_{i\in I} X_i Y \tag{3.14}$$

Para demostrar la otra contención en la ecuación 3.8, supongamos que existe un elemento $g \in G$ tal que:

$$g \in \bigcap_{i\in I} X_i Y \setminus \left(\bigcap_{i\in I} X_i\right) Y. \tag{3.15}$$

Ahora, si $h \in gY^{-1} \cap \left(\bigcap_{i\in I} X_i\right)$, obtenemos que $h = gy^{-1}$ para algún $y \in Y$ y $h \in X_i$ para todo $i \in I$. Al multiplicar a la derecha por y se

sigue que $g = hy \in \left(\bigcap_{i\in I} X_i\right) Y$, esto contradice a nuestra hipótesis de la ecuación 3.15. Concluimos que:

$$gY^{-1} \cap \left(\bigcap_{i\in I} X_i\right) = \bigcap_{i\in I} \left(gY^{-1} \cap X_i\right) = \emptyset. \tag{3.16}$$

Observemos que, como Y es cerrado y la función $(\_)^{-1}$ del lema 3.2 es un homeomorfismo, se tiene que Y^{-1} es un cerrado. Además, por el inciso b) de la proposición 3.8, se sigue que gY^{-1} es cerrado; mientras que por hipótesis tenemos que $\{X_i\}_{i\in I}$ son cerrados.
Consideremos la familia de cerrados $\mathcal{A} = \left\{gY^{-1} \cap X_i\right\}_{i\in I}$. Notemos que no posee la propiedad de la intersección finita (vea definición A.57), pues en caso contrario, ya que G es compacto, se tendría que la familia $\mathcal{A}$ tiene intersección no vacía. Esto es, $\bigcap_{i\in I} \left(gY^{-1} \cap X_i\right) \neq \emptyset$, contradiciendo a la ecuación 3.16.
Del hecho de que $\mathcal{A}$ no posee la propiedad de la intersección finita, se sigue que existe $J \subseteq I$ tal que $|J| < \infty$ y que satisface:

$$gY^{-1} \cap \left(\bigcap_{i\in J} X_i\right) = \emptyset.$$

Por la observación hecha al inicio de esta prueba (vea ecuación 3.12), existe $\lambda \in I$ tal que:

$$X_\lambda \subseteq \bigcap_{i\in J} X_i. \tag{3.17}$$

Al intersecar cada miembro de la ecuación 3.17 con el cerrado gY^{-1}, obtenemos:

$$X_\lambda \cap gY^{-1} \subseteq \bigcap_{i\in J} X_i \cap gY^{-1} = \emptyset,$$

Es decir:

$$X_\lambda \cap gY^{-1} = \emptyset. \tag{3.18}$$

De la ecuación 3.18 se sigue que $g \notin X_\lambda Y$, contradiciendo a la hipótesis de la ecuación 3.15. Pues en caso contrario, si $g \in X_\lambda Y$, entonces $g = hy$ con $h \in X_\lambda$ y $y \in Y$, y así $gy^{-1} = h \in X_\lambda \cap gY^{-1}$, contradiciendo a la ecuación 3.18. Para evitar contradicciones, el elemento $g \in G$ que satisface la ecuación 3.15 no existe. Por lo tanto, queda probada la siguiente contención:

$$\bigcap_{i\in I} X_i Y \subseteq \left(\bigcap_{i\in I} X_i\right) Y. \tag{3.19}$$

De las ecuaciones 3.19 y 3.14, se concluye la igualdad de la ecuación 3.8.

d) Notemos que si G es Hausdorff, de la proposición A.32 se sigue que todo conjunto unitario de G es cerrado, en particular $\{e\}$ es cerrado de G.

Por otra parte, supongamos que $\{e\}$ es cerrado en G. Como la función ζ es continua (vea definición 3.1), de la proposición A.37 se tiene que $\zeta^{-1}(\{e\}) \subseteq G \times G$ es cerrado.

Se afirma que $\zeta^{-1}(\{e\}) = \triangle_X$. Notemos que si $(x,x) \in \triangle_X$, se tiene que $\zeta((x,x)) = x \cdot x^{-1} = e$. Por lo que $\triangle_X \subseteq \zeta^{-1}(\{e\})$.
Por otra parte, si $(x,y) \in \zeta^{-1}(\{e\})$, entonces se tiene que $x \cdot y^{-1} = e$. De este modo, se sigue que $x = y$. Concluimos que $\zeta^{-1}(\{e\}) \subseteq \triangle_X$. Por lo tanto, se verifica la igualdad deseada.

Hemos probado que $\triangle_X$ es cerrado, por lo que, a partir de la proposición A.33, se sigue que G es Hausdorff.

Ahora probemos las demás afirmaciones que se enuncian en este inciso.

Si G es un grupo topológico totalmente disconexo, de la proposición A.81 se sigue que, para todo $x \in G$, la componente conexa $\mathcal{C}(x) = \{x\}$ es un cerrado de G. En particular se concluye que $\{e\}$ es un cerrado de G, y del inciso d) de la proposición 3.13, se tiene que G es Hausdorff.

Hemos probado que si $H \trianglelefteq G$ entonces G/H es un grupo topológico con neutro H (vea proposición 3.13). Por lo tanto, G/H será Hausdorff si y solo si H es un subgrupo normal cerrado en G, en virtud a la primera parte del inciso d) de la proposición 3.13.

□

Proposición 3.14 *Sean G un grupo topológico compacto y $H \trianglelefteq G$. Entonces G/H es un grupo topológico compacto con la topología cociente.*

Demostración. Primero notemos que, por el inciso a) de la proposición 3.13, se tiene que G/H es un grupo topológico con la topología cociente y que la función $\pi : G \longrightarrow G/H$ es abierta. Además, ya que π es suprayectiva, entonces para todo $Y \subseteq G/H$, se tiene $\pi(\pi^{-1}(Y)) = Y$.
Para probar la compacidad de G/H, tomemos $\{V_i\}_{i\in I}$ una familia de abiertos de G/H tal que $G/H = \bigcup_{i\in I} V_i$. Afirmamos que se verifica la siguiente ecuación:

$$\bigcup_{i\in I} \pi^{-1}(V_i) = G \tag{3.20}$$

Notemos que si $x \in G$, se tiene que $\pi(x) = xH \in G/H$. De modo que existe $j \in I$ tal que $xH \in V_j$, y de esta forma llegamos a que $x \in \pi^{-1}(V_j)$. Así, se

concluye que $G \subseteq \bigcup_{i\in I} \pi^{-1}(V_i)$.
La otra contención de la ecuación 3.20 es clara, pues es una unión de subconjuntos de G.
Como G es compacto y se satisface la ecuación 3.20, se sigue que existe $J \subseteq I$ tal que $|J| < \infty$ y $G = \bigcup_{i\in J} \pi^{-1}(V_i)$. Afirmamos que:

$$G/H = \bigcup_{i\in J} V_i. \tag{3.21}$$

Para probar la ecuación 3.21, consideremos $xH \in G/H$ un elemento cualquiera, entonces existe $j \in J$ tal que $x \in \pi^{-1}(V_j)$ es decir, $xH \in V_j$. La contención $\bigcup_{i\in J} V_i \subseteq G/H$ es clara, pues es una unión de subconjuntos de G/H. Concluimos que se satisface la ecuación 3.21, y por lo tanto G/H es compacto. □

Lema 3.15 *Sean G un grupo topológico y $T \subseteq G$ tal que $T = T^{-1}$ y $e \in T$. Entonces se satisface que:*

$$\langle T\rangle = \bigcup_{i=1}^{\infty} T^i. \tag{3.22}$$

Más aún, si T es un abierto de G, entonces $\langle T\rangle$ es un subgrupo abierto de G.

Demostración. Para probar la ecuación 3.22, consideremos $\alpha \in \langle T\rangle$. De la definición de subgrupo generado por un subconjunto (vea definición 1.11), se sigue que:

$$\alpha = t_1^{e_1} \cdots t_n^{e_n}, \text{ donde para todo } i, e_i \in \{1, -1\}, t_i \in T \text{ y } n \in \mathbb{Z}^+.$$

Ya que $T = T^{-1}$, entonces para todo $i \in \{1, ..., n\}$, se tiene que $t_i^{e_i} \in T$ y por lo tanto $\alpha \in T^n \subseteq \bigcup_{i=1}^{\infty} T^i$. De esta forma obtenemos que $\langle T\rangle \subseteq \bigcup_{i=1}^{\infty} T_i$.
La otra contención de la ecuación 3.22 se concluye a partir de la definición 1.11 y del desarrollo del lado derecho de la igualdad, se deja de ejercicio al lector.
Para probar que $\langle T\rangle$ es abierto, supongamos que T es abierto. Por el inciso b) de la proposición 3.8, se tiene que, para todo $y \in T$, yT es un abierto de G. Entonces:

$$T^2 = TT = \bigcup_{y\in T} yT. \tag{3.23}$$

Y así, T^2 es abierto.
Si T^{n-1} es abierto, de forma similar a como se hizo en la ecuación 3.23, puede probarse que T^n es abierto.
Al ser $\langle T\rangle$ la unión de conjuntos abiertos, se tiene que $\langle T\rangle$ es abierto en G. □

Proposición 3.16 *Sean G un grupo topológico compacto y $C \subseteq G$ un abierto y cerrado de G tal que $e \in C$. Entonces C contiene un subgrupo normal abierto de G.*

Demostración. Como C es un abierto de G, definimos, para cada $x \in C$, el conjunto $W_x = Cx^{-1}$. Por el inciso b) de la proposición 3.8, se tiene que, para todo $x \in C$, W_x es un abierto y $e \in W_x$. Además, si $\alpha = cx^{-1} \in W_x$, entonces $\alpha x \in C$. Por lo tanto:

$$W_x x \subseteq C. \tag{3.24}$$

Además, C contiene a la unión de cualquier familia de conjuntos de la forma $W_x x$ para todo $x \in C$.
Como la función $\star$ (vea lema 3.2) es continua y para todo $x \in C, W_x$ es un abierto de G, existen $V_x, U_x \subseteq G$ abiertos tales que $\star^{-1}(W_x) = V_x \times U_x$ y contienen al neutro de G. Ahora, por la observación 3.12, se sigue que:

$$V_x U_x \subseteq W_x.$$

Para cada $x \in C$ consideremos $S_x = V_x \cap U_x$. Notemos que $S_x \subseteq W_x$ y que S_x es un abierto de G tal que $e \in S_x$. Por lo tanto, $S_x x$ es un abierto que contiene a x y está contenida en $W_x x$. También observemos que se satisfacen los siguientes hechos:

$$S_x S_x = (V_x \cap U_x) \cdot (V_x \cap U_x) \subseteq V_x U_x \subseteq W_x \tag{3.25}$$

$$C \subseteq \bigcup_{x \in C} S_x x. \tag{3.26}$$

Por otro lado, ya que G es compacto y C es cerrado en G , de la proposición A.59 obtenemos que C es un subespacio compacto de G. Ahora, de la proposición A.60 y de la ecuación 3.26, se sigue que existen $n \in \mathbb{Z}^+$ y $\{x_1, ..., x_n\} \subseteq C$ tales que:

$$C \subseteq \bigcup_{i=1}^{n} S_{x_i} x_i.$$

Consideremos el siguiente conjunto abierto de G, $\mathcal{F} = \bigcap_{i=1}^{n} S_{x_i}$. Es claro que $e \in \mathcal{F}$ y, para todo $i \in \{1, ..., n\}$, se satisface que $\mathcal{F} \subseteq S_{x_i}$. De la ecuación 3.25 se obtiene:

$$\mathcal{F} S_{x_i} \subseteq S_{x_i} S_{x_i} \subseteq W_{x_i}. \tag{3.27}$$

Esto implica que $\mathcal{F}S_{x_i}x_i \subseteq W_{x_i}x_i$.
A partir de las ecuaciones 3.27 y 3.24 tenemos:

$$\mathcal{F}C \subseteq \bigcup_{i=1}^{n} \mathcal{F}S_{x_i}x_i \subseteq \bigcup_{i=1}^{n} W_{x_i}x_i \subseteq C. \tag{3.28}$$

Ya que C contiene al neutro de G, de la ecuación 3.28 se deduce que:

$$\mathcal{F} = \mathcal{F} \cdot \{e\} \subseteq \mathcal{F} \cdot C \subseteq C. \tag{3.29}$$

Por lo tanto, $\mathcal{F} \subseteq C$. De igual forma, ya que la función $(\_)^{-1}$ del lema 3.2 es un homeomorfismo, se tiene que $\mathcal{F}^{-1}$ es un abierto de G y $e \in \mathcal{F}^{-1}$.
Tomemos el abierto $T = \mathcal{F} \cap \mathcal{F}^{-1}$. Observemos que $e \in T$ y $T = T^{-1}$, esto último se satisface debido a que:

$$\begin{aligned} T^{-1} &= \left\{t^{-1} \in G : t \in T\right\} \\ &= \left\{t^{-1} \in G : t \in \mathcal{F} \cap \mathcal{F}^{-1}\right\} \\ &= \left\{t^{-1} \in G : t \in \mathcal{F}\right\} \cap \left\{t^{-1} \in G : t \in \mathcal{F}^{-1}\right\} \\ &= \mathcal{F}^{-1} \cap \mathcal{F} \\ &= T. \end{aligned}$$

Sea $H = \bigcup_{n=1}^{\infty} T^n$. Por el lema 3.15, se sigue que H es un subgrupo abierto de G y contiene al neutro de G.
Notemos que $T \subseteq \mathcal{F} \subseteq C$. A partir de este hecho y de la ecuación 3.29, se sigue que, si $T^n \subseteq C$, entonces:

$$T^{n+1} = T \cdot T^n \subseteq \mathcal{F} \cdot C \subseteq C.$$

De esta forma, concluimos que:

$$H \subseteq C. \tag{3.30}$$

Como G es compacto y H es abierto, del inciso d) proposición 3.8, se sigue que H tiene índice finito sobre G, esto significa que existen $g_1 = e, g_2, ..., g_m \in G$ de tal forma que $G = \bigcup_{i=1}^{m} g_i H$.
Sea $\mathcal{H} = \bigcap_{i=1}^{m} g_i H g_i^{-1}$. Notemos que $\mathcal{H}$ es un subgrupo de G, y, dado que $e \in H$, se tiene que $e \in \mathcal{H}$. Ahora, del inciso b) de la proposición 3.8, se tiene que, para todo $i \in \{1, ..., m\}$, $g_i H g_i^{-1}$ es abierto, por lo que $\mathcal{H}$ es un subgrupo abierto de G. Ahora, por la proposición 1.48, obtenemos que $\mathcal{H} \trianglelefteq G$, además, de la ecuación 3.30, se tiene que:

$$\mathcal{H} = \bigcap_{i=1}^{m} g_i H g_i^{-1} \subseteq eHe^{-1} = H \subseteq C$$

Por lo tanto, $\mathcal{H} \subseteq C$. Concluimos que $\mathcal{H}$ es un subgrupo normal abierto de G y queda contenido en C, que es lo que debíamos de probar. $\square$

El siguiente resultado, con ayuda de la proposición 3.16, nos muestra que en un grupo topológico G, que es compacto y totalmente disconexo, podemos hallar una base cuyos abiertos constan de clases de subgrupos normales abiertos. Además, bajo las mismas hipótesis del grupo G, se caracterizan los subconjuntos abiertos y cerrados de G, así como la identificación de las cerraduras de sus subconjuntos y en particular de los cerrados de G.

Proposición 3.17 *Sea G un grupo topológico compacto y totalmente disconexo. Las siguientes condiciones se satisfacen.*

a) Todo conjunto abierto de G es unión de clases laterales de subgrupos normales abiertos en G.

b) Si $U \subseteq G$, entonces U es cerrado y abierto en G si y solo si U es unión finita de clases laterales de subgrupos normales abiertos de G.

c) Si $X \subseteq G$, entonces:

$$\overline{X} = \bigcap \{NX : N \text{ es abierto y normal en } G\}. \tag{3.31}$$

Más aún, la intersección de todos los subgrupos normales y abiertos de G es el subgrupo trivial $\{e\}$.

Demostración.

a) Primero notemos que, como G es totalmente disconexo, por el inciso d) de la proposición 3.13, se tiene que G es Hausdorff, mientras que, de la proposición A.91, obtenemos que G es cero dimensional (vea definición A.89). Por lo tanto G es T_1 y posee una base $\mathcal{B}$ de abiertos y cerrados de G.
Sea U un abierto no vacío de G. Entonces, para cada $x \in U$, existe $U_x \in \mathcal{B}$ tal que $x \in U_x \subseteq U$. Ahora, por el inciso b) de la proposición 3.8, se tiene que $x^{-1}U_x$ es abierto y cerrado de G. Además:

$$e = x^{-1} \cdot x \in x^{-1}U_x.$$

Es decir, $x^{-1}U_x$ es un abierto y cerrado que contiene a la identidad de G. Ya que G es compacto, de la proposición 3.16, se sigue que existe K_x un subgrupo normal abierto de G tal que $K_x \subseteq x^{-1}U_x$. De este modo, para cada $x \in G$, se tiene que:

$$xK_x \subseteq U_x \subseteq U.$$

Notemos además que $x = xe \in xK_x$, por lo que se concluye que:

$$\bigcup_{x\in U} xK_x = U. \tag{3.32}$$

Por lo tanto, U es la unión de clases laterales de subgrupos normales de G.

b) Primero supongamos que U es un subconjunto abierto y cerrado de G. Al ser abierto, de forma similar a como se hizo en la ecuación 3.32 del inciso a) de la proposición 3.17, se sigue que $U = \bigcup_{x\in U} xK_x$, con K_x subgrupo normal y abierto de G.
Por otro lado, dado que U es cerrado de G, por la proposición A.59 obtenemos que U es compacto. Por lo tanto, existen $x_1, ..., x_n \in U$ tales que $U = \bigcup_{i=1}^{n} x_iK_{x_i}$. Esto significa que U es unión finita de clases laterales de subgrupos normales abiertos de G.

Ahora bien, si U puede escribirse como $U = \bigcup_{i=1}^{n} x_iK_i$, con $x_i \in G$ y K_i normal y abierto de G para todo $i \in \{1, ..., n\}$, se sigue que U es abierto de G. Además, del inciso c) de la proposición 3.8, se tiene que, para todo $i \in \{1, ..., n\}$, K_i es cerrado de G. Finalmente, del inciso b) de la proposición 3.8, se sigue que para todo $i \in \{1, ..., n\}$, x_iK_i es cerrado. Así, U es unión finita de cerrados, por lo que, en virtud de c) de la proposición A.9, se concluye que U es cerrado de G. Por lo tanto, U es abierto y cerrado de G.

c) Para demostrar que $\overline{X} \subseteq \bigcap_{\substack{N\trianglelefteq G\\ N\in\tau}} NX$, primero probaremos que:

$$G \setminus \bigcap_{\substack{N\trianglelefteq G\\ N\in\tau}} NX \subseteq G \setminus \overline{X}. \tag{3.33}$$

Sea $\alpha \in G\setminus \bigcap_{\substack{N\trianglelefteq G\\ N\in\tau}} NX$. Esto significa que existe un subgrupo normal abierto N de G tal que para todo $x \in X$ se tiene que $\alpha \in G\setminus Nx$, esto es, $\alpha \notin Nx$. Notemos que como N es abierto, del inciso b) de la proposición 3.8, se tiene que $N\alpha$ es un abierto en G, y como N es un subgrupo de G, entonces $\alpha \in N\alpha$.

Supongamos que $\alpha \notin G \setminus \overline{X}$, es decir, $\alpha \in \overline{X}$. De la proposición A.13 tenemos que $N\alpha \cap X \neq \emptyset$, esto significa que existe $\beta = n\alpha = x$, con $n \in N$

y $x \in X$. Como N es un subgrupo de G, se obtiene que $\alpha = n^{-1}x \in Nx$, esto naturalmente constituye una contradicción. De esta forma concluimos que $\alpha \in G \setminus \overline{X}$, por lo que se verifica la ecuación 3.33.
Al aplicar el complemento respecto a G a la ecuación 3.33, obtenemos la contención que deseábamos.

Ahora probemos que:

$$G \setminus \overline{X} \subseteq G \setminus \bigcap_{\substack{N \lhd G \\ N \in \tau}} NX. \tag{3.34}$$

Sea $\alpha \in G \setminus \overline{X}$. Esto implica que existe un abierto U de G tal que $\alpha \in U$ y $U \cap X = \emptyset$ (ver proposición A.13). Como U es abierto, del inciso a) de la proposición 3.17 y del hecho de que una clase lateral izquierda determinada por un subgrupo normal es también una clase lateral derecha (ver definición 1.41), se tiene que $U = \bigcup_{v \in U} K_v v$ con K_v subgrupo normal y abierto de G. Por lo tanto, llegamos a que

$$\bigcup_{v \in U} (K_v v \cap X) = \emptyset. \tag{3.35}$$

En particular, como $\alpha \in U$, se tiene que $K_\alpha \alpha \cap X = \emptyset$. De esto último se sigue que $\alpha \notin K_\alpha X$, pues en caso contrario, si $\alpha = kx$ con $k \in K_\alpha$ y $x \in X$, entonces $k^{-1}\alpha = x \in K_\alpha \alpha \cap X$, lo cual contradice que $K_\alpha \alpha \cap X = \emptyset$. Por lo tanto, $\alpha \notin \bigcap_{\substack{N \lhd G \\ N \in \tau}} NX$.
Así, obtenemos que $\alpha \in G \setminus \bigcap_{\substack{N \lhd G \\ N \in \tau}} NX$. De esta forma, concluimos que se satisface la ecuación 3.34.

Al tomar complemento respecto a G en las ecuaciones 3.33 y 3.34, concluimos que se verifica la ecuación 3.31.

Finalmente, notemos que, por la proposición A.81, $\{e\}$ es un subgrupo cerrado de G ya que G es totalmente disconexo. De la ecuación 3.31, se sigue que:

$$\begin{aligned} \{e\} = \overline{\{e\}} &= \bigcap \{N\{e\} : N \text{ es normal y abierto en } G\} \\ &= \bigcap \{N : N \text{ es normal y abierto en } G\}. \end{aligned}$$

Es decir, la intersección de todos los subgrupos normales y abiertos de G es el subgrupo trivial.

□

Al haber obtenido información acerca de las propiedades que poseen y adquieren los grupos topológicos cuando son Hausdorff, compactos o totalmente disconexos, presentamos el siguiente resultado, que nos ayuda a generar un nuevo grupo topológico a partir de una familia de grupos topológicos, haciendo válidos los teoremas vistos anteriormente, pues las propiedades de ser Hausdorff, compacto y totalmente disconexo se preservan bajo productos, en virtud de las proposiciones A.53, A.62 y A.92.

Lema 3.18 *Sean* $\{(G_i, \star_i, \tau_i)\}_{i\in I}$ *una familia de grupos topológicos no vacíos y* $\mathcal{X} = \prod_{i\in I} G_i$. *Entonces, se verifican las siguientes propiedades:*

a) $\mathcal{X}$ *es un grupo con la operación* $\star_{\mathcal{X}}$ *dada por:*

$$(x_i)_{i\in I} \star_{\mathcal{X}} (y_i)_{i\in I} = (x_i \star_i y_i)_{i\in I}.$$

b) $\mathcal{X}$ *es un espacio topológico al ser dotado con la topología producto* $\tau_{\mathcal{X}}$ *(vea definición A.51).*

Demostración. Se deja de ejercicio al lector. □

Observación 3.19 *Si la familia de grupos topológicos del lema 3.18 consta de grupos finitos y además* $|I| = n$, *para algún* $n \in \mathbb{Z}^+$, *entonces* $|\mathcal{X}| = |G_1|\cdots|G_n| < \infty$.

Teorema 3.20 *Sean* $\{(G_i, \star_i, \tau_i)\}_{i\in I}$ *una familia de grupos topológicos no vacíos y* $\mathcal{X} = \prod_{i\in I} G_i$. *Entonces* $\mathcal{X}$ *es un grupo topológico.*

Demostración. En virtud del lema 3.18, basta probar que la siguiente función es continua:

$$\zeta_{\mathcal{X}} : \mathcal{X}\times\mathcal{X} \longrightarrow \mathcal{X}$$
$$((x_i)_{i\in I}, (y_i)_{i\in I}) \longmapsto (x_i \star_i y_i^{-1})_{i\in I}\ .$$

Para cada $i \in I$, consideremos el siguiente diagrama de funciones continuas:

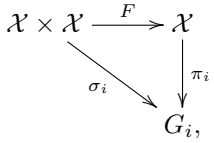
$$\begin{array}{ccccc} & & \overset{\sigma_i}{\frown} & & \\ \mathcal{X}\times\mathcal{X} & \xrightarrow{\pi_i\times\pi_i} & G_i\times G_i & \xrightarrow{\zeta_i} & G_i\ , \\ ((x_i)_{i\in I}, (y_i)_{i\in I}) & \longmapsto & (x_i, y_i) & \longmapsto & x_i \star_i y_i^{-1}\ , \end{array}$$

donde $\sigma_i = \zeta_i \circ (\pi_i \times \pi_i)$ es una función continua para cada $i \in I$, pues es composición de funciones continuas. Ahora, de la propiedad universal del producto

cartesiano (vea proposición A.49), se sigue que existe la siguiente función:

$$F : \mathcal{X} \times \mathcal{X} \longrightarrow \mathcal{X}$$
$$((x_i)_{i\in I}, (y_i)_{i\in I}) \longrightarrow (x_i \star_i y_i^{-1})_{i\in I} \ .$$

Además, la función F es tal que, para cada $i \in I$, se satisface que $\sigma_i = \pi_i \circ F$. Es decir, para cada $i \in I$, el siguiente diagrama conmuta:



con σ_i continua. Por lo que, a partir de la proposición A.52, se sigue que F es continua.
Por otra parte, es claro que $F = \zeta_{\mathcal{X}}$, y por lo tanto $\zeta_{\mathcal{X}}$ es una función continua. Así concluimos que $\mathcal{X}$ es un grupo topológico. □

3.2. Límites inversos

En este trabajo hemos hablado de estructuras concretas como grupos, anillos, campos, espacios vectoriales, espacios topológicos y finalmente grupos topológicos. Aunque la naturaleza de los objetos de estudio difiere, se tienen propiedades básicas en común que pueden abstraerse, ello da lugar al concepto de *categoría*. Para leer más sobre este tema le recomendamos consultar [2].

En esta sección empezaremos dando la noción de categoría para después estudiar a fondo el concepto de límite inverso. Esta última noción será importante para el estudio de los grupos profinitos esto con el fin de probar, en el corolario 4.22, que el grupo $Gal(K/F)$ es profinito.

Definición 3.21 *Una* ***categoría*** $\mathcal{C}$ *es una cuarteta* $\mathcal{C} = (\mathcal{O}, hom, id, \circ)$ *que consiste de:*

a) Una clase $\mathcal{O}$ *cuyos elementos son llamados* ***objetos*** *de la categoría* $\mathcal{C}$*. El hecho de que* A *es un objeto de* $\mathcal{C}$ *es abreviado como* $A \in \mathcal{C}$*.*

b) Para cada par de objetos A, B *en* $\mathcal{O}$*, hay un conjunto* $hom_{\mathcal{C}}(A, B)$ *que consiste de todos los* $\mathcal{C}$*-morfismos de* A *en* B*. Si* $f \in hom_{\mathcal{C}}(A, B)$*, se expresa como* $f : A \longrightarrow B$ *.*

c) Para cada objeto $A \in \mathcal{O}$*, existe el morfismo* $id_A : A \longrightarrow A$ *llamado* ***identidad en A****.*

d) En los morfismos de $\mathcal{C}$ hay una ***ley de composición*** *definida como sigue:*

Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son $\mathcal{C}$-morfismos, entonces existe un $\mathcal{C}$-morfismo $g \circ f : A \longrightarrow C$ llamado la ***composición*** *de f con g.*

Esta ley de composición en la categoría $\mathcal{C}$ queda sujeta a las siguientes condiciones:

a') La ley de composición $\circ$ es ***asociativa*** *para los morfismos de la categoría $\mathcal{C}$. Es decir, si tomamos cualesquiera $\mathcal{C}$-morfismos tales que $f : A \longrightarrow B$, $g : B \longrightarrow C$ y $h : C \longrightarrow D$, entonces:*

$$(h \circ g) \circ f = h \circ (g \circ f)\,.$$

b') Si $f : A \longrightarrow B$ es un morfismo, entonces las identidades de A y de B actúan como neutros bajo la composición, de la siguiente forma:

$$f \circ id_A = f \text{ y } id_B \circ f = f.$$

c') Los conjuntos $hom_{\mathcal{C}}(A, B)$ son disjuntos por pares.

Definición 3.22 *Sean $\mathcal{C}$ una categoría y A, B dos objetos de $\mathcal{C}$. Un morfismo $f : A \longrightarrow B$ es llamado un* ***isomorfismo*** *si existe un morfismo en $\mathcal{C}$, $g : B \longrightarrow A$, tal que:*

$$f \circ g = id_B \text{ y } g \circ f = id_A.$$

En el caso en que $A = B$, el isomorfismo es denominado ***automorfismo****.*

El concepto de categoría trata esencialmente de lo mínimo indispensable para generar conocimiento a partir de una globalidad de objetos que tienen la misma naturaleza (los objetos de la categoría) que son: las posibles relaciones entre dichos objetos según su naturaleza (los morfismos entre objetos) y la transitividad de dicha relación entre objetos (la ley de composición de morfismos).

El lector deberá notar que son varios los ejemplos explícitos que se conocen de categorías, por ejemplo, la categoría de los grupos cuyos morfismos piden verificar separar o abrir la operación (vea definición 1.18) y la ley de composición es la misma que la composición de funciones.

Nosotros trabajaremos con las categorías de espacios topológicos y grupos topológicos donde, en cada una de estas categorías, los morfismos se comprenden de funciones continuas y de homomorfismos continuos, respectivamente. Como dichas funciones están construidas a partir de funciones conjuntistas, el lector puede probar que efectivamente trabajaremos con categorías.

Definición 3.23 *Sea $(I, \leq)$ un conjunto parcialmente ordenado. Se dice que I es un* ***conjunto dirigido superiormente*** *si, para cualesquiera $x, y \in I$, existe $z \in I$ tal que $x \leq z$ y $y \leq z$.*

Observación 3.24 *a) En lo sucesivo, si $(I, \leq)$ es un conjunto dirigido superiormente, lo abreviaremos simplemente por I, entendiendo que $\leq$ es el orden parcial en I, a menos que requiera una especificación.*

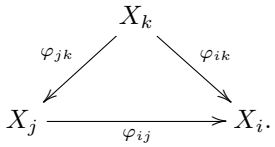
b) Si I es un conjunto dirigido superiormente, $n \in \mathbb{Z}^+$ y $a_1, ..., a_n \in I$, entonces, existe $r \in I$ tal que $a_i < r$ para todo $i \in \{1, ..., n\}$.

La naturaleza de los objetos y las propiedades de los morfismos en una categoría determinan propiedades globales dentro de la categoría, como lo es la existencia de objetos con ciertas características. A continuación, se presentan los *sistemas inversos*, que veremos dan lugar a la existencia de *límites inversos* dentro de una categoría.

Definición 3.25 *Sean $\mathcal{C}$ una categoría e I un conjunto dirigido superiormente. Un* ***sistema inverso*** *dentro de la categoría $\mathcal{C}$ es un par $\left(\{X_i\}_{i\in I}, \{\varphi_{ij}\}\right)$ donde:*

a) $\{X_i\}_{i\in I}$ es una familia de objetos de la categoría $\mathcal{C}$.

b) $\{\varphi_{ij}\}_{i,j\in I} = \left\{ \varphi_{ij} : X_j \longrightarrow X_i : i \leq j \right\}$ es una familia de $\mathcal{C}$-morfismos tal que, si $i = j$, entonces $\varphi_{ii} = id_{X_i}$. Además, esta familia verifica la siguiente propiedad:
Para cualesquiera $i, j, k \in I$ tales que $i \leq j \leq k$, el siguiente diagrama es conmutativo, es decir, $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$:



Observación 3.26 *Un sistema inverso $\left(\{X_i\}_{i\in I}, \{\varphi_{ij}\}\right)$ será abreviado simplemente con el símbolo (X_i, φ_{ij}), suponiendo que está indexado por el conjunto dirigido superiormente I, y que si $i, j \in I$, entonces $i \leq j$, a menos que se indique lo contrario.*

Definición 3.27 *Sean $(I, \leq)$ y $(J, \leq')$ dos conjuntos dirigidos superiormente tales que existe una biyección $\gamma : I \longrightarrow J$ que satisface que, para todo $i, j \in I$, se tiene que $i \leq j$ si y solo si $\gamma(i) \leq' \gamma(j)$.*
Sean (X_i, φ_{ij}) y (Y_r, φ'_{rs}) dos sistemas inversos indexados sobre I y J respectivamente. Se dice que los sistemas inversos (X_i, φ_{ij}) y (Y_r, φ'_{rs}) son ***equivalentes*** *si para cada $i \in I$ existe un isomorfismo $\theta_i : X_i \longrightarrow Y_{\gamma(i)}$ tal que, si*

$i \leq j$, entonces el siguiente diagrama conmuta:

$$\begin{array}{ccc} X_j & \xrightarrow{\theta_j} & Y_{\gamma(j)} \\ {\scriptstyle \varphi_{ij}}\downarrow & & \downarrow{\scriptstyle \varphi'_{\gamma(i)\gamma(j)}} \\ X_i & \xrightarrow{\theta_i} & Y_{\gamma(i)}. \end{array}$$

Definición 3.28 *Sea (X_i, φ_{ij}) un sistema inverso en una categoría $\mathcal{C}$. Se dice que un par $\left(Y, \{\psi_i\}_{i\in I}\right)$ es* ***compatible*** *con el sistema inverso dado, si se satisface lo siguiente:*

a) Y es un objeto de $\mathcal{C}$.

b) $\{\psi_i\}_{i\in I} := \left\{ \psi_i : Y \longrightarrow X_i \ : i \in I \right\}$ es una familia de $\mathcal{C}$-morfismos que verifican $\varphi_{ij} \circ \psi_j = \psi_i$ para todo $i, j \in I$.

$$\begin{array}{ccc} & Y & \\ {\scriptstyle \psi_j}\swarrow & & \searrow{\scriptstyle \psi_i} \\ X_j & \xrightarrow[\varphi_{ij}]{} & X_i. \end{array}$$

Observación 3.29 *El hecho de que $\left(Y, \{\psi_i\}_{i\in I}\right)$ es compatible con el sistema inverso (X_i, φ_{ij}) lo denotaremos simplemente por (Y, ψ_i) entendiendo que el conjunto dirigido superiormente con el cual se está indexando es I.*

Definición 3.30 *Un* ***límite inverso*** *de un sistema inverso (X_i, φ_{ij}) es un par (L, ϕ_i) compatible con el sistema inverso, que satisface la siguiente propiedad, denominada* ***la propiedad universal del límite inverso****:*

Si (Y, ψ_i) es compatible con el sistema inverso (X_i, φ_{ij}), entonces existe un único morfismo $\phi : Y \longrightarrow L$ de tal forma que el siguiente diagrama es conmutativo para cualesquiera $i, j \in I$ con $i \leq j$:

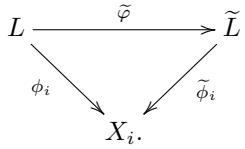
$$\begin{array}{ccccc} & & Y & & \\ & & \downarrow{\scriptstyle \phi} & & \\ & {\scriptstyle \psi_j}\swarrow & L & \searrow{\scriptstyle \psi_i} & \\ & {\scriptstyle \phi_j}\swarrow & & \searrow{\scriptstyle \phi_i} & \\ X_j & & \xrightarrow[\varphi_{ij}]{} & & X_i. \end{array}$$

Como puede verse en la definición de límite inverso, este es un objeto dentro de la categoría que se esté trabajando. De hecho, veremos que es el único objeto, salvo isomorfismos, dentro de la categoría que verifica la *propiedad universal del*

límite inverso.
A simple vista parece difícil identificar el límite inverso de un sistema inverso dentro de una categoría, sin embargo, en categorías donde existe el *producto cartesiano*, como en la categoría de conjuntos y aquellas que se derivan de esta, como la categoría de espacios topológicos, grupos o de grupos topológicos, se puede obtener una caracterización del límite inverso como veremos en la siguiente proposición.

Proposición 3.31 *Para (X_i, φ_{ij}) un sistema inverso dentro de una categoría $\mathcal{C}$, se verifican las siguientes propiedades:*

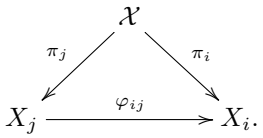
a) Si (L, ϕ_i) y $(\widetilde{L}, \widetilde{\phi}_i)$ son límites inversos de (X_i, φ_{ij}), entonces existe un isomorfismo $\widetilde{\varphi} : L \longrightarrow \widetilde{L}$ dentro de la categoría, tal que para todo $i \in I$, el siguiente diagrama es conmutativo:



b) Si la categoría $\mathcal{C}$ es la categoría de espacios topológicos o la categoría de grupos, tomamos el siguiente subconjunto del producto de los X_i :

$$\mathcal{X} = \left\{ c \in \prod_{i \in I} X_i : (\varphi_{ij} \circ \pi_j)(c) = \pi_i(c), i \leq j \right\}, \tag{3.36}$$

y la familia de morfismos definida, para cada $i \in I$, como $\phi_i = \pi_i|_{\mathcal{X}}$, donde π_i es la proyección canónica. Entonces, se verifica que $(\mathcal{X}, \phi_i)$ es un límite inverso de (X_i, φ_{ij}).
Notemos que el límite $\mathcal{X}$ está construido a partir de los elementos en el producto de la familia $\{X_i\}_{i \in I}$ que hacen que el siguiente diagrama conmute:



c) Si (X_i, φ_{ij}) es un sistema inverso de grupos topológicos con homomorfismos continuos, entonces, el límite $\mathcal{X}$, descrito en la ecuación 3.36, es un grupo topológico y la familia de morfismos $\{\phi_i\}_{i \in I}$, definida en el inciso b) de la proposición 3.31, consta de homomorfismos continuos.

Demostración.

a) Basta usar la propiedad universal del límite inverso, se deja de ejercicio al lector.

b) La prueba que presentaremos es en el contexto de los espacios topológicos. Consideremos a $\prod_{i\in I} X_i$ con la topología producto (vea definición A.51) y a $\mathcal{X}$ con la topología de subespacio. Además, en este caso tenemos que la familia $\{\phi_i\}_{i\in I}$ es de funciones continuas, ya que cada una de dichas funciones es la restricción de las proyecciones canónicas π_i para cualquier $i \in I$, que, por la definición A.51, son funciones continuas. Más aún, la definición de $\mathcal{X}$ nos asegura que $\varphi_{ij} \circ \phi_j = \phi_i$ para cualesquiera $i, j \in I$ tales que $i \leq j$.

Sea (Y, ψ_i) un par compatible con (X_i, φ_{ij}), es decir, para cualesquiera $i, j \in I$, con $i \leq j$, tenemos $\varphi_{ij} \circ \psi_j = \psi_i$.
Ya que para cada $i \in I$ se tiene el morfismo continuo, $\psi_i : Y \longrightarrow X_i$, de la propiedad universal del producto (vea proposición A.49), se sigue que existe la siguiente función:

$$F : Y \longrightarrow \prod_{i\in I} X_i,$$

$$y \longmapsto (\psi_i(y))_{i\in I} .$$

Esta función es tal que $\pi_i \circ F = \psi_i$, para todo $i \in I$. De este hecho, y de la proposición A.52, obtenemos que F es continua.
Probaremos que la imagen de F se queda contenida en $\mathcal{X}$.

Sean $i, j \in I$ tales que $i \leq j$, entonces:

$$\pi_i \circ F = \psi_i = \varphi_{ij} \circ \psi_j = \varphi_{ij} \circ \pi_j \circ F.$$

Por lo tanto, para cada $y \in Y$, se tiene que:

$$\pi_i \left(F(y)\right) = \left(\varphi_{ij} \circ \pi_j\right)\left(F(y)\right).$$

Concluimos que $F(y) \in \mathcal{X}$, es decir, $Im(F) \subseteq \mathcal{X}$.

Ahora podemos definir el siguiente morfismo:

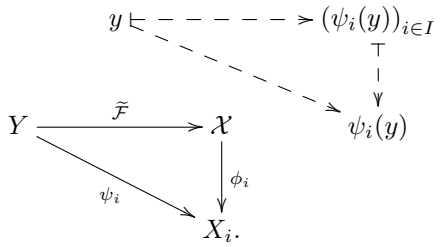
$$\widetilde{\mathcal{F}} : Y \longrightarrow \mathcal{X}$$

$$\widetilde{\mathcal{F}}(y) \longmapsto F(y) .$$

Notemos que $\widetilde{\mathcal{F}}$ es un morfismo continuo ya que está definido a partir del morfismo F, que es continuo. Además, para todo $i \in I$, se verifica:

$$\phi_i \circ \widetilde{\mathcal{F}} = \psi_i. \tag{3.37}$$

Es decir, el siguiente diagrama conmuta:



Ahora probaremos que $\widetilde{\mathcal{F}}$ es un morfismo único con la propiedad de la ecuación 3.37. Para ello supongamos que existe una función continua $\vartheta : Y \longrightarrow \mathcal{X}$, tal que para cada $i \in I$:

$$\phi_i \circ \vartheta = \psi_i. \tag{3.38}$$

Si $y \in Y$, entonces $\vartheta(y) \in \mathcal{X}$, y la ecuación 3.38 nos dice que al proyectar su i-ésima coordenada en X_i, esta coincide con $\psi_i(y)$. A su vez, este elemento se corresponde con la i-ésima entrada de $\widetilde{\mathcal{F}}(y)$, es decir, las funciones ϑ y $\widetilde{\mathcal{F}}$ coinciden. Por lo tanto, $\widetilde{F} = \vartheta$.
Concluimos que $\widetilde{F}$ es un morfismo único con la propiedad de la ecuación 3.37. De esta forma, $(\mathcal{X}, \phi_i)$ es el límite inverso del sistema inverso (X_i, φ_{ij}) de espacios topológicos.

c) Si (X_i, φ_{ij}) es un sistema inverso de grupos topológicos, del teorema 3.20 se tiene que $\prod_{i\in I} X_i$ es un grupo topológico. Además tenemos que $\mathcal{X}$ es un subespacio topológico del producto y es un subgrupo con las operaciones definidas en el lema 3.18. En efecto, si $(e_i)_{i\in I}$ es el elemento neutro del producto de los X_i, entonces, para cualesquiera $i, j \in I$ tales que $i \leq j$, se tiene:

$$\begin{aligned}(\varphi_{ij} \circ \pi_j)(e_i)_{i\in I} &= \phi_i(e_i)_{i\in I} \\ &= e_i \text{ por definición de } \phi_i \\ &= \pi_i((e_i)_{i\in I}).\end{aligned}$$

Por lo tanto $(e_i)_{i\in I} \in \mathcal{X}$. Ahora, si tomamos $(x_i)_{i\in I}, (y_i)_{i\in I} \in \mathcal{X}$, entonces:

$$\begin{aligned}(\varphi_{ij}\circ\pi_j)((x_i)_{i\in I} \star_{\mathcal{X}} ((y_i)_{i\in I})^{-1}) &= (\varphi_{ij}\circ\pi_j)((x_i \star_i y_i^{-1})_{i\in I})\\ &= (\varphi_{ij})(x_j \star_j y_j^{-1})\\ &= \varphi_{ij}(x_j) \star_i \varphi_{ij}(y_j^{-1})\\ &= (\varphi_{ij}\circ\pi_j)((x_i)_{i\in I}) \star_i (\varphi_{ij}\circ\pi_j)((y_i^{-1})_{i\in I})\\ &= \pi_i((x_i)_{i\in I}) \star_i \pi_i((y_i^{-1})_{i\in I})\\ &= x_i \star_i y_i^{-1}\\ &= \pi_i((x_i \star_i y_i^{-1})_{i\in I})\\ &= \pi_i((x_i)_{i\in I} \star_{\mathcal{X}} ((y_i)_{i\in I})^{-1})\end{aligned}$$

Por lo tanto, concluimos que $(x_i)_{i\in I} \star_{\mathcal{X}} ((y_i)_{i\in I})^{-1} \in \mathcal{X}$. De la proposición 1.9 se tiene que $\mathcal{X}$ es un subgrupo del grupo $\prod_{i\in I} X_i$. Por lo tanto, a partir de la proposición 3.5, concluimos que $\mathcal{X}$ es un grupo topológico. Por otro lado, para cada $i \in I$, el morfismo $\phi_i = \pi_i|_{\mathcal{X}}$ es un homomorfismo continuo, pues es una restricción de una proyección canónica, que es un homomorfismo continuo de grupos.
Concluimos que el límite inverso de un sistema inverso de grupos topológicos es a su vez un grupo topológico.

□

Observación 3.32 *a) Si (X_i, φ_{ij}) es un sistema inverso dentro de cualquier categoría, entonces al límite inverso lo abreviaremos usando el símbolo $\varprojlim X_i$.*

En lo sucesivo, usaremos $\mathcal{X}$ para citar a $\varprojlim X_i$, a menos que se indique lo contrario.

b) Notemos que en el inciso b) de la proposición 3.31, el límite inverso de un sistema inverso de espacios topológicos puede ser descrito como:

$$\mathcal{X} = \bigcap_{i\leq j} \left\{ c \in \prod_{i\in I} X_i : (\varphi_{ij}\circ\pi_j)(c) = \pi_i(c) \right\}.$$

Ahora, al ser $\mathcal{X}$ la intersección de ciertos subconjuntos del producto de X_i, nada nos garantiza que el límite inverso será distinto del vacío. El inciso e) de la proposición 3.33 nos proporcionará una condición bajo la cual puede afirmarse que hay, por lo menos, un elemento en el límite inverso $\mathcal{X}$.

Proposición 3.33 *Para un sistema inverso (X_i, φ_{ij}) de espacios topológicos no vacíos, se verifican las siguientes propiedades:*

a) Si cada X_i es Hausdorff, entonces también lo es $\mathcal{X}$.

b) Si cada X_i es totalmente disconexo, $\mathcal{X}$ es totalmente disconexo.

c) Si para cada $i \in I, X_i$ es Hausdorff, entonces $\mathcal{X}$ es un subespacio cerrado de $\prod_{i\in I} X_i$.

d) Si para cada $i \in I, X_i$ es Hausdorff y compacto, entonces también lo es $\mathcal{X}$.

e) Si X_i es Hausdorff y compacto para cada $i \in I$, entonces $\mathcal{X} \neq \emptyset$.

Demostración.

a) Como cada X_i es Hausdorff, de la proposición A.53, se sigue que $\prod_{i\in I} X_i$ es Hausdorff. Ya que $\mathcal{X}$ es un subespacio del producto, de la proposición A.34, se concluye que $\mathcal{X}$ es Hausdorff.

b) Como cada X_i es totalmente disconexo, por el inciso a) de la proposición A.92 tenemos que el producto de los X_i también lo es. Ahora, por la proposición A.88, concluimos que $\mathcal{X}$ es totalmente disconexo.

c) Para cada $i \in I$ y cada $j \geq i$, consideremos las siguientes funciones continuas $\varphi_{ij} \circ \pi_j : \prod_{i\in I} X_i \longrightarrow X_i$ y $\pi_i : \prod_{i\in I} X_i \longrightarrow X_i$. Definimos el conjunto C_{ij} como sigue:

$$C_{ij} := \left\{ c \in \prod_{i\in I} X_i : \varphi_{ij} \circ \pi_j(c) = \pi_i(c) \right\}. \tag{3.39}$$

De la proposición A.36 se sigue que C_{ij} es cerrado del producto de los X_i, y ya que la intersección arbitraria de cerrados es cerrado (vea inciso b) de la proposición A.9), se sigue que $\mathcal{X}$ es cerrado de $\prod_{i\in I} X_i$ (vea observación 3.32 b)).

d) Del inciso c) de la proposición 3.33, tenemos que $\mathcal{X}$ es un cerrado en $\prod_{i\in I} X_i$.

Por otro lado, de la proposición A.62, tenemos que el producto de los X_i es compacto, pues para cada $i \in I$, X_i es compacto por hipótesis. De la proposición A.59 se tiene que $\mathcal{X}$ es compacto.

e) Para cada $i \in I$ y para cada $j \geq i$, definimos el conjunto C_{ij} de la misma forma a como se hizo en la ecuación 3.39.

De la definición de C_{ij}, y por la proposición A.36, se llega a que C_{ij} es un subespacio cerrado del producto de los X_i, y, gracias la proposición A.59,

tenemos que C_{ij} es compacto.
Del inciso b) de la observación 3.32 tenemos que:

$$\mathcal{X} = \bigcap_{j \geq i} C_{ij}.$$

Si suponemos que $\mathcal{X} = \emptyset$, al ser $\mathcal{X}$ compacto (vea inciso d) de la proposición 3.33) se tiene que la familia $\{C_{ij}\}_{j \geq i}$ no posee la propiedad de la intersección finita (vea proposición A.58), es decir, existe $n \in \mathbb{Z}^+$ tal que:

$$\bigcap_{k=1}^{n} C_{i_k j_k} = \emptyset, \text{ con } j_k \geq i_k. \tag{3.40}$$

Ya que I es un conjunto dirigido, se sigue, del inciso b) de la observación 3.24, que existe $r \in I$ tal que $i_k \leq j_k < r$ para todo $k \in \{1, ..., n\}$. Por hipótesis $X_i \neq \emptyset$ para todo $i \in I$, en particular para $r \in I$, existe $x_r \in X_r$. Definamos un elemento en el producto de los X_i de la siguiente forma:

$$(x_i)_{i \in I} = \begin{cases} x_i = \varphi_{ir}(x_r) \text{ si } i \leqslant r \\ x_i \text{ cualquier elemento en } X_i \text{ si } i \not\leqslant r. \end{cases} \tag{3.41}$$

Observemos que, para todo $i_k, j_k \in I$ tal que $i_k \leqslant j_k < r$, con $k \in \{1, ..., n\}$, se verifica:

$$\begin{aligned} \left(\varphi_{i_k j_k} \circ \pi_{j_k}\right)(x_i)_{i \in I} &= \varphi_{i_k j_k}(x_{j_k}) \quad \text{por def. proy. canónica, vea def. A.47} \\ &= \varphi_{i_k j_k}(\varphi_{j_k r}(x_r)) \text{ ya que } j_k \leqslant r, \text{ vea ecuación 3.41} \\ &= \varphi_{i_k r}(x_r) \quad \text{por def. sistema inverso, vea def. 3.25} \\ &= x_{i_k} \quad \text{ya que } i_k \leqslant r, \text{ vea ecuación 3.41} \\ &= \pi_{i_k}(x_i)_{i \in I} \quad \text{por def. proy. canónica, vea A.47.} \end{aligned}$$

Por lo tanto, concluimos que:

$$(x_i)_{i \in I} \in \bigcap_{k=1}^{n} C_{i_k j_k}. \tag{3.42}$$

La ecuación 3.42 contradice a la hipótesis de la ecuación 3.40, de esta forma, para evitar contradicciones debe verificarse que $\mathcal{X} \neq \emptyset$.

□

Proposición 3.34 *Sean (X_i, φ_{ij}) un sistema inverso en la categoría de grupos o de espacios topológicos, $\mathcal{X}$ su límite inverso tal como en la ecuación 3.36 y para cada $i \in I$, $\emptyset \neq Y_i \subseteq X_i$. Si al tomarse las restricciones $\varphi_{ij}|_{Y_i}$, para cada*

$i \in I$, se obtiene que $(Y_i, \varphi_{ij}|_{Y_i})$ es un sistema inverso tal que su límite inverso $\mathcal{Y}$ existe y está descrito similarmente a la ecuación 3.36, entonces:

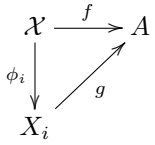
$$\mathcal{Y} \subseteq \mathcal{X}.$$

Demostración. El lector puede verificar la contención usando el hecho de que, al extender las funciones $\varphi_{ij}|_{Y_i}$ a todo X_i, se obtienen las funciones φ_{ij}, y se comportan con la misma regla de correspondencia sobre los elementos de Y_i que sus restricciones, de tal forma que se verifica la condición para ser un elemento del conjunto de la ecuación 3.36. Por lo tanto se cumple la contención. □

Proposición 3.35 *Sea $(\mathcal{X}, \phi_i)$ el límite inverso de un sistema inverso (X_i, φ_{ij}) de espacios topológicos no vacíos, Hausdorff y compactos. Entonces:*

a) Para cada $i \in I$, $\phi_i(\mathcal{X}) = \bigcap_{i \leq j} \varphi_{ij}(X_j)$.

b) Supongamos que los morfismos ϕ_i del límite inverso son suprayectivos para todo $i \in I$. Sean A un espacio topológico discreto y $f : \mathcal{X} \longrightarrow A$ una función continua. Entonces existen $i \in I$ y $g : X_i \longrightarrow A$ una función continua tal que el siguiente diagrama es conmutativo, es decir, $f = g \circ \phi_i$:



Demostración.

a) Ya que $(\mathcal{X}, \phi_i)$ es un sistema compatible con el sistema inverso (X_i, φ_{ij}), entonces para cada $i, j \in I$ tales que $i \leq j$, se tiene que $\phi_i = \varphi_{ij} \circ \phi_j$; de igual forma $\phi_j(\mathcal{X}) \subseteq X_j$. De estos hechos se sigue que, para cada $i \in I$ y $j \geq i$:

$$\phi_i(\mathcal{X}) = \varphi_{ij}\left(\phi_j\left(\mathcal{X}\right)\right) \subseteq \varphi_{ij}\left(X_j\right).$$

De esta forma, para cada $i \in I$ se obtiene:

$$\phi_i(\mathcal{X}) \subseteq \bigcap_{j \geq i} \varphi_{ij}(X_j).$$

Para demostrar la contención $\bigcap_{j \geq i} \varphi_{ij}(X_j) \subseteq \phi_i(\mathcal{X})$, fijemos $i \in I$ y tomemos $a \in \bigcap_{j \geq i} \varphi_{ij}(X_j)$.

Para cada $j \geq i$, consideremos el siguiente subconjunto de X_j:

$$Y_j = \{y \in X_j : \varphi_{ij}(y) = a\} = \varphi_{ij}^{-1}(\{a\}). \tag{3.43}$$

Ya que, para todo $j \geq i$, $a \in \varphi_{ij}(X_j)$, entonces $Y_j \neq \emptyset$. Ahora, como X_i es Hausdorff, por la proposición A.32, $\{a\}$ es cerrado de X_i. Como φ_{ij} es una función continua para cada $j \geq i$, entonces Y_j es un cerrado no vacío en X_j. Más aún, como X_j es compacto y Y_j es un cerrado en X_j, de la proposición A.59 se obtiene que Y_j es compacto.
Ahora, como (X_i, φ_{ij}) es un sistema inverso, si $j, k \in I$ son tales que $i \leq j \leq k$, entonces, para todo $y_k \in Y_k$:

$$\varphi_{ij} \circ \varphi_{jk}(y_k) = \varphi_{ik}(y_k) = a.$$

Por lo tanto, $\varphi_{jk}(y_k) \in Y_j$.
Definamos el sistema inverso (Z_l, θ_{lk}), indexado por I, de la siguiente forma:

$$Z_l := \begin{cases} Y_l, & \text{si } i \leq l. \\ X_l, & \text{en otro caso.} \end{cases}$$

También definimos θ_{lk} como:

$$\theta_{lk} := \begin{cases} \varphi_{lk}|_{Y_k}, & \text{si } l = i \text{ y } k \geq l \\ \varphi_{lk}, & \text{si } l \neq i \text{ y } k \geq l. \end{cases}$$

Naturalmente (Z_l, θ_{lk}) es un sistema inverso, pues está definido a partir de un sistema inverso.
De la proposición 3.34 se sigue que $\mathcal{Z} = \varprojlim Z_i \subseteq \varprojlim X_i = \mathcal{X}$. Además, como cada Z_l es compacto, Hausdorff y no vacío, del inciso e) de la proposición 3.33, se tiene que $\mathcal{Z} \neq \emptyset$. Esto implica que existe $b = (b_j)_{j \in I} \in \mathcal{Z}$, y por lo tanto, $b \in \mathcal{X}$. Por la definición de $\mathcal{X}$ (vea ecuación 3.36), para todo $j \geq i$, $\phi_j(b) = b_j$ (recordar que $\phi_j = \pi_j|_{\mathcal{X}}$ por proposición 3.31 b)). Ahora bien, como $(b_j)_{j \in I} \in \mathcal{Z}$, entonces para $j \geq i$ tenemos que $b_j \in Y_j$, y por construcción de Y_j (vea ecuación 3.43) se tiene que $\varphi_{ij}(b_j) = a$.
Por otro lado, $(b_j)_{j \in I} \in \mathcal{X}$, de la construcción de $\mathcal{X}$ (vea ecuación 3.36) se sigue que, para todo $j \geq i$:

$$\varphi_{ij}(b_j) = (\varphi_{ij} \circ \pi_j)((b_j)_{j \in I}) = \pi_i((b_j)_{i \in I}) = b_i.$$

Por lo tanto, $b_i = a$ y tenemos que $\phi_i(b) = a$, de donde se concluye que $a \in \phi_i(\mathcal{X})$. Probándose la contención $\bigcap_{i \leq j} \varphi_{ij}(X_j) \subseteq \phi_i(\mathcal{X})$.

b) Ya que $f : \mathcal{X} \longrightarrow A$ es una función continua, por la proposición A.63 se deduce que $f(\mathcal{X})$ es compacto, esto ya que $\mathcal{X}$ es compacto en virtud del inciso d) de la proposición 3.33. Además, como A es discreto, entonces $f(\mathcal{X})$ es un subespacio discreto de A. Del ejemplo A.56, se sigue que $f(\mathcal{X})$

es finito.
Por la observación A.10, tenemos que para cada $a \in f(\mathcal{X})$, $\{a\}$ es un abierto y cerrado en $f(\mathcal{X})$.
Para cada $a \in f(\mathcal{X})$, tomemos el siguiente subconjunto abierto y cerrado de $\mathcal{X}$:

$$Y_a = f^{-1}(\{a\}). \tag{3.44}$$

Notemos que $\mathcal{X} = \bigcup_{a \in f(\mathcal{X})} Y_a$, donde la unión es disjunta, pues f es una función.

Además, como $\mathcal{X}$ es compacto y Y_a es cerrado en $\mathcal{X}$ para cada $a \in f(\mathcal{X})$, de la proposición A.59, obtenemos que Y_a es compacto. De esta forma, por el inciso a) de la proposición 3.37, se sigue que cada Y_a es una unión finita de abiertos básicos de la forma $\phi_j^{-1}(U)$, con U un abierto en X_j y $j \in I$.

Por lo tanto, existe una cantidad finita de abiertos básicos de $\mathcal{X}$, digamos $\phi_1^{-1}(U_1), ..., \phi_{j_n}^{-1}(U_n)$, con U_s abierto en X_{j_s} para todo $s \leq n$. Dichos abiertos son tales que, para cada $a \in f(\mathcal{X}), Y_a$ es unión de algunos de esos abiertos básicos.

Como I es un conjunto dirigido superiormente, existe $k \in I$ tal que para todo $s \leq n$, se verifica que $j_s \leq k$.

Ya que $(\mathcal{X}, \phi_i)$ es un sistema compatible con (X_i, φ_{ij}), entonces en particular, para todo $j_s \leq k$ con $s \leq n$, se tiene:

$$\phi_{j_s}^{-1}(U_s) = (\varphi_{j_s k} \circ \phi_k)^{-1}(U_s) = \left(\phi_k^{-1}(\varphi_{j_s k}^{-1}(U_s))\right). \tag{3.45}$$

Veamos que para cada $a \in f(\mathcal{X})$, se tiene que $Y_a = \phi_k^{-1}(V_a)$ para algún abierto V_a de X_k. En efecto, tomemos $a \in f(\mathcal{X})$ fijo y arbitrario. Sin pérdida de generalidad supongamos que $Y_a = \bigcup_{s=1}^{r} \phi_{j_s}^{-1}(U_s)$ para algún $r \leq n$. De la ecuación 3.45 y de las propiedades de imagen inversa de una función, se sigue:

$$Y_a = \bigcup_{s=1}^{r} \phi_{j_s}^{-1}(U_s) = \bigcup_{s=1}^{r} \left(\phi_k^{-1}(\varphi_{j_s k}^{-1}(U_s))\right) = \phi_k^{-1}\left(\bigcup_{s=1}^{r} \varphi_{j_s k}^{-1}(U_s)\right).$$

Sea $V_a := \bigcup_{s=1}^{r} \varphi_{j_s k}^{-1}(U_s)$. Notemos que V_a es un subconjunto abierto de X_k.
Ahora, si $a, a' \in f(\mathcal{X})$ con $a \neq a'$, entonces:

$$V_a \cap V_{a'} = \emptyset. \tag{3.46}$$

Esto ya que $Y_a \cap Y_{a'} = \emptyset$ y ϕ_k es suprayectivo.

Sea

$$D := X_k \setminus \left(\bigcup_{a \in f(\mathcal{X})} V_a \right). \tag{3.47}$$

Notemos que D es cerrado en X_k y además $D \cap \phi_k(\mathcal{X}) = \emptyset$ ya que $\phi_k(\mathcal{X}) = \phi_k\Big(\bigcup_{a \in f(\mathcal{X})} Y_a \Big) = \bigcup_{a \in f(\mathcal{X})} \phi_k(Y_a) \subseteq \bigcup_{a \in f(\mathcal{X})} V_a$. Como X_k es compacto, de la proposición A.59 se sigue que D es compacto.
Por otro lado, del inciso a) de la proposición 3.35, se sigue que:

$$\emptyset = D \cap \phi_k(\mathcal{X}) = D \cap \left(\bigcap_{l \geq k} \varphi_{kl}(X_l) \right) = \bigcap_{l \geq k} (D \cap \varphi_{kl}(X_l)). \tag{3.48}$$

Además, para todo $l \geq k$, φ_{kl} es continua, y por hipótesis X_l es compacto, entonces, de la proposición A.63, se sigue que $\varphi_{kl}(X_l)$ es compacto. Como X_k es un espacio Hausdorff, de la proposición A.61, se concluye que $\varphi_{kl}(X_l)$ es cerrado en X_k.
Lo dicho previamente, junto con la ecuación 3.48, nos permite afirmar que la familia $\{D \cap \varphi_{kl}(X_l)\}_{l \geq k}$ de cerrados en X_k no posee la propiedad de la intersección finita (vea definición A.57), por lo que existe $\{l_1, ..., l_m\} \subseteq I$, con $k \leq l_s$ para todo $1 \leq s \leq m$, tales que:

$$D \cap \varphi_{kl_1}(X_{l_1}) \cap \varphi_{kl_2}(X_{l_2}) \cap ... \cap \varphi_{kl_m}(X_{l_m}) = \emptyset. \tag{3.49}$$

Del inciso b) de la observación 3.24, se sigue que existe $h \in I$ tal que $h \geq l_1, ..., l_m, k$. Ahora, para todo $k \leq l_s \leq h$ con $1 \leq s \leq m$, tenemos $\varphi_{l_s h}(X_h) \subseteq X_{l_s}$, se sigue que:

$$\varphi_{kh}(X_h) = (\varphi_{kl_s} \circ \varphi_{l_s h})(X_h) \subseteq \varphi_{kl_s}(X_{l_s}). \tag{3.50}$$

Por lo tanto, de las ecuaciones 3.49 y 3.50, llegamos a que:

$$D \cap \varphi_{kh}(X_h) \subseteq \bigcap_{s=1}^{m} D \cap \varphi_{kl_s}(X_{l_s}) = \emptyset.$$

Es decir:

$$D \cap \varphi_{kh}(X_h) = \emptyset. \tag{3.51}$$

Por lo tanto, de la definición de D (vea ecuación 3.47), tenemos que:

$$\varphi_{kh}(X_h) \subseteq \bigcup_{a \in f(\mathcal{X})} V_a. \tag{3.52}$$

Para cada $a \in f(\mathcal{X})$, consideremos el siguiente subconjunto abierto de $X_h, W_a = \varphi_{kh}^{-1}(V_a)$. Ya que $V_a \cap V_{a'} = \emptyset$, para $a, a' \in f(\mathcal{X})$ tales que $a \neq a'$, entonces:

$$W_a \cap W_{a'} = \emptyset. \tag{3.53}$$

Además,

$$\bigcup_{a \in f(\mathcal{X})} W_a \subseteq X_h. \tag{3.54}$$

Para probar la otra contención de la ecuación 3.54, tomemos $x_0 \in X_h$ un elemento fijo y arbitrario. De la ecuación 3.52, podemos concluir que $\varphi_{kh}(x_0) \in \varphi_{kh}(X_h) \subseteq \bigcup_{a \in f(\mathcal{X})} V_a$, por lo que existe $a_0 \in f(\mathcal{X})$ tal que $\varphi_{kh}(x_0) \in V_{a_0}$, es decir, $x_0 \in \varphi_{kh}^{-1}(V_{a_0}) = W_{a_0} \subseteq \bigcup_{a \in f(\mathcal{X})} W_a$.

Por lo tanto, hemos probado que:

$$X_h = \bigcup_{a \in f(\mathcal{X})} W_a, \tag{3.55}$$

Además, la unión de la ecuación 3.55 es disjunta en virtud de la ecuación 3.53. Por lo tanto, hemos generado una partición de subconjuntos abiertos de X_h.

Por otro lado, como la unión de la ecuación 3.55 es disjunta, y si tomamos $a' \in f(\mathcal{X})$, entonces:

$$\left(\bigcup_{a \in f(\mathcal{X})} W_a \right) \setminus W_{a'} = \bigcup_{a \in f(\mathcal{X}) \setminus \{a'\}} W_a.$$

Es decir, el complemento de $W_{a'}$ en X_h es abierto en X_h. Así, concluimos que $W_{a'}$ es cerrado de X_h.

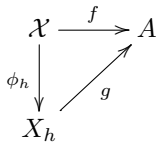
Consideremos la siguiente función que se comporta de forma constante en cada subconjunto W_a de X_h:

$$\begin{aligned} g : X_h &\longrightarrow A \\ g(x) &\longmapsto a \ , \end{aligned} \tag{3.56}$$

donde $a \in f(\mathcal{X})$ es tal que $x \in W_a$.

Observemos que la función g de la ecuación 3.56 está bien definida. Esto es, el elemento $a \in f(\mathcal{X})$ que existe tal que $g(x) = a$, es único en virtud de que la familia de abiertos $\{W_a\}_{a \in f(\mathcal{X})}$ proporciona una partición de X_h.

Verifiquemos que el siguiente diagrama conmuta:



En efecto, sea $(x_i)_{i\in I} \in \mathcal{X}$. Entonces tenemos que $\phi_h(x_i)_{i\in I} = x_h \in X_h$, donde x_h es la h-ésima coordenada de $(x_i)_{i\in I}$. Por la ecuación 3.55, se tiene $X_h = \bigcup_{a\in f(\mathcal{X})} W_a$, de donde se sigue que $x_h \in W_a$ para un único $a \in f(\mathcal{X})$.
Por lo tanto, de la definición de la función g se tiene que $g(x_h) = a$. Concluimos que $(g \circ \phi_h)((x_i)_{i\in I}) = a$.
Ahora verifiquemos que $f((x_i)_{i\in I}) = a$. Como $k \leq h$, se sigue que $\phi_k = \varphi_{kh} \circ \phi_h$; y así concluimos que $\phi_k((x_i)_{i\in I}) = \varphi_{kh}((x_h))$. Ahora bien, notemos que, como $x_h \in W_a = \varphi_{kh}^{-1}(V_a)$, entonces $\varphi_{kh}(x_h) \in V_a$. Es decir, tenemos que $\phi_k((x_i)_{i\in I}) \in V_a$; se sigue que $(x_i)_{i\in I} \in Y_a = \phi_k^{-1}(V_a)$. De la definición de Y_a (vea ecuación 3.44), tenemos que $f((x_i)_{i\in I}) = a$, probándose que $f = g \circ \phi_h$.

Finalmente, si $a \in A$, entonces $\{a\}$ es un abierto en A, pues A es un espacio discreto finito, y si $a \in f(\mathcal{X})$ entonces $g^{-1}(\{a\}) = W_a$. Por otro lado, si $a \notin f(\mathcal{X})$ entonces $g^{-1}(\{a\}) = \emptyset$. Ahora, tomemos un abierto arbitrario U de A. Sabemos que U es finito, digamos que es de la forma $U = \{a_1, ..., a_n\} = \bigcup_{i=1}^{n} \{a_i\}$. Al aplicarle la imagen inversa de g tenemos:

$$g^{-1}(U) = g^{-1}\left(\bigcup_{i=1}^{n} \{a_i\}\right) = \bigcup_{i=1}^{n} g^{-1}(\{a_i\}) = \bigcup_{i=1}^{n} W_{a_i}. \tag{3.57}$$

Nótese que el miembro del extremo derecho de la ecuación 3.57 es un abierto en X_h, ya que cada W_{a_i} es abierto en X_h para todo $i \in \{1, ..., n\}$.
Por lo tanto, concluimos que g es una función continua.

□

Observación 3.36 *En la demostración de 3.35 b) se utiliza fuertemente que los morfismos ϕ_i del límite inverso sean suprayectivos para demostrar que los conjuntos V_a y $V_{a'}$ son disjuntos, sin tal hipótesis no es claro que eso pase.*
Para un resultado parecido, ver [16, lema 1.1.16,pág. 12]. En dicho lema no se pide que los morfismos sean suprayectivos, pero sí se pide que cada espacio X_i sea un espacio profinito.

Proposición 3.37 *El límite inverso $(\mathcal{X}, \phi_i)$ de un sistema inverso (X_i, φ_{ij}) de espacios topológicos no vacíos verifica las siguientes condiciones:*

a) El conjunto:

$$\mathcal{A} := \left\{\phi_i^{-1}(U) : U \text{ es abierto en } X_i, i \in I\right\} \tag{3.58}$$

es una base para la topología de $\mathcal{X}$ como subespacio de $\prod_{i\in I} X_i$.

b) Si $Y \subseteq \mathcal{X}$ es tal que para todo $i \in I$ se tiene $\phi_i(Y) = X_i$, entonces Y es denso en $\mathcal{X}$.

c) Si Y es un espacio topológico y $\theta : Y \longrightarrow \mathcal{X}$ es una función, entonces θ es continua si y solo si $\phi_i \circ \theta$ es continua para todo $i \in I$.

Demostración.

a) De la definición A.51 tenemos que el conjunto:

$$\mathcal{A} = \left\{\pi_i^{-1}(U) : U \text{ es abierto en } X_i \text{ para todo } i \in I\right\}$$

es una subbase para la topología producto en $\prod_{i\in I} X_i$, mientras que de la observación A.26 se tiene que:

$$\left\{\mathcal{X} \cap \pi_i^{-1}(U) : i \in I, U \text{ es abierto en } X_i\right\}$$

es una subbase para $\mathcal{X}$ como subespacio del producto cartesiano de los X_i, es decir, todo conjunto abierto en $\mathcal{X}$ es unión arbitraria de conjuntos de la forma:

$$V = \mathcal{X} \cap \pi_{i_1}^{-1}(U_1) \cap ... \cap \pi_{i_n}^{-1}(U_n), \tag{3.59}$$

con U_j abierto en X_{i_j} para todo $j \in \{1, ..., n\}$.

Para continuar, sea V así como en la ecuación 3.59. Demostraremos que para cada $x \in V$, existe $k \in I$ y un abierto $U \subseteq X_k$ tal que $x \in \phi_k^{-1}(U) \subseteq V$.
Sea $x = (x_i)_{i\in I} \in V$. Entonces, para todo $j = 1, ..., n$, se tiene:

$$\phi_{i_j}(x) = \pi_{i_j}(x) = x_{i_j} \in U_j.$$

Como I es un conjunto dirigido superiormente, existe un índice k tal que para todo $j = 1, ..., n$, $i_j \leq k$. Consideremos la k-ésima coordenada de x, $x_k = \phi_k(x)$. Para todo $j = 1, ..., n$ se tiene:

$$\varphi_{i_j k}(x_k) = \varphi_{i_j k}(\phi_k(x)) = \phi_{i_j}(x) = \pi_{i_j}(x) = x_{i_j} \in U_j.$$

Por lo tanto, $x_k \in \varphi_{i_j k}^{-1}(\{x_{i_j}\}) \subseteq \varphi_{i_j k}^{-1}(U_j) \subseteq X_k$, para $j = 1, ..., n$. Definamos el siguiente abierto de X_k :

$$U := \bigcap_{j=1}^{n} \varphi_{i_j k}^{-1}(U_j) \subseteq X_k. \tag{3.60}$$

Notemos primero que $x_k \in U$. Consideremos el morfismo $\phi_k : \mathcal{X} \longrightarrow X_k$, entonces $\phi_k^{-1}(U) \subseteq \mathcal{X}$ es un abierto de $\mathcal{X}$, pues ϕ_k es continuo. Es claro que $x = (x_i)_{i\in I} \in \phi_k^{-1}(U)$, pues $\phi_k(x) = x_k \in U$.
Afirmamos que $\phi_k^{-1}(U) \subseteq V$.
Sea $z = (z_i)_{i\in I} \in \phi_k^{-1}(U)$, entonces $z_k = \phi_k(z) \in U$. De la definición de U (vea ecuación 3.60), se sigue que, para todo $j = 1, ..., n$, $\varphi_{i_j k}(z_k) \in U_j$. Además, $z_{i_j} = \phi_{i_j}(z) = \varphi_{i_j k}(\phi_k(z)) = \varphi_{i_j k}(z_k)$.
Luego, para todo i_j, con $j = 1, ..., n$, tenemos que $\phi_{i_j}(z) = z_{i_j} \in U_j$. Por lo tanto, $z = (z_i)_{i\in I} \in V = \mathcal{X} \cap \pi_{i_1}^{-1}(U_1) \cap \cdots \pi_{i_n}^{-1}(U_n)$. Concluimos que $x \in \phi_k^{-1}(U) \subseteq V$.

Sean U un abierto de $\mathcal{X}$ y $x \in U$. Entonces existe un conjunto V, descrito como en la ecuación 3.59, tal que $x \in V \subseteq U$. Por lo probado previamente, existen $k \in I$ y W un abierto en X_k tal que $x \in \phi_k^{-1}(W) \subseteq V \subseteq U$. Esto prueba que el conjunto de la ecuación 3.58 es una base para el límite $\mathcal{X}$ (vea proposición A.19).

b) Primero notemos que para todo $i \in I$, si U es cualquier abierto no vacío de X_i, de la hipótesis se sigue que:

$$U \cap \phi_i(Y) = U \cap X_i \neq \emptyset.$$

Es decir, existe $x_o \in U$ y $x_o \in \phi_i(Y)$, por lo que $x_0 = \phi_i(v)$ para algún $v \in Y$. Así:

$$v \in \phi_i^{-1}(U) \cap Y, \text{ es decir, } Y \cap \phi_i^{-1}(U) \neq \emptyset. \tag{3.61}$$

Con esto hemos probado que Y interseca a todas las imágenes inversas bajo ϕ_i de los abiertos de X_i, para cada $i \in I$.

Ahora, sea $U \subseteq \mathcal{X}$ un abierto no vacío, por el inciso a) de la proposición 3.37, se sigue que existe $\mathcal{B} \subseteq \{\phi_i^{-1}(U) : U \text{ es abierto en } X_i, i \in I\}$ tal que:

$$U = \bigcup_{\phi_i^{-1}(U)\in\mathcal{B}} \phi_i^{-1}(U). \tag{3.62}$$

Al intersecar Y con la ecuación 3.62, y en virtud de lo que se dijo en la ecuación 3.61, podemos concluir que:

$$Y \cap U = \bigcup_{\phi_i^{-1}(U)\in\mathcal{B}} Y \cap \phi_i^{-1}(U) \neq \emptyset.$$

Es decir, Y es denso en $\mathcal{X}$ (ver definición A.22).

c) Primero supongamos que θ es continua. Por el inciso b) de la proposición 3.31, sabemos que $\phi_i = \pi_i|_{\mathcal{X}}$ es continua para todo $i \in I$. Además, la composición de funciones continuas es una función continua, por lo tanto, para todo $i \in I$, la función $\phi_i \circ \theta$ es continua.

Para probar el recíproco, sea Y un espacio topológico y $\theta : Y \longrightarrow \mathcal{X}$ una función. Probaremos que θ es continua, para ello supongamos que, para todo $i \in I, \phi_i \circ \theta$ es una función continua

Para cada $i \in I$, tomemos U un abierto en X_i, como ϕ_i es continua, entonces $\phi_i^{-1}(U)$ es un abierto en $\mathcal{X}$. De este modo:

$$\theta^{-1}\left(\phi_i^{-1}(U)\right) = (\phi_i \circ \theta)^{-1}(U) \text{ es abierto en Y.}$$

Es decir, θ se comporta de forma continua sobre los elementos del conjunto $\mathcal{A}$ del inciso a) de la proposición 3.37.
Si U es un abierto en $\mathcal{X}$, se puede escribir como unión de elementos de $\mathcal{A}$. Del hecho de que la imagen inversa abre uniones arbitrarias y lo dicho previamente, se sigue que $\theta^{-1}(U)$ es abierto en Y.
Por lo tanto, θ es continua.

□

Observación 3.38 *Para otras versiones de la proposición 3.37 b) ver los siguientes resultados: [7, proposición 2.3(2), pág. 428]; [4, proposición 9, pág. 29] y [9, proposición 2.5.5, pág.99].*

Proposición 3.39 *Sea X un espacio Hausdorff, compacto y totalmente disconexo. Entonces X es el límite inverso de sus espacios cociente discretos.*

Demostración. Vea [25, proposición 1.1.7, pág. 16]. □

3.3. Grupos Profinitos

En este apartado se fusionan los grupos topológicos y los límites inversos de grupos topológicos para dar lugar a los grupos profinitos y posteriormente dar una descripción de ellos, por ejemplo se observará que son Hausdorff, compactos y totalmente disconexos. A lo largo de esta sección se dan resultados extraídos de [25] y [16].

Esta sección decanta en el capítulo 4 donde veremos que el grupo de Galois, visto como grupo topológico con la topología de Krull, es un grupo profinito (vea 4.22).

Proposición 3.40 *Sean (G, ϕ_i) el límite inverso de un sistema inverso (G_i, φ_{ij}) de grupos topológicos compactos y Hausdorff y L un subgrupo normal abierto de G. Entonces, existe $i \in I$ tal que $Ker(\phi_i)$ es un subgrupo de L y además $Ker(\phi_i)$ es un cerrado de G. Mas aún, G/L es isomorfo, como grupo topológico, a un grupo cociente de un subgrupo de G_i para algún $i \in I$.*

Demostración. Por el inciso a) de la proposición 3.37, tenemos que el siguiente conjunto es una base para la topología de G:

$$\mathcal{A} = \left\{\phi_i^{-1}(U) : i \in I, U \text{ abierto en } G_i\right\}.$$

Ya que L es un subgrupo abierto de G, entonces $(e_i)_{i\in I} \in L$, donde e_i es el elemento neutro de G_i para cada $i \in I$. Por lo tanto, existe $j \in I$ tal que $(e_i)_{i\in I} \in \phi_j^{-1}(U) \subseteq L$, con U un abierto en G_j. De esta forma, por la definición de ϕ_j (vea inciso b) de la proposición 3.31), se sigue que $\phi_j\left((e_i)_{i\in I}\right) = e_j \in U$. De lo anterior, se tiene que $(e_i)_{i\in I} \in ker(\phi_j)$.
Notemos que, si $x \in Ker(\phi_j)$, entonces $\phi_j(x) = e_j \in U$, y por lo tanto $x \in \phi_j^{-1}(U) \subseteq L$. Así, $Ker(\phi_j) \subseteq L$.
Por otro lado, como G_j es Hausdorff, entonces $\{e_j\}$ es un cerrado de G_j (vea proposición A.32). Ya que ϕ_j es continua, se sigue que $Ker(\phi_j) = \phi_j^{-1}(\{e_j\}) \subseteq L$ es un cerrado de G.
A continuación probaremos la segunda afirmación de nuestro enunciado.
Como $Ker(\phi_j)$ y L son subgrupos normales de G tales que $Ker(\phi_j) \leq L \leq G$, del teorema 1.59 se sigue que $L/Ker(\phi_j) \trianglelefteq G/Ker(\phi_j)$. Por lo tanto:

$$\left(G/Ker(\phi_j)\right)/\left(L/Ker(\phi_j)\right) \simeq G/L. \tag{3.63}$$

Ahora, del primer teorema de isomorfismo (vea teorema 1.56), sabemos que:

$$G/Ker(\phi_j) \simeq Im(\phi_j) \leq G_j. \tag{3.64}$$

Por lo tanto, G/L es isomorfo a un cociente de un subgrupo de G_j. □

Observación 3.41 *Si en la proposición 3.40, el morfismo ϕ_j es suprayectivo, donde j es el índice en I que existe tal que $(e_i)_{i\in I} \in \phi_j^{-1}(U)$, entonces se puede garantizar que $Im(\phi_j) = G_j$, y por lo tanto, en la ecuación 3.63, se tiene que $G/L \simeq G_j/(L/Ker(\phi_j))$. Es decir, G/L es isomorfo como grupo topológico a un grupo cociente de G_j.*

Definición 3.42 *Sean G un grupo topológico e I una familia de subgrupos normales abiertos (o cerrados) de G. Se dice que I es un* ***filtro base*** *si para cualesquiera $K_1, K_2 \in I$, existe $K_3 \in I$ tal que:*

$$K_3 \subseteq K_1 \cap K_2.$$

Lema 3.43 *Sean G un grupo topológico e I un filtro base de subgrupos normales cerrados de G. Entonces, I puede convertirse en un conjunto parcialmente ordenado de la siguiente forma:*

$$\text{Para } K, L \in I, \text{ se define } K \leq' L \text{ si y solo si } L \subseteq K. \tag{3.65}$$

Más aún, el filtro base I es un conjunto dirigido con el orden parcial descrito en la ecuación 3.65, y consideremos la siguiente familia de morfismos suprayectivos:

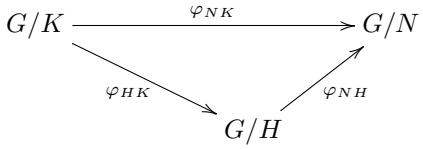
$$\left\{ \varphi_{KL} : G/L \longrightarrow G/K : K \leq' L \right\},$$

donde para cualesquiera $K \leq' L$ y $a \in G$, se define el morfismo φ_{KL} como

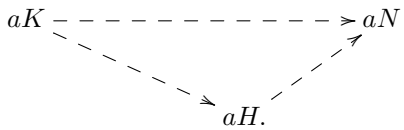
$$aL \overset{\varphi_{KL}}{\longmapsto} aK. \tag{3.66}$$

Entonces $((G/K)_{K\in I}, (\varphi_{KL})_{K\leq' L})$ es un sistema inverso.

Demostración. El lector puede corroborar que efectivamente el orden definido en la ecuación 3.65 es un orden parcial. Para corroborar que dicho orden hace de I un conjunto dirigido, basta usar el hecho de que I es un filtro base. Además, es fácil ver que si $K \leq' L$, entonces el morfismo φ_{KL} está bien definido y es un homomorfismo suprayectivo de grupos. Más aún, $\varphi_{LL} = id_{G/L}$ para todo $L \in I$. Ahora, sean $N, H, K \in I$ tales que $N \leq' H \leq' K$, la siguiente ilustración muestra que $((G/K)_{K\in I}, (\varphi_{KL})_{K\leq' L})$ es un sistema inverso.



(3.67)



□

La siguiente proposición hace uso del orden parcial creado para un filtro base de subgrupos normales cerrados de un grupo topológico G (vea ecuación 3.65), así como del sistema inverso de cocientes y morfismos descrito en el lema 3.43.

Proposición 3.44 *Sean G un grupo topológico, $(I, \leq')$ un filtro base de subgrupos normales cerrados de G y el sistema inverso $((G/K)_{K\in I}, (\varphi_{KL})_{K\leq' L})$ definido en el lema 3.43.*
Si $(\widetilde{G}, \phi_K) := \varprojlim(G/K, \varphi_{KL})$ es el límite inverso del sistema inverso dado inicialmente, entonces se verifica lo siguiente:

a) Existe un homomorfismo continuo $\theta : G \longrightarrow \widetilde{G}$ con las siguientes características:

$$Ker(\theta) = \bigcap_{K\in I} K \text{ e } Im(\theta) \text{ es un subgrupo denso en } \widetilde{G}.$$

b) Si G es compacto, entonces θ es suprayectivo. Si además se cumple que $Ker(\theta) = \{e\}$, entonces θ es un isomorfismo de grupos topológicos.

Demostración.

a) Consideremos el siguiente morfismo:

$$\begin{aligned} \theta : G &\longrightarrow \prod_{K\in I} G/K \\ g &\longmapsto (gK)_{K\in I} \ . \end{aligned} \tag{3.68}$$

Se deja de ejercicio al lector probar que θ es un homomorfismo de grupos. Para cada $H \in I$, consideremos las proyecciones canónicas:

$$\begin{aligned} \pi_H : \prod_{K\in I} G/K &\longrightarrow G/H \\ (gK)_{K\in I} &\longrightarrow gH \ . \end{aligned}$$

Ahora, si $(gK)_{K\in I} \in Im(\theta)$, entonces, para cualesquiera $H, L \in I$ tales que $H \leq' L$, se tiene:

$$\begin{aligned} (\varphi_{HL} \circ \pi_L)\left((gK)_{K\in I}\right) &= \varphi_{HL}(gL) \\ &= gH \quad \text{por def. de } \varphi_{HL} \text{ en lema 3.43} \\ &= \pi_H((gK)_{K\in I}). \end{aligned}$$

A partir de la construcción del límite inverso (vea ecuación 3.36), obtenemos que $(gK)_{K\in L} \in \widetilde{G}$, es decir, $Im(\theta) \subseteq \widetilde{G}$.
Ahora probaremos la continuidad de θ. Sean $H \in I$ un elemento arbitrario y $g \in G$. Entonces:

$$(\pi_H \circ \theta)(g) = \pi_H\left((gK)_{K\in I}\right) = gH = p_H(g),$$

donde $p_H : G \longrightarrow G/H$ es la proyección canónica en el cociente.
Por el inciso a) de la proposición A.43, sabemos que p_H es continua para todo $H \in I$. Por lo que θ es continua en virtud de la proposición A.52.
Por otra parte, si $g \in ker(\theta)$, entonces $\theta(g) = (eK)_{K\in I}$, con e el neutro para la operación de G. Así, para todo $K \in I$, se tiene que $g \in K$. Observe que el regreso de las implicaciones anteriores son verdaderas. Por lo tanto:

$$Ker(\theta) = \bigcap_{K\in I} K.$$

Recordemos que $Im(\theta) \subseteq \widetilde{G}$. Ahora, para cualquier $H \in I$, consideremos el morfismo $\phi_H : \widetilde{G} \longrightarrow G/H$ dado por ser $\widetilde{G}$ límite inverso. Entonces:

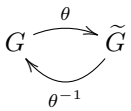
$$\begin{aligned}
\phi_H(Im(\theta)) = \phi_H\left(\theta(G)\right) &= \phi_H\left(\theta\left(\bigcup_{g\in G}\{g\}\right)\right) \\
&= \phi_H\left(\bigcup_{g\in G}\theta(\{g\})\right) \\
&= \bigcup_{g\in G}\left\{\phi_H\left((gK)_{K\in I}\right)\right\} \quad \text{por def. de } \theta \text{ (vea ecuación 3.68)} \\
&= \bigcup_{g\in G}\{gH\} \\
&= G/H.
\end{aligned}$$

Por lo tanto, del inciso b) de la proposición 3.37 y de la observación 1.21, concluimos que $Im(\theta)$ es un subgrupo denso de $\widetilde{G}$.

b) Si G es compacto, por la proposición A.63 tenemos que $\theta(G)$ es compacto. Por otra parte, como todo $K \in I$ es un subgrupo normal cerrado en G, por el inciso d) de la proposición 3.13, se tiene que G/K es Hausdorff, y de la proposición A.53 se deduce que $\prod_{K\in I} G/K$ es Hausdorff.
Así, gracias a la proposición A.34, se llega a que $\widetilde{G}$ es Hausdorff. Por lo tanto, de la proposición A.61, obtenemos que $\theta(G)$ es un subgrupo cerrado en $\widetilde{G}$.
Ahora, como al final del inciso anterior probamos que $\theta(G)$ es un subgrupo denso en $\widetilde{G}$, entonces $\overline{\theta(G)} = \widetilde{G}$. Como $\theta(G)$ es cerrado en $\widetilde{G}$, se sigue que $\theta(G) = \widetilde{G}$, es decir, θ es un morfismo suprayectivo.

Por otro lado, bajo la hipótesis de que G es compacto y que $ker(\theta) = \{e\}$, se tiene que θ es una biyección, además es continua por el inciso a) de la proposición 3.44. Por lo tanto, existe θ^{-1}, probaremos que es continua

para poder concluir que θ es un homeomorfismo entre grupos topológicos.



Para probar que θ^{-1} es continua, usaremos la equivalencia enunciada en la proposición A.37. Tomemos U un cerrado en G, al ser G compacto, de la proposición A.59 tenemos que U es compacto en G. Por la proposición A.63 se sigue que $\theta(U)$ es compacto en $\widetilde{G}$, el cual hemos visto es Hausdorff. Ahora, por la proposición A.61, tenemos que $\theta(U)$ es cerrado de $\widetilde{G}$, es decir, $(\theta^{-1})^{-1}(U) = \theta(U)$ es cerrado. Así, concluimos que θ^{-1} es una función continua.
Por lo tanto, θ es un homeomorfismo entre grupos topológicos.

□

Observación 3.45 *En la proposición previa hemos visto una condición bajo la cual un grupo topológico G es isomorfo (como grupo topológico) a un límite inverso de grupos topológicos, que, en el caso de la proposición, fueron grupos cociente. En lo sucesivo, el objetivo es estudiar grupos que son, bajo isomorfismo, límites inversos de grupos con las mismas propiedades que el grupo inicial. El siguiente concepto puntualiza un poco más sobre a qué nos referimos por propiedades de un grupo. Además, nos limitaremos al estudio de los grupos finitos.*

Definición 3.46 *Tomemos* ***Grp*** *la categoría de grupos cuyos morfismos son homomorfismos entre grupos. Una* ***clase de grupos finitos*** *es $\mathcal{C} \subset$ **Grp** tal que $\mathcal{C} \neq \emptyset$ y además, para todo $G \in \mathcal{C}$ y todo $G' \in$ **Grp** que satisfacen $G \simeq G'$, se tiene que $G' \in \mathcal{C}$, es decir, $\mathcal{C}$ es cerrada por isomorfismos.*
*A los elementos de la clase $\mathcal{C}$ les llamaremos $\mathcal{C}$-**grupos**.*

Ejemplo 3.47 *Hay una variada colección de clases de grupos finitos que se pueden llegar a estudiar, por ejemplo:*

a) La clase de todos los grupos finitos.

b) La clase de todos los grupos finitos y abelianos.

c) La clase de todos los grupos finitos que son $p-$grupos, para p un entero primo.

d) La clase de todos los grupos finitos nilpotentes.

Al tomar una clase $\mathcal{C}$ de grupos, se puede plantear la cuestión sobre si los subgrupos, los grupos cociente o los productos, son nuevamente $\mathcal{C}$ grupos, es decir, si cumplen las características para pertenecer a la clase $\mathcal{C}$. En este caso, la clase $\mathcal{C}$ adquiere una nueva denominación como lo indica la siguiente definición.

Definición 3.48 *Se dice que una clase $\mathcal{C}$ de grupos finitos es **cerrada bajo subgrupos** (resp. **cocientes**) si todo subgrupo (resp. cociente) de un $\mathcal{C}$-grupo es nuevamente un $\mathcal{C}$- grupo.*
*La clase $\mathcal{C}$ es **cerrada bajo productos finitos** si para cualesquiera $G, G' \in \mathcal{C}$, se tiene que $G \times G' \in \mathcal{C}$.*

Definición 3.49 *Sean $\mathcal{C}$ una clase de grupos finitos y G un grupo. Se dice que G es un **grupo pro-$\mathcal{C}$** si G es el límite inverso de un sistema inverso de $\mathcal{C}$-grupos.*

Observación 3.50 *En lo sucesivo estudiaremos clases de grupos finitos, por lo cual a cada grupo finito lo consideraremos como espacio topológico con la topología discreta.*

Proposición 3.51 *Un espacio topológico (X, τ) discreto y finito es Hausdorff, compacto y totalmente disconexo.*

Demostración. De acuerdo a la observación A.31 se tiene que X es Hausdorff, mientras que por la proposición A.55 se sigue que es compacto. Finalmente, cada grupo finito con la topología discreta es totalmente disconexo (vea proposición A.87). Por lo que se concluye lo deseado. □

Lo anterior nos permite dar una caracterización acerca de los grupos pro-$\mathcal{C}$ para una clase $\mathcal{C}$ de grupos finitos, que consideraremos grupos topológicos con la topología discreta (vea ejemplo 3.3, inciso a)).

Proposición 3.52 *Sea $\mathcal{C}$ una clase de grupos finitos que es cerrada bajo subgrupos y productos directos finitos tal que a los elementos de $\mathcal{C}$ les damos la topología discreta, y consideremos G un grupo topológico. Entonces, los siguientes enunciados son equivalentes:*

a) G es un grupo pro-$\mathcal{C}$.

b) G es isomorfo (como grupo topológico) a un subgrupo cerrado de un producto cartesiano de $\mathcal{C}$-grupos.

c) G es compacto y se satisface:

$$\bigcap \{N \trianglelefteq G : N \text{ es abierto en } G \text{ y } G/N \in \mathcal{C}\} = \{e\}, \tag{3.69}$$

donde e es la identidad de G.

d) G es compacto, totalmente disconexo, y para todo subgrupo normal abierto L de G, hay un subgrupo normal y abierto N de G, tal que $N \leq L$ y $G/N \in \mathcal{C}$.
Si la clase $\mathcal{C}$ es cerrada bajo cocientes, el inciso d) puede ser cambiado como sigue:

d') *G es compacto, totalmente disconexo y para todo subgrupo normal abierto L de G se tiene $G/L \in \mathcal{C}$.*

Demostración.

a)$\Longrightarrow$ b) Si G es un grupo pro-$\mathcal{C}$, entonces existe $(G_i, \varphi_{ij})_{i\in I}$ un sistema inverso de $\mathcal{C}$ grupos tal que $G = \varprojlim G_i$. Ahora, por la proposición 3.51, cada uno de los grupos G_i es un espacio discreto y por lo tanto Hausdorff. Finalmente, del inciso c) de la proposición 3.33, tenemos que G es un subgrupo cerrado y Hausdorff de $\prod_{i\in I} G_i$.

b)$\Longrightarrow$ c) Ya que cada $\mathcal{C}$-grupo G_i es finito y discreto para todo $i \in I$, de la proposición 3.51, se sigue que G_i es compacto y Hausdorff. Del inciso d) de la proposición A.59, se sigue que G es compacto.

Por otro lado, para cada $j \in I$, tomemos $\pi_j : \prod_{i\in I} G_i \longrightarrow G_j$ la proyección canónica (vea definición A.47), y $K_j := ker(\pi_j) = \pi_j^{-1}(\{e_j\})$. Como para cada $j \in I$, la función π_j es continua (vea definición A.51), entonces cada K_j es un subgrupo normal, abierto y cerrado, esto debido a que G_j es un espacio discreto para todo $j \in I$.

Ahora, para cada $j \in I$, definamos el conjunto $N_j := K_j \cap G \subseteq G$, que, por el teorema 1.57, es un subgrupo normal y abierto de G con la topología de subespacio.

Probaremos que $\bigcap_{j\in I} K_j = \{(e_j)_{j\in I}\}$, donde e_j es el elemento neutro en G_j para cada $j \in I$.

Sea $(x_j)_{j\in I} \in \bigcap_{j\in I} K_j$, entonces para todo $j \in I$, $x_j = \pi_j((x_j)_{j\in I}) = e_j$, por lo que $(x_j)_{j\in I} = (e_j)_{j\in I}$.

De esta forma, concluimos que $\bigcap_{j\in I} K_j = \{(e_j)_{j\in I}\}$. Por lo tanto:

$$\bigcap_{j\in I} N_j = \{(e_j)_{j\in I}\}.$$

Además, como para cada $j \in I$ se tiene que K_j es normal en el producto de los G_i, con $i \in I$, y G es un subgrupo del producto cartesiano de los G_i, entonces por la proposición 1.49 se tiene $GK_j \leq \prod_{i\in I} G_i$.

Por lo tanto:

$$\begin{aligned} G/N_j &\simeq GK_j/K_j \quad [\text{ por el segundo teorema de isomorfismo 1.57 }] \\ &\leq \left(\prod_{i\in I} G_i\right)/K_j \quad [\text{ por el teorema de la corresp. biyectiva 1.59 }] \\ &\simeq G_j \quad [\text{ por observación A.48 }]. \end{aligned}$$

Es decir, para cada $j \in I$, tenemos que G/N_j es isomorfo a un subgrupo de G_j, digamos H_j. Ahora, ya que la clase $\mathcal{C}$ es cerrada bajo subgrupos, entonces $H_j \in \mathcal{C}$ y al ser $\mathcal{C}$ una clase cerrada bajo isomorfismos, se tiene que, para cada $j \in I, G/N_j \in \mathcal{C}$. De esta forma, podemos concluir que:

$$\bigcap \{N \trianglelefteq G : N \text{ es abierto de } G \text{ y } G/N \in \mathcal{C}\} \subseteq \bigcap_{i\in I} N_i = \{(e_i)_{i\in I}\},$$

lo cual nos ayuda a concluir lo que se afirma en la ecuación 3.69.

c)$\Longrightarrow$ a) Tomemos el siguiente conjunto y probemos que es un filtro base (vea definición 3.42) de subgrupos normales cerrados:

$$I = \{N \trianglelefteq G : N \text{ es subgrupo abierto de } G \text{ y } G/N \in \mathcal{C}\}.$$

Primero notemos que por proposición 3.8 c), los elementos de I también son cerrados. Sean $N_1, N_2 \in I$ y consideremos el siguiente morfismo de grupos:

$$\begin{aligned} \theta : G &\longrightarrow G/N_1 \times G/N_2 \\ g &\longmapsto (gN_1, gN_2)\ . \end{aligned}$$

Notemos que $G/N_1 \times G/N_2 \in \mathcal{C}$, pues por hipótesis tenemos que la clase $\mathcal{C}$ es de cerrada bajo productos finitos. Además, $Ker(\theta) = N_1 \cap N_2$. Por lo tanto, del primer teorema de isomorfismo (vea teorema 1.56) se sigue que:

$$G/(N_1 \cap N_2) \simeq Im(\theta) \leq G/N_1 \times G/N_2.$$

Como la clase $\mathcal{C}$ es cerrada bajo subgrupos e isomorfismos, concluimos que $G/(N_1 \cap N_2) \in \mathcal{C}$ y se satisface que $N_1 \cap N_2 \trianglelefteq G$, además dicha intersección es de abiertos, por lo que es abierto. Por el inciso c) de la proposición 3.8, tenemos que $N_1 \cap N_2$ es cerrado. De esta forma, $N_3 := N_1 \cap N_2 \in I$ y además $N_3 \subseteq N_1 \cap N_2$. Por lo tanto, I es un filtro base de subgrupos normales cerrados.

El hecho de que G sea un grupo pro-$\mathcal{C}$ se sigue de la proposición 3.44, pues G es compacto por hipótesis, y el morfismo $\theta : G \longrightarrow \widetilde{G}$ de la

proposición 3.44 satisface que

$$Ker(\theta) = \bigcap \{N \trianglelefteq G : N \text{ es abierto en } G \text{ y } G/N \in \mathcal{C}\} = \{e\}.$$

Por el inciso b) de la proposición 3.44, se obtiene que θ es un isomorfismo de grupos topológicos. Por lo tanto, G es un grupo pro-$\mathcal{C}$.

a)$\Longrightarrow$ d) Sea $G = \varprojlim G_i$, con $G_i \in \mathcal{C}$ para todo $i \in I$. Por la proposición 3.51, tenemos que la familia $\{G_i\}_{i\in I}$ consta de espacios topológicos Hausdorff, compactos y totalmente disconexos, por lo cual, de la proposición 3.33, se sigue que G es Hausdorff, compacto y totalmente disconexo.

Para probar la segunda afirmación, tomemos L un subgrupo normal abierto de G. De la proposición 3.40, se sigue que existe $j \in I$, $\phi_j : G \longrightarrow G_j$ tal que $Ker(\phi_j)$ es un subgrupo de L. Además, como G_j es un espacio discreto, entonces $\{e_j\}$ es un abierto y cerrado de G_j, donde e_j es el neutro de G_j.
Por lo tanto, $Ker(\phi_j) = \phi_j^{-1}(\{e_j\})$ es un abierto y cerrado. A partir del primer teorema de isomorfismo (vea teorema 1.56), se tiene que:

$$G/Ker(\phi_j) \simeq Im(\phi_j) \leq G_j.$$

Como la clase $\mathcal{C}$ es cerrada bajo subgrupos e isomorfismos, se concluye que:

$$G/Ker(\phi_j) \in \mathcal{C}.$$

d)$\Longrightarrow$c) Sea U un subgrupo normal y abierto de G. De la hipótesis se sigue que existe un subgrupo normal y abierto N_U de G (no necesariamente único) tal que

$$N_U \subseteq U \text{ y } G/N_U \in \mathcal{C}.$$

Por lo tanto, tenemos las siguientes contenciones de conjuntos:

$$\begin{aligned}
&\bigcap \{N : N \text{ es normal, abierto en } G \text{ y } G/N \in \mathcal{C}\} \\
&\subseteq \bigcap \{N_U : U \trianglelefteq G \text{ y abierto de } G\} \\
&\subseteq \bigcap \{U : U \trianglelefteq G \text{ y abierto de } G\} = \{e\},
\end{aligned}$$

donde la primera contención es debido a que en el siguiente conjunto $\bigcap\{N : N \text{ es normal, abierto en } G \text{ y } G/N \in \mathcal{C}\}$ estamos intersectando más conjuntos que en $\bigcap\{N_U : U \trianglelefteq G \text{ y abierto de } G\}$; y la última igualdad es por el inciso c) de la proposición 3.17.
De esta forma, se concluye que:

$$\bigcap \{N : N \text{ es normal, abierto en } G \text{ y } G/N \in \mathcal{C}\} = \{e\}.$$

a)$\Longrightarrow$d') Ya que se ha demostrado que $a) \Longrightarrow d)$, basta probar que $d) \Longrightarrow d')$.

Sea L un subgrupo normal abierto de G. Por el inciso $d)$ tenemos que existe N un subgrupo normal y abierto de G tal que $N \subseteq L$ y $G/N \in \mathcal{C}$. Por el inciso b) del teorema correspondencia biyectiva (vea teorema 1.59), se sigue que $L/N \trianglelefteq G/N$ y que $G/L \simeq (G/N)/(L/N)$. Como $\mathcal{C}$ es cerrada bajo cocientes y $G/N \in \mathcal{C}$, concluimos que $G/L \in \mathcal{C}$. Finalmente , notemos que $d') \Longrightarrow d)$. Por lo tanto, $d)$ es equivalente a $d')$ y así, $d')$ es equivalente a $a)$.

□

Observación 3.53 *Notemos que en la proposición 3.52 no se pide que G sea Hausdorff. Sin embargo, G resulta ser Hausdorff por la proposición 3.13 d) ya que G es totalmente disconexo.*

Aunque hemos hecho notar que hay una gran variedad de clases de grupos finitos (vea ejemplo 3.47), tomaremos en general a la clase de todos los grupos finitos.

Definición 3.54 *Se dice que un grupo G es **profinito** si G es un grupo topológico que es isomorfo (como grupo topológico) al límite inverso de un sistema inverso de grupos finitos con la topología discreta.*

Observación 3.55

a) Naturalmente, la caracterización de los grupos pro-$\mathcal{C}$ (vea proposición. 3.52) para una clase $\mathcal{C}$ de grupos finitos, se contextualiza para la clase de grupos finitos.

b) A partir de la proposición 3.52 y la observación 3.53 se tiene que cualquier grupo profinito es Hausdorff, compacto y totalmente disconexo.

Notemos que la clase de los grupos finitos es cerrada bajo cocientes, entonces, de la proposición 3.52 que caracteriza a los grupos profinitos, se sigue el siguiente resultado.

Corolario 3.56 *Si G es un grupo profinito, entonces:*

$$\bigcap \{N \trianglelefteq G : N \text{ es abierto en } G\} = \{e\}\,, \tag{3.70}$$

donde e es el elemento neutro en G.

Demostración. Tomemos $\mathcal{C}$ la clase de grupos finitos. Por el inciso $d)$ de la proposición 3.52, y dado que G es profinito, entonces G es compacto y totalmente disconexo. Luego, del inciso c) de la proposición 3.17, se concluye la ecuación 3.70. □

Proposición 3.57 *Sean G un grupo profinito y e el elemento neutro de G. Si I es un filtro base de subgrupos normales cerrados de G tales que $\bigcap_{N\in I} N = \{e\}$, entonces:*

$$G \simeq \varprojlim (G/N)_{N\in I}. \tag{3.71}$$

Más aún, si H es un subgrupo cerrado de G y K es un subgrupo normal y cerrado de G, entonces se satisface:

$$H \simeq \varprojlim \left(\frac{H}{H\cap N}\right)_{N\in I} \quad y \quad G/K \simeq \varprojlim \left(G/(KN)\right)_{N\in I}.$$

Demostración. Ya que G es profinito, del inciso b) de la observación 3.55 se tiene que G es compacto. A partir de la hipótesis $\bigcap_{N\in I} N = \{e\}$ y de la proposición 3.44, se sigue la afirmación de la ecuación 3.71.

Para demostrar la segunda parte de esta proposición, tomemos H un subgrupo cerrado de G y consideremos la siguiente familia de subgrupos normales cerrados de G :

$$J := \{H\cap N : N \in I\}. \tag{3.72}$$

El conjunto J es un filtro base, en virtud de que I es un filtro de subgrupos normales cerrados. Esto debido a que, si $H\cap N_1, H\cap N_2 \in J$ con $N_1, N_2 \in I$, entonces existe $N_3 \in I$ tales que $N_3 \subseteq N_1 \cap N_2$. Al intersecar de ambos lados con H se sigue que, $H\cap N_3 \subseteq (H\cap N_1)\cap(H\cap N_2)$ y $H\cap N_3 \in J$.
A partir de la hipótesis $\bigcap_{N\in I} N = \{e\}$, se sigue:

$$\bigcap_{M\in J} M = \bigcap_{N\in I} H\cap N = H\cap \bigcap_{N\in I} N = H\cap\{e\} = \{e\}. \tag{3.73}$$

Ya que H es un grupo topológico, del lema 3.43 se obtiene el siguiente sistema inverso $((H/M)_{M\in J}, (\varphi_{ML})_{M\leq' L})$.
Por otro lado, como H es cerrado en G, que es un grupo topológico compacto, de la proposición A.59 concluimos que H es compacto. Ahora, gracias a la proposición 3.44 y a la ecuación 3.73 se concluye que:

$$H \simeq \varprojlim (H/(H\cap N))_{N\in I}.$$

Para la tercera afirmación de esta proposición consideremos la siguiente familia:

$$J' = \{KN : N \in I\}.$$

Notemos que, por la proposición 1.49, los elementos de la familia J' son subgrupos de G. Además, usando el hecho de que G es compacto y Hausdorff, se puede

probar, de forma similar a como se hizo con la familia J (vea ecuación 3.72), que el conjunto J' es un filtro base de subgrupos normales y cerrados de G (vea proposición 3.13 b)) y cada uno de los elementos de J' contiene a K.
Ahora, ya que N y K son subgrupos normales de G para todo $N \in I$, entonces, de la proposición 1.51, se tiene $NK = KN$. Además, por hipótesis tenemos que $\bigcap_{N\in I} N = \{e\}$, y del inciso c) de la proposición 3.13, se sigue:

$$\bigcap_{M\in J'} M = \bigcap_{N\in I} KN = \bigcap_{N\in I} NK = \left(\bigcap_{N\in I} N\right) K = \{e\}\, K = K.$$

De forma similar al lema 3.43, en J' podemos inducir un orden parcial de tal forma que J' sea un conjunto dirigido superiormente:

$$\text{para } KN_1, KN_2 \in J', \text{ se define } KN_1 \leq' KN_2 \text{ si y solo si } N_2 \subseteq N_1.$$

Como $K \trianglelefteq G$, entonces podemos considerar el grupo cociente G/K. Ahora, para cada $KN \in J'$ con $N \in I$, tenemos que $K \trianglelefteq KN \trianglelefteq G$.
Del tercer teorema de isomorfismo (vea teorema 1.58), tenemos que $KN/K \trianglelefteq G/K$. Veamos que $J'' = \{KN/K : N \in I\}$ es un filtro base de subgrupos normales cerrados de G/K. En efecto, consideremos la proyección canónica $p : G \longrightarrow G/K$. Como $p^{-1}(KN/K) = KN$, tenemos que $p^{-1}(G/K \setminus KN/K) = p^{-1}(G/K)\setminus p^{-1}(KN/K) = G\setminus KN$ es abierto de G pues KN es cerrado. Luego, por la definición de la topología cociente en G/K, tenemos que $G/K \setminus KN/K$ es abierto en G/K y así KN/K es un cerrado de G/K.
Ahora, sean $KN_1/K, KN_2/K \in J''$. Como J' es un filtro base de subgrupos normales de G, existe $KN_3 \in J'$ tal que $KN_3 \subseteq KN_1 \cap KN_2$. Por el teorema de la correspondencia (teorema 1.59) tenemos que $KN_3/K \subseteq \Big(KN_1/K\Big) \cap \Big(KN_2/K\Big)$. Por lo tanto, $J'' = \{KN/K : N \in I\}$ es un filtro base de subgrupos normales cerrados de G/K. Se define orden parcial en J'' como sigue:

$$KN_1/K \leq'' KN_2/K \quad \text{si y solo si } N_2 \subseteq N_1.$$

Además, tenemos que

$$\bigcap_{N\in I} (KN/K) = (\bigcap_{N\in I} KN)/K = K/K = \{K\},$$

donde K es el elemento neutro del grupo G/K. Como G es compacto, por proposición 3.14 tenemos que G/K es compacto. Por lo tanto, por proposición 3.44, tenemos un isomorfismo

$$G/K \simeq \varprojlim \left(\frac{G/K}{KN/K}\right)_{N\in I}.$$

Del tercer teorema de isomorfismo tenemos que $\frac{G/K}{KN/K} \simeq G/KN$ y el siguiente diagrama conmuta si $N_2 \subseteq N_1$:

$$\begin{array}{ccc} \frac{G/K}{KN_2/K} & \xrightarrow{\simeq} & G/KN_2 \\ {\scriptstyle \varphi_{\frac{KN_2}{K}\,\frac{KN_1}{K}}}\downarrow & & \downarrow{\scriptstyle \varphi_{KN_1\,KN_2}} \\ \frac{G/K}{KN_1/K} & \xrightarrow{\simeq} & G/KN_1 \end{array}$$

donde los morfismos verticales son definidos de forma similar al lema 3.43. Por lo tanto,

$$G \simeq \varprojlim \left(\frac{G/K}{KN/K}\right)_{N\in I} \simeq \varprojlim (G/(KN))_{N\in I}.$$

□

Proposición 3.58 *Sea $\mathcal{C}$ una clase de grupos finitos de tal forma que es cerrada bajo subgrupos y productos directos arbitrarios. Entonces, los subgrupos cerrados, productos cartesianos y límites inversos de grupos pro-$\mathcal{C}$ son grupos pro-$\mathcal{C}$. Más aún, si $\mathcal{C}$ es una clase cerrada bajo cocientes, y tomamos G un grupo pro-$\mathcal{C}$ y K un subgrupo normal cerrado de G, entonces G/K es un grupo pro-$\mathcal{C}$.*

Demostración. Vea [25, teorema 1.2.5, pág. 19]. □

Si bien el siguiente resultado no se utilizará de forma directa en la tesis, se expone debido a que es un resultado interesante de los grupos profinitos.

Proposición 3.59 *Sean G un grupo profinito, A un espacio topológico discreto y $f : G \longrightarrow A$ una función. Entonces, f es continua si y solo si existe un subgrupo normal abierto K de G y una función $\phi : G/K \longrightarrow A$ continua tal que $f = \phi \circ \pi_K$, donde $\pi_K : G \longrightarrow G/K$ es la proyección canónica.*

Demostración. Primero supongamos que $f : G \longrightarrow A$ es una función continua. Ya que G es un grupo profinito, entonces G es compacto (vea observación 3.55 b)), y de la proposición A.63 se sigue que $f(G)$ es un subespacio compacto de un espacio discreto (vea ejemplo A.3). De esta forma, por la proposición A.56, tenemos que $f(G)$ es finito. Supongamos que $f(G) = \{a_1, ..., a_n\}$.
Ahora, para cada $i = 1, ..., n$ tomemos:

$$O_i := f^{-1}(\{a_i\}) \subseteq G.$$

Notemos que $G = \bigcup_{i=1}^{n} O_i$ y que tal unión es disjunta ya que f es una función. Al ser A un espacio discreto, entonces para todo $i = 1, ..., n$, se tiene que $\{a_i\}$ es un abierto y cerrado en A (vea observación A.10). Ya que f es continua,

se tiene que O_i es un abierto y cerrado en G, por lo que O_i es compacto (vea proposición A.59).
Como G es un grupo profinito, es totalmente disconexo (vea observación 3.55 inciso b)). Del inciso b) de la proposición 3.17, se sigue que cada O_i, con $i \in \{1, ..., n\}$, es unión de clases laterales de subgrupos normales abiertos, y como O_i es compacto, dichas clases son una cantidad finita. Así:

$$O_i = \bigcup_{j=1}^{n_i} x_{ij}K_{ij} \text{ con } x_{ij} \in O_i, K_{ij} \trianglelefteq G \text{ y } n_i \in \mathbb{N}.$$

Tomemos $K = \bigcap_{i,j=1}^{\substack{i=n \\ j=n_i}} K_{ij}$, que es un subgrupo normal en G (vea proposición 1.50), entonces contiene al elemento neutro e de G. De esta forma, para cada $i \in \{1, ..., n\}$ y cada $x \in O_i$, se tiene que:

$$O_i = \bigcup_{x \in O_i} xK \quad \text{con } xK \text{ abierto en } G \text{ por b) de prop. 3.8.} \tag{3.74}$$

Esto ya que, para todo $x \in O_i$ con $i \in \{1, ..., n\}$, se tiene:

$$O_i = \bigcup_{x \in O_i} x\{e\} \subseteq \bigcup_{x \in O_i} xK.$$

Por otro lado, tomemos xK para algún $x \in O_i = \bigcup_{j=1}^{n_i} x_{ij}K_{ij}$. Entonces existe j tal que $x \in x_{ij}K_{ij}$. Así, $xK_{ij} \subseteq x_{ij}K_{ij}$. Además, como $K \subseteq K_{ij}$, entonces:

$$xK \subseteq xK_{ij} \subseteq x_{ij}K_{ij} \subseteq O_i.$$

Al ser O_i compacto, para cada $i \in \{1, ..., n\}$ existen $x_{i1}, ...x_{im_i} \in O_i$ de tal forma que la ecuación 3.74 puede reescribirse como:

$$O_i = \bigcup_{j=1}^{m_i} x_{ij}K.$$

Consideremos la proyección canónica $\pi_K : G \longrightarrow G/K$, con G/K considerado como espacio cociente. Notemos que π_K es continua (vea definición A.42).
Ahora, definamos $\phi : G/K \longrightarrow A$. Para esto, primero recordemos que $G = \bigcup_{i=1}^{n} O_i$ y que tal unión es disjunta. También cada $O_i = \bigcup_{j=1}^{m_i} x_{ij}K$ es unión disjunta pues las clases laterales distintas son disjuntas. Por lo tanto $G = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m_i} x_{ij}K$ y tal unión es disjunta. Además las clases laterales determinadas por K estan dadas como sigue:

$$G/K := \{x_{ij}K\}_{1 \leq i \leq n, 1 \leq j \leq m_i.}$$

Entonces para $x_{ij}K \in G/K$, definimos $\phi(x_{ij}K) = a_i$ (pues $x_{ij}K \subseteq O_i = f^{-1}(\{a_i\})$).
Veamos que $\phi \circ \pi_K = f$. En efecto, sea $g \in G$ y consideremos $\pi_K(g) = gK \in G/K$. Entonces existen i, j tal que $gK = x_{ij}K$. Por lo tanto, $\phi(\pi_K(g)) = \phi(gK) = \phi(x_{ij}K) = a_i$ y además como $g \in gK = x_{ij}K \subseteq O_i$, tenemos que $f(g) = a_i$. Por lo tanto, tenemos que $\phi \circ \pi_K = f$.
Ahora veamos que ϕ es continua.
Sea i fijo, notemos que $\phi^{-1}(\{a_i\}) = \{x_{ij}K\}_{j=1}^{m_i} \subseteq G/K$; veamos que esto es abierto en G/K. Por la definición de la topología en G/K, sabemos que $U \subseteq G/K$ es abierto en G/K si y solo si $\pi_K^{-1}(U)$ es abierto en G. Entonces, basta ver que $\pi^{-1}(\{x_{ij}K\}_{j=1}^{m_i})$ es un abierto de G. Afirmamos que $\pi^{-1}(\{x_{ij}K\}_{j=1}^{m_i}) = O_i$. Sea $g \in G$ tal que $\pi_K(g) = gK \in \{x_{ij}K\}_{j=1}^{m_i}$, entonces existe j tal que $\pi_K(g) = gK = x_{ij}K$. Como $g \in gK = x_{ij}K \subseteq O_i$, tenemos que $g \in O_i$. Por otro lado, si $g \in O_i = \bigcup_{j=1}^{m_i} x_{ij}K$, entonces existe j tal que $g \in x_{ij}K$ y así $g = x_{ij}k$ para algún $k \in K$ y por lo tanto, tenemos que $\pi(g) = gK = (x_{ij}k)K = x_{ij}K$. De esta manera hemos demostrado que $\pi^{-1}(\{x_{ij}K\}_{j=1}^{m_i}) = O_i$ el cual es abierto en G y por lo tanto, tenemos que $\{x_{ij}K\}_{j=1}^{m_i}$ es un abierto de G/K.
Ahora notemos que si $U \subseteq A$ es una abierto de A, entonces $\phi^{-1}(U) = \phi^{-1}(U \cap \{a_1, \cdots, a_n\}) = \phi^{-1}(\{a_{i_1}\}) \cup \cdots \cup \phi^{-1}(\{a_{i_m}\})$ para algunos $i_1, \cdots, i_m \in \{1, \cdots, n\}$. Por lo tanto, $\phi^{-1}(U)$ es abierto y así ϕ es continua. $\square$

Capítulo 4

Teoría de Galois para extensiones infinitas

En este capítulo se muestra que el grupo de Galois $Gal(K/F)$ de una extensión K/F es isomorfo, como grupo, a un límite inverso de grupos de Galois. Luego, en el grupo de Galois se construirá una base para una topología denominada la topología de Krull la cual consta de abiertos y cerrados. Con esto en mente se prueba que $Gal(K/F)$ es un grupo topológico, más aún, un grupo profinito Hausdorff, compacto y totalmente disconexo. Se demuestra el teorema de Krull que nos describe ciertos cerrados de $Gal(K/F)$ y también describe la cerradura de subgrupos de $Gal(K/F)$ con esta topología. Finalmente, el capítulo concluye con el Teorema de Galois para extensiones infinitas y se muestra que cuando K/F es una extensión finita, entonces la topología de Krull de $Gal(K/F)$ coincide con la topología discreta.

4.1. Extensiones infinitas de Galois

El objetivo de esta sección es probar que el grupo de Galois asociado a una extensión infinita de Galois es un grupo profinito y para lograrlo se construirá la topología de Krull en el grupo de Galois. Esto permitirá establecer una relación entre los campos intermedios de la extensión y los subgrupos cerrados del grupo de Galois. Para ello es necesario exponer algunos resultados que nos ayuden a construir la topología de Krull. Para el desarrollo de esta sección se han consultado [14],[25] y [6].

En el desarrollo de esta sección nuestro interés estará centrado en las extensiones K/F que satisfacen ser infinitas y algebraicas. Además, cualquier extensión algebraica K/F se dice que es de Galois si $F = K^{Gal(K/F)}$, esto en

virtud de la definición 2.18. Por la proposición 2.67 podemos caracterizar a las extensiones infinitas de Galois como algebraicas, normales y separables.

Los resultados de esta sección pueden adaptarse a extensiones finitas o infinitas, sin embargo, en el progreso de este capítulo la médula serán las extensiones infinitas.
Tomemos K/F una extensión de Galois y consideremos los conjuntos:

$$\mathcal{F} := \{L : F \subseteq L \subseteq K \text{ y } L/F \text{ es finita y de Galois}\}, \tag{4.1}$$

$$\mathcal{N} := \{Gal(K/L) : L \in \mathcal{F}\}. \tag{4.2}$$

Con la ayuda de los conjuntos $\mathcal{F}$ y $\mathcal{N}$ podemos formar dos sistemas inversos, los cuales veremos que coinciden en términos de la definición 3.27. Para ello primero definamos un orden parcial en $\mathcal{F}$.
Para cualesquiera $L, L' \in \mathcal{F}$, se define:

$$L' \leq L \text{ si y solo si } L' \subseteq L. \tag{4.3}$$

Además, para $L' \leq L$, consideremos el siguiente morfismo de grupos.

$$\begin{aligned} \varphi_{L'L} : Gal(L/F) &\longrightarrow Gal(L'/F), \\ \sigma &\longmapsto \sigma|_{L'} \ . \end{aligned} \tag{4.4}$$

Si $L' \leq L$ entonces el morfismo $\varphi_{L'L}$ está bien definido en el sentido de que efectivamente $\sigma|_{L'} : L' \longrightarrow L'$. Para ver una prueba de esta afirmación puede ver la proposición 4.1.
Es posible probar que $\mathcal{F}$, con el orden parcial descrito en la ecuación 4.3, es un conjunto dirigido superiormente (vea definición 3.23), esto ya que si $L_1, L_2 \in \mathcal{F}$, entonces $L_1/F, L_2/F$ son extensiones finitas de Galois. El composite $L_1(L_2)$ contiene a L_1 y L_2 y además, por los incisos b) y g) de la proposición 2.74, tenemos que $L_1(L_2)/F$ es una extensión finita de Galois, y por lo tanto $L_1(L_2) \in \mathcal{F}$.
Notemos que si dotamos con la topología discreta a los grupos de Galois del dominio y contradominio del morfismo de la ecuación 4.4, entonces el morfismo $\varphi_{L'L}$ es continuo.
Además, si $L'', L', L \in \mathcal{F}$ son tales que $L'' \leq L' \leq L$, entonces, de la observación A.40 se tiene que $\varphi_{L''L} = \varphi_{L''L'} \circ \varphi_{L'L}$.
Por lo tanto, $(Gal(L/F), \varphi_{L'L})_{L \in \mathcal{F}}$ es un sistema inverso indexado por $\mathcal{F}$.

Para crear un sistema inverso indexado por $\mathcal{N}$, requerimos de las siguientes dos proposiciones, que además nos servirán para probar que los sistemas inversos creados a apartir de $\mathcal{F}$ y $\mathcal{N}$ son equivalentes, esto en términos de la definición 3.27.

Proposición 4.1 *Sean K/F una extensión de Galois y $H = Gal(K/L) \in \mathcal{N}$ con $L \in \mathcal{F}$, entonces $L = K^{Gal(K/L)}$ y $H \trianglelefteq Gal(K/F)$. Además, se satisface el siguiente isomorfismo de grupos:*

$$Gal(K/F)/Gal(K/L) \simeq Gal(L/F). \tag{4.5}$$

Así, $[Gal(K/F) : H] < \infty$.

Demostración. Si K/F es de Galois y $H = Gal(K/L) \in \mathcal{N}$ con $L \in \mathcal{F}$, entonces, del corolario 2.70, se sigue que K/L es de Galois, por lo tanto, concluimos $L = K^{Gal(K/L)}$. Consideremos el siguiente morfismo:

$$\begin{aligned} \theta : Gal(K/F) &\longrightarrow Gal(L/F) \ , \\ \sigma &\longmapsto \sigma|_L \ . \end{aligned} \tag{4.6}$$

Notemos que el morfismo θ está bien definido. En efecto, tomemos $\sigma \in Gal(K/F)$ y la siguiente cadena de campos intermedios de K/F:

$$F \subseteq L \subseteq L \subseteq K.$$

Por la definición de θ sabemos que $\theta(\sigma) = \sigma|_L : L \longrightarrow K$. Además, ya que σ fija a F, entonces también lo hace $\theta(\sigma)$. Ahora, ya que L/F es de Galois, entonces, por la proposición 2.66 es en particular una extensión normal. De esta forma, por el inciso c) de la proposición 2.55, tenemos que $Im(\theta(\sigma)) \subseteq L$.
Por lo tanto, $\theta(\sigma) \in Gal(L/F)$ y así, θ está bien definido.
Se deja de ejercicio al lector probar que θ es un morfismo de grupos.
Para probar la suprayectividad de θ, tomemos $\sigma' \in Gal(L/F)$ y la cadena de campos $F \subseteq L \subseteq K \subseteq K$. Notemos que $\sigma' : L \longrightarrow K$. Como la extensión K/F es normal, se sigue, del inciso c) de la proposición 2.55 que existe $\tau \in Gal(K/F)$ tal que $\tau|_L = \sigma'$, es decir, $\theta(\tau) = \sigma'$.
Examinemos el kernel del morfismo θ.

$$\begin{aligned} Ker(\theta) &= \{\sigma \in Gal(K/F) : \sigma|_L = id_L\} \\ &= Gal(K/L) \text{ por ecuación 2.1.} \end{aligned}$$

Por lo tanto, de la observación 1.45, tenemos que $H = Gal(K/L) \trianglelefteq Gal(K/F)$. Ahora, del primer teorema de isomorfismo (vea teorema 1.56) se puede concluir la ecuación 4.5.
Para probar la última parte de nuestro enunciado, observemos que, como $L \in \mathcal{F}$, entonces L/F es una extensión finita y de Galois, así que, por el teorema 2.20, se sigue que

$$|Gal(L/F)| = [L : F] < \infty.$$

De la proposición 1.53 y de la ecuación 4.5 se sigue que:

$$[Gal(K/F) : H] = |Gal(K/F)/Gal(K/L)| = |Gal(L/F)| = [L : F] < \infty.$$

Así, concluimos que $[Gal(K/F) : H] < \infty$. $\square$

Proposición 4.2 *Sean K/F una extensión de Galois, $H_1 = Gal(K/L_1)$ y $H_2 = Gal(K/L_2) \in \mathcal{N}$, con $L_1, L_2 \in \mathcal{F}$. Entonces, $Gal(K/L_1L_2) = H_1 \cap H_2$ y $H_1 \cap H_2 \in \mathcal{N}$.*

Demostración. De los incisos b) y g) de la proposición 2.74 se sigue que L_1L_2/F es finita y de Galois, por lo que $L_1L_2 \in \mathcal{F}$. Así, $Gal(K/L_1L_2) \in \mathcal{N}$.
Ahora, probaremos que $Gal(K/L_1L_2) = H_1 \cap H_2$. Sea $\sigma \in Gal(K/L_1L_2)$, entonces, de la definición 2.10, de campo fijo, se sigue que:

$$\begin{aligned}
\sigma|_{L_1L_2} = id_{L_1L_2} &\iff L_1L_2 \subseteq K^{\{\sigma\}} \\
&\iff L_1, L_2 \subseteq K^{\{\sigma\}}, \text{ pues } L_1, L_2 \subseteq L_1L_2, \text{ vea def. 2.73.} \\
&\iff \sigma|_{L_1} = id_{L_1} \text{y } \sigma|_{L_2} = id_{L_2} \\
&\iff \sigma \in Gal(K/L_1) \text{ y } \sigma \in Gal(K/L_2) \\
&\iff \sigma \in H_1 \cap H_2.
\end{aligned}$$

Es decir, que $Gal(K/L_1L_2) = Gal(K/L_1) \cap Gal(K/L_2)$. Por lo tanto, concluimos que $H_1 \cap H_2 \in \mathcal{N}$. $\square$

Ahora podemos crear un sistema inverso indexado por $\mathcal{N}$, para ello inducimos un orden parcial en $\mathcal{N}$ como sigue:
Sean $H, H' \in \mathcal{N}$, entonces:

$$H' \leq' H \text{ si y solo si } H \subseteq H'. \tag{4.7}$$

Veamos que el orden definido en la ecuación 4.7 hace de $\mathcal{N}$ un conjunto dirigido superiormente, vea definición 3.23.
Por la proposición 4.2, si $H_1, H_2 \in \mathcal{N}$, entonces $H_1 \cap H_2 \in \mathcal{N}$ y además, es claro que $H_1 \cap H_2 \subseteq H_1$ y $H_1 \cap H_2 \subseteq H_2$. Por lo tanto, $H_1 \leq' H_1 \cap H_2$ y $H_2 \leq' H_1 \cap H_2$.
Por otro lado, si $H \in \mathcal{N}$ entonces, por la proposición 4.1 se sigue que H es normal en $Gal(K/F)$, esto significa que tiene sentido tomar el grupo $Gal(K/F)/H$.
Consideremos la siguiente familia de morfismos entre grupos: si $H', H \in \mathcal{N}$ con $H' \leq' H$, entonces, se define el morfismo $\varphi'_{H'H}$ como:

$$\begin{aligned}
\varphi'_{H'H} : Gal(K/F)/H &\longrightarrow Gal(K/F)/H' \\
\sigma H &\longmapsto \sigma H'.
\end{aligned}$$

Por la forma en la que se ha definido el morfismo $\varphi'_{H'H}$ cuando $H' \leq' H$, se tiene que, si $H'' \leq' H' \leq' H$, entonces $\varphi'_{H''H} = \varphi'_{H''H'} \circ \varphi'_{H'H}$. Así, obtenemos el sistema inverso:

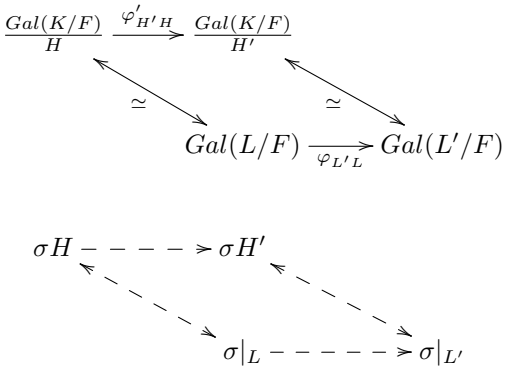
$$(Gal(K/F)/H, \varphi'_{H'H})_{H \in \mathcal{N}}.$$

Además, si $H = Gal(K/L) \in \mathcal{N}$, entonces, de la proposición 4.1 tenemos que:

$$Gal(K/F)/H \simeq Gal(L/F).$$

Es decir, los objetos en el sistema inverso inducido por $\mathcal{N}$ son los mismos objetos (salvo isomorfismo) del sistema inverso inducido por $\mathcal{F}$, vea ecuación 4.4.
Además, si $H, H' \in \mathcal{N}$ son tales que $H' \leq' H$, entonces existen $L, L' \in F$ tales que $H = Gal(K/L)$ y $H' = Gal(K/L')$. Según el orden $\leq'$ de la ecuación 4.7 se tiene que $Gal(K/L) \subseteq Gal(K/L')$. Ahora, ya que K/F es de Galois, entonces, del corolario 2.70 se tiene que K/L y K/L' son de Galois, esto es $L = K^{Gal(K/L)}$ y $L' = K^{Gal(K/L')}$. Del inciso c) del lema 2.13 se sigue que $L' \subseteq L$, es decir, $L' \leq L$ según el orden $\leq$ de la ecuación 4.3. De igual forma se puede corroborar el converso. Esto nos permite concluir que hay una correspondencia biyectiva que respeta los órdenes entre $\mathcal{F}$ y $\mathcal{N}$.

Para exponer lo que se ha dicho y mostrar la igualdad de los morfismos $\varphi_{L'L}$ y $\varphi'_{H'H}$ bajo el isomorfismo dado en la proposición 4.1, consideremos el siguiente diagrama conmutativo cuando $H = Gal(K/L), H' = Gal(K/L') \in \mathcal{N}$ y se satisface que $H' \leq' H$.



Es decir, los sistemas inversos inducidos por $\mathcal{F}$ y $\mathcal{N}$ son equivalentes, en virtud de la definición 3.27.
Por lo tanto, se concluye que $\varprojlim \left(\dfrac{Gal(K/F)}{H} \right)_{H \in \mathcal{N}} \simeq \varprojlim Gal(E/F)_{E \in \mathcal{F}}$.

Observación 4.3 *Sean K/F una extensión de Galois, $E \in \mathcal{F}$ un campo arbitrario y el siguiente morfismo:*

$$\begin{aligned} \phi_E : Gal(K/F) &\longrightarrow Gal(E/F) \\ \sigma &\longmapsto \sigma|_E. \end{aligned}$$

Puede probarse que ϕ_E es un homomorfismo de grupos bien definido de forma similar a como se probó que el morfismo θ de la ecuación 4.6 está bien definido.

Además, por el inciso c) de la proposición 2.55, tenemos que ϕ_E es un morfismo suprayectivo. Para ver una prueba de estas afirmaciones vea el inicio de la prueba de la proposición 4.1.
Por lo tanto, $\{\phi_E\}_{E\in\mathcal{F}}$ es una familia de morfismos suprayectivos de grupos, el lector puede probar que $(Gal(K/F),\phi_E)_{E\in\mathcal{F}}$ es compatible (vea definición 3.28), con el sistema inverso $(Gal(E/F),\varphi_{E'E})_{E\in\mathcal{F}}$. Ahora, por la propiedad universal del producto (vea proposición A.49), tenemos que existe una única función:

$$\varrho : Gal(K/F) \longrightarrow \prod_{E\in\mathcal{F}} Gal(E/F)$$
$$\sigma \longmapsto (\sigma|_E)_{E\in\mathcal{F}} .$$

Usando la caracterización del límite inverso de un sistema inverso, vea inciso b) de la proposición 3.31, se deja como ejercicio al lector probar que se satisface $Im(\varrho) \subseteq \varprojlim(Gal(E/F))_{E\in\mathcal{F}}$.

Proposición 4.4 *Sean K/F una extensión de Galois y $\alpha_1,...,\alpha_n \in K$, entonces existe $E \in \mathcal{F}$ tal que $\alpha_1,...,\alpha_n \in E$.*

Demostración. Ya que la extensión de Galois K/F es algebraica, entonces, para todo $i \in \{1,...,n\}$, existe $q_i(x) := min(F,\alpha_i) \in F[x]$. Consideremos el polinomio $f(x) = \prod_{i=1}^{n} min(F,\alpha_i) \in F[x]$. Notemos que K contiene una raíz para cada polinomio irreducible $q_i(x)$ con $i \in \{1,...,n\}$. Ahora, ya que K/F de Galois, entonces, por la proposición 2.67, se tiene en particular que K/F es normal. Ahora, del inciso d) de la proposición 2.55 se sigue que K contiene un campo de descomposición para $q_i(x)$. Sea X el conjunto de todas las raíces de cada $q_i(x)$ con $i \in \{1,...,n\}$, en particular $\alpha_i \in X$ para todo $i \in \{1,...,n\}$. Tomemos el campo $E = F(X)$ y notemos que E es campo de descomposición de $f(x)$, y por lo tanto, la extensión E/F es normal. Además, de la proposición 1.179 se sigue que $[E:F] < \infty$.
Como K/F es de Galois, en particular es separable, y de la proposición 2.62 se sigue que E/F es separable, por lo tanto E/F es una extensión finita de Galois. Concluimos que $E \in \mathcal{F}$ y es tal que para todo $i \in \{1,...,n\}$, $\alpha_i \in E$. □

Corolario 4.5 *Si K/F es una extensión de Galois, entonces*

$$K = \bigcup_{E\in\mathcal{F}} E. \tag{4.8}$$

Demostración. Si $\alpha \in K$, de la proposición 4.4 existe $L \in \mathcal{F}$ tal que satisface $\alpha \in L \subseteq \bigcup_{E\in\mathcal{F}} E$. Por lo tanto, $K \subseteq \bigcup_{E\in\mathcal{F}} E$.

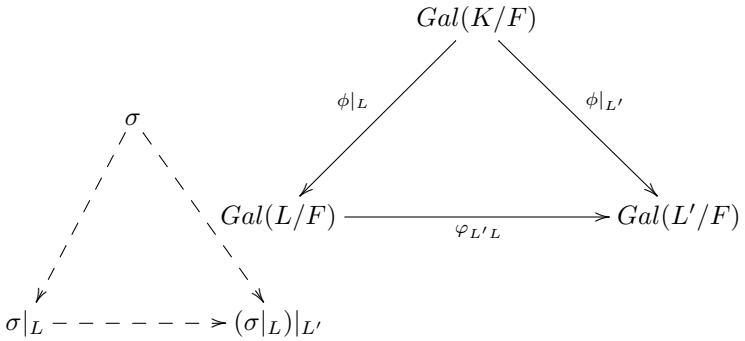
Por otro lado, para todo $L \in \mathcal{F}$, $F \subseteq L \subseteq K$ y de esta forma, se concluye que $L \subseteq \bigcup_{E \in \mathcal{F}} E \subseteq K$. Por lo tanto, se satisface la ecuación 4.8. $\square$

Proposición 4.6 *El siguiente homomorfismo de grupos es un isomorfismo de grupos:*

$$\varrho : Gal(K/F) \longrightarrow \varprojlim (Gal(L/F))_{L \in \mathcal{F}}$$

$$\sigma \longmapsto (\sigma|_L)_{L \in \mathcal{F}} .$$

Demostración. De la observación 4.3 se sigue que ϱ es una función bien definida y es fácil ver que también es un morfismo de grupos.
Por otro lado, notemos que $(Gal(K/F), \phi_L)_{L \in \mathcal{F}}$ es un sistema compatible con el sistema inverso $(Gal(L/F), \varphi_{L'L})_{L \in \mathcal{F}}$ (vea ecuación 4.3), esto queda demostrado considerando la observación A.40 y por el siguiente diagrama conmutativo cuando $L' \leq L$:



A continuación, probaremos que el morfismo ϱ es inyectivo y suprayectivo.
Sea $\sigma \in Gal(K/F)$ tal que $\varrho(\sigma) = (id_E)_{E \in \mathcal{F}}$, entonces $(\sigma|_E)_{E \in \mathcal{F}} = (id_E)_{E \in \mathcal{F}}$, se sigue que para todo $E \in \mathcal{F}$, $\sigma|_E = id_E = id_K|_E$. Ahora, si $\alpha \in K$, del corolario 4.5 se sigue que $\alpha \in E$ para algún $E \in \mathcal{F}$. Así, $\sigma(\alpha) = \sigma|_E(\alpha) = id_E(\alpha) = id_K(\alpha)$. Concluimos que $\sigma = id_K$ y, por lo tanto $ker(\varrho) = \{id_K\}$, esto prueba que ϱ es inyectiva.
Por otra parte, sea $(\gamma_E)_{E \in \mathcal{F}} \in \varprojlim (Gal(E/F))_{E \in \mathcal{F}}$ con $\gamma_E \in Gal(E/F)$ para todo $E \in \mathcal{F}$.
Construyamos un morfismo en $Gal(K/F)$ de la siguiente forma: sea $\alpha \in K$, de la proposición 4.4 se sigue que existe $E \in \mathcal{F}$ tal que $\alpha \in E$. Tomemos $\gamma_E \in Gal(E/F)$ dado por la $E-$ésima coordenada de $(\gamma_E)_{E \in \mathcal{F}}$. Definamos $\tau : K \longrightarrow K$ como:

$$\tau(\alpha) = \gamma_E(\alpha).$$

Probemos que la definición de $\tau(\alpha)$ no depende del campo intermedio E de K/F tales que $\alpha \in E$.

Sean $L_1, L_2 \in \mathcal{F}$ tal que $\alpha \in L_1$ y $\alpha \in L_2$. Entonces, $\alpha \in L_1 \cap L_2$ y además $F \subseteq L_1 \cap L_2 \subseteq L_1$. Ya que L_1/F es finita y de Galois, de la proposición 2.72 se sigue que $(L_1 \cap L_2)/F$ es una extensión finita y de Galois. Por lo tanto, $L_1 \cap L_2 \in \mathcal{F}$. Recordemos que tenemos el siguiente diagrama conmutativo cada vez que $E \leq L$

$$\begin{array}{ccc} \varprojlim_{E\in\mathcal{F}} \big(\mathrm{Gal}(E/F)\big) & \xrightarrow{\phi_L} & \mathrm{Gal}(L/F) \\ & \searrow^{\phi_E} & \downarrow{\scriptstyle \varphi_{EL}} \\ & & \mathrm{Gal}(E/F) \end{array}$$

Sea $E := L_1 \cap L_2$, en particular, para $E \leq L_1$ y $E \leq L_2$, tenemos los siguientes diagramas conmutativos:

$$\begin{array}{ccc} \varprojlim_{E\in\mathcal{F}} Gal\big(E/F\big) & \xrightarrow{\phi_{L_1}} & Gal\big(L_1/F\big) \\ & \searrow^{\phi_E} & \downarrow{\scriptstyle \varphi_{EL_1}} \\ & & Gal\big(E/F\big) \end{array}$$

$$\begin{array}{ccc} \varprojlim_{E\in\mathcal{F}} Gal\big(E/F\big) & \xrightarrow{\phi_{L_2}} & Gal\big(L_2/F\big) \\ & \searrow^{\phi_E} & \downarrow{\scriptstyle \varphi_{EL_2}} \\ & & Gal\big(E/F\big) \end{array}$$

Como $(\gamma_E)_{E\in\mathcal{F}} \in \varprojlim_{E\in\mathcal{F}} \big(\mathrm{Gal}(E/F)\big)$, entonces, de los dos diagramas anteriores tenemos que

$$\gamma_{L_1}|_E = \varphi_{EL_1}(\gamma_{L_1}) = \varphi_{EL_1}\Big(\phi_{L_1}\Big((\gamma_E)_{E\in\mathcal{F}}\Big)\Big) = \phi_E\Big((\gamma_E)_{E\in\mathcal{F}}\Big) = \gamma_E$$

$$\gamma_{L_2}|_E = \varphi_{EL_2}(\gamma_{L_2}) = \varphi_{EL_2}\Big(\phi_{L_2}\Big((\gamma_E)_{E\in\mathcal{F}}\Big)\Big) = \phi_E\Big((\gamma_E)_{E\in\mathcal{F}}\Big) = \gamma_E$$

Por lo tanto, $\gamma_{L_1}|_E = \gamma_{L_2}|_E$. Como $\alpha \in E = L_1 \cap L_2$, concluimos que $\gamma_{L_1}(\alpha) = \gamma_{L_2}(\alpha)$, y por consiguiente, tenemos que la definición de $\tau(\alpha)$ no depende del campo intermedio $E \in \mathcal{F}$ de la extensión K/F tal que $\alpha \in E$.
Claramente $\tau \neq 0$. Se deja al lector probar que τ es un morfismo entre campos, luego del inciso b) de la observación 1.106 se obtiene que τ es inyectiva.
Ahora, tomemos $\beta \in K$, entonces por la proposición 4.4 existe $E \in \mathcal{F}$ con $\beta \in E$. Tomemos $\gamma_E \in Gal(E/F)$, la $E-$ésima coordenada de $(\gamma_E)_{E\in\mathcal{F}}$. Como γ_E es suprayectivo, existe $\alpha \in E \subseteq K$ tal que $\gamma_E(\alpha) = \beta$, apartir de esto es claro que $\tau(\alpha) = \beta$, de esta forma se sigue que τ es suprayectivo. En conclusión, τ es un isomorfismo.

Por la construcción de τ se sigue que $\tau|_F = id_F$, así, $\tau \in Gal(K/F)$.
Por lo tanto:

$$\varrho(\tau) = (\tau|_E)_{E\in\mathcal{F}} = (\gamma_E)_{E\in\mathcal{F}}.$$

Concluimos que ϱ es un isomorfismo de grupos. □

4.2. Topología de Krull

Para comenzar esta sección se le pide al lector recuerde la definiciones de los conjuntos $\mathcal{F}$ y $\mathcal{N}$ (vea ecuaciones 4.1 y 4.2 respectivamente).

Proposición 4.7 *Sea K/F una extensión de Galois, entonces:*

$$\bigcap_{H\in\mathcal{N}} H = \{id_K\}.$$

Donde id_K es el neutro del grupo $Gal(K/F)$.

Demostración. Sean $\tau \in \bigcap_{H\in\mathcal{N}} H$ y $\alpha \in K$. De la proposición 4.4 se sigue que existe $E \in \mathcal{F}$ tal que $\alpha \in E$. Tomemos $N = Gal(K/E) \in \mathcal{N}$. Por lo tanto $\tau \in N$, esto implica que τ deja fijo a E, en particular, $\tau(\alpha) = \alpha$. De esta forma, obtenemos que $\tau = id_K$. Concluimos que $\bigcap_{H\in\mathcal{N}} H = \{id_K\}$. □

Si $H = Gal(K/E) \in \mathcal{N}$ es un subgrupo del grupo de Galois $Gal(K/F)$ y $\sigma \in Gal(K/F)$, entonces, el siguiente lema ofrece una caracterización de la clase lateral σH.

Lema 4.8 *Si K/F es una extensión de Galois, entonces, para todo $\sigma \in Gal(K/F)$ y $H = Gal(K/E) \in \mathcal{N}$ con $E \in \mathcal{F}$, se verifica:*

$$\sigma H = \{\tau \in Gal(K/F) : \tau|_E = \sigma|_E\}.$$

Demostración. Tenemos que $\tau' \in \sigma H$ si y solo si $\tau' H = \sigma H$, si y solo si $\sigma^{-1} \circ \tau' \in H$, si y solo si $(\sigma^{-1} \circ \tau')|_E = id_E$, si y solo si $\sigma|_E = \tau'|_E$ si y solo si $\tau' \in \{\tau \in Gal(K/F) : \tau|_E = \sigma|_E\}$. □

Observación 4.9 *Para todo $\sigma \in Gal(K/F)$ y $H = Gal(K/E) \in \mathcal{N}$ con $E \in \mathcal{F}$, se cumple que $\sigma \in \sigma H$. En otras palabras, $\sigma H \neq \emptyset$.*

Corolario 4.10 *Para cualquier $\sigma \in Gal(K/F)$, se satisface:*

$$\bigcap_{H\in\mathcal{N}} \sigma H = \{\sigma\}. \tag{4.9}$$

Demostración. Sea $\tau \in \bigcap_{H\in\mathcal{N}} \sigma H$, entonces, para todo $H \in \mathcal{N}$ se tiene que $\tau \in \sigma H$ y así $\tau H = \sigma H$, finalmente $\sigma^{-1}\tau \in H$ para todo $H \in \mathcal{N}$. De la proposicion 4.7 obtenemos que $\sigma^{-1}\tau = id_K$ y por lo tanto, $\sigma = \tau$.
Por otro lado, de la observación 4.9 tenemos que $\{\sigma\} \subseteq \sigma H$ para todo $H \in \mathcal{N}$, por lo tanto $\{\sigma\} \subseteq \bigcap_{H\in\mathcal{N}} \sigma H$.
De esta forma, se satisface la ecuación 4.9. □

Ahora estamos preparados para definir la topología de Krull y con los resultados previos, mostrar que efectivamente es una topología.

Lema 4.11 *El siguiente conjunto de clases forma una base para una topología en* $Gal(K/F)$.

$$\mathcal{B} = \{\sigma H : \sigma \in Gal(K/F) \text{ y } H \in \mathcal{N}\}.$$

Demostración. Por el corolario 2.69 tenemos que F/F es una extensión de Galois de grado 1, así, $Gal(K/F) \in \mathcal{N}$ y por lo tanto, la clase lateral $id_K Gal(K/F) = Gal(K/F) \in \mathcal{B}$. Ahora, para probar que $\mathcal{B}$ es una base para una topología en $Gal(K/F)$ usaremos el corolario A.20.
Sean $\sigma_1 H, \sigma_2 H' \in \mathcal{B}$, y $\tau \in \sigma_1 H \cap \sigma_2 H'$ entonces:

$$\tau H = \sigma_1 H \text{ y } \tau H' = \sigma_2 H'. \tag{4.10}$$

Notemos que:

$$\begin{aligned}
\alpha \in \tau(H \cap H') &\iff \tau(H \cap H') = \alpha(H \cap H') \\
&\iff \alpha^{-1}\tau \in (H \cap H') \\
&\iff \alpha^{-1}\tau \in H \text{ y } \alpha^{-1}\tau \in H' \\
&\iff \tau H = \alpha H \text{ y } \tau H' = \alpha H' \\
&\iff \alpha \in \tau H \text{ y } \alpha \in \tau H' \\
&\iff \alpha \in \tau H \cap \tau H'.
\end{aligned}$$

Por lo tanto, se concluye que $\tau(H \cap H') = \tau H \cap \tau H' = \sigma_1 H \cap \sigma_2 H'$. Además, de la proposición 4.2, se sigue que $H \cap H' \in \mathcal{N}$, por lo tanto $\tau \in \tau H \cap \tau H' = \sigma_1 H \cap \sigma_2 H' \in \mathcal{B}$.
Al conjunto $\mathcal{B}$ podríamos unirle el conjunto $\{\emptyset\}$, sin embargo, se puede probar que $\emptyset \in \mathcal{B}$. En efecto, sea $H \in \mathcal{N}$ con $H \neq G = Gal(K/F)$, es decir, que $2 \leq [Gal(K/F) : H]$. Por lo tanto, podemos tomar $\sigma_1, \sigma_2 \in G$, tales que $\sigma_1 H \neq \sigma_2 H$, de esta manera, de la proposición 1.28, se sigue que $\emptyset = \sigma_1 H \cap \sigma_2 H \in \mathcal{B}$, así concluimos que $\emptyset \in \mathcal{B}$.
Del corolario A.20 se sigue que $\mathcal{B}$ es una base para una topología única en $Gal(K/F)$, que además consiste de todas las uniones de elementos de $\mathcal{B}$. □

Observación 4.12 *La observación 4.9 y el lema 4.11 nos permiten concluir que, para un elemento $\sigma \in Gal(K/F)$, un abierto básico que contiene a σ es una clase de la forma σH con $H \in \mathcal{N}$.*
En virtud de la proposición A.19 se tiene que $U \subseteq Gal(K/F)$ es abierto si y solo si, para todo $\sigma \in U$, existe $H \in \mathcal{N}$ tal que $\sigma \in \sigma H \subseteq U$.

Observación 4.13 *Para todo $Gal(K/L) = H \in \mathcal{N}$, con $L \in \mathcal{F}$, se tiene que:*

$$id_K H = \{\tau \in Gal(K/F) : \tau|_L = id_K|_L\} = H.$$

Por lo tanto, $id_K \in H$ y todo elemento de $\mathcal{N}$ es un abierto básico de $Gal(K/F)$ es decir, $\mathcal{N} \subseteq \mathcal{B}$. Además, de las proposiciones 4.1 y 4.2 se sigue que $\mathcal{N}$ es un filtro base de subgrupos normales abiertos en $Gal(K/F)$ (vea definición 3.42). En lo sucesivo, probaremos que los elementos de $\mathcal{N}$ son cerrados.

Corolario 4.14 *Si $\sigma H \in \mathcal{B}$ es tal que $id_K \in \sigma H$, entonces $\sigma H = H$.*

Demostración. Si $id_K \in \sigma H$ entonces $id_K H = \sigma H$. De la observación 4.13 se sigue que $H = \sigma H$. □

En otras palabras, la observación 4.13 y el corolario 4.14 nos dicen que los abiertos básicos de $\mathcal{B}$, que contienen al elemento neutro de $Gal(K/F)$ son precisamente los elementos de $\mathcal{N}$.

Definición 4.15 *Sea K/F una extensión de Galois. Se define la **topología de Krull** en el grupo $Gal\big(K/F\big)$ como aquella que tiene por base al siguiente conjunto:*

$$\mathcal{B} = \{\sigma H : \sigma \in Gal(K/F) \text{ y } H \in \mathcal{N}\}.$$

Observación 4.16 *Sea $L \in \mathcal{F} := \{L : F \subseteq L \subseteq K \text{ y } L/F \text{ es finita y de Galois}\}$, entonces por proposición 4.1, tenemos que $H := \mathrm{Gal}(K/L) \trianglelefteq \mathrm{Gal}(K/F)$ y $|\mathrm{Gal}(K/F)/H| = n < \infty$. Luego,*

$$\mathrm{Gal}(K/F)/H = \{H, \sigma_1 H, \cdots, \sigma_{n-1} H\},$$

con $\sigma_i \in \mathrm{Gal}(K/F)$ para $i = 1, \cdots, n-1$ (ver figura 4.1). Notemos entonces que el conjunto $\mathcal{B}$ de la definición 4.15 puede ser descrito como sigue:

$$\mathcal{B} = \bigcup_{H \in \mathcal{N}} \mathrm{Gal}(K/F)/H.$$

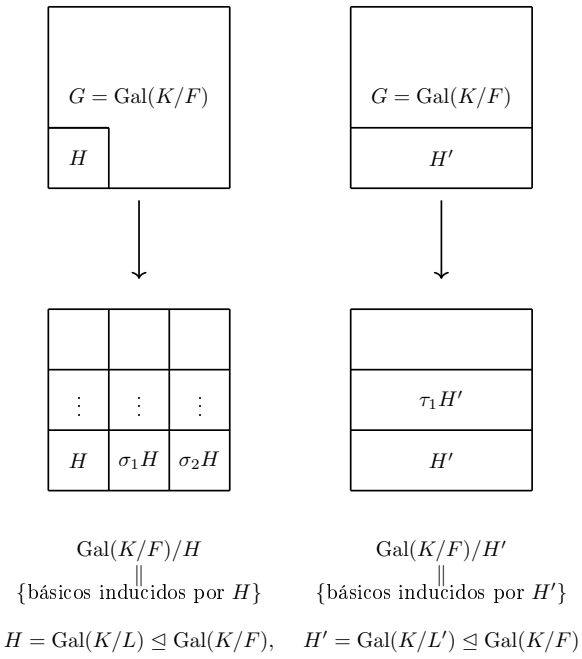


Figura 4.1: Descripción de los básicos en $\mathcal{B}$ inducidos por dos elementos distintos $H = \mathrm{Gal}(K/L)$ y $H' = \mathrm{Gal}(K/L')$ en $\mathcal{N}$.

Por lema 4.8, tenemos las siguientes igualdades:

$$\begin{aligned} H &= \{\alpha \in \mathrm{Gal}(K/F) : \alpha|_L = 1_L\}, \\ \sigma_1 H &= \{\alpha \in \mathrm{Gal}(K/F) : \alpha|_L = \sigma_1|_L\}, \\ &\vdots \\ \sigma_{n-1} H &= \{\alpha \in \mathrm{Gal}(K/F) : \alpha|_L = \sigma_{n-1}|_L\}. \end{aligned}$$

Además, para $L, L' \in \mathcal{F}$ con $L' \subseteq L$, tenemos que $H = \mathrm{Gal}(K/L) \leq H' = \mathrm{Gal}(K/L')$ (ver figura 4.1).

En lo sucesivo, si K/F es una extensión de Galois, nos referiremos al grupo $Gal(K/F)$ como un espacio topológico con la topología de Krull.

El lema 4.8 nos ayuda a visualizar de manera informal cómo son los abiertos básicos en la topología de Krull. Tomemos $\sigma H \in \mathcal{B}$ con $H = Gal(K/L)$ y $F \subseteq L \subseteq K$ con L/F finita y de Galois. Si σH es un abierto *grande* es porque hay muchos elementos $\tau \in Gal(K/F)$ tales que al restringirse a L se *asemejan* a $\sigma|_L$, es decir, $\sigma|_L = \tau|_L$. Esta cantidad de elementos sólo puede aumentar si L se asemeja a F, lo cual significa que $[L : F]$ se aproxima a 1, en cuyo caso $[K : L] = |Gal(K/L)| = |H|$ es muy grande (es decir, que L se *aleja de* K).
De igual forma, un abierto σH con $H = Gal(K/L)$, es un abierto básico *pequeño* si L está alejado de F, es decir si $[L : F]$ es *grande*, y por lo tanto $[K : L]$ es pequeña, es decir que L es un campo intermedio de K/F muy parecido a K.
En pocas palabras, un abierto σH con $H = Gal(K/L)$ y $L \in \mathcal{F}$, es muy grande si proviene de una extensión K/L grande, es decir que L está lejos de ser K. Y un abierto básico σH es pequeño si H es el grupo de Galois de una extensión K/L con L un campo intermedio muy próximo a K.
Además, notemos que si $H \in \mathcal{N}$ es un subgrupo abierto de $Gal(K/F)$, de la proposición 4.1 se sigue que $[Gal(K/F) : H] < \infty$. Por lo tanto, existen $\sigma_1, ..., \sigma_n \in Gal(K/F)$ tales que $Gal(K/F) = H \cup \sigma_1 H \cdots \cup \sigma_n H$, de esta forma se tiene que $Gal(K/F) \setminus H = \sigma_1 H \cup \cdots \cup \sigma_n H$, es decir, $Gal(K/F) \setminus H$ es unión de abiertos básicos, por lo tanto es un abierto en $Gal(K/F)$. Así, concluimos que para todo $H \in \mathcal{N}, H$ es cerrado.
Además, de la proposición 4.2, se sigue que $\mathcal{N}$ es un filtro base de subgrupos normales abiertos y cerrados en $Gal(K/F)$ (vea definición 3.42).

Finalmente observemos que, si $\tau H \in \mathcal{B}$, entonces por el mismo razonamiento utilizado anteriormente se sigue que existen $\sigma_1, ..., \sigma_n \in Gal(K/F)$ tal que $Gal(K/F) = \bigcup_{i=1}^{n} \sigma_i H$ y por lo tanto $\tau H = \sigma_j H$ para un $j \in \{1, ..., n\}$. De esta forma $Gal(K/F) \setminus \tau H = \bigcup_{i \neq j} \sigma_i H$. Concluyendo que τH es cerrado en $Gal(K/F)$.
Con estos argumentos hemos probado el siguiente resultado:

Corolario 4.17 *La topología de Krull consta de una base $\mathcal{B}$ de abiertos y cerrados.*

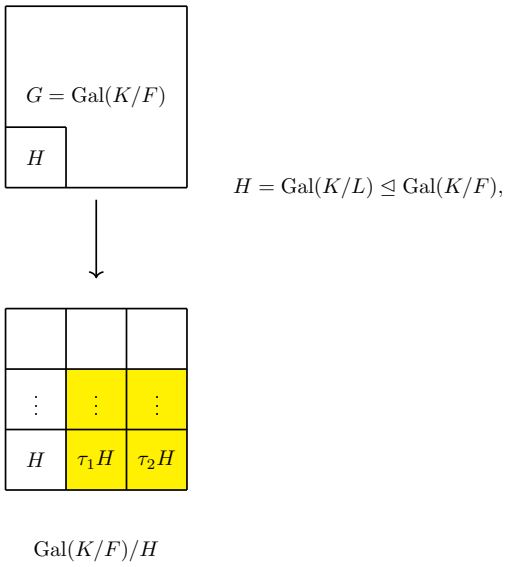


Figura 4.2: En la parte sombreada están las clases laterales $\tau_i H$ con $\tau_i \in G$ tal que $\tau_i|_L = \sigma$. Así, los elementos de G que están en las clases laterales de la parte sombreada forman un subconjunto de $\mathrm{Gal}(K/F)$ y representa a $\varrho^{-1}(\pi_L^{-1}(\{\sigma\})) = \bigcup_{\substack{\tau \in \mathrm{Gal}(K/F) \\ \tau|_L = \sigma}} \tau H$

El conjunto $\mathcal{N}$ tiene la siguiente propiedad:

Proposición 4.18 *Sea K/F una extensión de Galois. El conjunto*

$$\mathcal{N} = \{Gal(K/E) : E/F \text{ es de Galois y } [E:F] < \infty\}$$

es una base local (vea definición A.21) de $id_K \in Gal(K/F)$.

Demostración. Por la observación 4.13 se sigue que todo elemento de $\mathcal{N}$ es un abierto de $Gal(K/F)$ y que cada uno de ellos contiene a $\{id_K\}$.
Ahora, sea U un abierto de $Gal(K/F)$ tal que $id_K \in U$. Ya que $\mathcal{B}$ es una base para $Gal(K/F)$, entonces, existe un abierto básico $\sigma H \in \mathcal{B}$ tal que $id_K \in \sigma H \subseteq U$. Del corolario 4.14 se sigue que $\sigma H = H$. Concluimos que $\mathcal{N}$ es una base local de id_K. □

El siguiente resultado ofrece una caracterización del grupo de Galois de una extensión de Galois K/F. Además nos brindará más información topológica del grupo $Gal(K/F)$ considerado como un espacio topológico con la topología de Krull.
Recordemos que, para todo $E \in \mathcal{F}$, $Gal(E/F)$ es considerado un grupo topológico con la topología discreta, de esta forma, el grupo $\prod_{E\in\mathcal{F}} Gal(E/F)$ es un grupo topológico en virtud del teorema 3.20. Por lo tanto, $\varprojlim Gal(E/F)_{E\in\mathcal{F}}$ es un grupo topológico con la topología inducida del producto. Por las proposiciones 3.37 inciso a), y 3.31 inciso b), tenemos que una base para la topología de $\varprojlim Gal(E/F)_{E\in\mathcal{F}}$, está dada por el conjunto:

$$\left\{\phi_E^{-1}(U) : U \text{ es abierto de } Gal(E/F), E \in \mathcal{F}\right\} =$$
$$\left\{\pi_E^{-1}(U) : U \text{ es abierto de } Gal(E/F), E \in \mathcal{F}\right\},$$

donde $\phi_E = \pi_E|_{\varprojlim Gal(E/F))_{E\in\mathcal{F}}} : \varprojlim Gal(E/F)_{E\in\mathcal{F}} \longrightarrow Gal(E/F)$ es la $E-$ésima proyección canónica restringida a $\varprojlim Gal(E/F)_{E\in\mathcal{F}}$.
Ahora, como $Gal(E/F)$ posee la topología discreta y es finito, entonces cada abierto U de $Gal(E/F)$ es una unión finita de elementos de $Gal(E/F)$. Luego, $\pi_E^{-1}(U)$ es una unión finita de abiertos de la forma $\pi_E^{-1}(\{\sigma\})$ con $\sigma \in Gal(E/F)$.

Considerando $Gal(K/F)$ como espacio topológico con la topología de Krull, el isomorfismo de grupos ϱ de la proposición 4.6 es un isomorfismo de grupos topológicos como muestra la siguiente proposición.

Proposición 4.19 *Si K/F es una extensión de Galois, entonces, el morfismo de grupos*

$$\varrho : Gal(K/F) \longrightarrow \varprojlim(Gal(E/F))_{E\in\mathcal{F}} , \tag{4.11}$$

$$\sigma \longmapsto (\sigma|_E)_{E\in\mathcal{F}} .$$

es un isomorfismo de espacios topológicos.

Demostración. En primer lugar, probaremos que ϱ es continua, para ello tomemos un abierto básico $\pi_L^{-1}(\{\sigma\})$ en el codominio de ϱ con $\sigma \in Gal(L/F)$ y $L \in \mathcal{F}$. Probemos que $\varrho^{-1}(\pi_L^{-1}(\{\sigma\}))$ es un abierto de $Gal(K/F)$, lo haremos obteniendo una descripción de este conjunto.
Sea $\tau \in \varrho^{-1}(\pi_L^{-1}(\{\sigma\}))$, entonces $\varrho(\tau) = (\tau|_E)_{E\in\mathcal{F}} \in \pi_L^{-1}(\{\sigma\})$ y de esta manera $\pi_L\left((\tau|_E)_{E\in\mathcal{F}}\right) = \tau|_L \in \{\sigma\}$. Es decir, los elementos de $\varrho^{-1}(\pi_L^{-1}(\{\sigma\}))$ constan de elementos de $Gal(K/F)$ que son extensiones de $\sigma : L \longrightarrow L$. Además, de la observación 4.9 se tiene que $\tau \in \tau Gal(K/L)$. Esto demuestra la siguiente contención:

$$\varrho^{-1}(\pi_L^{-1}(\{\sigma\})) \subseteq \bigcup_{\substack{\tau\in Gal(K/F)\\ \tau|_L=\sigma}} \tau Gal(K/L). \tag{4.12}$$

Por otro lado, si tomamos cualquier $\tau \in Gal(K/F)$ tal que $\tau|_L = \sigma$, el lema 4.8 nos dice que los elementos en $\tau Gal(K/L)$ son elementos de $Gal(K/F)$ que son extensiones de σ. Por lo tanto, se satisface la siguiente contención (ver figura 4.2):

$$\bigcup_{\substack{\tau\in Gal(K/F)\\ \tau|_L=\sigma}} \tau Gal(K/L) \subseteq \varrho^{-1}(\pi_L^{-1}(\{\sigma\})). \tag{4.13}$$

De las ecuaciones 4.12 y 4.13 se sigue:

$$\varrho^{-1}(\pi_L^{-1}(\{\sigma\})) = \bigcup_{\substack{\tau\in Gal(K/F)\\ \tau|_L=\sigma}} \tau Gal(K/L). \tag{4.14}$$

El conjunto de la ecuación 4.14 es un abierto de $Gal(K/F)$ por ser unión de abiertos básicos de la topología de Krull (vea definición 4.15). Por lo tanto, el morfismo ϱ es continuo.
De la proposición 4.6 sabemos que ϱ es biyectiva, así, para probar que ϱ es un homeomorfismo, basta probar que ϱ es abierta.
Sea σH un abierto básico de $Gal(K/F)$ con $\sigma \in Gal(K/F)$ y $H = Gal(K/L)$ con $L \in \mathcal{F}$. Luego, se satisface lo siguiente:

$$\varrho(\sigma H) = \pi_L^{-1}(\{\sigma|_L\}), \tag{4.15}$$

donde $\pi_L : \varprojlim_{E\in\mathcal{F}} \big(\mathrm{Gal}(E/F)\big) \longrightarrow \mathrm{Gal}(L/F)$ es la L-ésima proyección.
La ecuación 4.15 se satisface ya que si tomamos $\varrho(\tau) \in \varrho(\sigma H)$ con $\tau \in \sigma H$, entonces $\tau \in Gal(K/F)$ y $\tau|_L = \sigma|_L$, esto por lema 4.8. Por lo tanto $\pi_L(\varrho(\tau)) = \pi_L((\tau|_E)_{E\in\mathcal{F}}) = \tau|_L = \sigma|_L$, de esta manera concluimos que $\varrho(\tau) \in \pi_L^{-1}(\{\sigma|_L\})$. Por otro lado, sea $x \in \pi_L^{-1}(\sigma|_L) \subseteq \varprojlim_{E\in\mathcal{F}} Gal(E/F)$. Por la proposición 4.6 se tiene que ϱ es biyectiva. Luego, existe $\tau \in Gal(K/F)$ tal que $x = \varrho(\tau) = (\tau|_E)_{E\in\mathcal{F}}$. Ahora, como $x = \varrho(\tau) \in \pi_L^{-1}(\{\sigma|_L\})$, concluimos que $\tau|_L = \sigma|_L$. Así, por el lema 4.8, tenemos que $\tau \in \sigma H$. Esto nos dice que $x = \varrho(\tau) \in \varrho(\sigma H)$, probándose la contención $\pi_L^{-1}(\{\sigma|_L\}) \subseteq \varrho(\sigma H)$. Por lo tanto, se satisface la ecuación 4.15.
De esta forma, ϱ es un morfismo abierto. Por la proposición A.41 concluimos que ϱ es un isomorfismo de espacios topológicos. □

Corolario 4.20 *Si K/F es una extensión de Galois, entonces $Gal(K/F)$ es un grupo topológico.*

Demostración. En efecto, por el inciso c) de la proposición 3.31, se obtiene que $\varprojlim Gal(E/F)_{E\in\mathcal{F}}$ es un grupo topológico, y de la proposición 4.19, se tiene el siguiente isomorfismo de espacios topológicos:

$$Gal(K/F) \simeq \varprojlim_{E\in\mathcal{F}} Gal\big(K/E\big). \tag{4.16}$$

Por lo tanto, $Gal(K/F)$ es un grupo topológico. □

Observación 4.21 *El isomorfismo de la ecuación 4.16 es un isomorfismo de grupos topológicos.*

Corolario 4.22 *Si K/F es una extensión de Galois, entonces $Gal(K/F)$ es un grupo profinito (vea definición 3.54) y por lo tanto $Gal(K/F)$ es Hausdorff, compacto y totalmente disconexo.*

Demostración. Por la observación 4.21 se sigue que $Gal(K/F)$ es un profinito. La segunda parte del enunciado se sigue del inciso b) de la observación 3.55. □

Dada una extensión de Galois K/F, el siguiente resultado ofrece información sobre los subgrupos cerrados de $Gal(K/F)$ y las cerraduras de sus subgrupos. Esta importante descripción, debida a Wolfgang Krull (1899-1971), nos permitirá finalmente establecer una correspondencia biyectiva entre los campos intermedios de una extensión K/F y los subgrupos cerrados de $Gal(K/F)$.

Teorema 4.23 (W. Krull) *Consideremos K/F una extensión de Galois y el grupo de Galois asociado $Gal(K/F)$ con la topología de Krull. Entonces, se satisfacen las siguientes condiciones:*

a) Para todo campo intermedio E de K/F, se tiene que $Gal(K/E)$ es un subgrupo cerrado de $Gal(K/F)$.

b) Para todo subgrupo H de $Gal(K/F)$, $\overline{H} = Gal(K/K^H)$.

c) Si H es un cerrado de $Gal(K/F)$, entonces $H = Gal(K/K^H)$.

Demostración.

a) Tomemos E un campo intermedio de la extensión K/F. Probaremos que $Gal(K/F) \setminus Gal(K/E)$ es abierto de $Gal(K/F)$. Si este conjunto es vacío, no hay algo que probar. Supongamos que existe $\sigma \in Gal(K/F) \setminus Gal(K/E)$, es decir, que $\sigma \in Aut(K)$, pero σ no fija a E, por lo que existe $\alpha \in E$ de tal forma que $\sigma(\alpha) \neq \alpha$.
Por la proposición 4.4, existe $L \in \mathcal{F}$ un campo intermedio de K/F tal que $\alpha \in L$. Consideremos el abierto básico $\sigma Gal(K/L)$ (vea definición 4.15). Afirmamos que:

$$\sigma Gal(K/L) \cap Gal(K/E) = \emptyset. \tag{4.17}$$

La ecuación 4.17 se satisface ya que si tomamos $\tau \in Gal(K/F)$ que pertenece a esta intersección, del lema 4.8 tenemos:

$$\tau|_L = \sigma|_L \text{ y } \tau|_E = id_E.$$

Como $\alpha \in E \cap L$, al evaluar tendríamos que $\tau|_L(\alpha) = \sigma|_L(\alpha) \neq \alpha$ y que $\tau|_E(\alpha) = id_E(\alpha) = \alpha$, lo cual es una contradicción, pues $\tau|_{E\cap L}$ es función. Para evitar contradicciones se debe satisfacer la ecuación 4.17.
De la observación 4.9 y de la ecuación 4.17, tenemos

$$\sigma \in \sigma Gal(K/L) \subseteq Gal(K/F) \setminus Gal(K/E).$$

De la proposición A.7 se sigue que $Gal(K/F) \setminus Gal(K/E)$ es un abierto y por lo tanto $Gal(K/E)$ es un subgrupo cerrado de $Gal(K/F)$.

b) A partir del inciso d) del lema 2.13 se sigue que $H \subseteq Gal(K/K^H)$. Ahora, por el inciso a) de la proposición 4.23 obtenemos que $Gal(K/K^H)$ es un cerrado de $Gal(K/F)$. Por lo tanto:

$$\overline{H} \subseteq Gal(K/K^H). \tag{4.18}$$

Basta probar que $Gal(K/K^H) \subseteq \overline{H}$. Para lograrlo haremos uso de la proposición A.13, es decir, probaremos que para $\sigma \in Gal(K/K^H)$ y U un abierto de $Gal(K/F)$ con la topología de Krull, tal que $\sigma \in U$, se tiene que $U \cap H \neq \emptyset$. Basta ver que si tomamos σN un abierto básico con $N \in \mathcal{N}$ (notemos que por la observación 4.12, $\sigma \in \sigma N$), entonces $\sigma N \cap H \neq \emptyset$.

Sean $\sigma \in Gal(K/K^H)$ y σN con $N \in \mathcal{N}$ un abierto básico en la topología de Krull.

De la definición de $\mathcal{N}$ (vea ecuación 4.2), se sigue que $N = Gal(K/L)$ donde L/F es una extensión finita de Galois. Consideremos el grupo $Gal(L/F)$. Como L/F es finita y de Galois, del teorema 2.20 se tiene:

$$|Gal(L/F)| = [L : F] < \infty.$$

Consideremos el morfismo de la ecuación 4.6 en la proposición 4.1:

$$\begin{aligned} \theta : Gal(K/F) &\longrightarrow Gal(L/F) \\ \tau &\longmapsto \tau|_L \end{aligned}$$

Como $H \leq Gal(K/F)$, entonces:

$$H_0 := \theta(H) = \{\rho|_L : \rho \in H\} \tag{4.19}$$

es un subgrupo de $Gal(L/F)$. Luego, podemos considerar el campo fijo asociado a H_0 :

$$\begin{aligned} L^{H_0} &= \{a \in L : \gamma(a) = a, \text{ para todo } \gamma \in H_0\} \\ &= \{a \in L : \rho|_L(a) = a, \text{ para todo } \rho \in H\}. \end{aligned}$$

Afirmamos que:

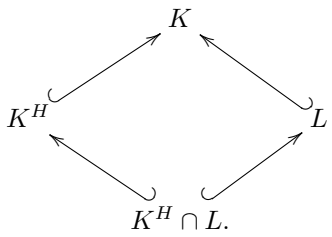
$$L^{H_0} = K^H \cap L$$

donde $K^H := \{k \in K : \rho(k) = k, \text{ para todo } \rho \in H\}$.
En efecto, sea $a \in L^{H_0}$, entonces, $a \in L$ y $\rho|_L(a) = a$ para todo $\rho \in H$. Así, $\rho(a) = a$ para todo $\rho \in H$ y por lo tanto, $a \in K^H$. Como $a \in L$, se sigue que $a \in K^H \cap L$. Esto prueba que $L^{H_0} \subseteq K^H \cap L$.
Ahora, consideremos $a \in K^H \cap L$. Entonces, $a \in L$ y $\rho(a) = a$ para todo $\rho \in H$. Esto nos dice que $a \in L$ y que $\rho|_L(a) = a$ para todo $\rho \in H$. Así, tenemos que $a \in L^{H_0}$, probándose la contención $K^H \cap L \subseteq L^{H_0}$. Por lo tanto, hemos demostrado la igualdad $L^{H_0} = K^H \cap L$.
Ahora, por el teorema fundamental de Galois para extensiones finitas, vea teorema 2.75, aplicado a la extensión finita de Galois L/F, tenemos que H_0 se corresponde de forma biyectiva con su campo fijo L^{H_0}, esto es:

$$H_0 = Gal(L/L^{H_0}) = Gal\left(L/(K^H \cap L)\right)$$

Como $\sigma \in Gal(K/K^H) \subseteq Gal(K/F)$, tenemos que $\sigma : K \longrightarrow K$ es tal que $\sigma|_{K^H} = id_{K^H}$. Sea $\theta(\sigma) = \sigma|_L \in Gal(L/F)$ y consideremos el siguiente

diagrama de contenciones de campos:



Entonces, tenemos que:

$$(\sigma|_L)\,|_{K^H\cap L} = (\sigma|_{K^H})\,|_{K^H\cap L} = (id_{K^H})|_{K^H\cap L} = id_{K^H\cap L}.$$

Por lo tanto, $\sigma|_L \in Gal\left(L/(K^H \cap L)\right) = H_0$. Luego, por definición de H_0, vea ecuación 4.19, tenemos que existe $\rho \in H$ tal que $\rho|_L = \sigma|_L$. Por el lema 4.8 concluimos que $\rho \in \sigma N$. Por lo tanto, $\rho \in \sigma N \cap H$, probándose que $\sigma N \cap H \neq \emptyset$. Así, tenemos que $Gal(K/K^H) \subseteq \overline{H}$ y como ya habíamos mostrado que $Gal(K/K^H)$ es un cerrado de $Gal(K/F)$ que contiene a H, vea ecuación 4.18, concluimos que:

$$Gal(K/K^H) = \overline{H}.$$

c) Es inmediato a partir de b).

□

4.3. Teorema de Galois para extensiones infinitas

Recordemos que, en virtud de la proposición 2.67, definimos las extensiones de Galois como algebraicas, normales y separables.

Teorema 4.24 (Teorema de Galois para Extensiones Infinitas.)
Sea K/F una extensión de Galois y el grupo topológico $Gal(K/F)$. Se cumplen las siguientes condiciones:

a) (Correspondencia de Galois)
Las siguientes funciones determinan correspondencias biyectivas que invierten inclusiones.

$$\Psi : \{E : F \subseteq E \subseteq K\} \longrightarrow \{H : H \text{ es subgrupo cerrado en } Gal(K/F)\}\,,$$
$$E \longmapsto Gal(K/E)\,.$$

$$\Phi : \{H : H \text{ es cerrado en } Gal(K/F)\} \longrightarrow \{E : F \subseteq E \subseteq K\}\,,$$
$$H \longmapsto K^H\,.$$

b) Si E es un campo intermedio de K/F y H un subgrupo cerrado de $Gal(K/F)$ tal que E se corresponde con H de forma biyectiva mediante las funciones Φ y Ψ, entonces, los siguientes enunciados son equivalentes:

1) $[Gal(K/F) : H] < \infty$.

2) $[E : F] < \infty$.

3) H es un subgrupo abierto de $Gal(K/F)$.

c) Bajo las mismas hipótesis del inciso anterior y si una de las condiciones $1), 2)$ o $3)$ del inciso b) se satisface, entonces:

$$[Gal(K/F) : H] = [E : F].$$

d) Para cualquier subgrupo H de $Gal(K/F)$ de la forma $H = Gal(K/L)$ con L un campo intermedio de la extensión K/F se tiene que:

$$H \text{ es normal en } Gal(K/F) \text{ si y sólo si } L/F \text{ es de Galois.}$$

Más aún, si $H \trianglelefteq Gal(K/F)$, entonces también se satisface el siguiente isomorfismo de grupos

$$Gal(K/F)/H \simeq Gal(L/F). \tag{4.20}$$

e) Si $Gal(K/L) \trianglelefteq Gal(K/F)$ y el grupo $Gal(K/F)/Gal(K/L)$ está dotado de la topología cociente (vea definición A.42), entonces, el isomorfismo de la ecuación 4.20, dado por:

$$\nu : Gal(K/F)/Gal(K/L) \longrightarrow Gal(L/F)$$
$$\sigma Gal(K/L) \longmapsto \theta(\sigma) = \sigma|_L \ ,$$

es un homeomorfismo, donde al grupo $Gal(L/F)$ se le dota de la topología de Krull.

f) Para cualquier subgrupo H de $G = Gal(K/F)$ se tiene que $K^H = K^{\overline{H}}$.

Demostración.

a) De forma similar al teorema fundamental de Galois para extensiones finitas (vea lema 2.13), las funciones Ψ y Φ invierten inclusiones. Ahora verifiquemos que determinan una correspondencia biyectiva, es decir, que Ψ y Φ son inversas una de la otra.
Tomemos E un campo intermedio de la extensión de Galois K/F, entonces,

del corolario 2.70 se tiene que K/E es de Galois, es decir, $E = K^{Gal(K/E)}$. Se sigue que:

$$(\Phi \circ \Psi)(E) = \Phi(Gal(K/E)) = K^{Gal(K/E)} = E.$$

Por otro lado, tomemos H un subgrupo cerrado de $Gal(K/F)$.

$$\begin{aligned}(\Psi \circ \Phi)(H) &= \Psi(K^H) \\ &= Gal(K/K^H) \\ &= \overline{H} \text{ por inciso b) teorema } 4.23. \\ &= H \text{ pues } H \text{ es cerrado.}\end{aligned}$$

Concluimos que Φ y Ψ determinan una correspondencia biyectiva entre los campos intermedios de la extensión K/F y los subgrupos cerrados de $Gal(K/F)$.

b) En la demostración de este inciso supondremos que E es un campo intermedio de la extensión K/F y $H = Gal(K/E)$ es un subgrupo cerrado del grupo $Gal(K/F)$.

1) $\Longrightarrow$ 3) Ya que H es un subgrupo cerrado de índice finito del grupo topológico $Gal(K/F)$, entonces, del inciso c) de la proposición 3.8 se sigue que H es abierto de $Gal(K/F)$.

3) $\Longrightarrow$ 2) Supongamos que $H = Gal(K/E)$ es un subgrupo abierto del grupo $Gal(K/F)$. Ya que H es subgrupo, se tiene $id_K \in H$. Por la proposición 4.18 tenemos que $\mathcal{N}$ es una base local de id_K, luego, existe $Gal(K/L) \in \mathcal{N}$ con $L \in \mathcal{F}$ y $id_K \in Gal(K/L) \subseteq H$. De la correspondencia de Galois (vea inciso a) del teorema 4.24) se sigue que $L = K^{Gal(K/L)}$ (ya que $Gal(K/L)$ también es cerrado de $Gal(K/F)$ por inciso a) del teorema 4.23).
Afirmamos que $E \subseteq L \subseteq K$. Esto ya que si tomamos $\alpha \in E$ y $\sigma \in Gal(K/L)$, entonces $\sigma \in H$ ya que $Gal(K/L) \subseteq H$; y por lo tanto σ fija a E, en particular fija a α y de esta manera tenemos que $\alpha \in K^{Gal(K/L)} = L$.
Como $L \in \mathcal{F}$, entonces $[L : F] < \infty$. Además, como tenemos la cadena de campos $F \subseteq E \subseteq L \subseteq K$, de la proposición 1.146 se sigue:

$$[L : F] = [L : E] \cdot [E : F] < \infty$$

Concluimos que $[E : F] < \infty$.

2) $\Longrightarrow$ 1) Supongamos que $[E : F] < \infty$, por lo tanto, existen $\alpha_1, ..., \alpha_n \in K$ tal que $E = F(\alpha_1, ..., \alpha_n)$. De la proposición 4.4, existe $L \in \mathcal{F}$ tal que $\alpha_1, ..., \alpha_n \in L$. Ya que $F \subseteq L$, de lo anterior se sigue que $F \subseteq E \subseteq L$.

De la correspondencia de Galois, vea inciso a) del teorema 4.24, se sigue que:

$$Gal(K/L) \leq Gal(K/E) \leq Gal(K/F).$$

De esta forma concluimos que:

$$[Gal(K/F) : Gal(K/E)] \leq [Gal(K/F) : Gal(K/L)] < \infty.$$

En efecto, la segunda desigualdad se satisface en virtud de la proposición 4.1, ya que $Gal(K/L)$ con $L \in \mathcal{F}$ es un abierto básico en la topología de Krull sobre $Gal(K/F)$ (vea observación 4.13). Y así, la primera desigualdad se verifica por la proposición 1.31.

c) Si cualquiera de los enunciados equivalentes del inciso b) del teorema 4.24 se satisface, podemos asumir en particular que $[E : F] < \infty$, luego existen $\alpha_1, ..., \alpha_n \in K$ tal que $E = F(\alpha_1, ..., \alpha_n)$. Ahora, por la proposición 4.4 existe $L \in \mathcal{F}$ tal que $\alpha_1, ..., \alpha_n \in L$. De esta forma se tiene la siguiente cadena de contenciones: $F \subseteq E \subseteq L \subseteq K$. Ya que la correspondencia de Galois invierte inclusiones, vea inciso a) del teorema 4.24, obtenemos:

$$Gal(K/L) \leq Gal(K/E) \leq Gal(K/F). \tag{4.21}$$

Ya que $L \in \mathcal{F}$, entonces $Gal(K/L) \in \mathcal{N}$. Luego, de la proposición 4.1 se tiene que $Gal(K/L) \trianglelefteq Gal(K/F)$ y el siguiente isomorfismo:

$$Gal(K/F)/Gal(K/L) \simeq^{\nu} Gal(L/F).$$

Donde el morfismo $\theta : Gal(K/F) \longrightarrow Gal(L/F)$ dado por $\theta(\sigma) = \sigma|_L$ hace que ν definido como $\nu(\sigma Gal(K/L)) = \theta(\sigma)$, para todo $\sigma \in Gal(K/F)$, sea un isomorfismo.

Por el teorema de la correspondencia biyectiva (vea teorema 1.59) aplicado a la ecuación 4.21, tenemos que:

$$Gal(K/E)/Gal(K/L) \leq Gal(K/F)/Gal(K/L),$$

y por lo tanto $N := \nu(Gal(K/E)/Gal(K/L)) = \{\rho|_L : \rho \in Gal(K/E)\}$ es un subgrupo de $Gal(L/F)$.
Veamos que $L^N = E$. En efecto, sea $\rho|_L \in N$ con $\rho \in Gal(K/E)$. Entonces $(\rho|_L)|_E = \rho|_E = id_E$ y por lo tanto $E \subseteq L^N$. Por otro lado, sea $a \in L^N$, entonces $a \in L$ y para todo $\rho \in Gal(K/E), \rho|_L(a) = a$. Por la correspondencia biyectiva de Galois (vea inciso a) del teorema 4.24), sabemos que $Gal(K/E)$ se corresponde de forma biyectiva con E, es decir, $E = K^{Gal(K/E)}$. Por lo tanto, $L^N \subseteq L \cap K^{Gal(K/E)} = L \cap E = E$, esto ya que $E \subseteq L$. Así, hemos probado que $L^N = E$.

Ya que la extensión L/F es finita y de Galois y E y N se corresponden de forma biyectiva, entonces, del inciso a) del teorema fundamental de Galois para extensiones finitas 2.75, se sigue que $|N| = [L : E] < \infty$. Por otro lado, como $H = Gal(K/E)$ y $H/Gal(K/L)$ es isomorfo a N vía ν, tenemos que $|H/Gal(K/L)| = |N| = [L : E] < \infty$. Por lo tanto:

$$\begin{aligned}
[Gal(K/F) : H] &= [Gal(K/F)/Gal(K/L) : H/Gal(K/L)] \text{ Por a) teo. 1.59} \\
&= \frac{|Gal(K/F)/Gal(K/L)|}{|H/Gal(K/L)|} \text{ Por teo. 1.34 de Lagrange} \\
&= \frac{|Gal(L/F)|}{[L : E]} \text{ Vea prop. 4.1} \\
&= \frac{[L : F]}{[L : E]} \text{ Por teorema 2.20} \\
&= [E : F] \text{ Por proposición 1.146.}
\end{aligned}$$

Concluimos que $[Gal(K/F) : H] = [E : F]$.

d) Supongamos que $H = Gal(K/L) \trianglelefteq Gal(K/F)$. Ya que K/F es de Galois, de la proposición 2.67 se sigue que K/F es normal y separable. Como $F \subseteq L \subseteq K$, se sigue, de la proposición 2.62 que L/F es separable. Basta probar que la extensión L/F es normal y para ello aplicaremos el inciso d) de la proposición 2.55. Tomemos $p(x) \in F[x]\backslash\{0\}$ un polinomio irreducible sobre F y $\alpha \in L$ una raíz de $p(x)$.
Como la extensión K/F es normal, se sigue que K contiene un campo de descomposición de $p(x)$. Sea $\beta \in K$ cualquier otra raíz de $p(x)$, probaremos que $\beta \in L$. Ya que id_F es un automorfismo, en virtud del teorema 2.51 dicho automorfismo puede extenderse a un automorfismo $\tau : K \longrightarrow K$ tal que $\tau|_F = id_F$ y puede elegirse de tal forma que $\tau(\alpha) = \beta$. Sea $\sigma \in H$ cualquier elemento, entonces:

$$\sigma(\beta) = (\sigma \circ \tau)(\alpha) = \tau\left(\tau^{-1}\sigma\tau\right)(\alpha) = \tau(\alpha) = \beta.$$

Esto ya que $H \trianglelefteq G$ y por lo tanto, $\tau^{-1}\sigma\tau \in H$; y todos los elementos de H fijan a L, en particular fijan a $\alpha \in L$. Luego, hemos probado que $\sigma(\beta) = \beta$ para todo $\sigma \in H$ y $\beta \in K$ raíz de $p(x)$. De esta forma, se concluye que $\beta \in K^{Gal(K/L)}$. Por la correspondencia de Galois (vea inciso a) del teorema 4.24) se sabe que $L = K^{Gal(K/L)}$ y así $\beta \in L$. Es decir, que todas las raíces de $p(x)$ pertenecen a L, y por lo tanto L contiene un campo de descomposición para $p(x)$. Concluimos que L/F es una extensión normal. De la proposición 2.67 obtenemos que L/F es una extensión de Galois.

Por otro lado, supongamos que L/F es una extensión de Galois. Probaremos que $H = Gal(K/L) \trianglelefteq Gal(K/F)$.

Consideremos el siguiente morfismo de grupos:

$$\theta : Gal(K/F) \longrightarrow Gal(L/F) \ ,$$
$$\sigma \longmapsto \sigma|_L \ .$$

De la misma manera a como se hizo en la proposición 4.1 puede probarse que el morfismo θ está bien definido en virtud de que L/F es, en particular, una extensión normal (vea proposición 2.67).
Entonces:

$$ker\,(\theta) = \{\sigma \in Gal(K/F) : \sigma|_L = id_L\} = Gal(K/L).$$

De la observación 1.45 se sigue que $Gal(K/L)$ es un subgrupo normal de $Gal(K/L)$.
Para probar que θ es suprayectiva, sea $\tau \in Gal(L/F)$ un elemento cualquiera. Como K/F es normal, entonces K es el campo de descomposición de una familia de polinomios con coeficientes en F. De esta forma por el teorema 2.51, tenemos que τ puede extenderse a un automorfismo único $\sigma : K \longrightarrow K$ tal que $\sigma|_L = \tau$. Por lo tanto $\sigma \in Gal(K/F)$ satisface $\theta(\sigma) = \sigma|_L = \tau$. De esta forma θ es suprayectiva. Del primer teorema de isomorfismo (vea teorema 1.56) concluimos el siguiente isomorfismo de grupos:

$$Gal(K/F)/Gal(K/L) \simeq Gal(L/F). \tag{4.22}$$

Sea $H := Gal(K/L)$ un subgrupo normal de $Gal(K/F)$. Para la demostración del inciso e), recordemos que en el primer teorema de isomorfismo (vea teorema 1.56), el isomorfismo ν hace conmutar el siguiente diagrama, esto es, $\theta = \nu \circ \pi$

$$\begin{array}{ccc} Gal(K/F) & \xrightarrow{\ \theta\ } & Gal(L/F) \\ {\scriptstyle \pi}\downarrow & \nearrow_{\nu} & \\ Gal(K/F)/Gal(K/L) & & \end{array} \tag{4.23}$$

donde π es la proyección canónica al grupo cociente.

e) Ya que $H = Gal(K/L) \trianglelefteq Gal(K/F)$, entonces, por el inciso d) del teorema 4.24 se sigue que L/F es una extensión de Galois y por lo tanto, al grupo $Gal(L/F)$ se le puede dotar de la topología de Krull (vea definición 4.15).
Recordemos que $\theta = \nu \circ \pi$, vea diagrama 4.23. Ahora, para probar la continuidad de ν, basta probar que θ es una función continua, esto en virtud del inciso b) de la proposición A.43

Sea $\rho Gal(L/E)$ un abierto básico en $Gal(L/F)$ tal que $F \subseteq E \subseteq L$ y E/F una extensión finita y de Galois con $\rho \in Gal(L/F)$. Entonces $Gal(K/E)$ es un abierto básico en $Gal(K/F)$ (vea observación 4.13).
Afirmamos que:

$$\theta^{-1}\big(Gal(L/E)\big) = Gal\big(K/E\big). \tag{4.24}$$

Esto ya que si $\tau \in \theta^{-1}\left(Gal(L/E)\right)$ entonces $\tau \in Gal(K/F)$ y $\theta(\tau) = \tau|_L \in Gal(L/E)$, es decir que $(\tau|_L)|_E = \tau|_E = id_E$ y por lo tanto $\tau \in Gal(K/E)$. Por otro lado, si tomamos $\sigma \in Gal(K/E)$, entonces $\sigma|_E = id_E$ y al aplicar θ tenemos que $\theta(\sigma) = \sigma|_L : L \longrightarrow K$. Ahora, como L/F es una extensión de Galois y $F \subseteq E \subseteq L$, por la proposición 2.70 se sigue que L/E es de Galois. Por la proposición 2.67, tenemos que L/E es una extensión normal. Consideremos la cadena de campos $E \subseteq L \subseteq L \subseteq K$. Ya que $\sigma|_L : L \longrightarrow K$ y L/E es normal, por el inciso c) de la proposición 2.55, se tiene que $\sigma|_L : L \longrightarrow L$ y de esta forma concluimos que $\sigma \in \theta^{-1}\left(Gal(L/E)\right)$. Hemos probado que se satisface la ecuación 4.24.
Ya que $\rho \in Gal(L/F)$, por el teorema 2.51 se sigue que ρ puede extenderse a un automorfismo $\eta : K \longrightarrow K$ tal que $\eta|_L = \rho$ Además, $\eta|_F = (\eta|_L)|_F = \rho|_F = id_F$, por lo tanto $\eta \in Gal(K/F)$. Entonces se tiene:

$$\begin{aligned}
\theta^{-1}\left(\rho Gal(L/E)\right) &= \theta^{-1}\left(\{\tau' \in Gal(L/F) : \tau'|_E = \rho|_E\}\right) \\
&= \{\tau \in Gal(K/F) : \theta(\tau) \in Gal(L/F) \text{ y } \tau|_E = \rho|_E\} \\
&= \{\tau \in Gal(K/F) : \tau|_E = \rho|_E = (\eta|_L)|_E\} \\
&= \{\tau \in Gal(K/F) : \tau|_E = \eta|_E\} \\
&= \eta Gal(K/E).
\end{aligned}$$

Donde la primera y la última igualdad se satisfacen por el lema 4.8.
Por lo tanto, $\theta^{-1}\left(\rho Gal(L/E)\right) = \eta Gal(K/E)$ y de esta forma concluimos que θ es continua. Además, por el inciso b) de la proposición A.43, y al ser $\theta = \nu \circ \pi$ continua, se llega a que ν es continua.

Veamos que θ es un morfismo cerrado. En efecto, primero notemos que por el corolario 4.22 el grupo $Gal(K/F)$ es compacto. Ahora, sea C un subconjunto cerrado de $Gal(K/F)$. Por la proposición A.59, C es compacto. Luego, como el morfismo θ es continuo, tenemos que $\theta(C)$ es un subconjunto compacto de $Gal(L/F)$. Por el corolario 4.22, $Gal(L/F)$ es Hausdorff y de la proposición A.61 se concluye que $\theta(C)$ es cerrado de $Gal(L/F)$. Así, θ es un morfismo cerrado.

Probemos que ν es un morfismo cerrado. Consideremos C un cerrado en el espacio $X := Gal(K/F)/Gal(K/L)$, entonces $X \setminus C$ es abierto en X

y por definición de topología cociente (vea definición A.42), se sigue que $\pi^{-1}(X \setminus C) = \pi^{-1}(X) \setminus \pi^{-1}(C) = Gal(K/F) \setminus \pi^{-1}(C)$ es un abierto de $Gal(K/F)$, por lo tanto, $\pi^{-1}(C)$ es un cerrado de $Gal(K/F)$. Como π es suprayectiva, tenemos que $\pi\left(\pi^{-1}(C)\right) = C$. Por lo tanto, $\nu(C) = \nu\left(\pi\left(\pi^{-1}(C)\right)\right) = \theta\left(\pi^{-1}(C)\right)$ y como θ es cerrada, concluimos que $\nu(C)$ es un cerrado de $Gal(L/F)$.

De la proposición A.41 se sigue que ν es un homeomorfismo.

f) Notemos que:

$$\begin{aligned} K^{\overline{H}} &= K^{Gal(K/K^H)} \text{ por inciso b) de teorema 4.23} \\ &= K^H \text{ por la correspondencia de Galois (vea inciso a) teorema 4.24).} \end{aligned}$$

□

La topología de Krull en el grupo $Gal(K/F)$ para K/F una extensión de Galois es demasiado general, de tal forma que cuando la extensión K/F es finita, dicha topología coincide con la topología discreta, obteniendo el teorema de Galois para extensiones finitas. Es decir, tenemos el siguiente resultado.

Corolario 4.25 *Si K/F una extensión de Galois finita, entonces la topología de Krull en el grupo $Gal(K/F)$ es la topología discreta.*

Demostración. Ya que K/F es finita y de Galois, entonces del ejercicio 2.77 tenemos que sólo hay una cantidad finita de campos intermedios en K/F, por lo tanto el conjunto $\mathcal{N}$ (vea ecuación 4.2) posee una cantidad finita de elementos. De la proposición 4.7 se tiene lo siguiente:

$$\bigcap_{H \in \mathcal{N}} H = \left\{id_{Gal(K/F)}\right\} \tag{4.25}$$

El conjunto de la ecuación 4.25 es una intersección finita de abiertos (vea observación 4.13), por lo tanto es un abierto en $Gal(K/F)$. Así, $\{id_{Gal(K/F)}\}$ es un subgrupo abierto. De la proposición 3.11 se sigue que la topología de Krull en $Gal(K/F)$ coincide con la topología discreta.

Más aún, si $Gal(K/L) \leq Gal(K/F)$ es cualquier subgrupo, entonces es un cerrado de $Gal(K/F)$. Por lo tanto, de la correspondencia del inciso a) del teorema 4.24, se sigue que hay una correspondencia biyectiva entre los subgrupos de $Gal(K/F)$ y todos los campos intermedios de K/F. Es decir, si la extensión de Galois K/F es finita, la topología de Krull coincide con la topología discreta en $Gal(K/F)$, de tal forma que se obtiene el caso particular del teorema fundamental de la teoría clásica de Galois (vea teorema 2.75). □

Apéndice A

A.1. Elementos de Topología

En esta sección haremos mención de los resultados de topología que son necesarios para el desarrollo de la sección 3.1. Citaremos las demostraciones de las proposiciones. Al lector interesado en repasar las pruebas le recomendamos ver [5].
En lo sucesivo, si X es un conjunto cualquiera usaremos el símbolo $\wp(X)$ para indicar el conjunto potencia de X.

Definición A.1 *Sea X un conjunto. Se dice que $\tau \subseteq \wp(X)$ es una* ***topología*** *en X si se satisfacen las siguientes condiciones:*

a) $\emptyset \in \tau$ *y* $X \in \tau$.

b) Si $\{U_i\}_{i\in I} \subseteq \tau$, *entonces* $\bigcup_{i\in I} U_i \in \tau$.

c) Si $U, V \in \tau$, *entonces* $U \cap V \in \tau$.

A los elementos de τ les llamaremos ***abiertos en X*** *y a los elementos de X les llamaremos* ***puntos****. En caso de que exista una topología τ sobre un conjunto X, diremos que (X, τ) es un* ***espacio topológico.*** *En caso de que no haya confusiones escribiremos simplemente X entendiendo que X es un espacio topológico con una topología τ.*

Observación A.2 *Notemos que si* $\{U_1, \ldots, U_n\} \subseteq \tau$, *entonces* $\bigcap_{i=1}^{n} U_i \in \tau$.

Dado un conjunto, hay una variada cantidad de subconjuntos de la potencia que cumplen las condiciones para ser una topología, esto induce una retícula de topologías con mínimo y máximo respecto a la contención. Estos elementos se definen a continuación.

Ejemplo A.3 *Sea X un conjunto. Se define la* ***topología discreta*** *en X como $\tau = \wp(X)$, en cuyo caso se dice que $(X, \wp(X))$ es un* ***espacio discreto****. La* ***topología indiscreta*** *para X es $\tau = \{\emptyset, X\}$, en este caso decimos que $(X, \{\emptyset, X\})$ es un* ***espacio indiscreto****.*

A pesar de que las topologías del ejemplo A.3 se describen de forma simple, en el corolario 4.25, se expone un caso no trivial de la topología discreta.

Definición A.4 *Sean X un espacio topológico y τ_1, τ_2 dos topologías sobre X. Se dice que τ_1 es más* ***gruesa*** *que τ_2 si $\tau_1 \subseteq \tau_2$. De igual forma, τ_2 es más* ***fina*** *que τ_1 si $\tau_1 \subseteq \tau_2$.*

Observación A.5 *Naturalmente, el conjunto de todas las topologías sobre un conjunto X queda ordenado parcialmente por la relación $\subseteq$, donde la topología más gruesa es la indiscreta y la más fina es la topología discreta sobre X.*

Definición A.6 *Sean X un espacio topológico, $x \in X$ y $V \subseteq X$. Se dice que V es una* ***vecindad*** *para x si existe $U \in \tau$ tal que $x \in U \subseteq V$.*
Al conjunto de todas las vecindades de $x \in X$ lo abreviaremos por $\mathcal{N}_x$.

Los conjuntos abiertos quedan caracterizados de la siguiente forma:

Proposición A.7 *Sean X un espacio topológico y $V \subseteq X$. Entonces, V es abierto en X si y solo si, para todo $x \in V$, existe $U \subseteq X$ abierto tal que $x \in U \subseteq V$.*
En otras palabras, V es abierto en X si y solo si es vecindad para cada uno de sus puntos.

Demostración. Se deja de ejercicio al lector. □

Definición A.8 *Sean X un espacio topológico y $F \subseteq X$. Se dice que F es* ***cerrado en X*** *si $X \setminus F$ es abierto en X.*

Por la forma en la que interactúan las operaciones conjuntistas de resta, unión e intersección, el lector puede comprobar que se verifican propiedades, relativas a conjuntos cerrados de un espacio topológico X, similares a las expuestas en la definición A.1. Tales propiedades se enuncian en la siguiente proposición.

Proposición A.9 *Sea X un espacio topológico. Respecto a los conjuntos cerrados de X se satisface lo siguiente:*

a) X y $\emptyset$ son cerrados de X.

b) Si $\{F_i\}_{i \in I}$ es una familia arbitraria de cerrados de X, entonces $\bigcap_{i \in I} F_i$ es cerrado en X.

c) Si $\{F_i\}_{i=1}^n$ *es una familia finita de cerrados de* X*, entonces* $\bigcup_{i=1}^{n} F_i$ *es cerrado en* X*.*

Demostración. Se deja como ejercicio al lector. □

Observación A.10 *Todos los subconjuntos de un espacio topológico discreto son abiertos y cerrados simultáneamente.*

Con las definiciones de conjunto abierto y cerrado de un espacio topológico, observamos que podemos clasificar casi a todos los subconjuntos de un espacio topológico como abiertos, cerrados, o quizá como ambos. Sin embargo, en un espacio topológico hay subconjuntos que no son cerrados ni abiertos. Respecto a tales conjuntos, es interesante estudiar a los abiertos del espacio que se quedan contenidos en ellos, también a los cerrados que contienen a tales subconjuntos. En ambos casos, las nociones que se exponen a continuación, pueden traducirse a *aproximar* un subconjunto por conjuntos abiertos o cerrados del espacio, es decir, buscar el abierto y cerrado más parecido al subconjunto.

Definición A.11 *Sean* (X, τ) *un espacio topológico y* $A \subseteq X$*.*

a) Se define el ***interior*** *de* A *como:*

$$int(A) = \bigcup_{U \in \tau} \{U \subseteq X : U \subseteq A\}.$$

b) La ***cerradura*** *de* A *está dada por:*

$$\overline{A} = \bigcap_{X \setminus F \in \tau} \{F \subseteq X : A \subseteq F\}.$$

Observación A.12 *A partir de la definición A.1 y de la proposición A.9, se sigue que* $int(A)$ *es abierto y que* $\bar{A}$ *es cerrado en* X*. Además, es claro que* A *es abierto en* X *(resp. cerrado) si y solo si* $int(A) = A$ (*resp.* $\overline{A} = A$).

La siguiente proposición nos provee de una caracterización para la cerradura de un subconjunto de un espacio topológico.

Proposición A.13 *Sean* X *un espacio topológico y* $A \subseteq X$*. Entonces,* $x \in \overline{A}$ *si y solo si, para todo* U *abierto de* X *tal que* $x \in U$*, se tiene* $U \cap A \neq \emptyset$*.*

Demostración. La prueba de este hecho es a partir de la definición de cerradura, puede revisar una prueba en [9, proposición 1.1.1, pág. 13]. □

A continuación se exponen las propiedades elementales del interior y la cerradura de un subconjunto de un espacio topológico.

Proposición A.14 *Sean X un espacio topológico y $A, B \subseteq X$. Entonces se verifican las siguientes propiedades:*

a) $int(X) = X$

b) $int(A) \subseteq A$

c) $int(A \cap B) = int(A) \cap int(B)$

d) $int(int(A)) = int(A)$

De forma análoga se tienen las propiedades para la cerradura de A, salvo que en el inciso c) la intersección cambia por unión.

Definición A.15 *Sean X un espacio topológico y $\emptyset \neq A \subseteq X$. Un punto $x_0 \in X$ es un* ***punto de acumulación*** *de A si, para todo abierto U de X tal que $x_0 \in U$, se tiene que $U \cap (A \setminus \{x_0\}) \neq \emptyset$.*
En lo sucesivo, el conjunto de todos los puntos de acumulación de A será denotado por A'.

La cerradura de un conjunto puede ser caracterizada de la siguiente manera:

Proposición A.16 *Sean X un espacio topológico y $A \subseteq X$. Entonces $\overline{A} = A \cup A'$.*

Demostración. Es una consecuencia de aplicar las definiciones de los conceptos involucrados, se deja de ejercicio al lector. □

Proposición A.17 *Un subconjunto A de un espacio topológico X es cerrado en X si y solo si $\overline{A} = A$.*

Demostración. Puede revisar una prueba en [5, proposición 2.6, pág. 45]. □

Definición A.18 *Sean (X, τ) un espacio topológico y $\mathcal{B} \subseteq \tau$. Diremos que $\mathcal{B}$ es una* ***base*** *para τ si todo abierto en τ puede escribirse como unión de elementos en $\mathcal{B}$.*

Naturalmente todo espacio topológico posee una base, esto ya que la topología es una base para el espacio; sin embargo, las bases que son de interés son aquellas que están formadas por abiertos *elementales* de la topología, y que por lo tanto, describen a la topología.
En la siguiente proposición exponemos una caracterización de las bases que traduce de forma más precisa el enunciado anterior.

Proposición A.19 *Sean (X, τ) un espacio topológico y $\mathcal{B} \subseteq \tau$. Entonces, $\mathcal{B}$ es base de τ si y solo si, para todo $a \in X$ y todo $U \in \tau$ con $a \in U$, existe $B \in \mathcal{B}$ tal que $a \in B \subseteq U$.*

Demostración. Se deja de ejercicio al lector. □

Corolario A.20 *Sea $\beta = \{U_i\}_{i\in I}$ una familia de subconjuntos de un espacio topológico X. Si β satisface la condición:*

Para cualquier $x \in U_i \cap U_j$ con $i, j \in I$, existe $k \in I$ tal que $x \in U_k \subseteq U_i \cap U_j$.

Entonces, la familia $\tau(\beta)$, que consiste de $\emptyset, X$ y todas las uniones arbitrarias de elementos de β, forman una topología para X. Además, $\tau(\beta)$ es una topología única con esta propiedad y es la más pequeña (gruesa) de las topologías en X que contienen a β.

Demostración. Vea [7, Teorema 3.2, pág. 67.] □

La proposición A.19 proporciona una caracterización para una base de forma global, es decir, que todo punto del espacio pertenece a un elemento de la base. Ya que todo lo global se puede adecuar a lo particular, introducimos las bases locales de espacios topológicos.

Definición A.21 *Sean (X, τ) un espacio topológico y $x_0 \in X$. Se dice que un subconjunto $\mathcal{B}$ de τ es una **base local de** x_0 si para todo $B \in \mathcal{B}$ se tiene que $x_0 \in B$ y además, para todo $U \in \tau$ tal que $x_0 \in U$, existe $B \in \mathcal{B}$ tal que $x_0 \in B \subseteq U$.*

En general, hay subconjuntos de un espacio topológico que pueden llegar a cumplir un hecho similar al de la proposición A.19 sin necesidad de que los elementos del subconjunto sean abiertos o cerrados.

Definición A.22 *Sea (X, τ) un espacio topológico. Se dice que $\mathcal{D} \subseteq X$ es **denso en X** si para todo abierto $U \in \tau$, se verifica que $U \cap \mathcal{D} \neq \emptyset$.*

Observación A.23 *El lector puede probar que, si X es un espacio topológico y $D \subseteq X$, entonces D es denso en X si y solo si $\overline{D} = X$.*

Definición A.24 *Sea (X, τ) un espacio topológico. Se dice que el conjunto $\mathcal{B} \subseteq \tau$ es una **subbase** para τ, si el conjunto de las intersecciones finitas de elementos de $\mathcal{B}$ es una base para τ.*

Como es usual, si X es un conjunto, se busca estudiar a los subconjuntos de X que poseen las mismas características o estructura que X, y las condiciones que deben imponerse para que las adquiera. En breve, se presentan los subconjuntos de un espacio topológico X que son de interés.

Consideremos (X, τ) un espacio topológico, $Y \subseteq X$ con $Y \neq \emptyset$ y la siguiente familia de subconjuntos de Y :

$$\tau|_Y = \{U \cap Y : U \in \tau\} \subseteq \wp(Y).$$

Proposición A.25 *Sean (X,τ) un espacio topológico y $Y \subseteq X$ con $Y \neq \emptyset$. Los elementos de $\tau|_Y$ determinan una topología sobre Y.*

Demostración. Se deja de ejercicio al lector. □

A $\tau|_Y$ le llamaremos **topología relativa o topología inducida** por (X,τ) y diremos que $(Y,\tau|_Y)$ es un **subespacio** de (X,τ).

Observación A.26 *El lector puede probar que si (X,τ) es un espacio topológico, Y es un subespacio de X y $B \subseteq \tau$ es una base para X, entonces:*

$$\{Y \cap B : B \in \mathcal{B}\} \text{ es una base para } Y \text{ como espacio topológico.}$$

De forma similar, el lector puede describir una subbase para un subespacio a partir de una subbase para X.

Definición A.27 *Se dice que un espacio topológico X es T_1 si para cualesquiera puntos distintos $x, y \in X$, existen abiertos U y V de X tales que $y \in V \setminus U$ y $x \in U \setminus V$.*
Es irrelevante si los abiertos U y V se intersecan en puntos que no sean x o y.

Proposición A.28 *Un espacio topológico X es T_1 si y solo si, para todo $x \in X$, $\{x\}$ es cerrado en X.*

Demostración. [5, teorema 5.6, pág. 151]. □

Observación A.29 *Ya que la unión finita de conjuntos cerrados es cerrado (vea inciso c) de la proposición A.9), de la proposición A.28 se sigue que un espacio topológico X es T_1 si y solo si, para cualesquiera $x_1, ..., x_n \in X$, se tiene que $\{x_1, ..., x_n\}$ es cerrado en X.*

Definición A.30 *Se dice que un espacio topológico X es **Hausdorff** o T_2 si para cualesquiera $x, y \in X$ con $x \neq y$, existen $U, V \subseteq X$ abiertos tales que $x \in U, y \in V$ y $U \cap V = \emptyset$.*

Observación A.31 *Notemos que todo espacio T_2 es T_1 y que todo espacio topológico dotado de la topología discreta (vea definición A.3) es Hausdorff.*

En general, en un espacio topológico los conjuntos unitarios no tienen que ser conjuntos cerrados, si se impone la condición de que el espacio sea Hausdorff, entonces esta propiedad sí se satisface.

Proposición A.32 *Si X es un espacio topológico Hausdorff, entonces todo subconjunto de X de la forma $\{x\}$ es cerrado.*

Demostración. Es inmediato a partir de la proposición A.28 y de la observación A.31. □

Proposición A.33 *Un espacio topológico X es Hausdorff si y solo si el conjunto $\triangle_X = \{(x,x) : x \in X\}$ es cerrado en $X \times X$.*

Demostración. Vea [5, proposición 5.22, pág. 159]. □

Proposición A.34 *Si X es un espacio topológico Hausdorff y Y es un subespacio topológico de X, entonces Y es Hausdorff.*

Demostración. La prueba es inmediata a partir del hecho de que X es Hausdorff. Se deja de ejercicio al lector. □

Definición A.35 *Sean $(X,\tau),(Y,\sigma)$ espacios topológicos y $f : X \longrightarrow Y$ una función. Se dice que f es **continua** si para todo $U \in \sigma$, se tiene que $f^{-1}(U) \in \tau$. Además, diremos que f es un **homeomorfismo** si es biyectiva y tanto f como su inversa, f^{-1}, son continuas.*

Proposición A.36 *Sean X y Y espacios topológicos de tal forma que Y es Hausdorff. Consideremos dos funciones continuas $f, g : X \longrightarrow Y$. Entonces el siguiente conjunto es un cerrado de X :*

$$\{x \in X : f(x) = g(x)\}.$$

Demostración. En virtud de la definición A.8 y de la proposición A.7, basta probar que el siguiente conjunto es vecindad para cada uno de sus puntos:

$$\{x \in X : f(x) \neq g(x)\} \text{ es abierto en X .}$$

Sea $x_0 \in X$ tal que $f(x_0) \neq g(x_0)$. Como Y es Hausdorff, existen $U, V \in Y$ tales que:

$$f(x_0) \in U \text{ y } g(x_0) \in V \text{ y } U \cap V = \emptyset. \tag{A.1}$$

Por lo tanto, $x_0 \in f^{-1}(U) \cap g^{-1}(V) \subseteq \{x \in X : f(x) \neq g(x)\}$.
Al ser f y g funciones continuas, el conjunto $f^{-1}(U) \cap g^{-1}(V)$ es un abierto de X que contiene a x_0. De esta forma obtenemos lo que deseabamos probar. □

Proposición A.37 *Sean (X,τ) y (Y,σ) espacios topológicos y $f : X \longrightarrow Y$ una función entre ellos. Los siguientes enunciados son equivalentes:*

a) f es continua.

b) Si $F \subseteq Y$ es cerrado, entonces $f^{-1}(F)$ es cerrado en X.

Demostración. Se deja como ejercicio al lector. □

Definición A.38 *Sean (X,τ), (Y,σ) espacios topológicos y $f : X \longrightarrow Y$ una función entre ellos. Se dice que f es* ***abierta*** *si para todo $U \in \tau$, se tiene que $f(U) \in \sigma$.*
De forma similar se define una función ***cerrada****.*

Proposición A.39 *Consideremos $(X,\tau),(Y,\sigma),(Z,\rho)$ espacios topológicos, así como las funciones $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$. Entonces se verifica lo siguiente:*

a) Si f y g son continuas, entonces $g \circ f$ es continua.

b) Si f y g son homeomorfismos, entonces $g \circ f$ también lo es.

c) Si f y g son abiertas, entonces $g \circ f$ también lo es.

d) Si f es un homeomorfismo, entonces f es abierta y cerrada.

e) Si f es continua y A es un subespacio topológico de X, la restricción $f|_A$ también es continua.

Demostración. Se deja de ejercicio al lector. □

Observación A.40 *Si $f : X \longrightarrow Y$ es una función entre conjuntos y $A \subseteq B \subseteq X$, se sigue que $f|_A = (f|_B)|_A$.*

Proposición A.41 *Sea $f : X \longrightarrow Y$ una función biyectiva entre espacios topológicos. Las siguientes condiciones son equivalentes:*

a) f es un homemorfismo.

b) f es continua y abierta.

c) f es continua y cerrada.

d) Para cada $A \subseteq X$, $f(\overline{A}) = \overline{f(A)}$.

Demostración. Vea [7, teorema 12.2, pág. 89]. □

En el siguiente apartado recordaremos la construcción de la topología cociente y la topología producto.

Definición A.42 *Sean (X,τ) un espacio topológico, $\sim$ una relación de equivalencia en X y la función $\pi : X \longrightarrow X/\sim$ que satisface $x \xrightarrow{\pi} [x]_\sim$. Al conjunto $X/\sim$ se le puede dotar de la* ***topología cociente*** *definida de la siguiente forma:*

$$\tau_\sim := \left\{U \subseteq X/\sim : \pi^{-1}(U) \in \tau\right\}.$$

Esta topología es la más fina sobre $X/\sim$ de entre todas las que hacen a π una función continua.

Una topología similar a la construida en la definición A.42 puede ser construida en cualquier conjunto Y a partir de una función entre un espacio topológico y Y.

Proposición A.43 *Sean X un espacio topológico, Y un conjunto no vacío y $f : X \longrightarrow Y$ una función. En Y puede inducirse una topología a través de la función f como sigue:*

$$\tau_Y := \left\{U \subseteq Y : f^{-1}(U) \text{ es abierto en } X\right\}.$$

Además, considerando a Y como espacio topológico con dicha topología, se cumplen las siguientes propiedades:

a) f es una función continua y τ_Y es la más fina de las topologías en Y que hacen a f una función continua.

b) τ_Y es la única topología definida en Y que satisface lo siguiente:

Para toda función $g : Y \longrightarrow Z$, con Z un espacio topológico, se tiene que:

$$g \text{ es continua si y solo si } g \circ f \text{ es continua.}$$

Demostración. Vea [5, teorema 4.20, pág. 126.] □

Como una consecuencia inmediata tenemos el siguiente resultado.

Corolario A.44 *Sea $f : X \longrightarrow Y$ una función biyectiva, con X un espacio topológico y Y un conjunto. Si en Y inducimos la topología τ_Y de la proposición A.43, entonces f es un homeomorfismo.*

Demostración. Claramente f es una función continua por el inciso a) de la proposición A.43. Consideremos $f^{-1} : Y \longrightarrow X$ y probemos que es una función continua. Sea U un abierto en X. Para probar que $(f^{-1})^{-1}(U) = f(U)$ es un abierto en Y con la topología τ_Y, basta notar que $f^{-1}(f(U)) = U$ es abierto en X. □

Definición A.45 *Sea $\{X_i\}_{i\in I}$ una familia de conjuntos no vacíos. Se define el* ***producto cartesiano conjuntista*** *como:*

$$\prod_{i\in I} X_i = \left\{ f : I \longrightarrow \bigcup_{i\in I} X_i \ : f \text{ es función y } f(i) \in X_i \text{ para todo } i \in I \right\}.$$

Usaremos la notación $f(i) = x_i$ para cada $i \in I$. A los elementos de $\prod_{i\in I} X_i$ los escribiremos como $(x_i)_{i\in I}$ tal que, para cada $i \in I$, se tiene que $x_i \in X_i$.

Observación A.46 *El axioma de elección de la teoría de los conjuntos es equivalente a que, para toda familia de conjuntos no vacíos* $\{X_i\}_{i\in I}$, *se tiene que* $\prod_{i\in I} X_i \neq \emptyset$.

Definición A.47 *Sea* $\{X_i\}_{i\in I}$ *una familia de conjuntos no vacía y* $\mathcal{X} = \prod_{i\in I} X_i$. *Para cada* $j \in I$, *se define la* ***j-ésima proyección canónica*** *como la siguiente función:*

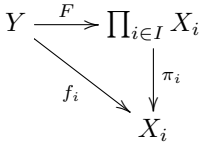
$$\pi_j : \prod_{i\in I} X_i \longrightarrow X_j$$

$$(x_i)_{i\in I} \longmapsto x_j \ .$$

Observación A.48 *En el caso en que* $\{G_i\}_{i\in I}$ *sea una familia de grupos, se tiene que* $\prod_{i\in I} G_i$ *es un grupo, las proyecciones canónicas son morfismos suprayectivos de grupos; y del primer teorema de isomorfismo (vea teorema 1.56) se sigue que, para todo* $j \in I$:

$$\left(\prod_{i\in I} G_i\right) / ker(\pi_j) \simeq G_j.$$

Proposición A.49 ***(Propiedad universal del producto cartesiano)*** *Consideremos* $\{X_i\}_{i\in I}$ *una familia de conjuntos no vacíos,* Y *un conjunto no vacío tal que, para cada* $i \in I$, *existe una función* $f_i : Y \longrightarrow X_i$. *Entonces existe una única función* $F : Y \longrightarrow \prod_{i\in I} X_i$ *dada por* $F(y) \longrightarrow (f_i(y))_{i\in I}$, *tal que, para cada* $i \in I$, *el siguiente diagrama es conmutativo:*



Es decir, $\pi_i \circ F = f_i$.

Observación A.50 *La propiedad universal del producto cartesiano se sigue verificando si los objetos involucrados son espacios topológicos (resp. grupos), las funciones* f_i *son funciones continuas (resp. morfismos de grupos) y en este caso la función* F *resulta ser una función continua (resp. morfismo de grupos).*

Definición A.51 *Sean $\{(X_i, \tau_i)\}_{i\in I}$ una familia de espacios topológicos. Tomemos el producto $\mathcal{X} = \prod_{i\in I} X_i$. Se pueden definir dos topologías sobre $\mathcal{X}$:*
*Si $|I| < \infty$, se puede considerar la **topología caja** en $\mathcal{X}$ de la siguiente forma:*

$$\tau = \left\{ \prod_{i\in I} U_i : U_i \in \tau_i \right\}. \tag{A.2}$$

*Si $|I| = \infty$, se define la **topología producto** τ en $\mathcal{X}$ como la más gruesa (vea definición A.4) de las topologías en $\mathcal{X}$ que hacen a cada una de las proyecciones $\pi_i : \mathcal{X} \longrightarrow X_i$ continuas. La topología producto tiene por base el siguiente conjunto:*

$$\left\{ \prod_{i\in I} U_i : U_i \in \tau_i \text{ y } U_i \neq X_i \text{ para una cantidad finita de índices } i \in I \right\}.$$

Además, dicha topología tiene por subbase a la colección de conjuntos abiertos:

$$\mathcal{S} = \left\{ \pi_i^{-1}(U) : U \in \tau_i, i \in I \right\}.$$

Proposición A.52 *Sean $\{X_i\}_{i\in I}, Y$ espacios topológicos y $g : Y \longrightarrow \prod_{i\in I} X_i$ una función. Entonces, g es continua si y solo si $\pi_i \circ g$ es continua para cada $i \in I$.*

Demostración. Revise [5, proposición 4.15, pág. 121]. □

Proposición A.53 *Sea $\{X_i\}_{i\in I}$ una familia de espacios topológicos no vacíos y Hausdorff, entonces $\prod_{i\in I} X_i$ es Hausdorff.*

Demostración. [5, teorema 5.20, pág. 157]. □

Definición A.54 *Sea X un espacio topológico. Se dice que X es **compacto** si para toda familia de abiertos $\{U_i\}_{i\in I} \subseteq \wp(X)$ tal que $X = \bigcup_{i\in I} U_i$, se tiene que existe $J \subseteq I$ con $|J| < \infty$ de tal forma que $X = \bigcup_{i\in J} U_i$.*
Se dice que un subconjunto Y de un espacio topológico X es compacto, si al ser considerado con la topología inducida por X (vea definición A.25), se tiene que Y es compacto.

Ejemplo A.55 *Notemos que si X es un espacio topológico finito, entonces X es compacto sin importar la topología de la que esté dotado, pues esta sólo posee una cantidad finita de abiertos debido a que toda topología tiene cardinal menor o igual a $|\wp(X)|$, que es un número finito.*

Ejemplo A.56 *Si X es un espacio discreto y compacto, entonces X es finito. Basta notar que para cada $x \in X$, el conjunto $\{x\}$ es un subconjunto abierto de X, además $X = \bigcup_{x \in X} \{x\}$. El resultado se sigue de la compacidad de X.*

A continuación proporcionaremos una caracterización de los espacios topológicos compactos.

Definición A.57 *Sean X un espacio topológico y $\mathcal{F} = \{F_i\}_{i \in I} \subseteq \wp(X)$. Se dice que $\mathcal{F}$ posee la* ***propiedad de la intersección finita*** *si $\mathcal{F} \neq \emptyset$ y para todo $J \subseteq I$, con $|J| < \infty$, se verifica que $\bigcap_{i \in J} F_i \neq \emptyset$.*

Proposición A.58 *Un espacio topológico X es compacto si y solo si, para toda familia $\mathcal{F} \subseteq \wp(X)$ de cerrados que satisface la propiedad de la intersección finita, se satisface que $\bigcap \mathcal{F} \neq \emptyset$.*

Demostración. [5, proposición 7.3, pág. 210]. □

En general, los subespacios de un espacio topológico compacto, no son compactos. Para garantizar la compacidad de un subespacio es necesario pedir que sea cerrado. Esto se muestra en la siguiente proposición.

Proposición A.59 *Todo subespacio cerrado de un espacio compacto X es compacto.*

Demostración. [5, proposición 7.4, pág. 211]. □

Proposición A.60 *Si Y es un subespacio compacto de un espacio topológico X, entonces, para toda familia de abiertos $\{U_i\}_{i \in I} \subseteq X$ tal que $Y \subset \bigcup_{i \in I} U_i$, existe $J \subseteq I$ con $|J| < \infty$ que satisface $Y \subseteq \bigcup_{i \in J} U_i$.*

Demostración. Por la proposición A.25, se tiene que los conjuntos $V_i = U_i \cap Y$ son abiertos en Y para todo $i \in I$. Notemos que la familia $\{V_i\}_{i \in I} \subseteq \wp(Y)$ es una cubierta abierta de Y, esto debido a que:

$$\bigcup_{i \in I} V_i = \bigcup_{i \in I} (U_i \cap Y) = Y \cap \left(\bigcup_{i \in I} U_i \right) = Y.$$

Como Y es un subespacio compacto de X, existe $J \subseteq I$ tal que $|J| < \infty$ y satisface que $Y = \bigcup_{i \in J} V_j$. Por lo tanto $Y = Y \cap \left(\bigcup_{i \in J} U_i \right)$, en otras palabras:

$$Y \subseteq \bigcup_{i \in J} U_i.$$

□

Proposición A.61 *Todo subespacio compacto de un espacio Hausdorff X es un subespacio cerrado de X.*

Demostración. Para una prueba de este hecho, vea [5, corolario 7.8, pág 213]. □

Proposición A.62 (Tychonoff) *Sea $\{X_i\}_{i\in I}$ una familia de espacios topológicos no vacíos. El producto $\prod_{i\in I} X_i$ es compacto si y solo si X_i es compacto para todo $i \in I$.*

Demostración. Para una versión de la prueba vea [5, teorema 7.10, pág. 215]. □

Proposición A.63 *Sean X y Y espacios topológicos con X compacto. La existencia de una función continua $f : X \longrightarrow Y$ tal que $f(X) = Y$, implica que Y es compacto.*

Demostración. [5, proposición 7.6, pág. 212]. □

Observación A.64 *Si f es una función continua entre espacios topológicos X y Y, y además A es un subespacio compacto de X, por el inciso e) de la proposición A.39 se sigue que $f|_A$ es continua, y de la proposición A.63 obtenemos que $f|_A(A) \subseteq Y$ es un subespacio compacto.*

Definición A.65 *Un espacio topológico no vacío X es llamado **localmente compacto** si para todo $x \in X$ existe una vecindad $U \subseteq X$ tal que U es un subespacio compacto de X.*

Observación A.66 *Si X es un espacio topológico compacto, al ser X una vecindad para cada uno de sus puntos, se tiene que X es localmente compacto.*

Definición A.67 *Se dice que un espacio topológico X es **conexo** si no existen subconjuntos abiertos no vacíos Y_1, Y_2 de X tales que $X = Y_1 \cup Y_2$ y $Y_1 \cap Y_2 = \emptyset$. En caso contrario, diremos que X es **disconexo**. Es decir, X es disconexo si existen subconjuntos abiertos no vacíos Y_1 y Y_2 tales que $X = Y_1 \cup Y_2$ con $Y_1 \cap Y_2 = \emptyset$.*

La siguiente definición es extraída de [9, pág. 68].

Definición A.68 *Dos subconjuntos Y_1 y Y_2 de un espacio topológico X se dicen **separados** en X si $Y_1 \cap \overline{Y_2} = \emptyset = \overline{Y_1} \cap Y_2$.*
En caso contrario, diremos que los subconjuntos Y_1 y Y_2 no están separados.

A continuación proporcionamos una caracterización de los espacios conexos.

Proposición A.69 *Sea X un espacio topológico. Los siguientes enunciados son equivalentes:*

a) X es un espacio conexo.

b) $\emptyset$ y X son los únicos subconjuntos abiertos y cerrados (simultáneamente) de X.

c) Si $X = Y_1 \cup Y_2$, con Y_1, Y_2 subconjuntos separados de X, entonces $Y_1 = \emptyset$ o $Y_2 = \emptyset$.

d) Si $f : X \longrightarrow \{0,1\}$ es una función continua, entonces f es constante

Demostración. [9, teorema 6.1.1, pág. 352]. □

El inciso c) de la proposición A.69 nos ayuda a visualizar los espacios conexos, pues estos son, de forma intuitiva, aquellos que no pueden ser separados en dos subconjuntos cercanos entre ellos. El hecho de que un espacio sea conexo no significa que sus subespacios también lo sean, como veremos en lo sucesivo.

De la anterior proposición se obtiene el siguiente resultado, que es una consecuencia inmediata y se deja como ejercicio al lector.

Corolario A.70 *Un espacio topológico X es conexo si y solo si no puede ser expresado como $X = Y_1 \cup Y_2$ con Y_1, Y_2 cerrados disjuntos y no vacíos de X.*

Observación A.71 *Note que si X es un espacio topológico discreto (vea definición A.3), los únicos subconjuntos conexos de X son de la forma $\{x\}$ con $x \in X$.*

Corolario A.72 *Sean X un espacio topológico y C un subconjunto conexo de X, entonces la cerradura de C es un subconjunto conexo en X.*

Demostración. Supongamos que $\overline{C} = Y_1 \cup Y_2$ con Y_1 y Y_2 cerrados disjuntos y no vacíos de $\overline{C}$. Como $\overline{C}$ es cerrado en X, se sigue que Y_1 y Y_2 son subconjuntos cerrados de X.
Al intersecar la igualdad inicial con C, tenemos que $C = (C \cap Y_1) \cup (C \cap Y_2)$, con $C \cap Y_1$ y $C \cap Y_2$ cerrados disjuntos en C considerado como subespacio de X. Veamos que $C \cap Y_1$ y $C \cap Y_2$ no son vacíos. En efecto, si $C \cap Y_1 = \emptyset$, de la igualdad anterior tenemos que $C = C \cap Y_2$ y así $C \subseteq Y_2$. Como Y_2 es cerrado, tenemos que $Y_1 \cup Y_2 = \overline{C} \subseteq Y_2$ y así $Y_1 \subseteq Y_2$, contradiciendo el hecho de que Y_1 y Y_2 son disjuntos. Por lo tanto $C \cap Y_1 \neq \emptyset$ y similarmente $C \cap Y_2 \neq \emptyset$.
En virtud del corolario A.70, tenemos que C no es conexo, lo cual, naturalmente, contradice a la hipótesis. Concluimos que $\overline{C}$ es conexo. □

Proposición A.73 *Sea $f : X \longrightarrow Y$ una función continua entre espacios topológicos. Si X es conexo, entonces $f(X) \subseteq Y$ es conexo.*

Demostración. La prueba se sigue a partir de las definiciones de conexidad y continuidad. Se deja de ejercicio al lector. □

Proposición A.74 *Un subespacio topológico Y de X es conexo si y solo si, para todo par X_1, X_2 de subconjuntos de X separados tal que $Y = X_1 \cup X_2$, se cumple que $X_1 = \emptyset$ o $X_2 = \emptyset$.*

Demostración. Vea [9, teorema 6.1.7, pág. 353]. □

El siguiente resultado puede hallarse en [9, corolario 6.1.8, pág. 353].

Corolario A.75 *Si X es un espacio topológico y Y es un subespacio conexo de X, entonces, para todo par Y_1, Y_2 de subconjuntos separados de X tal que $Y \subseteq Y_1 \cup Y_2$, se tiene que $Y \subseteq Y_1$ o $Y \subseteq Y_2$. Además, sólo se verifica una de estas dos contenciones.*

Proposición A.76 *Sea $\{C_i\}_{i\in I}$ una familia de subespacios conexos de un espacio topológico X tal que existe $j \in I$ de tal modo que C_j y C_i no están separados para todo $i \in I$. Entonces $\bigcup_{i\in I} C_i$ es conexo.*

Demostración. Vea [9, teorema 6.1.9, pág. 353]. □

Corolario A.77 *Sea X un espacio topológico y $\{C_i\}_{i\in I}$ una familia de subespacios conexos de X tales que $\bigcap_{i\in I} C_i \neq \emptyset$, entonces $\bigcup_{i\in I} C_i$ es conexo.*

Demostración. Para una prueba ver [9, corolario 6.1.0, pág. 354]. □

Definición A.78 *Sean X un espacio topológico y $x \in X$ un elemento cualquiera. La **componente conexa** de $x \in X$ es el mayor de los subconjuntos conexos de X que tienen a x como elemento. Este conjunto será abreviado por $\mathcal{C}_X(x)$. En otras palabras:*

$$\mathcal{C}_X(x) = \bigcup_{\substack{C-conexo \\ x\in C}} C.$$

En caso de no haber confusión, denotaremos como $\mathcal{C}(x)$ a la componente conexa de un elemento x en un espacio topológico X.

Observación A.79 *La existencia de la componente conexa de un elemento de X queda garantizada por el corolario A.77.*

Proposición A.80 *Si X es un espacio topológico y Y es un subespacio de X, entonces, para todo $y \in Y$, $\mathcal{C}_Y(y) \subseteq \mathcal{C}_X(y)$.*

Demostración. Basta ver que si $C \subseteq Y$ es conexo en Y entonces C es conexo en X. En efecto, supongamos que C no es conexo en X. Entonces existen U_1 y U_2 subconjuntos disjuntos abiertos y no vacíos de X tal que $C = U_1 \cup U_2$. Notemos que como $U_1 \subseteq C \subseteq Y$, entonces $U_1 = U_1 \cap Y$, y así U_1 es un abierto de Y. De manera similar U_2 es un abierto de Y y como $C = U_1 \cup U_2$ concluimos que C no es conexo en Y, lo cual es una contradicción.
Por lo tanto, C es conexo en X. □

Proposición A.81 *Sean X un espacio topológico y $x \in X$ cualquier elemento. La componente conexa $\mathcal{C}(x)$ es un cerrado en X.*

Demostración. De las propiedades de la cerradura de un conjunto (vea proposición A.14) se sigue que $\mathcal{C}(x) \subseteq \overline{\mathcal{C}(x)}$, y por lo tanto $x \in \overline{\mathcal{C}(x)}$. Además, del corolario A.72, se sabe que $\overline{C(x)}$ es un subconjunto conexo de X, de donde:

$$x \in \overline{\mathcal{C}(x)} \subseteq \bigcup_{\substack{C-\text{conexo} \\ x \in C}} C = \mathcal{C}(x).$$

Concluimos que $\mathcal{C}(x) = \overline{\mathcal{C}(x)}$, es decir, $\mathcal{C}(x)$ es un subconjunto cerrado del espacio topológico X. □

La siguiente definición puede hallarse en [9, pág. 356].

Definición A.82 *Sean X un espacio topológico y $x \in X$ un elemento cualquiera. La **quasi-componente** de x en X, se define como el siguiente conjunto:*

$$\mathcal{Q}(x) = \bigcap \{A \subseteq X : x \in A,\ A \text{ es abierto y cerrado en } X\}.$$

Observación A.83 *Sean X un espacio topológico, $x \in X$, $C \subseteq X$ un subconjunto conexo y $Y \subseteq X$ un abierto y cerrado de X de tal forma que $x \in C \cap Y$. Al ser Y y $X \setminus Y$ conjuntos separados (vea definición A.68), y dado que $C \subseteq Y \cup (X \setminus Y)$, se sigue, del corolario A.75 que $C \subseteq Y$.*
De esta observación se concluye que, para todo $x \in X$, $\mathcal{C}(x) \subseteq \mathcal{Q}(x)$.
Notemos que, por la proposición A.9, la quasi-componente de un elemento en X es siempre un subconjunto cerrado de X, pues es intersección arbitraria de cerrados.

El hecho de que la componente conexa de todo punto de un espacio topológico sea unipuntual, proporciona una nueva clasificación de espacios topológicos como lo muestra la siguiente definición.

Definición A.84 *Un espacio topológico X es **totalmente disconexo** si, para todo $x \in X$, $\mathcal{C}(x) = \{x\}$.*

Observación A.85 *En algunos lugares a la noción de totalmente disconexo lo llaman hereditariamente disconexo (ver por ejemplo [5, definición 8.50, pág. 289] y [9, sección 6.2, pág. 360]).*

Observación A.86 *Sea X un espacio topológico que verifica que $\mathcal{Q}(x) = \{x\}$ para todo $x \in X$.*

a) De la observación A.83, se sigue que X es totalmente disconexo.

b) Ya que las componentes conexas son subconjuntos cerrados de X (vea proposición A.81), se sigue que $\{x\}$ es un cerrado. Finalmente, de la proposición A.28, se sigue que X es T_1.

Ejemplo A.87 *Sea X un espacio topológico dotado de la topología discreta (vea definición A.3). Entonces X es totalmente disconexo, pues los únicos subconjuntos conexos de X son de la forma $\{x\}$ con $x \in X$.*

Proposición A.88 *Todo subespacio de un espacio totalmente disconexo es totalmente disconexo.*

Demostración. El resultado se sigue de la proposición A.80. □

Definición A.89 *Un espacio topológico no vacío X es **cero dimensional** si es T_1 y X tiene una base que consiste de abiertos y cerrados.*

Proposición A.90 *Si X es un espacio topológico Hausdorff, localmente compacto y totalmente disconexo, entonces X es un espacio cero dimensional.*

Demostración. Vea [5, proposición 8.59, pág. 294]. □

Corolario A.91 *Si X es un espacio topológico compacto, Hausdorff y totalmente disconexo, entonces X es cero dimensional.*

Demostración. De la observación A.66 se sigue que X es localmente compacto, mientras que por la proposición A.90, se concluye que X es cero dimensional. □

Proposición A.92 *Sean $\{X_i\}_{i\in I}$ una familia de espacios topológicos no vacíos y $\mathcal{X} = \prod_{i\in I} X_i$. Entonces se verifica lo siguiente:*

a) $\mathcal{X}$ es totalmente disconexo si y solo si, para todo $i \in I$, X_i es totalmente disconexo.

b) $\mathcal{X}$ es cero dimensional si y solo si, para todo $i \in I$, X_i es cero dimensional.

Demostración. [5, proposición 8.53, pág. 290]. □

Bibliografía

[1] F. de M. Aceff, E. Lluis, *Teoría de Galois, un primer curso*, Publicaciones electrónicas Sociedad Matemática Mexicana, **14**, (2016), no. 3.

[2] J. Adámek, H. Herrlich, G.E. Strecker, *Abstract and Concrete Categories The Joy of Cats*, edición electrónica, (2006).

[3] I. Boreico, *Linear Independence of Radicals*, The Harvard College Mathematics Review, **2**, (2008), no. 1, 87.

[4] N. Bourbaki, *Elements of Mathematics. General Topology. Chapters 1-4*, Springer-Verlag Berlin, Heidelberg New York London Paris Tokyo, (1987).

[5] F. Casarrubias, A. Tamariz, *Elementos de Topología General*, Aportaciones Matemáticas de la SMM, Ciudad de México, (2015).

[6] K. Conrad, *Infinite Galois Theory*, Course notes UCONN, (2020).

[7] J. Dugundji. *Topology*, Allyn and Bacon, Chicago, (1978).

[8] D.S. Dummit, R.M. Foote, *Abstract Algebra*, tercera edición, John Wiley & Sons, Inc, EUA, (2003).

[9] R. Engelking, *General Topology*, Hieldermann Verlag Berlin, Berlin,(1989).

[10] W. Feit, J. G. Thompson, *Solvability of Groups of Odd Order*, Pacific Journal, **13**, (1963), no. 3, 775-1027.

[11] J. M. Howie, *Fields and Galois Theory*, Springer-Verlag, Londres, (2006).

[12] S. Lang, *Algebra*, tercera edición revisada, Springer-Verlag, New York, (2002).

[13] J.S. Milne, *Fields and Galois Theory*, Course notes, (2012).

[14] P. Morandi, *Fields and Galois Theory*, Springer-Verlag, New York, (1996).

[15] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Springer-Verlag, Berlín, (2000).

[16] L.Ribes, P. Zalesskii, *Profinite Groups*, segunda edición, Springer-Verlag Berlin Heidelberg, Berlín, (2010).

[17] J.M. Rodríguez, *Otra caracterización de los grupos cíclicos finitos*, Miscelánea Matemática, **53**, (2011), 33-37.

[18] S. Roman, *Fundamentals of Group Theory: An Advanced Approach*, Birkhäuser Basel, (2012).

[19] J.J. Rotman, *Advanced Modern Algebra*, segunda edición, Prentice Hall, (2003).

[20] J.J. Rotman, *An Introduction to the Theory of Groups*, cuarta edición, Springer-Verlag, New York, (1995).

[21] J.J. Rotman, *Galois Theory*, segunda edición, Springer-Verlag, New York, (1998).

[22] I.R. Shafarevich, *Construction of field of algebraic numbers given solvable Galois group*, American Mathematical Society translations, **4**, (1956), no. 2, 185-237.

[23] J. Sonn, *Groups of Small Order as Galois Groups over Q*, The Rocky Montain Journal of Mathematics, **19**,(1989), no. 3, 947-956.

[24] W.C. Waterhouse, *Profinite Groups are Galois Groups*, Proceedings of the American Mathematical Society, **42**, (1974), no. 2, 639-640.

[25] J.S. Wilson, *Profinite Groups*, Clarendon Press, Oxford, (1997).

[26] F. Zaldívar, *Teoría de Galois*, Anthropos, Ciudad de México, (1996).