Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Licenciatura en Matemática

Introducción a la Teoría de Galois Infinita

Tesina Licenciatura en Matemática

DANILO SALVADOR AMIGO PEÑA
2019

Profesora Guía: Michela Artebani
Departamento de Matemática
Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Índice general

Agradecimientos

Quiero agradecer a mi familia, por su apoyo y motivación para realizar este trabajo, que significa mucho para mí.
A mi Profesora Guia, Michela Artebani por su infinita preocupación al momento de resolver mis dudas, por su paciencia para concluir este trabajo, y por todos los conocimientos que me entregó en todas las asignaturas que cursé con ella.

Una mención especial a mi Madre y a Paula, que fueron muy importantes en este proceso, que me animaron y me ayudaron cuando lo necesité y que me inspiran para poder llegar más lejos.

Introducción

Dada una extensión de campos finita de Galois K/k, la teoría de Galois clásica muestra que se puede establecer una correspondencia biunívoca entre los campos intermedios $k \subseteq L \subseteq K$ y los subgrupos H de $Gal(K/k)$ que revierte la inclusión. ¿Qué pasa si quitamos la condición de finitud? ¿Será cierto lo anterior?

Las motivaciones para estudiar extensiones algebraicas infinitas han sido varias. Una motivación natural vino de la construcción de la clausura algebraica de un campo, por ejemplo la clausura algebraica $\bar{\mathbb{Q}}$ de $\mathbb{Q}$, que coincide con la unión de todas las extensiones de Galois finitas de $\mathbb{Q}$. Correspondientemente su grupo de Galois $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, llamado *grupo de Galois absoluto*, se puede construir a partir de sus cuocientes finitos, o más precisamente es limite inverso de grupos finitos. El grupo de Galois absoluto de $\mathbb{Q}$ es un objeto todavía misterioso, que ha llevado por ejemplo a la teoría de los *dessins d'enfants* de A. Grothendieck. Otra motivación vino de la teoría algebraica de números, por ejemplo el estudio de las torres de extensiones ciclotómicas, que dió lugar a la Teoría de Iwasawa (ver [8] por un survey sobre la teoría de Galois moderna).

En general la respuesta a la pregunta anterior es no, o sea la correspondencia de Galois clásica no existe para extensiones infinitas. Es decir, no todos los subgrupos de $Gal(K/k)$ se corresponden con un campo intermedio L. Esto fue descubierto en primera instancia por R. Dedekind, quien vio en algunos casos particulares que habían distintos subgrupos de $Gal(K/k)$ que se correspondían con un mismo campo intermedio L. Sucesivamente, W. Krull aclaró el problema en el artículo [10]: se dio cuenta que, dotando a $Gal(K/k)$ de una topología adecuada, se obtiene la biyección pedida considerando a los subgrupos cerrados. Esta topología se conoce como Topología de Krull. Esto explicó el ejemplo de Dedekind en el cual dos subgrupos distintos tenían el mismo campo fijo: uno de los subgrupos era la clausura topológica del otro en la topología de Krull.

En esta tesina probaremos el Teorema de correspondencia de Galois en el caso infinito, o sea mostraremos lo siguiente:

Sea K/k una extensión de Galois infinita y $Gal(K/k)$ su grupo de Galois dotado de la topología de Krull. Entonces existe una correspondencia biyectiva que revierte la inclusión entre los campos intermedios $k \subseteq L \subseteq K$ y los subgrupos cerrados H de $Gal(K/k)$.

A lo largo de este trabajo, se dispondrán de las herramientas necesarias para probar este resultado, siendo necesario introducir conocimientos de Topología y Teoría de Categorías.
En el primer capítulo vamos a introducir los conceptos necesarios sobre grupos topológicos y límites inversos. También analizaremos el concepto de grupo profinito y veremos la

relación entre ésto y los límites inversos. La topología jugará un rol importante en este capítulo, pues veremos que los grupos profinitos se pueden ver como grupos topológicos, y que poseen varias propiedades topológicas interesantes.
El segundo capítulo iniciará con los preliminares sobre la teoría de la extensiones de campos y el Teorema de correspondencia de Galois en el caso finito. Sucesivamente se consideran extensiones de Galois infinitas K/k y se muestra que su grupo de Galois es isomorfo al grupo profinito que se obtiene como límite inverso de los grupos $Gal(L/k)$, donde L/k es una extensión de Galois finita con $k \subseteq L \subseteq K$. Finalmente introduciremos la topología de Krull sobre $Gal(K/k)$, que será compatible con la estructura de grupo. Esto nos permitirá extender la versión clásica del Teorema de Correspondencia de Galois al caso infinito.

Daremos por hecho que los resultados sobre Topología general y Teoría de Galois clásica ya son conocidos.

Capítulo 1

Preliminares

1.1. Grupos Topológicos

Definición 1.1. Un **grupo topológico** es una terna $(G, \tau, \cdot)$ tal que (G, τ) es un espacio topológico, $(G, \cdot)$ es un grupo, y se cumplen las siguientes condiciones:

(A1) La operación de grupo

$$\cdot \colon G \times G \longrightarrow G, \quad (x, y) \longmapsto x \cdot y$$

es continua, donde $G \times G$ tiene la topología producto.

(A2) La aplicación

$$\cdot^{-1} \colon G \longrightarrow G, \quad x \longmapsto x^{-1}$$

es continua.

Proposición 1.2. *Las condiciones (A1) y (A2) son equivalentes a la siguiente:*

(A) La aplicación $G \times G \to G, \quad (x, y) \mapsto x \cdot y^{-1}$ es continua.

Demostración. Supongamos que *(A1)* y *(A2)* son ciertas. La aplicación

$$G \times G \to G \times G, \ (x, y) \longmapsto (x, y^{-1})$$

es continua porque ambas componentes lo son, la primera por ser la proyección en el primer factor, la segunda por ser la proyección en el segundo factor compuesta con la función en *(A2)*. Haciendo la composición de esta función con la multiplicación, que es continua por *(A1)*, se obtiene la función en *(A)*. Luego dicha función es continua por ser composición de funciones continuas.

Supongamos que *(A)* es cierta. La aplicación $G \to G \times G, \ y \longmapsto (1_G, y)$ es continua porqué ambas componentes lo son. Luego la función en *(A2)* es continua porque es composición de esta función con la función en *(A)*. Esto implica que la aplicación $G \times G \to G \times G, \ (x, y) \longmapsto (x, y^{-1})$ es continua. La composición de esta función con la función en *(A)* es la función de multiplicación, luego *(A1)* se cumple también. □

Notación 1. *Por simplicidad, denotaremos al grupo topológico $(G, \tau, \cdot)$ por G. Además, si x e y son elementos de G, en vez de escribir $x \cdot y$ escribiremos xy.*

Observación 1.3. Notemos que si G es un grupo topológico, la aplicación

$$\cdot^{-1}\colon G \longrightarrow G,\ x \longmapsto x^{-1}$$

coincide con su inversa, así que es un homeomorfismo. Por otro lado si $g \in G$ es fijo, entonces las aplicaciones

$$\begin{aligned} G &\longrightarrow G \times G \\ x &\longmapsto (x, g) \end{aligned} \qquad \begin{aligned} G &\longrightarrow G \times G \\ x &\longmapsto (g, x) \end{aligned}$$

son continuas porque sus coordenadas lo son, luego usando *(A1)* tenemos que las funciones

$$\begin{aligned} r_g\colon G &\longrightarrow G \\ x &\longmapsto xg \end{aligned} \qquad \begin{aligned} \ell_g\colon G &\longrightarrow G \\ x &\longmapsto gx \end{aligned}$$

son continuas por ser composición de funciones continuas. Observamos que las inversa de r_g y ℓ_g son $r_{g^{-1}}$ y $\ell_{g^{-1}}$ respectivamente, que son continuas también, luego r_g y ℓ_g son homeomorfismos para cada $g \in G$.

Por último recordamos que si $f\colon U \to V$ es un homeomorfismo entre espacios topológicos U y V, entonces también es una aplicación abierta (cerrada), es decir si $T \subseteq U$ es abierto (cerrado) entonces $f(T) \subseteq V$ es abierto (cerrado). De esto sigue que si $H \subseteq G$ es abierto (cerrado), entonces $r_g(H) = Hg$ y $\ell_g(H) = gH$ son abiertos (cerrados) de G.

Proposición 1.4. *Sea G un grupo topológico. Cualquier subgrupo H de G es también un grupo topológico con la topología inducida por G.*

Demostración. Sigue de inmediato ocupando la definición de topología inducida. □

Proposición 1.5. [1, Proposición 1, §2.1] *Sea G un grupo topológico. Si H es un subgrupo de G, entonces la clausura topológica $\bar{H}$ de H es un subgrupo de G. Más aún, si H es además normal, entonces $\bar{H}$ es un subgrupo normal de G.*

Demostración. Sea H un subgrupo de G. Debemos probar que $1_G \in \bar{H}$ y que para cada $a, b \in \bar{H}$ se tiene $ab^{-1} \in \bar{H}$.

Es claro que $1_G \in \bar{H}$ pues $1_G \in H \subseteq \bar{H}$. Sea W un entorno de ab^{-1}. Por *(A)*, existen entornos abiertos U y V de a y b respectivamente, tales que $UV^{-1} \subset W$. Por otro lado, como $a, b \in \bar{H}$, $U \cap H \neq \emptyset$ y $V \cap H \neq \emptyset$. Luego, siendo H un subgrupo, $V^{-1} \cap H \neq \emptyset$. Siendo H cerrado para la multiplicación, esto implica que $UV^{-1} \cap H \neq \emptyset$, luego $W \cap H \neq \emptyset$.

La demostración de la última parte de la Proposición es similar. □

Proposición 1.6. *Sea G un grupo topológico. Entonces las siguientes son ciertas:*

i) Los subgrupos abiertos de G son cerrados. Si H es un subgrupo cerrado de G que tiene índice finito entonces es abierto. Además, si G es compacto, todos los subgrupos abiertos de G tienen índice finito.

ii) Si H es un subgrupo de G que contiene algún subconjunto abierto U no vacío de G, entonces H es abierto en G.

iii) G es Hausdorff si y sólo si $\{1_G\}$ es cerrado en G.

iv) Si K es un subgrupo normal de G, entonces el grupo cuociente G/K es Hausdorff si y sólo si K es cerrado en G.

v) Si G es compacto y Hausdorff, y H, N son subgrupos cerrados de G, entonces HN es cerrado en G.

Demostración. i) Supongamos que H es un subgrupo abierto de G. Entonces

$$G \setminus H = \bigcup_{g \notin H} Hg,$$

luego $G \setminus H$ es abierto por ser unión de abiertos, por la Observación 1.3. Por tanto H es cerrado.

Supongamos ahora que H es cerrado con $[G : H] = n < \infty$. Luego existen $g_1, \ldots, g_n \in G \setminus H$ tales que $G \setminus H = \cup_{i=1}^{n} Hg_i$ y cada Hg_i es cerrado por la Observación 1.3, luego H es abierto.

Si ahora G es compacto, entonces para cada H subgrupo abierto de G tenemos que $\{Hg : g \in G\}$ es un cubrimiento abierto de G, por la Observación 1.3. Por la compacidad, existen $g_1, \ldots, g_n \in G$ tales que $G = \cup_{i=1}^{n} Hg_i$. Luego $[G : H] \leq n$.

ii) Si H contiene un abierto no vacío U, entonces $H = \cup_{h \in H} Uh$ es unión de abiertos, por la Observación 1.3, luego H es abierto.

iii) $\Rightarrow$ En cualquier espacio Hausdorff, un conjunto finito es cerrado [1, Teorema 4, §8.1].

$\Leftarrow$ Supongamos que $\{1_G\}$ es cerrado, luego como la función $(x, y) \longmapsto xy^{-1}$ es continua, entonces la diagonal Δ de $G \times G$ es cerrada. Por un argumento de Topología, G es Hausdorff [1, Proposición 4, §8.1].

iv) Sigue fácilmente de *iii)*.

v) Notemos que siendo H, N cerrados en un compacto, ambos son compactos. [1, Proposición 3, §9.3] Por el Teorema de Tychonoff [1, Teorema 3, §9,5], $H \times N$ es compacto, y la imagen de éste por la operación de grupo es HN. Siendo esta operación continua y $H \times N$ compacto, HN es compacto. Como G es Hausdorff, HN es cerrado [1, Proposición 4, §9.3].

□

Ejemplo 1.7. Sea $(\mathbb{C}^*, \times)$ el grupo multiplicativo de $\mathbb{C}$ con la topología inducida por la topología usual de $\mathbb{C}$. El subconjunto $S^1 := \{z \in \mathbb{C}^* : |z| = 1\}$ es un subgrupo topológico compacto de $\mathbb{C}^*$.

En efecto, si $z_1, z_2 \in S^1$ entonces $|z_1 z_2^{-1}| = |z_1||z_2^{-1}| = 1$. Así que S^1 es un subgrupo de $\mathbb{C}^*$. Además es acotado y cerrado, luego por el Teorema de Heine-Borel tenemos la compacidad. Por la Proposición 1.4 concluimos.

Ejemplo 1.8. Sea $(G, \cdot)$ un grupo, y sea τ la topología discreta sobre G. Luego $(G, \tau, \cdot)$ es un grupo topológico.

Por último, definimos el concepto de morfismo entre grupos topológicos.

Definición 1.9. Un **homomorfismo de grupos topológicos** G_1, G_2 es un homomorfismo de grupos $f : G_1 \to G_2$ que es continuo con las topologías de G_1, G_2.
Un **isomorfismo de grupos topológicos** es un homomorfismo de grupos topológicos que es un isomorfismo de grupos y un homeomorfismo.

1.2. Límites inversos

Iniciamos esta sección recordando qué es una categoría.

Definición 1.10. $\mathcal{A}$ es una **categoría** si consta de lo siguiente:

1) Una clase $Ob(\mathcal{A})$, llamada **clase de objetos** de $\mathcal{A}$.

2) Para cada par de objetos $A, B \in Ob(\mathcal{A})$, un conjunto que denotamos $Hom_{\mathcal{A}}(A, B)$. Los elementos de este conjunto se denominan **morfismos** de A en B. Si $f \in Hom_{\mathcal{A}}(A, B)$, lo denotaremos con $f\colon A \to B$.

3) Una operación binaria, que llamamos **composición de morfismos** y denotada por $\circ$. Dados 3 objetos A, B y C de $\mathcal{A}$, la composición es una aplicación:

$$\circ\colon\ Hom_{\mathcal{A}}(B, C) \times Hom_{\mathcal{A}}(A, B) \longrightarrow Hom_{\mathcal{A}}(A, C).$$

La composición de un morfismo $g\colon B \longrightarrow C$ con otro morfismo $f\colon A \longrightarrow B$ se denota por $g \circ f$. Esta operación de composición satisface las siguientes propiedades:

i) **Asociatividad**: si $f\colon A \longrightarrow B$, $g\colon B \longrightarrow C$ y $h\colon C \longrightarrow D$ son morfismos entre los objetos A, B, C, D de $\mathcal{A}$, entonces $h \circ (g \circ f) = (h \circ g) \circ f$.

ii) **Existencia de elemento identidad**: Para cada objeto A de $\mathcal{A}$, existe un morfismo de A a si mismo, que se denota por Id_A, llamado **morfismo identidad** y tal que cualquiera sean los morfismos $f\colon A \longrightarrow B$ y $g\colon C \longrightarrow A$ se cumplen $f \circ Id_A = f$ y $Id_A \circ g = g$.

Definición 1.11. Sea $\mathcal{A}$ una categoría, y A, $B \in Ob(\mathcal{A})$. Diremos que $f \in Hom_{\mathcal{A}}(A, B)$ es un **isomorfismo** si existe $g \in Hom_{\mathcal{A}}(B, A)$ tal que $f \circ g = Id_B$ y $g \circ f = Id_A$.

Ejemplo 1.12. Sea $Ob(\mathcal{A})$ la colección de todos los espacios topológicos.
Para cada $A, B \in Ob(\mathcal{A})$, sea $Hom_{\mathcal{A}}(A, B)$ el conjunto de las funciones continuas de A en B, y sea $\circ$ la composición de funciones. Ésta categoría es la de los espacios topológicos. Los isomorfismos son los homeomorfismos.

Ejemplo 1.13. Sea $Ob(\mathcal{G})$ la colección de todos los grupos.
Para cada $A, B \in \in Ob(\mathcal{G})$, sea $Hom_{\mathcal{G}}(A, B)$ el conjunto de los homomorfismos de grupos de A en B, y $\circ$ la composición de homomorfismos. Ésta categoría es la de los grupos. Los isomorfismos son los isomorfismos de grupos.

Ejemplo 1.14. Sea $Ob(\mathcal{G}^{\text{top}})$ la colección de todos los grupos topológicos.
Para cada $A, B \in \in Ob(\mathcal{G}^{\text{top}})$, sea $Hom_{\mathcal{G}^{\text{top}}}(A, B)$ el conjunto de los homomorfismos de grupos topológicos de A en B, y $\circ$ la composición de homomorfismos. Ésta categoría es la de los grupos topológicos. Los isomorfismos son los isomorfismos de grupos topológicos.

Ejemplo 1.15. Sea $Ob(\mathcal{R})$ la colección de todos los anillos conmutativos con unidad.
Para cada $A, B \in \in Ob(\mathcal{R})$, sea $Hom_{\mathcal{R}}(A, B)$ el conjunto de los homomorfismos de anillos con unidad de A en B, y $\circ$ la composición de homomorfismos de anillos. Ésta categoría es la de los anillos conmutativos con unidad. Los isomorfismos son los isomorfismos de anillos.

Definición 1.16. Sea $(I, \leq)$ un conjunto parcialmente ordenado. Entonces $(I, \leq)$ es un **conjunto director** si para cada $i_1, i_2 \in I$, existe $i_3 \in I$ tal que $i_1 \leq i_3$ e $i_2 \leq i_3$.

Definición 1.17. Sea $\mathcal{A}$ una categoría. Un **sistema inverso** en $\mathcal{A}$ consta de un conjunto director $(I, \leq)$, una familia de objetos $\{X_n\}_{n\in I}$, y una familia de morfismos $\varphi_{nm} : X_m \to X_n$ con $n \leq m$ tales que las siguientes condiciones se satisfacen:

a) $\varphi_{nn} = Id_{X_n}$ para cada $n \in I$.

b) Para cada $n \leq m \leq k$, el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} X_k & \xrightarrow{\varphi_{nk}} & X_n \\ {\scriptstyle \varphi_{mk}}\downarrow & \nearrow_{\varphi_{nm}} & \\ X_m & & \end{array}$$

Notación 2. *Denotaremos a un sistema inverso por (I, X_n, φ_{nm}).*

Ejemplo 1.18. Sea $\mathcal{R}$ la categoría de Anillos conmutativos con unidad. Sea $A \in Ob(\mathcal{R})$ y sea $A[x] = A[x_1, \ldots, x_k]$ el anillo de polinomios a coeficientes en A en k variables, donde $k \in \mathbb{N}$. Sea $I = \mathbb{N}$ con el orden usual, y consideremos $M_n = A[x]/J^n$, donde J es el ideal maximal $(x_1, \ldots, x_k)$. Para cada $n \leq m$, sea

$$\begin{array}{rccc} \varphi_{nm}\colon & M_m & \longrightarrow & M_n \\ p(x_1, \ldots, x_k) + J^m & & \longmapsto & p(x_1, \ldots, x_k) + J^n \end{array}$$

Luego $(\mathbb{N}, M_n, \varphi_{nm})$ es un sistema inverso.

Definición 1.19. Sea $\mathcal{A}$ una categoría, (I, X_n, φ_{nm}) un sistema inverso de $\mathcal{A}$, y sea Y un elemento de $Ob(\mathcal{A})$. Diremos que la familia de morfismos $\{\psi_n\colon Y \to X_n : n \in I\}$ es **compatible** con (I, X_n, φ_{nm}) si para cada $n \leq m$ el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} Y & \xrightarrow{\psi_n} & X_n \\ {\scriptstyle \psi_m}\downarrow & \nearrow_{\varphi_{nm}} & \\ X_m & & \end{array}$$

Definición 1.20. Un **límite inverso** de un sistema inverso (I, X_n, φ_{nm}) es un par (X, φ_n) donde $X \in Ob(\mathcal{A})$ y $\{\varphi_n\colon X \longrightarrow X_n : n \in I\}$ es una familia de morfismos compatible con (I,X_n,φ_{nm}) y tal que satisface la siguiente propiedad:

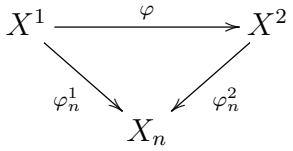
$\mathcal{U}$) Dado cualquier $Y \in Ob(\mathcal{A})$, y una familia de morfismos $\{\psi_n\colon Y \to X_n : n \in I\}$ compatible con (I, X_n, φ_{nm}), existe y es único un morfismo $\psi\colon Y \to X$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} Y & \xrightarrow{\psi_n} & X_n \\ {\scriptstyle \psi}\downarrow & \nearrow_{\varphi_n} & \\ X & & \end{array}$$

La propiedad $\mathcal{U}$) se conoce como la propiedad universal del límite inverso.

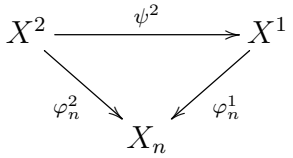
Veremos ahora que dada una categoría $\mathcal{A}$ y un sistema inverso (I, X_n, φ_{nm}) de $\mathcal{A}$, los límites inversos de dicho sistema inverso son únicos salvo isomorfismos.

Teorema 1.21. [7, Proposición 1.12] *Sea (I, X_n, φ_{nm}) un sistema inverso en una categoría. Si (X^1, φ_n^1) y (X^2, φ_n^2) son límites inversos del sistema inverso, entonces existe un isomorfismo $\varphi\colon X^1 \longrightarrow X^2$ tal que el siguiente diagrama es conmutativo:*

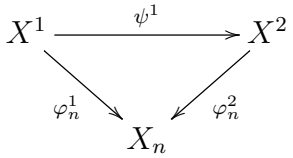


para cada $n \in I$.

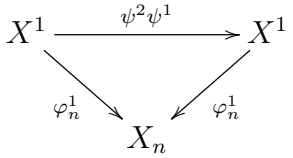
Demostración. Aplicamos la propiedad universal a (X^1,φ_n^1) con la familia $\{\varphi_n^2\}_{n\in I}$: existe un único morfismo ψ^2 tal que el siguiente diagrama es conmutativo, para cada $n \in I$:



Repetimos con (X^2, φ_n^2) y $\{\varphi_n^1\}_{n\in I}$: existe un único morfismo ψ^1 tal que el siguiente diagrama es conmutativo, para cada $n \in I$



Por lo anterior, el siguiente diagrama también será conmutativo:



Por la propiedad universal de (X^1, φ_n^1), la aplicación $\psi^2\psi^1$ es única y luego $\psi^2\psi^1 = Id_{X^1}$.

Se razona de la misma manera con (X^2, φ_n^2). Finalmente ψ^1 y ψ^2 son inversas una de la otra y son únicas. Luego tomamos $\varphi = \psi^1$. □

Teorema 1.22. [7, Proposición 1.12] *Sea (I, X_n, φ_{nm}) un sistema inverso en la categoría de los espacios topológicos. Sea $C := \prod_{n\in I} X_n$ y para cada $n \in I$, sea π_n la proyección de C en X_n. Definimos*

$$X := \{c \in C : \varphi_{nm}\pi_m(c) = \pi_n(c), \forall n \leq m\}$$

y $\varphi_n = \pi_n|_X$ para cada $n \in I$. Entonces (X, φ_n) es un límite inverso de (I, X_n, φ_{nm}).

Demostración. El conjunto C es un espacio topológico con la topología producto y X también lo es con la topología inducida por C. Observamos que los morfismos φ_n son compatibles con (I, X_n, φ_{nm}) por definición de C. Supongamos tener una familia $\{\psi_n\colon Y \longrightarrow X_n : n \in I\}$ de funciones continuas compatible con (I, X_n, φ_{nm}). Debemos probar que existe y

es única una función continua $\psi : Y \longrightarrow X$ tal que $\varphi_n\psi = \psi_n$. Consideremos la siguiente función

$$\begin{aligned}\bar{\psi}\colon \quad & Y \longrightarrow C \\ & y \longmapsto (\psi_n(y))_{n\in I}.\end{aligned}$$

Notemos que ψ_n es continua para cada $n \in I$, así que $\bar{\psi}$ es continua. Ahora, para cada $m \geq n$ tenemos

$$\pi_n\bar{\psi} = \psi_n = \varphi_{nm}\psi_m = \varphi_{nm}\pi_m\bar{\psi},$$

donde la primera y tercera igualdad son por lo anterior y la segunda es porque $\{\psi_n\colon Y \longrightarrow X : n \in I\}$ es compatible con (I, X_n, φ_{nm}). Por lo tanto $\bar{\psi}(Y) \subseteq X$ por definición de X, esto prueba la existencia.

Para la unicidad, si existiera $\psi' : Y \to X$ tal que $\varphi_n\psi' = \psi_n$ para cada n, entonces si proyectamos $\psi'(y)$ en la n-ésima coordenada obtenemos ψ_n para cada n. Luego $\psi' = \bar{\psi}$ es la función pedida. □

Por el Teorema 1.21 el límite inverso de un sistema inverso es único salvo isomorfismo. En la categoría de los espacio topológicos resulta más práctico trabajar con el límite inverso definido en el Teorema anterior, que denotaremos por $s\varprojlim X_n$ y llamaremos *límite inverso especial*.

Un ejemplo que puede resultar interesante es un sistema inverso (I, X_n, φ_{nm}) tal que $s\varprojlim X_n = \varnothing$. En el siguiente ejemplo ilustramos este caso.

Ejemplo 1.23. Sea $I = \mathbb{N}$ con el orden usual, y para cada $n \in I$ sea $X_n = \mathbb{N}$. Para cada $n \leq m$, sean

$$\begin{aligned}\varphi_{nm}\colon X_m &\longrightarrow X_n \\ x &\longmapsto x + (m - n).\end{aligned}$$

Con esto, (I, X_n, φ_{nm}) es un sistema inverso. Sean $C = \prod_{n\in\mathbb{N}} X_n$, $X = s\varprojlim X_n$ y consideremos $m = n + 1$. Luego $\varphi_{n(n+1)}(x) = x + 1$.

Supongamos que $X \neq \varnothing$. Si $c = (x_i)_{n\in\mathbb{N}} \in X$, entonces

$$x_n = \varphi_n(c) = \varphi_{n(n+1)}\varphi_{n+1}(c) = x_{n+1} + 1$$

Es decir, tenemos $x_{n+1} = x_n - 1$. Luego:

$$x_1 = x_0 - 1,\ x_2 = x_1 - 1 = x_0 - 2, \ldots,\ x_{n+1} = x_n - 1 = x_0 - (n + 1)$$

Pero si escogemos $n = x_0$ entonces $x_{x_0+1} = -1 \notin \mathbb{N}$. Por lo tanto, tenemos que $X = \varnothing$.

Proposición 1.24. *Sea (I, X_n, φ_{nm}) un sistema inverso donde los X_n son grupos topológicos y φ_{nm} son homomorfismos continuos. Luego $X = s\varprojlim X_n$ es un grupo topológico y φ_n son homomorfismos continuos.*

Demostración. Sea $C := \prod_{n\in I} X_n$, y sobre C definimos la siguiente operación

$$\begin{aligned}\otimes\colon C \times C &\longrightarrow C \\ ((x_n), (y_n))_{n\in I} &\longmapsto (x_n y_n)_{n\in I},\end{aligned}$$

donde en cada componente se aplica la respectiva operación de cada X_n. Con esto, (C, τ_p, $\otimes$) es un grupo topológico, donde τ_p es la topología producto.

Ahora quisieramos ver que X es un subgrupo de C, es decir, que $1_C \in X$ y que para cada $a, b \in X$, $ab^{-1} \in X$. Es claro que X contiene al elemento identidad. Por otro lado, sean a, $b \in X$. Luego:

$$\begin{aligned} a \in X &\Rightarrow \varphi_{nm}\pi_m(a) = \pi_n(a) \\ b \in X &\Rightarrow \varphi_{nm}\pi_m(b) = \pi_n(b) \end{aligned}$$

Por lo tanto, como π_n y φ_{nm} son homomorfismos de grupos se tiene:

$$\begin{aligned} \varphi_{nm}\pi_m(ab^{-1}) = \varphi_{nm}(\pi_m(a)\pi_m(b^{-1})) &= (\varphi_{nm}\pi_m(a))(\varphi_{nm}\pi_m(b))^{-1} \\ &= (\pi_n(a))(\pi_n(b))^{-1} \\ &= \pi_n(ab^{-1}), \end{aligned}$$

así que $ab^{-1} \in X$. Esto prueba que X es un subgrupo de C. Por la Proposición 1.4 tenemos que X es un grupo topológico. Claramente las funciones $\varphi_n = \pi_n|_X$ son homomorfismos continuos. □

Definición 1.25. Sea (X,τ) un espacio topológico. Decimos que X es **totalmente disconexo** si los únicos subconjuntos conexos de X son los que poseen sólo un elemento.

Teorema 1.26. [7, Proposición 1.13] *Sea (I, X_n, φ_{nm}) un sistema inverso de espacios topológicos y sea $X = \varprojlim X_n$.*

i) Si cada X_n es Hausdorff o totalmente disconexo, también lo es X.

ii) Si cada X_n es Hausdorff, entonces X es cerrado en C.

iii) Si cada X_n es compacto y Hausdorff, también lo es X. Si además cada X_n es no vacío, entonces X es no vacío.

Demostración. Los ítem *i)* y *iii)* siguen de propiedades topológicas del producto ocupando el *Teorema de Tychonoff* [6, pág 147, Teor. 6.28]. El más delicado de tratar es el ítem *ii)*, donde se utiliza el hecho de que si $f, g\colon X \longrightarrow Y$ son funciones continuas e Y es Hausdorff, entonces el conjunto $C = \{x \in X : f(x) = g(x)\}$ es un subconjunto cerrado de X. Luego solo reescribimos $\varprojlim X_n$ como

$$\varprojlim X_n = \bigcap_{n \leq m} \{c \in C : \varphi_{nm}\pi_m(c) = \pi_n(c)\},$$

que es una intersección arbitraria de conjuntos cerrados por la observación anterior. Luego $\varprojlim X_n$ es cerrado en C. □

Teorema 1.27. [7, Proposición 1.14] *Sea (I, X_n, φ_{nm}) un sistema inverso de espacios topológicos no vacíos, compactos y Hausdorff, y sea $X = \varprojlim X_n$. Las siguientes son ciertas:*

i) Los conjuntos $\varphi_n^{-1}(U)$ con $n \in I$, U abierto en X_n forman una base para la topología en X.

ii) Si $Y \subseteq X$ cumple $\varphi_n(Y) = X_n$ para cada $n \in I$, entonces Y es denso en X.

iii) Si $\theta : Y \to X$ es una función, entonces θ es continua sí y sólo si $\varphi_n\theta$ es continua para cada $n \in I$.

Demostración. i) Notemos que cada abierto en X se puede escribir como unión de conjuntos de la forma

$$P = X \cap \bigcap_{r=1}^{n} \pi_{i_r}^{-1}(U_r)$$

donde $n \in \mathbb{N}$, $i_r \in I$ para cada r y $U_r \subseteq X_{i_r}$ es abierto para cada r. Para probar que los conjuntos $\varphi_i^{-1}(U)$ con U abierto en X_i forman una base para la topología en X, basta probar que dado $a \in P$, existe $\varphi_m^{-1}(U)$ con U abierto en X_m tal que $a \in \varphi_m^{-1}(U) \subseteq P$.

Sea $a \in P$ y sea $m = max\{i_r : r = 1, \dots, n\}$ (notemos que m existe pues por hipótesis I es un conjunto director, luego el conjunto de los i_r tiene una cota superior), así que $\varphi_{im}(a_m) = a_i$ para cada $i \leq m$. Sea

$$U = \bigcap_{r=1}^{n} \varphi_{i_r m}^{-1}(U_r)$$

Luego U es un entorno abierto de $a_m \in X_m$ ya que $\varphi_{i_r m}(a_m) = a_{i_r}$ para cada i_r. Luego $\varphi_m^{-1}(U)$ es un entorno abierto de $a \in X$. Para mostrar que $\varphi_m^{-1}(U) \subseteq P$, basta notar que si $b \in \varphi_m^{-1}(U)$, entonces $b_m \in U$ así que $b_{i_r} = \varphi_{i_r m}(b_m) \in U_r$ para cada $r = 1, \dots, n$.

ii) Sea $Y \subseteq X$ tal que $\varphi_i(Y) = X_i$ para cada i. Entonces para cada abierto U de X_i se tiene $Y \cap \varphi_i^{-1}(U) \neq \varnothing$. Pero por *i)* como los $\varphi_i^{-1}(U)$ con U abierto en X_i forman una base para la topología en X, para cada $x \in X$, existe $i \in I$ y existe U abierto en X_i tal que $x \in \varphi_i^{-1}(U)$ y además $Y \cap \varphi_i^{-1}(U) \neq \varnothing$. Luego $\bar{Y} = X$.

iii) Es trivial, usando propiedades de las funciones continuas.

□

Ejemplo 1.28. Sea p un número primo. Definimos el sistema inverso de grupos topológicos finitos $(\mathbb{N}, \mathbb{Z}/p^n\mathbb{Z}, \varphi_{nm})$, donde cada $\mathbb{Z}/p^n\mathbb{Z}$ está dotado de la topología discreta y, para $m \geq n$ se define

$$\begin{aligned} \varphi_{nm}: \quad \mathbb{Z}/p^m\mathbb{Z} &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ x + p^m\mathbb{Z} &\longmapsto x + p^n\mathbb{Z}, \end{aligned}$$

que claramente es continua. Vamos a caracterizar el conjunto $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Por la Proposición 1.24 $\mathbb{Z}_p$ es un grupo topológico.

Por definición un elemento $z \in \mathbb{Z}_p$ es de la forma $z = (z_1, z_2, \dots)$ donde $z_k \in \mathbb{Z}/p^k\mathbb{Z}$ y además el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathbb{Z}/p^m\mathbb{Z} & \xrightarrow{\varphi_{nm}} & \mathbb{Z}/p^n\mathbb{Z} \\ {\scriptstyle \pi_m}\uparrow & \nearrow_{\pi_n} & \\ \mathbb{Z}_p, & & \end{array}$$

o sea dado $z \in \mathbb{Z}_p$ se cumple $\varphi_{nm}\pi_m(z) = \pi_n(z)$. Sea $m = n + 1$, entonces

$$z_{n+1} + p^n\mathbb{Z} = \varphi_{n(n+1)}(z_{n+1} + p^{n+1}\mathbb{Z}) = z_n + p^n\mathbb{Z},$$

así que obtenemos $z_{n+1} \equiv z_n \,(\mathrm{mod}\, p^n)$. Dicho límite inverso se conoce como grupo de los *Enteros p-ádicos.*

Ejemplo 1.29. Sea $I = \mathbb{Z}_{>0}$ con el orden dado por la divisibilidad, es decir $n \leq m$ si y sólo si $n|m$. Para cada $n \in I$, sea $X_n = \mathbb{Z}/n\mathbb{Z}$ con la operación de suma y dotado de la topología discreta. Para cada $n \leq m$, consideramos los siguientes homomorfismos de grupo:

$$\begin{aligned} \varphi_{nm} \colon \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x + m\mathbb{Z} &\longmapsto x + n\mathbb{Z}. \end{aligned}$$

Luego $(I,\ X_n,\ \varphi_{nm})$ es un sistema inverso de grupos topológicos finitos y φ_{nm} es un homomorfismo de grupos para cada $n \leq m$. En efecto, es claro que I es un conjunto director pues si $n, m \in I$, basta escoger $j = mcm(n, m)$. Si $m = n$ entonces

$$\begin{aligned} \varphi_{nn} \colon \mathbb{Z}\big/_{n\mathbb{Z}} &\longrightarrow \mathbb{Z}\big/_{n\mathbb{Z}} \\ x + n\mathbb{Z} &\longmapsto x + n\mathbb{Z} \end{aligned}$$

Asi que $\varphi_{nn} = Id_{X_n}$. Sean ahora $n \leq m \leq k$, luego :

$$\begin{aligned} \varphi_{nm}\varphi_{mk}(x + k\mathbb{Z}) &= \varphi_{nm}(x + m\mathbb{Z}) \\ &= x + n\mathbb{Z} \\ &= \varphi_{nk}(x + k\mathbb{Z}) \end{aligned}$$

Asi que $(I,\ X_n,\ \varphi_{nm})$ es un sistema inverso. Sea $\hat{\mathbb{Z}} = \varprojlim X_n$. Si $c = (c_i)_{i=1}^{\infty} \in \hat{\mathbb{Z}}$ entonces

$$\begin{aligned} c_n + n\mathbb{Z} &= \pi_n(c) \\ &= \varphi_{nm}\pi_m(c) \\ &= \varphi_{nm}(c_m + m\mathbb{Z}) \\ &= c_m + n\mathbb{Z}. \end{aligned}$$

Es decir, para cada $n \leq m$, $c_m \equiv c_n$ *(mod n)*. En particular si $m = n + 1$ entonces se obtiene $c_{n+1} \equiv c_n$ *(mod n)*. El grupo $\hat{\mathbb{Z}}$ se conoce como *Completación Profinita* de $\mathbb{Z}$.

Observación 1.30. Se puede probar que

$$\hat{\mathbb{Z}} \simeq \prod_{p\ primo} \mathbb{Z}_p$$

donde $\mathbb{Z}_p$ denota el grupo de los enteros p-ádicos.

1.3. Grupos Profinitos

Definición 1.31. Un **grupo profinito** G es un grupo topológico isomorfo a un límite inverso de un sistema inverso de grupos finitos con la topología discreta.

Teorema 1.32. *Sea G un grupo profinito. Entonces G es Hausdorff, compacto y totalmente disconexo.*

Demostración. Si G es profinito, luego es isomorfo a un límite inverso de grupos finitos, digamos G_n. Siendo G_n grupos topológicos finitos con la topología discreta, es inmediato que éstos son compactos, Hausdorff y totalmente disconexos. Por el Teorema 1.26 concluimos. □

Ejemplo 1.33. En los Ejemplos 1.28 y 1.29 tenemos que $\mathbb{Z}_p$ y $\hat{\mathbb{Z}}$ son límites inversos de grupos finitos, así que ambos son grupos profinitos.

Proposición 1.34. *Sea (G, φ_n) un límite inverso de un sistema inverso (I, G_n, φ_{nm}) de grupos topológicos compactos Hausdorff y sea L un subgrupo normal abierto de G. Entonces $Ker(\varphi_n)$ es un subgrupo cerrado de L por algún $n \in I$. Además G/L es isomorfo como grupo topológico a un grupo cociente de un subgrupo de algún G_n. Si además cada φ_n es sobreyectiva, entonces G/L es isomorfo a un grupo cociente de algún G_n.*

Demostración. Por el Teorema 1.27, siendo L un subgrupo normal abierto de G que contiene 1_G, $\varphi_n^{-1}(U) \subseteq L$, por algún n y por algún abierto U de G_n que contiene $1 = 1_{G_n}$. Luego $Ker(\varphi_n) = \varphi_n^{-1}(\{1\}) \subseteq L$. Así, $Ker(\varphi_n)$ es un subgrupo cerrado de L por algún n.

Por el 3^{er} Teorema de isomorfismo, se tiene

$$G/L \cong (G/\mathrm{Ker}(\varphi_n))/(L/\mathrm{Ker}(\varphi_n)).$$

Como $G/\mathrm{Ker}(\varphi_n) \simeq \mathrm{Im}(\varphi_n)$ (1^{er} Teorema de isomorfismo), sigue que G/L es isomorfo a un cociente de $\mathrm{Im}(\varphi_n)$. Si φ_n es sobreyectiva, entonces $\mathrm{Im}(\varphi_n) = G_n$. □

Definición 1.35. Sea G un grupo topológico y sea I una familia de subgrupos normales abiertos de G. Decimos que I es una **base filtrada** si para cada $H_1, H_2 \in I$ existe $H_3 \in I$ tal que $H_3 \subseteq H_1 \cap H_2$.

Proposición 1.36. [7, Proposición 1.19] *Sea G un grupo topológico e I una base filtrada de subgrupos normales cerrados de G. Para $H, N \in I$, definimos la siguiente relación (de orden) en I:*

$$H \preceq N \Leftrightarrow N \subseteq H$$

Las siguientes son ciertas:

i) $(I, \preceq)$ es un conjunto director.

ii) Los homomorfismos $\varphi_{HN} \colon G/N \to G/H$ definidos para $H \preceq N$ son tales que $(I, G/H, \varphi_{HN})$ es un sistema inverso.

iii) Sea $\bar{G} = \varprojlim G/H$. Existe un homomorfismo continuo $\psi \colon G \to \bar{G}$ con Kernel $\bigcap_{H \in I} H$ y cuya imagen es un subgrupo denso de $\bar{G}$.

iv) Si en iii) además consideramos G compacto y $\bigcap_{H \in I} H = \{1_G\}$ entonces ψ es un isomorfismo de grupos topológicos.

Demostración. i) Primero mostramos que $(I, \preceq)$ es un conjunto director. Es claro que $\preceq$ define un orden parcial sobre I. Dados $H_1, H_2 \in I$, consideramos $H_3 \in I$ tal que $H_3 \subseteq H_1 \cap H_2$. Luego $H_1 \preceq H_3$, $H_2 \preceq H_3$.
ii) Mostramos que $(I, G/H, \varphi_{HN})$ es un sistema inverso. Si $H = N$ entonces

$$\begin{aligned} \varphi_{HH} \colon G/H &\longrightarrow G/H \\ gH &\longmapsto gH, \end{aligned}$$

así que $\varphi_{HH} = Id_{G/H}$. Por otro lado si H, N, $K \in I$ son tales que $H \preceq N \preceq K$ luego

$$\begin{aligned} \varphi_{HN}\varphi_{NK}(gK) &= \varphi_{HN}(gN) \\ &= gH \\ &= \varphi_{HK}(gK). \end{aligned}$$

Por lo tanto $(I, G/H, \varphi_{HN})$ es un sistema inverso de grupos.

iii) Consideremos la aplicación

$$\begin{aligned} \psi \colon G &\longrightarrow C = \prod_{H \in I} G/H \\ g &\longmapsto (gH)_{H \in I}. \end{aligned}$$

Claramente φ es un homomorfismo de grupos, y notamos que $\mathrm{Im}(\varphi) \subseteq \bar{G}$ pues dado $(gH)_{H \in I} \in C$ se tiene:

$$\varphi_{HN}\varphi_N((gH)_{H \in I}) = gH = \varphi_H((gH)_{H \in I})$$

donde $\varphi_H = \pi_H|_{\bar{G}}$.

Ahora recordamos que $q_H \colon G \to G/H$ es continua en la topología cociente, y la proyección $\pi_H \colon C \to G/H$ es continua en la topología producto, luego ψ es continua. En efecto, notemos que

$$q_H = \varphi_H \psi$$

Luego, por la continuidad de q_H, para cada abierto U en G/H se tiene que

$$q_H^{-1}(U) = (\varphi_H \psi)^{-1} = \psi^{-1}\varphi_H^{-1}(U)$$

es abierto. Como los conjuntos $\varphi_H^{-1}(U)$ forman una base de la topología de $\bar{G}$ por el Teorema 1.27 i), concluimos que ψ es continua. Luego ψ es un homomorfismo continuo.

Sea ahora $g \in G$. Luego $g \in \mathrm{Ker}(\psi)$ si y sólo si $gH = H$ para cada $H \in I$, es decir $g \in H$ para cada H en I así que $\mathrm{Ker}(\psi) = \bigcap_{H \in I} H$.
Por otro lado, como $q_H = \varphi_H \psi$, luego $\varphi_H(\mathrm{Im}(\psi)) = \mathrm{Im}(q_H) = G/H$ ya que q_H es sobreyectiva para cada $H \in I$. Concluímos que $\mathrm{Im}(\psi)$ es denso en $\bar{G}$ por el Teorema 1.27 ii).

iv) Supongamos ahora que G es compacto. Observamos que G/H es Hausdorff para cada $H \in I$ por la Proposición 1.6, iv). Luego $\bar{G}$ es Hausdorff por el Teorema 1.26 i).

Como ψ es continua, $\psi(G)$ es compacto en $\bar{G}$, y como éste último es Hausdorff, tenemos que $\psi(G)$ es cerrado en $\bar{G}$. Como $\psi(G)$ es denso en $\bar{G}$, tenemos que $\psi(G) = \bar{G}$, así que ψ es sobreyectiva. Si además $\mathrm{Ker}(\psi) = \bigcap_{H \in I} H = \{1_G\}$ entonces ψ es inyectiva, luego es un isomorfismo de grupos.

Para probar que ψ es un homeomorfismo de espacios topológicos, basta probar que ψ es una aplicación cerrada, es decir que para cada cerrado L de G, $\psi(L)$ es cerrado en $\bar{G}$. Esto sigue de un resultado estándar en topología por el hecho que G es compacto y $\bar{G}$ es Hausdorff. Esto prueba que ψ es un isomorfismo de grupos topológicos. □

Teorema 1.37. [7, Teorema 1.26] *Sea G un grupo profinito. Si I es una base filtrada de subgrupos normales cerrados de G tal que $\cap_{H\in I} H = \{1_G\}$ entonces*

i) $G \simeq \varprojlim_{H\in I} G/H$.

ii) Para cada N, K cerrados en G, tenemos

$$N \simeq \varprojlim_{H\in I} N/(N\cap H)$$

y

$$G/K \simeq \varprojlim_{H\in I} G/KH$$

Demostración. Las primeras dos afirmaciones son consecuencia de la Proposición 1.36. Para la tercera afirmación, notemos que $J = \{KH : H \in I\}$ es una base filtrada de subgrupos normales cerrados de G/K, donde $\cap_{H\in I} KH = K$ y de nuevo por la Proposición 1.36 concluimos. □

Teorema 1.38. [7, Corolario 1.25] *Sea G un grupo topológico. Las siguientes son equivalentes*

1) G es profinito.

2) Como grupo topológico, G es isomorfo a un subgrupo cerrado de un producto de grupos finitos.

3) G es compacto y $\cap\{H : H$ es subgrupo normal abierto de $G\} = \{1_G\}$.

Demostración.
1) ⇒ 2) Si G es profinito entonces existe un conjunto I de grupos finitos tal que $G \simeq \varprojlim_{H\in I} H$. éste último es cerrado en C por el Teorema 1.26 ii).

2) ⇒ 3) Cada grupo finito es compacto, asi que un producto $\mathcal{C} = \prod_j G_j$ de ellos también lo es por el Teorema de Tychonoff. Siendo G isomorfo (como grupo topológico) a un subgrupo cerrado $\hat{G}$ de $\mathcal{C}$, luego G es compacto.

Sea $I = \{H$: H es un subgrupo normal abierto de $\hat{G}\}$. Sea K_j el kernel de la proyección $\pi_j : \mathcal{C} \to G_j$. Observamos que K_j es un subgrupo normal abierto de $\mathcal{C}$ (recordamos que los grupos G_j tienen la topología discreta). Luego $N_j := K_j \cap \hat{G}$ es un subgrupo normal abierto de $\hat{G}$, y luego pertenece a I. Luego $\cap_{H\in I} H \subseteq \cap_j N_j \subseteq \cap_j K_j = \{1_{\hat{G}}\}$. Siendo G isomorfo a $\hat{G}$ como grupo topológico, la misma propiedad se cumple para G.

3) ⇒ 1) Sea $I = \{H : H$ subgrupo normal abierto de $G\}$. Para cada $H_1, H_2 \in I$, claramente tenemos que $H_1 \cap H_2 \in I$, asi que I es una base filtrada. Concluimos por la Proposición 1.36. □

Capítulo 2

Teoría de Galois

En éste capítulo vamos a introducir el concepto de extensión de Galois para una extensión cualquiera de campos, no necesariamente finita. Luego, vamos a enunciar y probar el Teorema de Correspondencia de Galois. En el caso infinito, necesitaremos introducir una topología llamada Topología de Krull. Éste capítulo está basado en las referencias [2–5, 7, 9].

2.1. Extensiones de campos y Grupo de Galois

Definición 2.1. Una **extensión de campos** es una inclusión de un campo k en otro campo K tal que las operaciones en k son inducidas por las de K. Denotamos la extensión por K/k.

Definición 2.2. Si K/k es una extensión de campos luego K es un espacio vectorial sobre k. La dimensión de éste se llama **grado de la extensión** y se denota por $[K : k]$. Diremos que K/k es una **extensión finita** si $[K : k]$ es finito.

Sea K/k una extensión de campos y sea $a \in K$. Consideremos la aplicación

$$\begin{aligned} \varphi_a : \quad & k[x] \longrightarrow K \\ & p(x) \longmapsto p(a). \end{aligned}$$

Notemos que $\varphi_a(p+q) = \varphi_a(p) + \varphi_a(q)$ y $\varphi_a(pq) = \varphi_a(p)\varphi_a(q)$, así que φ_a es un homomorfismo de anillos. Como $Ker(\varphi_a)$ es un ideal de $k[x]$ y K es un dominio íntegro, $Ker(\varphi_a)$ es un ideal primo de $k[x]$. Por otro lado, siendo $k[x]$ es un dominio por ideales principales, hay dos casos: $Ker(\varphi_a) = \{0\}$ y decimos que a es **trascendental**, o bien $Ker(\varphi_a) = (p_a(x))$ donde $p_a(x)$ es mónico e irreducible sobre $k[x]$, y en este caso decimos que a es **algebraico**. El polinomio $p_a(x)$ se llama **polinomio mínimo** de a.

Definición 2.3. Sea K/k una extension de campos. Diremos que K/k es una **extensión algebraica** si cada $a \in K$ es algebraico sobre k.

Teorema 2.4 (de Kronecker)**.** *Sea k un cuerpo y $p(x) \in k[x]$ un polinomio de grado $n \geq 1$. Luego existe una extensión K/k tal que K contiene una raíz α de $p(x)$.*

Demostración. Descomponemos $p(x)$ en factores irreducibles sobre $k[x]$:

$$p(x) = p_1(x) \cdots p_m(x).$$

El campo K pedido es $K := k[x]/(p_1(x))$ y una raíz es $\alpha = x + (p_1(x))$. □

Definición 2.5. Sea $p(x) \in k[x]$. Un **campo de descomposición** de $p(x)$ es una extensión de campos F/k que contiene todas las raíces de $p(x)$ y es la más chica que cumple con esto.

De ésta definición surge la siguiente pregunta: Dado un polinomio $p(x) \in k[x]$, ¿Siempre existe un campo de descomposición para $p(x)$? La respuesta es sí y lo probamos en la siguiente proposición.

Proposición 2.6. [3, Proposición 2.4] *Para cada $p(x) \in k[x]$, existe una extensión F/k tal que F es campo de descomposición de $p(x)$ y $[F : k] \leq (deg(p))!$.*

Demostración. Por inducción sobre $n = deg(p)$. Si $n = 1$ entonces tomamos $F = k$. Supongamos que $deg(p) > 1$. Por el Teorema 2.4 existe un campo $F_1 := k(a_1)$ tal que $p(a_1) = 0$. Luego $p(x) = (x - a_1)q(x)$, donde $deg(q) = deg(p)$ - 1. Usando la hipótesis de inducción, existe un campo de descomposición $F_2 := F_1(a_2, ..., a_n)$ de $q(x)$ sobre F_1. Por lo tanto $p(x) = (x - a_1)...(x - a_n)$ en $F_2[x]$ y $F := k(a_1, ..., a_n)$ es campo de descomposición de $p(x)$ sobre k. Concluimos aplicando la *Ley de la Torre* [2, pág 6, Teor. 1.1.6]. □

Definición 2.7. Sea K/k una extensión de campos. Diremos que K/k es **normal** si cualquier polinomio irreducible en $k[x]$ que tiene una raíz en K, tiene todas las raíces en K.

Teorema 2.8. [2, Teorema 1.4.2] *Sea K/k una extensión de campos. Las siguientes son equivalentes:*

a) K/k es finita y normal.

b) K es campo de descomposición de algún polinomio $p \in k[x]$.

Demostración. Ver [2, Teorema 1.4.2].

□

Definición 2.9. Sea K/k una extensión algebraica de campos.

i) Un polinomio $p \in k[x]$ no constante es **separable** si no tiene raíces múltiples en un campo de descomposición.

ii) Un elemento $a \in K$ es **separable** si $p_a(x) \in k[x]$ es separable.

iii) La extensión K/k es **separable** si cada $a \in K$ es separable.

Definición 2.10. Sean L, K dos campos. Un **isomorfismo** de L en K es una función $\sigma\colon L \to K$ que satisface las siguientes propiedades para cada $a, b \in L$:

a) $\sigma(a + b) = \sigma(a) + \sigma(b)$,

b) $\sigma(ab) = \sigma(a)\sigma(b)$,

c) $\sigma(1) = 1$,

Un **automorfismo** de K es un isomorfismo $K \to K$.

El conjunto de automorfismos de un campo K con la composición de automorfismos forma un grupo que denotamos por $\mathrm{Aut}(K)$.

Definición 2.11. Sean $k \subseteq L \subseteq K$ extensiones de campos. Un isomorfismo σ de L en K se llama **k-isomorfismo** si $\sigma(a) = a$ para cada $a \in k$. Si $K = L$ entonces σ se dice **k-automorfismo**.

Definición 2.12. Sea K/k una extensión de campos. Definimos el **Grupo de Galois** de K/k como:

$$Gal(K/k) = \{\sigma \in Aut(K) : \sigma(a) = a,\ \forall a \in k\}.$$

Notemos que $Gal(K/k)$ es un subgrupo de $Aut(K)$ con la composición.

Definición 2.13. Sea K/k una extensión de campos, y sea G un subgrupo de $Gal(K/k)$. Definimos el **campo fijo** por G como

$$K^G = \{x \in K : \sigma(x) = x,\ \forall\ \sigma \in G\}.$$

Teorema 2.14 (Extensión de Isomorfismo)**.** [5, Proposición 2, §10] *Sean K/L y L/k extensiones algebraicas de campos con K/k normal y sea $\sigma\colon L \to K$ un k-isomorfismo. Existe un k-automorfismo $\tau\colon K \to K$ tal que $\tau(a) = \sigma(a)$, para cada $a \in L$.*

Demostración. Sea $\mathcal{G}$ el conjunto de los pares (F, ρ) tales que F es un campo con $L \subseteq F \subseteq K$ y ρ es un $k-$isomorfismo $F \to K$ que cumple $\rho|_L = \sigma$. Si (F_1, ρ_1) y (F_2, ρ_2) están en $\mathcal{G}$, ponemos $(F_1, \rho_1) \leq (F_2, \rho_2)$ si $F_1 \subseteq F_2$ y también $\rho_1 = \rho_2|_{F_1}$. Luego $(\mathcal{G}, \leq)$ es un conjunto parcialmente ordenado y no vacío pues $(L, \sigma) \in \mathcal{G}$. Además, claramente cada cadena en $\mathcal{G}$ tiene una cota superior. Por el *Lema de Zorn*, $\mathcal{G}$ tiene elemento maximal, digamos (F', ρ'). Vamos a mostrar que $F' = K$.

Supongamos que existe $a \in K$ tal que $a \notin F'$. El polinomio mínimo $p_a(x) \in k[x]$ tiene una raiz en K y luego se descompone en $K[x]$ por ser K/k normal. Escribimos $p_a(x) = f(x)g(x)$, donde $f(x)$ es el polinomio minimo de a sobre F' y $g(x) \in F'[x]$. Luego $p_a(x) = (\rho' f)(x)(\rho' g)(x)$ y por lo tanto $(\rho' f)(x)$ se descompone en $K[x]$. Sea a_1 una raíz de $(\rho' f)(x)$ en K, luego existe un k-isomorfismo ρ'' de $F'(a)$ sobre $\rho' F'(a_1)$ tal que $\rho''(a) = a_1$ y además $\rho''|_{F'} = \rho'|_{F'}$. Por lo tanto $(F', \rho') < (F'(a), \rho'')$, lo cual es una contradicción. Así que $F' = K$ y $\rho' = \tau$ es el k-isomorfismo pedido. □

Definición 2.15. Sea K/k una extensión algebraica de campos. Diremos que la extensión K/k es de **Galois** si es normal y separable.

En algunos textos de Teoría de Galois clásica se define una extensión de Galois como una extensión K/k que cumple $K^{Gal(K/k)} = k$. En el siguiente Teorema mostraremos que ésta condición es equivalente a la dada en la definición anterior, tanto en el caso finito como en el caso infinito.

Teorema 2.16. [5, Teorema 20, §10] *Sea K/k una extensión algebraica de campos. Entonces K/k es una extensión de Galois si y sólo si $K^{Gal(K/k)} = k$.*

Demostración. $\Rightarrow$) Será suficiente mostrar que $K^{Gal(K/k)} \subseteq k$. Sea $a \in K^{Gal(K/k)}$ y sea $p_a(x) \in k[x]$ su polinomio mínimo. Como la extensión K/k es normal, $p_a(x)$ tiene todas sus raíces en K. Luego existe un campo de descomposición L de $p_a(x)$ y la extensión L/k es normal y finita por el Teorema 2.8. Por otro lado, siendo K/k separable, $p_a(x)$ es separable y luego L/k es una extensión de Galois finita.
Sea ahora $\sigma \in Gal(L/k)$. Por el Teorema 2.14 existe $\tau \in Gal(K/k)$ tal que $\tau(b) = \sigma(b)$ para cada $b \in L$. Pero $a \in K^{Gal(K/k)}$ implica que $a = \tau(a) = \sigma(a)$, es decir $a \in L^{Gal(L/k)}$

$= k$ [5, Teorema 4].

$\Leftarrow$) Sea $a \in K$ y consideremos el conjunto $A = \{\sigma(a)\colon \sigma \in Gal(K/k)\}$. Notemos que, siendo a una raíz de $p_a(x)$, y $\sigma \in Aut(K)$, entonces

$$0 = \sigma(0) = \sigma(p_a(a)) = \sigma(\sum_{i=1}^{n} b_i a^i) = \sum_{i=1}^{n} b_i \sigma(a)^i.$$

Luego $\sigma(a)$ es también una raíz de $p_a(x)$. Por lo tanto dicho automorfismo actúa como permutación sobre A.

Definimos el polinomio $f(x) = \prod_{b\in A}(x - b)$ y notamos que sus coeficientes están en $K^{Gal(K/k)} = k$, pues por lo anterior cada $\sigma \in Gal(K/k)$ actúa como permutación sobre las raíces de $p_a(x)$. Luego $f(x)$ divide a $p_a(x)$ pero como $p_a(x)$ es el polinomio mínimo de a la única opción es que $f(x) = p_a(x)$. Por lo tanto a es separable para cada $a \in K$ y entonces la extensión K/k es separable, y la normalidad es inmediata. □

Proposición 2.17. [3, Proposición 7.3] *Sea K/k una extensión de Galois. Para cualquier campo entremedio $k \subseteq L \subseteq K$, la extensión K/L es también de Galois.*

Demostración. Sea $p(x) \in L[x]$ irreducible que tiene una raíz a en K. Como K/k es normal y separable, $p_a(x) \in k[x]$ tiene todas sus raíces distintas en K. Finalmente como $p(x)$ divide a $p_a(x)$ en $L[x]$, entonces $p(x)$ tiene todas sus raíces distintas en K. □

2.2. Caso finito

En esta sección vamos a recordar el Teorema de correspondencia de la Teoría de Galois clásica. Veremos un ejemplo para recordar su aplicación y finalmente vamos a ver un ejemplo en el cual dicho Teorema no es verdadero, ver [2, Teorema 2.4.1].

Teorema 2.18 (Correspondencia de Galois, caso finito)**.** *Sea K/k una extensión de Galois finita. Las siguientes afirmaciones se cumplen:*

1. *Para cada campo F entremedio $k \subseteq F \subseteq K$, se tiene*

$$K^{Gal(K/F)} = F \qquad |Gal(K/F)| = [K : F] \qquad [Gal(K/k) : Gal(K/F)] = [F : k]$$

Además, F/k es de Galois si y sólo si $Gal(F/k)$ es un subgrupo normal de $Gal(K/k)$. En este caso tenemos el siguiente isomofismo

$$Gal(F/k) \simeq {}^{Gal(K/k)}\!/_{Gal(K/F)}$$

2. *Para cada subgrupo H de $Gal(K/k)$ se tiene*

$$Gal(K/K^H) = H \qquad [K : K^H] = |H| \qquad [K^H : k] = [Gal(K/k) : H]$$

Ejemplo 2.19. Vamos a aplicar el Teorema de Correspondencia a la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$, donde ζ es una raíz primitiva 7-ésima de la unidad. Es claro que dicha extensión es normal y separable, luego es de Galois. La Teoría de Galois clásica nos dice que

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^{\times} \cong \mathbb{Z}/6\mathbb{Z}.$$

Sea $\tau \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ tal que $\tau(\zeta) = \zeta^3$. Luego $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) = \langle\tau\rangle$. Los subgrupos de $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ no triviales son $\langle\tau^3\rangle$ y $\langle\tau^2\rangle$, de órdenes 2 y 3 respectivamente. Sabemos que los campos entremedios de $\mathbb{Q}(\zeta)/\mathbb{Q}$ que se corresponden con dichos subgrupos de $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ son $\mathbb{Q}(\zeta)^{\langle\tau^3\rangle}$ y $\mathbb{Q}(\zeta)^{\langle\tau^2\rangle}$. Vamos a caracterizar dichos campos.

Sea $a = \zeta + \bar{\zeta} = \zeta + \zeta^{-1}$. Notemos que $a \in \mathbb{Q}(\zeta)^{\langle\tau^3\rangle}$ y por lo tanto $\mathbb{Q}(a) \subseteq \mathbb{Q}(\zeta)^{\langle\tau^3\rangle}$. Además, la inclusión $\mathbb{Q}(a) \subseteq \mathbb{Q}(\zeta)$ tiene grado ≤ 2, porqué ζ es raiz del polinomio $x^2 - ax + 1 \in \mathbb{Q}(a)[x]$. Por otro lado sabemos que $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^{\langle\tau^3\rangle}$ tiene grado dos. Aplicando la *Ley de la Torre* a la cadena de inclusiones

$$\mathbb{Q}(a) \subseteq \mathbb{Q}(\zeta)^{\langle\tau^3\rangle} \subseteq \mathbb{Q}(\zeta)$$

se concluye que $\mathbb{Q}(a) = \mathbb{Q}(\zeta)^{\langle\tau^3\rangle}$.

Falta caracterizar el subcampo $\mathbb{Q}^{\langle\tau^2\rangle}$. Para ello, recordamos que una base para la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$ es $\mathcal{B} = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$. Por lo tanto si $b \in \mathbb{Q}(\zeta)$, entonces existen únicos $\alpha_i \in \mathbb{Q}$, $i = 0, ..., 5$ tales que

$$b = \alpha_0 + \alpha_1\zeta + \alpha_2\zeta^2 + \alpha_3\zeta^3 + \alpha_4\zeta^4 + \alpha_5\zeta^5 \tag{1}$$

Asi que $b \in \mathbb{Q}^{\langle\tau^2\rangle}$ si y sólo si

$$\begin{aligned} b &= \tau^2(b) \\ &= \alpha_0 + \alpha_1\zeta^2 + \alpha_2\zeta^4 + \alpha_3\zeta^6 + \alpha_4\zeta^8 + \alpha_5\zeta^{10} \\ &= \alpha_0 + \alpha_4\zeta + \alpha_1\zeta^2 + \alpha_5\zeta^3 + \alpha_2\zeta^4 + \alpha_3\zeta^6 \\ &= (\alpha_0 - \alpha_3) + (\alpha_4 - \alpha_3)\zeta + (\alpha_1 - \alpha_3)\zeta^2 + (\alpha_5 - \alpha_3)\zeta^3 + (\alpha_2 - \alpha_3)\zeta^4 - \alpha_3\zeta^5 \end{aligned}$$

donde la última igualdad es porque $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta 5 + \zeta^6 = 0$.

De la igualdad anterior y de (1) se deduce que $\alpha_3 = \alpha_5 = 0$, y $\alpha_1 = \alpha_2 = \alpha_4$. Por lo tanto $b \in \mathbb{Q}^{\langle\tau^2\rangle}$ si y sólo si $b = a + c(\zeta + \zeta^2 + \zeta^4)$, con $a, c \in \mathbb{Q}$. Luego $\mathbb{Q}^{<\tau^2>} = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$.

Por último, vamos a ver un caso particular de una extensión de grado infinito en el que no es posible aplicar el Teorema de Correspondencia.

Ejemplo 2.20. Dado p un número primo, sea $\mathbb{F}_p$ el campo finito con p elementos y sea $\mathbb{F}$ su clausura algebraica. La extensión $\mathbb{F}/\mathbb{F}_p$ es infinita, normal y separable, luego es de Galois.

Sea H el subgrupo de $Gal(\mathbb{F}/\mathbb{F}_p)$ generado por el homomorfismo de Frobenius $x \mapsto x^p$. Observamos que el campo fijo de H y $Gal(\mathbb{F}/\mathbb{F}_p)$ es $\mathbb{F}_p$. Mostraremos que $H \neq Gal(\mathbb{F}/\mathbb{F}_p)$. Supongamos por absurdo que $H = Gal(\mathbb{F}/\mathbb{F}_p)$.

Recordemos que dado $m \in \mathbb{Z}_{>0}$, existe un subcuerpo de $\mathbb{F}$ con p^m elementos. Para cada $k \in \mathbb{Z}_{>0}$, sea F_k el subcuerpo de $\mathbb{F}$ con p^{2^k} elementos. Luego se obtiene una sucesión creciente $F_1 \subseteq F_2 ... \subseteq F_k \subseteq F_{k+1} \ldots$ de subcampos de $\mathbb{F}$. Definimos $\Omega := \bigcup_{k=1}^{\infty} F_k$ y notamos fácilmente que Ω es un subcampo propio de $\mathbb{F}$, pues si j es un entero que no es de la forma 2^k, entonces $\mathbb{F}$ contiene un subcuerpo con p^j elementos que no está contenido en Ω.

Por la Proposición 2.17 $\mathbb{F}/\Omega$ es de Galois. Como $F \neq \Omega$, luego $Gal(\mathbb{F}/\Omega)$ no es trivial. Sea $\tau \in Gal(\mathbb{F}/\Omega)$ distinto de la identidad. Por hipótesis $\tau(y) = y^{p^n}$ para algún $n \in \mathbb{Z}_{>0}$ y para cada $y \in \mathbb{F}$. Luego todos los elementos de Ω serían raices de $x^{p^n} - x$, una contradicción.

Así, mostramos que $\mathbb{F}_p$ es el campo fijo de dos subgrupos distintos de $Gal(\mathbb{F}/\mathbb{F}_p)$: H y $Gal(\mathbb{F}/\mathbb{F}_p)$. Luego no hay una biyección entre campos entremedios $\mathbb{F}_p \subseteq M \subseteq \mathbb{F}$ y subgrupos de $Gal(\mathbb{F}/\mathbb{F}_p)$.

2.3. Caso infinito

En ésta sección vamos a enunciar y probar el Teorema de Correspondencia en el caso infinito. Para ello, vamos a introducir una Topología sobre el grupo de Galois de una extensión algebraica K/k infinita.

Consideremos una extensión K/k de Galois infinita. Definimos los siguientes conjuntos:

$$\mathcal{F} = \{L : k \subseteq L \subseteq K \text{ tal que } L/k \text{ es de Galois y finita}\}$$

$$\mathcal{N} = \{Gal(K/L) : L \in \mathcal{F}\}$$

y vamos a definir sistemas inversos que son indexados por $\mathcal{F}$ y $\mathcal{N}$.

Sobre $\mathcal{F}$ definimos el siguiente orden parcial: $L_1 \leq_{\mathcal{F}} L_2 \Leftrightarrow L_1 \subseteq L_2$. A partir de esto, para $L \leq_{\mathcal{F}} L'$, definimos los homomorfismos continuos:

$$\begin{aligned} \varphi_{LL'}: \quad Gal(L'/k) &\longrightarrow Gal(L/k) \\ \sigma &\longmapsto \sigma|_L. \end{aligned}$$

Para $L \leq_{\mathcal{F}} L'$, $\varphi_{LL'}$ está bien definida (porque L/k es normal), además $\varphi_{LL}(\sigma) = \sigma|_L = \sigma$, entonces $\varphi_{LL} = Id_{(GalL/k)}$. Finalmente para $L_1 \leq L_2 \leq L_3$:

$$(\varphi_{L_1L_2} \circ \varphi_{L_2L_3})(\sigma) = \varphi_{L_1L_2}(\sigma|_{L_2}) = \sigma|_{L_1} = \varphi_{L_1L_3}(\sigma),$$

para cada $\sigma \in Gal(L_3/k)$. Esto prueba que $(\mathcal{F}, Gal(L/k), \varphi_{LL'})$ es un sistema inverso en la categoría de grupos topológicos.

Proposición 2.21. [7, Lema 2.1] *Sea K/k una extensión de Galois infinita, y $H = Gal(K/L) \in \mathcal{N}$. Entonces H es un subgrupo normal de $Gal(K/k)$ y*

$$Gal(L/k) \simeq Gal(K/k)/Gal(K/L).$$

Demostración. Consideremos la aplicación

$$\begin{aligned} \varphi: \quad Gal(K/k) &\longrightarrow Gal(L/k) \\ \sigma &\longmapsto \sigma|_L. \end{aligned}$$

Dado $\tau \in Gal(L/k)$, por el Teorema 2.14 existe $\tau' \in Gal(K/k)$ tal que $\tau'|_L = \tau$ así que φ es sobreyectiva. Luego notemos que si $\varphi(\sigma) = \sigma|_L = Id_L$ entonces σ fija todos los elementos de L y luego $\text{Ker}(\varphi) = Gal(K/L)$, esto prueba la normalidad de $Gal(K/L)$. Por el 1^{er} Teorema de isomorfismo, se tiene lo pedido. □

Definimos ahora un sistema inverso que se indexe con $\mathcal{N}$. Sobre $\mathcal{N}$, definimos el siguiente orden parcial: $H_1 \leq_{\mathcal{N}} H_2 \Leftrightarrow H_2 \subseteq H_1$. Consideramos las aplicaciones

$$\varphi_{HH'} : Gal(K/k)/H' \longrightarrow Gal(K/k)/H$$
$$\sigma H' \longmapsto \sigma H.$$

Notemos que para $H \leq_{\mathcal{N}} H'$, $\varphi_{HH'}$ está bien definida y es un homomorfismo continuo.

Por lo tanto $(\mathcal{N}, Gal(K/k)/H, \varphi_{HH'})$ es un sistema inverso en la categoría de grupos topológicos.

Observación 2.22. Para cada $H \in \mathcal{N}$, sea

$$q_H : Gal(K/k) \longrightarrow Gal(K/k)/H$$
$$\sigma \longmapsto \sigma H$$

Notemos que $\varphi_{HH'} \circ q_{H'} = q_H$, para cada $H, H' \in \mathcal{N}$ tales que $H' \leq_{\mathcal{N}} H$. Así que la familia de morfismos $\{q_H : Gal(K/k) \to Gal(K/k)/H : H \in \mathcal{N}\}$ es compatible con el sistema inverso definido anteriormente.

Observación 2.23. De manera similar se puede probar que la familia

$$\{\eta_L : Gal(K/k) \to Gal(L/k) : L \in \mathcal{F}\}$$

donde $\eta_L(\sigma) = \sigma|_L$, es compatible con $(\mathcal{F}, Gal(L/k), \varphi_{LL'})$.

Observación 2.24. Para cada $L, L' \in \mathcal{F}$ con $L \leq_{\mathcal{F}} L'$ y para cada $H = Gal(K/L)$ y $H' = Gal(K/L') \in \mathcal{N}$ con $H' \leq_{\mathcal{N}} H$ el siguiente diagrama es conmutativo

$$\begin{array}{ccc} Gal(K/k)/H' & \xrightarrow{\varphi_{HH'}} & Gal(K/k)/H \\ \simeq\uparrow & & \uparrow\simeq \\ Gal(L'/k) & \xrightarrow[\varphi_{LL'}]{} & Gal(L/k). \end{array}$$

Por lo tanto $\varprojlim_{H\in\mathcal{N}} Gal(K/k)/H$ y $\varprojlim_{L\in\mathcal{F}} Gal(L/k)$ son isomorfos. Definimos

$$G := \varprojlim_{H\in\mathcal{N}} Gal(K/k)/H, \quad G' := \varprojlim_{L\in\mathcal{F}} Gal(L/k).$$

Por la Observación 2.22 y la Propiedad $\mathcal{U}$) existe y es única una aplicación

$$\gamma : Gal(K/k) \longrightarrow G$$

tal que el siguiente diagrama conmuta para cada $H \in \mathcal{N}$:

$$\begin{array}{ccc} Gal(K/k) & \xrightarrow{q_H} & Gal(K/k)/H \\ {\scriptstyle\gamma}\downarrow & \nearrow_{\varphi_H} & \\ G & & \end{array}$$

Por otro lado, sigue de la Observación 2.23, que el siguiente diagrama también es conmutativo para cada $L \in \mathcal{F}$:

$$\begin{array}{ccc} Gal(K/k) & \xrightarrow{\eta_L} & Gal(L/k) \\ {\scriptstyle\psi}\downarrow & \nearrow_{\varphi_L} & \\ G' & & \end{array}$$

donde $\psi(\sigma) = (\sigma|_L)_{L\in\mathcal{F}}$ y $\eta_L(\sigma) = \sigma|_L$, para cada $\sigma \in Gal(K/k)$.

Siendo el diagrama anterior conmutativo, por la propiedad universal ψ debe ser único, así que $\gamma = \alpha \circ \psi$ donde $\alpha : G' \to G$ es el isomorfismo definido anteriormente.

En breve veremos que en realidad ψ es un isomorfismo de grupos topológicos.

Lema 2.25. [4, Lema 17.1] *Sean $a_1, \ldots, a_n \in K$. Luego existe $L \in \mathcal{F}$ tal que $a_1,\ldots,a_n \in L$.*

Demostración. Sea L el campo de descomposición de $p(x) := p_{a_1}(x)\cdots p_{a_n}(x) \in k[x]$. Claramente L/k es normal por el Teorema 2.8. Como K/k es separable, entonces L/k lo es también. Luego L/k es de Galois. Finalmente $[L : k] \leq \deg(p)! < \infty$ por la Proposición 2.6. Así que $L \in \mathcal{F}$. □

De esto sigue inmediatamente el siguiente.

Corolario 2.26.

$$\bigcup_{L\in\mathcal{F}} L = K.$$

Ejemplo 2.27. Vamos a ver un ejemplo de extensión infinita. Sean $p_1, \ldots, p_n$ primos distintos entre ellos y sea q otro primo distinto de los p_i. Primero probamos que $\sqrt{q} \notin \mathbb{Q}(\sqrt{p}_1, \ldots, \sqrt{p}_n)$.

Por inducción sobre n. Si $n = 1$ entonces el polinomio mínimo de $\sqrt{p_1}$ sobre $\mathbb{Q}$ es $g(x) = x^2 - p_1$ y luego $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2$, por lo tanto una base de $\mathbb{Q}(\sqrt{p_1})$ sobre $\mathbb{Q}$ es $\{1, \sqrt{p_1}\}$. Si $\sqrt{q} \in \mathbb{Q}(\sqrt{p_1})$ entonces existen $a, b \in \mathbb{Q}$ tales que $\sqrt{q} = a + b\sqrt{p_1}$. Notemos que esto no es cierto pues si $a, b \neq 0$ entonces $\sqrt{p_1} = \frac{p-a^2-b^2p_1}{2ab} \in \mathbb{Q}$ lo cual es una contradicción. (Los casos a y/o b nulos son obvios)

Supongamos que esto es cierto hasta $n-1$ y sea $L = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{n-1}})$.
Como $p_n \neq p_i$ para cada $i \in \{1, .., n-1\}$ por hipótesis de inducción $\sqrt{p_n} \notin L$ y luego el polinomio mínimo de $\sqrt{p_n}$ sobre L es $f(x) = x^2 - p_n$. Luego $[L(\sqrt{p_n}) : L] = 2$ y una base de $L(\sqrt{p_n})$ sobre L es $\{1, \sqrt{p_n}\}$.

Si $\sqrt{q} \in L(\sqrt{p_n})$ entonces existen $a, b \in L$ tales que $\sqrt{q} = a + b\sqrt{p_n}$. Pero si $a, b \neq 0$ entonces $\sqrt{p_n} = \frac{q-a^2-b^2p_n}{2ab} \in L$ lo cual es una contradicción (los casos a y/o b nulos son fáciles de notar).
Bajo las mismas condiciones sobre los p_i, probamos ahora que $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

Por inducción sobre n. Si $n = 1$ entonces $p(x) = x^2 - p_1$ es el polinomio mínimo de $\sqrt{p_1}$ sobre $\mathbb{Q}$ así que $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2$.

Supongamos cierto para $n-1$ y sea $L = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. Luego $L(\sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Como $p_i \neq p_j$ para cada $i \neq j$, por lo anterior tenemos que $\sqrt{p_n} \notin L$ así que el polinomio mínimo de $\sqrt{p_n}$ sobre L es $p(x) = x^2 - p_n$. Luego por la Ley de la Torre

$$\begin{aligned}[L(\sqrt{p_n}) : Q] &= [L(\sqrt{p_n}) : L][L : Q] \\ &= 2 \cdot 2^{n-1} \quad \text{(Hipótesis de inducción)} \\ &= 2^n\end{aligned}$$

Demostramos ahora que la extensión $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}, ...) : \mathbb{Q}]$ es infinita:

Supongamos por absurdo que sea finita y que $[\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n},\dots):\mathbb{Q}] = a$ con $a \in \mathbb{Z}_{>0}$. Luego

$$\begin{aligned} a &= [\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n},\dots):\mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n},\dots):\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})]\cdot[\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n}):\mathbb{Q}] \\ &= x\,2^n \quad (\text{con } x = [\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n},\dots):\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})]) \\ &\geq 2^n. \end{aligned}$$

Es decir $2^n \leq a$ para cada $n \in \mathbb{N}$, lo cual es absurdo.

Teorema 2.28. [7, Proposición 2.5] *La aplicación definida por*

$$\begin{aligned} \psi\colon Gal(K/k) &\longrightarrow \varprojlim_{L\in\mathcal{F}} Gal(L/k) \\ \sigma &\longmapsto (\sigma|_L)_{L\in\mathcal{F}}, \end{aligned}$$

donde K/k es una extensión de Galois infinita, es un isomorfismo de grupos.

Demostración. Recordamos que $L_1 \leq_{\mathcal{F}} L_2$ si y sólo si $Gal(L_1/k) \leq Gal(L_2/k)$. Luego si $a \in L_1 \leq L_2$ entonces $\sigma|_{L_1}(a) = \sigma|_{L_2}(a)$, luego ψ está bien definida. Para la inyectividad, es suficiente probar que si $\psi(\tau) = (1_L)_{L\in\mathcal{F}}$ entonces $\tau = 1_K$, pero si esto es cierto entonces $\tau|_L = 1_L$ para cada $L \in \mathcal{F}$. Luego por el Corolario 2.26 tenemos que $\tau = 1_K$.

Para la sobreyectividad, sea $(\tau_L)_{L\in\mathcal{F}} \in \varprojlim_{L\in\mathcal{F}} Gal(L/k)$, y definimos $\tau \in Gal(K/k)$ como sigue. Sea $a \in K$. Por el Corolario 2.26 existe $L \in \mathcal{F}$ tal que $a \in L$. Luego se define $\tau(a) := \tau_L(a)$ para dicho L. De este modo definimos τ para cada $a \in K$. Esto prueba la sobreyectividad. □

Más adelante se probará que si a $Gal(K/k)$ se le equipa con la topología de Krull y a $\varprojlim_{L\in\mathcal{F}} Gal(L/k)$ con la topología de subespacio, dicha aplicación es un isomorfismo de grupos topológicos.

Lema 2.29. [4, Lema 17.3] *Para cada $\sigma \in Gal(K/k)$, se tiene*

$$\bigcap_{H\in\mathcal{N}} \sigma H = \{\sigma\}.$$

Demostración. Sea $\sigma\psi \in \cap_{H\in\mathcal{N}}\sigma H$ y sea $x \in K$. Por el Corolario 2.26 existe $L \in \mathcal{F}$ tal que $x \in L$. Sea $H = Gal(K/L)$, luego $\sigma\psi(x) = \sigma(x)$ para cada $\psi \in H$.
Asi que $\cap_{H\in\mathcal{N}}\sigma H = \{\sigma\}$. □

2.4. Topología de Krull

En ésta sección vamos considerando una extensión K/k infinita algebraica y $Gal(K/k)$ el grupo de Galois de dicha extensión. Sobre éste grupo vamos a definir una topología compatible con la estructura de grupo que nos permitirá establecer una versión general del Teorema de correspondencia de Galois.

Definición 2.30. Sean K/L_1, K/L_2 dos extensiones de campos. Se define el **compositum** de L_1 y L_2 como el subcampo más pequeño de K que contiene a L_1 y L_2, y se denota por L_1L_2.

Proposición 2.31. *Si L_1, $L_2 \in \mathcal{F}$, entonces $L_1L_2 \in \mathcal{F}$.*

Demostración. Notemos que $[L_1L_2 : k] \leq [L_1 : k][L_2 : k]$. En efecto, sean $\{x_1,\ldots,x_m\}$ una base de L_1 sobre k y $\{y_1,\ldots,y_n\}$ una base de L_2 sobre k, así que $[L_1 : k] = m$ y $[L_2 : k] = n$. Por otro lado, $[L_1L_2 : L_1] \leq n$ ya que $L_1L_2 = L_1(y_1, \ldots, y_n)$. Finalmente notamos que

$$\begin{aligned}[L_1L_2 : k] &= [L_1L_2 : L_1][L_1 : k] \qquad (\textit{por Ley de la Torre})\\ &\leq nm = [L_1 : k][L_2 : k].\end{aligned}$$

Esto prueba que L_1L_2 es finita. Para probar que es de Galois sólo basta notar que $L_1L_2 = k(x_1, \ldots, x_m, y_1, \ldots, y_n)$ y como L_1/k y L_2/k son de Galois, L_1L_2/k también lo es. □

Proposición 2.32. [7, Lema 17.4] *Si $H_1, H_2 \in \mathcal{N}$ entonces $H_1 \cap H_2 \in \mathcal{N}$.*

Demostración. Si $H_1 = Gal(K/L_1)$ con $L_1 \in \mathcal{F}$ y $H_2 = Gal(K/L_2)$ con $L_2 \in \mathcal{F}$, mostramos que $H_1 \cap H_2 = Gal(K/L_1L_2)$.

Sea $\sigma \in H_1 \cap H_2$, entonces $\sigma(a) = a$ para cada $a \in L_1$ y $\sigma(b) = b$ para cada $b \in L_2$. Luego $\sigma(ab) = ab$, asi que $\sigma \in Gal(K/L_1L_2)$. Por otro lado, si $\sigma \in Gal(K/L_1L_2)$ entonces $\sigma(ab) = ab$ para cada $a \in L_1$ y $b \in L_2$. Con $a = 1_{L_1}$ tenemos $\sigma(b) = b$ y con $b = 1_{L_2}$ tenemos $\sigma(a) = a$, asi que $\sigma \in H_1 \cap H_2$. Concluimos por la Proposición 2.31. □

Definición 2.33. Sea K/k una extensión de Galois infinita. Definimos la **Topología de Krull** en $Gal(K/k)$ como sigue: un subconjunto H de $Gal(K/k)$ es abierto si $H = \varnothing$ o $H = \bigcup_{i\in I} \sigma_i N_i$, con $\sigma_i \in Gal(K/k)$ y $N_i \in \mathcal{N}$.

Notemos que siendo k/k una extensión de Galois finita, $Gal(K/k) \in \mathcal{N}$.
Resta verificar que la intersección de dos abiertos es abierta, para que la definición anterior tenga sentido. Sabemos que para cada $\sigma \in Gal(K/k)$ y cada $H \in \mathcal{N}$, σH es abierto. Sean $\sigma_1, \sigma_2 \in Gal(K/k)$ y $N_1, N_2 \in \mathcal{N}$. Consideremos $\sigma' \in \sigma_1N_1 \cap \sigma_2N_2$. Luego $\sigma_1N_1 = \sigma' N_1$ y $\sigma_2N_2 = \sigma' N_2$ así que

$$\sigma_1N_1 \cap \sigma_2N_2 = \sigma' N_1 \cap \sigma' N_2 = \sigma'(N_1 \cap N_2) \in \mathcal{N}$$

por la Proposición 2.32.

Denotamos por τ_K a la Topología de Krull. Con esto, $(Gal(K/k), \tau_K)$ es un espacio topológico.

Proposición 2.34. [7, Proposición 2.13] *Sea K/k una extensión de Galois infinita. Sea $Gal(K/k)$ dotado con la topología de Krull, y sea $\bar{G} = \varprojlim_{L\in\mathcal{F}} Gal(L/k)$ dotado con la topología de subespacio ($Gal(L/k)$ es compacto, Hausdorff y totalmente disconexo para cada $L \in \mathcal{F}$).*
Luego la aplicación

$$\begin{aligned}\psi\colon Gal(K/k) &\longrightarrow \varprojlim_{L\in\mathcal{F}} Gal(L/k)\\ \sigma &\longmapsto (\sigma|_L)_{L\in\mathcal{F}}\end{aligned}$$

es un isomorfismo de grupos topológicos.

Demostración. Por el Teorema 2.28 ya tenemos que ψ es un isomorfismo de grupos, falta probar la bicontinuidad.

Daremos por hecho que $\mathcal{B} = \cup_{L\in\mathcal{F}} \{\pi_L^{-1}(\{\sigma\})\colon \sigma \in Gal(L/k)\}$ es una subbase para la topología en $\bar{G}$, donde $\pi_L : \bar{G} \to Gal(L/k)$ es la proyección natural ($\mathcal{B} \subset \mathcal{P}(X)$ es una subbase para una topología en X si la familia de interseciones finitas de elementos de $\mathcal{B}$ forma una base para una topología en X).

Para mostrar que ψ es continua, mostramos que la preimagen de un cualquier abierto en $\mathcal{B}$ es abierto en $Gal(K/k)$. Tenemos que:

$$\psi^{-1}(\pi_L^{-1}(\{\sigma\})) = \{\gamma \in Gal(K/k) : \gamma|_L = \sigma\} = \cup_{\gamma\in Gal(K/k)}\, \gamma Gal(K/L),$$

donde γ debe cumplir $\gamma|_L = \sigma$ y el último es abierto por definición de la Topología de Krull, esto prueba la continuidad de ψ.

Para mostrar la continuidad de ψ^{-1} es suficiente probar que ψ es una aplicación abierta. Sea σH un básico en $Gal(K/k)$, así que $\sigma \in Gal(K/k)$ y $H = Gal(K/F)$ para algún F en $\mathcal{F}$. Luego

$$\begin{aligned}
\psi(\sigma H) &= \{(\sigma\tau|_L)_{L\in\mathcal{F}} : \tau|_F = 1_F\} \\
&= \{(\rho|_L)_{L\in\mathcal{F}} : \sigma^{-1}\rho|_F = 1_F\} \quad (con\ \sigma\tau\ =\ \rho) \\
&= \{(\rho|_L)_{L\in\mathcal{F}} : \rho|_F = \sigma|_F\} \\
&= \pi_F^{-1}(\{\sigma|_F\}),
\end{aligned}$$

donde $\pi_F\colon \varprojlim Gal(L/k) \to Gal(F/k)$ es la proyección. Por lo tanto ψ es un isomorfismo de grupos topológicos. □

Corolario 2.35. *$(Gal(K/k), \tau_K, \cdot)$ donde*

$$\begin{aligned}
\cdot \quad : Gal(K/k) \times Gal(K/k) &\longrightarrow Gal(K/k) \\
(\sigma_1, \sigma_2) &\longmapsto \sigma_1\sigma_2
\end{aligned}$$

es un grupo topológico.

Corolario 2.36. *Si K/k es una extensión de Galois infinita, $(Gal(K/k), \tau_K)$ es un espacio topológico compacto, Hausdorff y totalmente disconexo.*

Demostración. Por la Proposición 2.34 $Gal(K/k)$ es isomorfo a un límite inverso de grupos finitos, así que es profinito, y por el Teorema 1.32 es Hausdorff, compacto y totalmente disconexo. □

2.5. El Teorema de Correspondencia de Galois

Terminamos con una última proposición y pasaremos a enunciar y probar el Teorema Fundamental de la Teoría de Galois infinita.

Lema 2.37. *Sean $k \subseteq L \subseteq K$ extensiones, donde K/k es de Galois infinita, $G = Gal(K/k)$ y $H' = Gal(K/L)$. Entonces H' es cerrado en G.*

Demostración. Sea $\sigma \in G\backslash H$. Entonces existe $\alpha \in L$ tal que $\sigma(\alpha) \neq \alpha$. Por el Corolario 2.26 existe $E \in \mathcal{F}$ con $\alpha \in E$. Sea $N = Gal(K/E)$. Para cada $\tau \in N$ se cumple $\tau(\alpha) = \alpha$ y $\sigma\tau(\alpha) = \sigma(\alpha) \neq \alpha$. Entonces σN es un entorno abierto de σ disjunto de H. Esto implica que $G\backslash H$ es abierto, y luego H es cerrado en G. □

Proposición 2.38. [3, Propoición 7.11 b)] *Sea K/k una extensión de Galois infinita y H un subgrupo de $Gal(K/k)$. Si $L = K^H$ y $H' = Gal(K/L)$, entonces $H' = \bar{H}$, donde $\bar{H}$ es la clausura topológica de H.*

Demostración. Es claro que $H \subseteq H'$ y H' es cerrado por el Lema 2.37, así que $\bar{H} \subseteq H'$.

Mostramos ahora que $H' \subseteq \bar{H}$. Sea $\sigma \in H'$, $E \in \mathcal{F}$ y $N = Gal(K/E) \in \mathcal{N}$. Consideremos $H_0 = \{\rho|_E : \rho \in H\}$ que es subgrupo de $Gal(E/k)$ y notemos que $E^{H_0} = L \cap E$. Por el Teorema de Correspondencia de Galois finito, $H_0 = Gal(E/E \cap L)$.
Por otro lado, como $\sigma \in H'$, $\sigma|_L = 1_L$, luego $\sigma|_E \in H_0$. Por lo tanto existe $\tau \in H$ tal que $\tau|_E = \sigma|_E$. Luego $\sigma^{-1}\tau \in Gal(K/E)$ y $\tau \in \sigma Gal(K/E) \cap H$. Es decir, para cada $\sigma \in H'$, existe $N \in \mathcal{N}$ tal que $\sigma N \cap H \neq \varnothing$, así que $\sigma \in \bar{H}$.

□

Teorema 2.39 (Correspondencia de Galois, caso infinito). [7, Teorema 2.17] *Sea K/k una extensión de Galois infinita y sea $Gal(K/k)$ dotado con la Topología de Krull.*

1) *Las aplicaciones $L \longmapsto Gal(K/L)$ y $H \longmapsto K^H$ nos entregan una correspondencia uno a uno que revierte la inclusión, entre los campos entremedios $k \subseteq L \subseteq K$ y los subgrupos cerrados H de $Gal(K/k)$.*

2) *Si L se corresponde con H, las siguientes son equivalentes*

   a) *$[Gal(K/k) : H]$ es finito,*
   b) *$[L : k]$ es finito,*
   c) *H es abierto.*

3) *Si 2) es cierta entonces $[Gal(K/k) : H] = [L : k]$.*

4) *Si $H = Gal(K/L)$ es un subgrupo cerrado de $Gal(K/k)$, entonces H es normal si y sólo si L/k es de Galois y luego tenemos el siguiente isomorfismo de grupos*

$$Gal(K/k)/H \simeq Gal(L/k).$$

Demostración.
1) Sean $k \subseteq L \subseteq K$ extensiones de campos. Por la Proposición 2.17 K/L es una extensión de Galois, así que $L = K^{Gal(K/L)}$.
Si H es un subgrupo cerrado de $Gal(K/k)$, por la Proposición 2.38, si $L = K^H$, entonces $Gal(K/L) = \bar{H} = H$. Esto prueba la correspondencia.

2) Supongamos que L y H se correspondan.

a) $\Rightarrow$ c) Como $[Gal(K/k) : H]$ es finito y H es cerrado, entonces H es abierto por la Proposición 1.6 i).

c) $\Rightarrow$ b) Si $H = Gal(K/L)$ es abierto, entonces existe $N \in \mathcal{N}$ tal que $N \subseteq H$. Si $E = K^N$ entonces $L \subseteq E$ y $E \in \mathcal{F}$ así que $[E : k]$ es finita.
Luego por la Ley de la Torre, $[E : k] = [E : L][L : k]$ así que $[L : k]$ es finito.

b) $\Rightarrow$ a) Si $[L : k]$ es finito, entonces escojemos $E \in \mathcal{F}$ tal que $L \subseteq E$ (se puede por el Lema 2.25) y $N = Gal(K/E)$. Entonces $N \subseteq H$ y luego $[G : H] \leq [G : N]$ y este último es finito.

3) Si *2)* es cierta, entonces $H = Gal(K/L) \in \mathcal{N}$, y por la Proposición 2.21 se tiene

$$Gal(K/k)/Gal(K/L) \simeq Gal(L/k).$$

Luego, como L/k es finita, usamos el Teorema de Correspondencia de Galois finito:

$$\begin{aligned}[Gal(K/k) : H] = [Gal(K/k) : Gal(K/L)] &= |Gal(L/k)| \\ &= [L : k].\end{aligned}$$

4) $\Rightarrow$) Supongamos que $H = Gal(K/L)$ es un subgrupo cerrado y normal de $Gal(K/k)$. Sea $a \in L$ y $p_a(x)$ su polinomio mínimo sobre k. Si b es otra raíz de $p_a(x)$, existe $\sigma \in Gal(K/k)$ tal que $\sigma(a) = b$. Si $\tau \in H$, entonces

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

Thus $b \in K^H = L$. Así que L/k es normal y es separable porque K/k lo es, luego L/k es de Galois.
$\Leftarrow$) Supongamos que L/k es de Galois. Entonces la aplicación $\tau : Gal(K/k) \to Gal(L/k)$ dada por $\tau(\sigma) = \sigma|_L$ está bien definida (porque L/k es normal) y $\text{Ker}(\tau) = Gal(K/L) = H$. Además τ es sobreyectiva por el Teorema 2.14 y finalmente por el 1^{er} Teorema de isomorfismo tenemos

$$Gal(K/k)/Gal(K/L) \simeq Gal(L/k).$$

□

Para concluir, notamos que al desarrollar esto en una extensión K/k que es finita, vamos a obtener el Teorema de Correspondencia clásico. En efecto, la topología de Krull en el grupo de Galois de una extensión finita es la topología discreta, luego sus subgrupos son abiertos y cerrados a la vez.

Veremos un último ejemplo para finalizar con este documento.

Ejemplo 2.40. Como en el Ejemplo 2.20 sea p primo, $\mathbb{F}_p$ el campo con p elementos y $\mathbb{F}$ su clausura algebraica. Siendo $\mathbb{F}/\mathbb{F}_p$ una extensión de Galois, para cualquier campo L entremedio, $\mathbb{F}/L$ también es de Galois por la Proposición 2.17. Ahora bien, si $n \in \mathbb{Z}_{>0}$ sea $\mathbb{F}_{p^n}$ el campo con p^n elementos. Por lo anterior tenemos que $\mathbb{F}/\mathbb{F}_{p^n}$ es de Galois.

Por el Teorema 2.28, $Gal(\mathbb{F}/\mathbb{F}_p)$ y $\varprojlim Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ son isomorfos como grupos topológicos.

Por otro lado, la Teoría de Galois clásica nos dice que $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$ y sobre ambos consideramos el orden inducido por la divisibilidad.

Luego el siguiente diagrama conmuta para cada $n, m \in \mathbb{Z}_{>0}$ con $n \leq m$

$$\begin{array}{ccc} Gal(\mathbb{F}_{p^m}/\mathbb{F}_p) & \xrightarrow{\varphi_{nm}} & Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \\ \simeq \uparrow & & \uparrow \simeq \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow[\psi_{nm}]{} & \mathbb{Z}/n\mathbb{Z}. \end{array}$$

Por lo tanto

$$Gal(\mathbb{F}/\mathbb{F}_p) \simeq \varprojlim Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}},$$

donde $\hat{\mathbb{Z}}$ es la completación profinita de $\mathbb{Z}$ del Ejemplo 1.29.

Bibliografía

[1] Nicolas Bourbaki. *General topology. Chapters 1–4*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French; Reprint of the 1989 English translation. ↑7, 8

[2] Antonio Laface. *Teoría de Galois*, 2018. Notas de curso, Universidad de Concepción, disponible en https://sites.google.com/site/teoriadegalois/. ↑19, 20, 22

[3] James S. Milne. *Fields and Galois Theory (v4.30)*, 2012. Disponible en www.jmilne.org/math/. ↑19, 20, 22, 30

[4] Patrick Morandi. *Field and Galois theory*. Graduate Texts in Mathematics, vol. 167. Springer-Verlag, New York, 1996. ↑19, 26, 27

[5] Paul J. McCarthy. *Algebraic extensions of fields*. Dover Publications, Inc., New York, 2nd ed., 1991. ↑19, 21, 22

[6] Gustavo N. Rubiano O. *Topología General*. Facultad de Ciencias, Universidad Nacional de Colombia, 2nd ed., 2002. ↑13

[7] Ignasi Sánchez Rodríguez. Infinite Galois theory, 2018. Tesis de grado, Universitat de Barcelona, disponible en http://diposit.ub.edu/dspace/bitstream/2445/122676/2/memoria.pdf. ↑11, 13, 16, 18, 19, 24, 27, 28, 30

[8] Tamás Szamuely. La teoria di Galois dopo Galois. *Lettera Matematica Pristem* 80-81:75–80, 2012. versión italiana de R. Betti, versión inglés disponible en http://pagine.dm.unipi.it/tamas/pristem.pdf. ↑4

[9] Javiera Zuñiga Gallegos. *Teoría de Iwasawa*, 2017. Tesis de Magíster, Pontificia Universidad Católica de Valparaíso. ↑19

[10] Wolfgang Krull. Galoissche Theorie der unendlichen algebraischen Erweiterungen. *Math. Ann.* 100 (1):687–698, 1928. ↑4