**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**
PROGRAMA DE MAESTRÍA Y DOCTORADO EN CIENCIAS MATEMÁTICAS Y
DE LA ESPECIALIZACIÓN EN ESTADÍSTICA APLICADA

# De la teoría de Galois para campos a las categorías de Galois

TESIS

QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN CIENCIAS

PRESENTA:
**JAIME ALEJANDRO GARCÍA VILLEDA**

DIRECTOR DE TESIS:
**DR. FRANK PATRICK MURPHY HERNÁNDEZ**

FACULTAD DE CIENCIAS

CIUDAD DE MÉXICO, JULIO DEL 2019.

| | |
|---|---|
| 1. Datos del alumno | 1. Datos del alumno |
| Apellido Paterno | García |
| Apellido Materno | Villeda |
| Nombres | Jaime Alejandro |
| Teléfono | 11-08-77-50 |
| Universidad Nacional Autónoma de México | Universidad Nacional Autónoma de México |
| Facultad de Ciencias | Facultad de Ciencias |
| Número de Cuenta | 308221031 |
| | |
| 2. Datos del tutor | 2. Datos del tutor |
| Grado | Doctor |
| Apellido Paterno | Murphy |
| Apellido Materno | Hernández |
| Nombre | Frank Patrick |
| | |
| 3. Datos del sinodal 1 | 3. Datos del sinodal 1 |
| Grado | Doctor |
| Apellido Paterno | Santiago |
| Apellido Materno | Vargas |
| Nombre | Valente |
| | |
| 4. Datos del sinodal 2 | 4. Datos del sinodal 2 |
| Grado | Doctor |
| Apellido Paterno | Garza |
| Apellido Materno | Ledesma |
| Nombres | Juan Salvador |
| | |
| 5. Datos del sinodal 3 | 5. Datos del sinodal 3 |
| Grado | Doctor |
| Apellido Paterno | Prieto |
| Apellido Materno | de Castro |
| Nombre | Carlos |
| | |
| 6. Datos del sinodal 4 | 6. Datos del sinodal 4 |
| Grado | Doctor |
| Apellido Paterno | Alvarado |
| Apellido Materno | García |
| Nombre | Alejandro |
| | |
| 7. Datos del trabajo escrito | Datos del trabajo escrito |
| Título | De la teoría de Galois para campos a las categorías de Galois. |
| Número de páginas | 144 páginas |
| Año | 2019 |

# Índice general

"... Désolé d'avoir l'air de vouloir me singulariser plus qu'il ne paraît permis! A mon propre soulagement je crois pourtant discerner une sorte de frère potentiel (et providentiel!) J'ai déjà eu tantôt l'occasion de l'évoquer, comme le premier dans la lignée de mes frères de tempérament, c'est Evariste Galois, dans sa courte et fulgurante vie, je crois discerner l'amorce d'une grande vision, celle justement des épousailles du nombre et de la grandeur dans une vision géométrique nouvelle. J'évoque ailleurs dans *Récoltes et Semailles* comment il y a deux ans est apparue en moi cette intuition nouvelle que le travail mathématique qui à ce moment exerçait sur moi la fascination la plus puissante j'étais en train de reprendre l'héritage de Galois". Cette intuition rarement évoquée depuis, a pourtant eu le temps de mûrir en silence. $\cdots$ La filiation la plus directe que je crois reconnaître à présent avec un mathématicien du passé, est bien celle qui me relie à Evariste Galois. A tort ou à raison, il me semble que cette vision que j'ai développée pendant quinze années de ma vie, et qui a continué de mûrir en moi et à s'enrichir pendant les seize années écoulées depuis mon départ de la scène mathématique- que cette vision est aussi celle que Galois n'aurait pu s'empêcher de développer s'il s'était trouvé dans les parages à ma place, et sans qu'une mort précoce ne vienne brutalement couper court un magnifique élan"

**Alexandre Grothendieck**
*Récoltes et semailles*

# Agradecimientos

En toda gran obra hay por lo general muchas personas detrás del artista que la realizó. Personas sin las cuales dicha obra no hubiera sido posible, pero sin un indicio explicíto que avale su contribución y, suele suceder que incluso el artista no se de cuenta de dicha contribución fundamental. Esta no es una gran obra y no soy un artista, pero este trabajo es una muestra de mi gusto por la matemática y en este estuvieron involucradas muchas personas, pues en mi caso suelo aprender algo de cualquier persona a la que conozco. Sin embargo, no quiero perder la oportunidad de dedicar esto:

A mi mamá Adriana y papá Jaime. Les agradezco por darme un lugar al cual puedo llamar casa y, sobre todo les agradezco su infinito apoyo en cada una de mis decisiones aunque estas no les parezcan las mejores en una gran variedad de ocasiones.

A mis hermanas Cynthia, Liliana, Adriana y Mariana. Les agradezco por todos los grandes momentos que hemos compartido a lo largo de nuestra vida. Ustedes son parte de la gran razón por la cual siento ánimo de hacer un largo viaje de regreso a casa todos los días.

A toda mi familia y muy en especial a mi tío Neri y primos Omar, Lalo, Rodrigo y Fer. Les agradezco por los grandes momentos que vivimos desde nuestra infancia juntos y lo que es mejor aún, por darse un tiempo para reunirnos hasta estos días.

A mi amigo y asesor de tesis Frank. De verdad no sé como agradecerte todo lo que has hecho por mi, ya que no sólo eres la persona que más me ha enseñado del maravilloso mundo de la matemática, sino que te agradezco por siempre considerarme en todos los proyectos que tienes aunque siento que a veces no te he respondido como se debe; me siento en deuda contigo. También quiero agradecer a mi tutor de la maestría, el Dr. Hugo Rincón, que a pesar de nunca haber trabajado con él directamente o haber sido su alumno, siempre me ha tratado como a cualquiera de sus colegas o alumnos. Le agradezco por el infinto apoyo que me brindó a lo largo de mis estudios de posgrado tanto en temas matemáticos, como personales y hasta en los trámites.

A mis amigas Mariana y Adriana Rosas, en especial a Mariana. Gracias por todas las ocasiones en las cuales me motivaste a seguir con esto cuando las cosas se veían oscuras y quería mandar todo a volar. Gracias por recordarme que cuando te gusta algo debes sacrificar otras cosas para lograr tus metas. También aprovecho para mencionar a mi amigo Yakami, con quien tuve la oportunidad de hacer música y explotar esa pequeña parte artística en mi interior.

A mis exalumnos y ahora amigos Luis, Alberto, Paty, Lore, Daysi, Adri y Leo. Quizá ahora no tengo muchas oportunidades de ver a la mayoría de ustedes, pero debo decir que de ustedes aprendí lo que es el trabajo duro y la perseverancia, así como que es posible confiar en la gente. Me siento muy afortunado de haberlos conocido.

Para concluir le agradezco infinitamente a mis sinodales, los doctores Valente Santiago, Juan Garza, Carlos Prieto y Alejandro Alvarado. Muchas gracias por revisar este trabajo a pesar de no tener el tiempo para hacerlo, por su interés en el mismo y por sus comentarios respecto a este. Aprovecho para agradecer a los doctores Omar Antolín y Pablo Peláez, por esos maravillosos cursos que tomé en el posgrado, que han transformado mi forma de ver las matemáticas. Esta tesis tiene muchos vestigios de lo que he aprendido con ustedes.

# Introducción

Citando el prefacio de [**BJ**]: "si Galois estuviera vivo seguramente estaría sorprendido de lo mucho que su nombre aparece en libros de texto o artículos de investigación modernos"; y no es para menos, pues las ideas en torno a su trabajo han tenido un alcance mucho mayor a la nada despreciable labor de ser uno de los pilares de lo que hoy en día se conoce como el álgebra moderna. Sin embargo, muchas de esas ideas se volvieron mucho más sistemáticas y han alcanzado un alto grado de generalidad gracias a los trabajos de Emil Artin, quien en su famoso libro de texto [**A**] dio la primera formulación moderna de dicha teoría. En sus palabras:

*Desde mi juventud matemática he estado bajo la influencia del hechizo de la teoría clásica de Galois. Este encanto me ha forzado a regresar a esta una y otra vez, y tratar de probar sus teoremas fundamentales.*

Esta frase pone en manifiesto una idea que el mismo Artin mencionó a lo largo de su vida y que es quizá la motivación más profunda que lo llevó a fundamentar y formalizar la teoría clásica de Galois para campos. Artin afirmaba que la fuerza de esta teoría no radicaba en la respuesta de los tres problemas griegos clásicos o del famoso resultado de Galois en torno a la solubilidad por radicales de las ecuaciones de grado mayor cinco, lo realmente importante eran las ideas involucradas en esta. Una de las personas que pareció entender más la potencia de las ideas contenidas en la teoría de Galois fue Grothendieck, quien entre otras cosas mostró que estas eran aplicables a teorías ajenas a la teoría de campos e incluso lejanas del álgebra. De hecho, a partir de estas ideas Grothendieck descubre las analogías que existen entre el grupo de Galois de una extensión y el grupo fundamental de un espacio topológico alrededor de 1961, las cuales se encuentran plasmadas en su Seminario de Geometría Algebraica [**SGA1**]. Una breve motivación de sus ideas se presenta a continuación.

Sea $K|\,k$ una extensión de campos finita con $K$ normal y $k$ de característica 0.[1] Dar una de tales extensiones es equivalente a dar morfismos en la categoría de campos, **Field**, $\iota : k \to K$, los cuales siempre son inyectivos. Dado que una de

[1]La hipótesis sobre la característica se pide para no tener problemas con extensiones inseparables.

tales extensiones $K|\,k$ es de Galois, entonces está definido el grupo de Galois de esta extensión, $\operatorname{Gal}(K|\,k)$, que por definición es el conjunto $\{\sigma \in \mathbf{Field}(K,K) \mid \sigma \circ \iota = \iota\}$. Entre otras cosas, uno de los teoremas fundamentales en torno al grupo de Galois es que su retícula de subgrupos captura toda la información de la retícula de campos intermedios entre $k$ y $K$. Este es el contenido del teorema fundamental de la teoría de Galois (TFTG) que en su forma moderna más simple dice lo siguiente:

Teorema 0.1. *(TFTG para extensiones finitas) Sea $K|\,k$ una extensión de Galois finita. Denótese por $\mathcal{E}_{K|\,k}$ al conjunto de extensiones intermedias entre $k$ y $K$, así como $\mathcal{S}(\operatorname{Gal}(K|\,k))$ al conjunto de subgrupos del grupo de Galois $\operatorname{Gal}(K|\,k)$. Así, las funciones*

$$\begin{aligned} \operatorname{Aut}(K|_{-}) : \mathcal{E}_{K|\,k} &\to \mathcal{S}(\operatorname{Gal}(K|\,k)) \\ L &\mapsto \operatorname{Aut}(K|L) \end{aligned}$$

$$\begin{aligned} K^{-} : \mathcal{S}(\operatorname{Gal}(K|\,k)) &\to \mathcal{E}_{K|\,k} \\ H &\mapsto K^H := \{a \in K \mid \forall \sigma \in H(\sigma(a) = a)\} \end{aligned}$$

*Son inversas una de la otra y establecen una correspondencia biyectiva que invierte el orden entre $\mathcal{E}_{K|\,k}$ y $\mathcal{S}(\operatorname{Gal}(K|\,k))$. Además, dado $L \in \mathcal{E}_{K|\,k}$, la extensión $K|L$ es de Galois si y sólo si $\operatorname{Aut}(K|L) \trianglelefteq \operatorname{Gal}(K|\,k)$. En tal caso $\operatorname{Gal}(L|\,k) \cong \operatorname{Gal}(K|\,k)/\operatorname{Gal}(K|L)$.*

Por otro lado, en la categoría de espacios topológicos, **Top**, existe el concepto de aplicación cubriente, que resultan ser morfismos suprayectivos, $p : Y \to X$, tales que para cada $x \in X$, existe $U \subseteq X$ vecindad abierta de $x$ tal que $Y \times_X U \cong \coprod_{i \in J} U$, donde el producto fibrado se toma de $p$ a través de la inclusión $U \hookrightarrow X$. Dada una aplicación cubriente $p : Y \to X$, existe el grupo de transformaciones cubrientes, $\operatorname{Aut}(p)$, definido por $\{f \in \mathbf{Top}(Y,Y) \mid p \circ f = p\}$. Con hipótesis adecuadas de conexidad en el dominio y codominio así como una acción transitiva en fibras de $\operatorname{Aut}(p)$, existe un TFTG para aplicaciones cubrientes, el cual establece una correspondencia biyectiva entre subgrupos de $\operatorname{Aut}(p)$ y factorizaciones de $p$, $Y \to Z \to X$, donde $Z \cong Y/G$ para $G \subseteq \operatorname{Aut}(p)$ un subgrupo.

La discusión anterior muestra una dualidad pues hay propiedades que comparten ciertos epimorfismos en la categoría **Top** y ciertos monomorfismos en la categoría **Field**. Sin embargo, esta dualidad no va más allá en este nivel pues por ejemplo existe la noción de producto de aplicaciones cubrientes con base común $X$, $Y \to X$ y $Z \to X$, cuyo espacio cubriente es el producto fibrado $Y \times_X Z$, y un coproducto cuyo espacio cubriente es la unión ajena $Y \coprod Z$, cosa que no existe para el caso de campos. Para solucionar esto Grothendieck piensa en trabajar estructuras relativas y además en sumergir la categoría de campos en una categoría más general, a saber la categoría de $k$-álgebras sobre el campo $k$. Es bien sabido que si $A$ y $B$ son $k$-álgebras, entonces $A \otimes_k B$ con las funciones de inclusión en la primera y segunda entrada es el coproducto de las $k$-álgebras dadas. Además, el producto de $k$-álgebras siempre está definido y con esto Grothendieck arregla el problema categórico. Sin embargo, el que existan más objetos lo lleva a buscar si es que entre esos objetos existen más que se comporten como las aplicaciones cubrientes, al menos respecto a sus propiedades pues en este nivel los morfismos no son necesariamente inyectivos. Para esto Grothendieck piensa en un análogo para la definición de aplicación cubriente en un contexto algebrico y comienza por analizar el caso de campos. Lo primero que nota es que dada una extensión $L|\, k$, existe su campo de descomposición $N$ para $L$. Así, existe $a \in L$ tal que $L = k[a] \cong k[x]/(min_k(a))$, con $min_k(a) \in k[x]$ el polinomio mínimo de $a$ con coeficientes en $k$. En este contexto se tiene una noción de que "$N$ escinde a $L$", que es una condición como la de trivialidad local en el caso de aplicaciones cubrientes. Esta condición dice que $N \otimes_k L \cong N^{\partial min_k(a)}$, con $\partial min_k(a)$ el grado de $min_k(a)$. Esto lleva a Grothendieck a considerar primero extesiones finitas y separables de $k$ para posteriormente tomar sus productos finitos, que es lo que se conocen como $k$-álgebras finitas étale. Nótese que estas son construidas al pensar nuevamente en la dualidad pues en el caso topológico lo que funcionaba era el coproducto. Además, estás tienen una teoría análoga a la de aplicaciones cubrientes en el sentido de que la categoría que definen es equivalente a una de conjuntos finitos con la topología discreta y una acción continua del grupo de Galois absoluto de $k$, cosa que sucede con las aplicaciones cubrientes finitas respecto al grupo fundamental. Esta es la analogía que notó Grothendieck entre dichos grupos y los primeros dos capítulos de esta tesis se dedican a presentar de manera puntual estos teoremas.

En este punto surgen dos posibles direcciones a seguir, ambas estudiadas por Grothendieck. La primera de ellas va en dirección de la definición de topología de Grothendieck como sustituto a la idea de estudiar espacios topológicos a partir de sus abiertos para ahora usar la idea de cubierta. La segunda dirección, que es la que se sigue en esta tesis, es el desarrollo de lo que se conoce como la "teoría de Galois de Grothendieck". En esta Grothendieck busca los morfismos análogos a las aplicaciones cubrientes para el caso de esquemas. Dichos morfismos se conocen como cubrientes étale finitos y tienen propiedades análogas a las que tienen las aplicaciones cubrientes sobre un espacio topológico. Además, en la busqueda de un teorema de caracterización de estos morfismos a partir de una equivalencia con una categoría de conjuntos finitos con acción de un grupo topológico, Grothendieck define un grupo que se conoce como el "grupo fundamental algebraico", que es un grupo profinito con el cual se da la equivalencia deseada. Vale la pena mencionar que esta teoría se llama de Galois pues tiene como caso particular la teoría de Galois para campos que corresponde a la teoría de $k$-esquemas donde el grupo fundamental es el grupo de Galois absoluto. Estas afirmaciones forman parte del material del tercer capítulo.

Pero la historia no se detiene aquí pues como siempre Grothendieck va más allá y lo que busca es el entendimiento de por qué funcionan las cosas. Para esto introduce un formalismo más general que muestre que todas ellas son manifestaciones de la misma teoría y donde los argumentos no requieran de especificaciones concretas del objeto particular en cuestión. Así, sus estudios lo llevan a definir las categorías de Galois en [**SGA1**] de manera axiomática como una pareja que consta de una categoría y una pregavilla covariante con dominio dicha categoría, las cuales cumplen condiciones especiales, que aunque son técnicas y algunas parecen artificiales, están justificadas de lo que sucedía en teoría de campos, aplicaciones cubrientes y morfismos étale finitos, donde estas categorías de hecho se vuelven ejemplos. Entre los resultados que demuestra es que en estas categorías siempre se tiene un grupo profinito que se obtienen al considerar los automorfismos del funtor que las define y que cada una de estas categorías es equivalente a una de conjuntos finitos con la acción continua de dicho grupo. Este es el material básico que se presenta en el último capítulo.

Dicho todo esto, el objetivo de esta tesis es presentar la definición y propiedades principales de las categorías de Galois motivadas por la teoría de Galois sobre campos, pasando por la teoría de aplicaciones cubrientes y morfismos étale finitos. La elección de esta presentación del tema es para motivar por qué las propiedades que definen a una categoría de Galois son importantes y necesarias para englobar en una sola teoría las teorías mencionadas. Además de lo mencionado anteriormente, el primer capítulo se dedica al estudio de algunos aspectos de la teoría de Galois en campos, comenzando por la obtención del TFTG para extensiones infinitas y concluyendo con el TFTG de Grothendieck que afirma que la categoría de $k$-álgebras finitas étale es equivalente a la de conjuntos finitos con una acción continua del grupo de Galois absoluto de $k$. En este capítulo también se discuten las principales propiedades de grupos profinitos necesarias para el desarrollo de la tesis.

En el segundo capítulo, además de discutir el TFTG para aplicaciones cubrientes y establecer la equivalencia de ciertas aplicaciones cubrientes finitas sobre un espacio $X$ con conjuntos finitos dotados con una acción continua de del grupo fundamental $\pi_1(X)$, se incluyen dos teoremas de carecterización de esta como categorías de gavillas localmente constantes y, funtores del grupoide fundamental en la categoría de conjuntos. Este último material no forma parte esencial del texto pero se da para mostrar otras equivalencias usuales de categorías de aplicaciones cubrientes sobre un espacio.

El capítulo tres se dedica al estudio de los morfismos étale finitos y del grupo fundamental algebraico así como de sus principales propiedades. Además de lo mencionado anteriormente, en este también se discute una comparación que existe entre el grupo fundamental algebraico y el grupo fundamental para esquemas de tipo finito sobre los complejos. Esta discusión es interesante pues la forma de conectar ambos grupos es mediante conceptos de geometría algebraica compleja, los cuales fueron estudiados por Serre en su famoso artículo [**GAGA**].

Para concluir, el último capítulo está dedicado al estudio de las propiedades básicas de las categorías de Galois y a probar el teorema de Grothendieck que caracteriza dichas categorías como aquellas que son equivalentes a una de conjuntos finitos con la acción continua de un grupo profinito, que se conoce como el grupo fundamental de una categoría de Galois. El capítulo concluye mostrando que la búsqueda de la funtorialidad del grupo fundamental de una categoría de Galois permite establecer una equivalencia de 2-categorías.

Antes de empezar, lo que se espera de esta tesis es mostrar toda la riqueza matemática en torno a la teoría de Galois desarrollada por Grothendieck, así como su manifestación en la topología y la geometría algebraica, para mostrar por qué esta es una de las teorías matemáticas más potentes y bellas de los últimos tiempos. El sabor de boca general que se espera dejar queda expresado en la siguiente frase de A. Weyl respecto a la teoría de Galois.

*Nada es más fructífero, como todos los matemáticos saben, que esas analogías oscuras, atisbos de niebla de una teoría con otra, esos contactos furtivos, esos revoltijos inexplicables; también nada da más placer al investigador. Un día llega cuando lo ilusorio se disipa; la vaguedad cambia en certeza; las teorías gemelas muestran su fuente común antes oculta ... La metafísica se ha transformado en matemáticas, lista para ser la sustancia de un trabajo cuya belleza tranquila pudiera no movernos más.*

# Notación

Para grupos que no son necesariamente abelianos ó que no lo sean se utilizará notación multiplicativa con $e$ el simbolo para el neutro, mientras que para grupos abelianos se usará notación aditiva con 0 el simbolo para el neutro.

Si $K$ es una extensión de campo de $k$, entonces esto se escribirá como $K|k$. En una de tales extensiones $\mathrm{Aut}(K|k)$ denota al grupo de automorfismos que fijan a $k$. Cuando la extensión $K|k$ es de Galois a dicho grupo se le conoce como el grupo de Galois y se le denota mediante $\mathrm{Gal}(K|k)$.

También se usan los siguientes simbolos:

$\overline{k}$ clausura algebraica del campo $k$.

$A^{\times}$ grupo de unidades del anillo $A$.

$\mathrm{car}(A)$ característica del anillo $A$.

$mcd$ máximo común divisor.

$X^I$ espacio de trayectorias en $X$.

$\Omega_x(X)$ espacio de lazos basados en $x \in X$.

$c_x$ lazo constante en $x \in X$.

$\mathrm{res}_V^W(\mathcal{F})$ morfismo de restricción de la gavilla $\mathcal{F}$ para $V \subseteq W$.

$\mathrm{supp}(\mathcal{F})$ soporte de la gavilla de grupos abelianos $\mathcal{F}$.

Respecto a la teoría de categorías, para una categoría $\mathcal{C}$ se denotará a su categoría opuesta por $\mathcal{C}^{op}$. El simbolo $A \in \mathcal{C}$ indica que $A$ es un objeto en $\mathcal{C}$. La identidad en el objeto $A \in \mathcal{C}$ se denota por $1_A$ y la familia de morfismos entre $A, B \in \mathcal{C}$ por $\mathcal{C}(A, B)$. El simbolo $\mathrm{Aut}_{\mathcal{C}}(A)$ indica la colección de automorfismos en $\mathcal{C}$ para el objeto $A \in \mathcal{C}$.

Además se van a usar las siguientes categorías con su estructura estándar.:

**Set** categoría de conjuntos.

**Top** categoría de espacios topológicos.

$\mathbf{Top}_*$ categoría de espacios topológicos basados.

**TopGrp** categoría de grupos topológicos.

$A - \mathbf{Mod}$ categoría de $A$-módulos izquierdos.

**Sh(X)** categoría de gavillas de conjuntos sobre el espacio topológico $X$.

**ASh(X)** categoría de gavillas de grupos abelianos sobre el espacio topológico $X$.

**Sm** categoría de esquemas.

**AfSm** categoría de esquemas afines.

Capítulo 1

# Sobre el teorema fundamental de la teoría de Galois

En el presente capítulo se estudian dos generalizaciones del Teorema Fundamental de la Teoría de Galois (TFTG), una para extesiones infinitas, debida a Krull, y la segunda para $k$-álgebras étale de dimensión finita debida a Grothendieck.

A nivel técnico la diferencia fundamental con el TFTG clásico radica en el hecho de que para estas versiones el uso de la topología se vuelve imprescindible. Por tal razón se incluyen un par de secciones donde por un lado se estudian los conceptos necesarios de grupos profinitos y por otro se analizan ciertas acciones continuas del grupo de Galois absoluto sobre conjuntos finitos, pues cada una de estas constituyen los pilares bajo los cuales se apoya cada uno de los teoremas mencionados.

## 1. Grupos profinitos

En la categoría de grupos el límite inverso de un sistema inverso de grupos siempre existe pues si $(\{G_\alpha\}_{\alpha\in\Lambda}, \{\phi_{\alpha\beta} : G_\beta \to G_\alpha\}_{\alpha\leq\beta})$ es un sistema inverso, entonces $\varprojlim_{\alpha\in\Lambda} G_\alpha = \{(x_\alpha)_{\alpha\in\Lambda} \in \prod_{\alpha\in\Lambda} G_\alpha \mid \forall\alpha \leq \beta(\phi_{\alpha\beta}(x_\beta) = x_\alpha)\}$ con la restricción de las proyecciones del producto define tal límite.

Esta construcción permite definir una importante clase de grupos.

Definición 1.1. *Un grupo es **profinito** si es límite inverso de un sistema inverso de grupos finitos.*

Todo grupo profinito está equipado con una topología canónica pues en la categoría de grupos topológicos todo sistema inverso tiene un límite inverso, que como conjunto es igual al conjunto que se define en el caso de la categoría de grupos, y es claro que las restricciones de las funciones proyección del producto son continuas. Más aún, el límite inverso es un subgrupo cerrado del producto cuando cada uno de los grupos del sistema es Hausdorff. Así, al dotar a cada grupo del sistema inverso con la topología discreta, el grupo adquiere la estructura topológica mencionada.

En virtud de la discusión anterior la **categoría de grupos profinitos** es la subcategoría plena de la categoría de grupos topológicos cuya clase de objetos es la clase de grupos profinitos.

El resultado que se busca dar en esta sección es un teorema de caracterización para grupos profinitos a partir de conceptos topológicos más usuales. En esta dirección se requiere del siguiente resultado de la teoría de grupos topológicos.

LEMA 1.2. *Los subgrupos abiertos de un grupo topológico compacto son precisamente los subgrupos cerrados de índice finito.*

DEMOSTRACIÓN. Sea $G$ un grupo topológico compacto y $H \subseteq G$ un subgrupo. Supóngase que $H$ es abierto en $G$. Dado que el conjunto de clases laterales de $H$ forman una partición de $G$ y cada una de ellas es un conjunto abierto, por compacidad de $G$ existen $g_1, ..., g_n \in G$ tales que $G = \cup_{i=1}^n g_i H$. Esto muestra que $[G : H] = n$, y dado que puede suponerse sin pérdida de generalidad que $g_1 = e$, el neutro del grupo, entonces $H = G \setminus \bigcup_{i=2}^n g_i H$. Así, $H$ es cerrado.

Si $H \subseteq G$ es un subgrupo de índice finito cerrado, entonces sea $\{H, g_1 H, ..., g_n H\}$ el conjunto de sus clases laterales. Por ser este conjunto una partición de $G$, $H = G \setminus \bigcup_{i=1}^n g_i H$. Dado que cada una de las clases laterales son cerradas, entonces la igualdad anterior muestra que $H$ es abierto. $\square$

TEOREMA 1.3. *Las siguientes afirmaciones son equivalentes:*

1. *$G$ es un grupo profinito.*
2. *$G$ es un grupo topológico compacto, Hausdorff y totalmente disconexo.*
3. *$G$ es un grupo topológico compacto, Hausdorff y la familia de subgrupos abiertos forman una base de vecindades del neutro tal que su intersección es el neutro.*

DEMOSTRACIÓN. $1 \Rightarrow 2$) Por hipótesis $G = \varprojlim_{\alpha \in \Lambda} G_\alpha$ para $(\{G_\alpha\}_{\alpha \in \Lambda}, \{\phi_{\alpha\beta}\}_{\alpha \leq \beta})$ un sistema inverso tal que para cada $\alpha \in \Lambda$, $G_\alpha$ es un grupo finito. Como $G$ es un subgrupo cerrado de $\prod_{\alpha \in \Lambda} G_\alpha$, pues cada grupo es un espacio Hausdorff, y dicho producto es un espacio compacto por el teorema de Tychonoff, entonces $G$ es compacto. Más aún, el producto $\prod_{\alpha \in \Lambda} G_\alpha$ es un espacio totalmente separado pues cada grupo lo es, así el producto es en partícular un espacio Hausdorff y totalmente disconexo, por lo que estas dos propiedades se heredan a $G$.

$2 \Rightarrow 3$) Lo único que se tiene que probar es la afirmación respecto al sistema fundamental de vecindades del neutro. Así, lo primero que se observa es que como en todo espacio compacto y Hausdorff la propiedad de ser totalmente disconexo es equivalente a la de ser 0-dimensional y también a la de ser totalmente separado, entonces la primera equivalencia implica que la colección de subconjuntos abiertos-cerrados forman una base para la topología de $G$, y la segunda que $\bigcap\{V \mid V \subseteq G$ es abierto-cerrado y $e \in V\} = \{e\}$. Así, la prueba de la afirmación se reduce a probar que todo subconjunto abierto-cerrado de $G$ que tiene como elemento al neutro contiene a un subgrupo abierto y normal de $G$.

En efecto, sea $V \subseteq G$ uno de tales subconjuntos. Se define $F := (G \setminus V) \cap V^2$. Lo primero que se observa es que $F$ es cerrado en $G$ por ser intersección de dos conjuntos cerrados, y así, es un subconjunto compacto. Sea $x \in V$, entonces por definición de $F$ se tiene que $x \in G \setminus F$. Al ser $G \setminus F$ abierto en $G$, la continuidad del producto implica que existen $V_x, S_x \subseteq V$ abiertos con $e \in V_x$ y $x \in S_x$, tales que $V_x S_x \subseteq G \setminus F$. Como $\{V_x \mid x \in V\}$ es una cubierta abierta de $V$ y $V$ es compacto, por ser un subconjunto cerrrado de $G$ que es compacto, entonces existen $x_1, ..., x_n \in V$ tales que $V = \bigcup_{i=1}^n V_{x_i}$. Se define entonces $S = \bigcap_{i=1}^n S_{x_i}$, y nótese que como $e \in S$ entonces $S \neq \emptyset$. Además, $S$ es abierto en $G$, así que al definir $W = S \cap S^{-1}$, se tiene que $W$ es una vecindad abierta simétrica del neutro.

Es claro que $VW \subseteq V^2$. Por otro lado, por construcción se tiene que $VW \subseteq G \setminus F$. Esto implica que $VW \subseteq V$ y siguiendo un argumento análogo se tiene que para todo $n \in \mathbb{N}^+$, $VW^n \subseteq V$. Considérese ahora el conjunto $H = \bigcup_{n=1}^\infty W^n$. Por ser $W$ una vecindad simétrica del neutro, se deduce que $H$ es un subgrupo de $G$. Más aún, este es abierto por ser unión de conjuntos abiertos. Así, al considerar $H_G = \bigcap_{x \in G} xHx^{-1}$, es claro que este subgrupo de $G$ es abierto y normal. Además, se tiene que $H_G \subseteq H \subseteq VH \subseteq \bigcup_{n=1}^\infty VW^n \subseteq V$, lo que prueba la afirmación.

$3 \Rightarrow 1$) Sea $\mathcal{U}$ el conjunto de subgrupos abiertos y normales de $G$. Dicho conjunto es dirigido al considerar como orden a la contención inversa, por lo que se tiene un sistema inverso $(\{G/U\}_{U \in \mathcal{U}}, \{\phi_{UV}\}_{U \leq V})$ de grupos finitos, donde la finitud y el hecho de que el cociente sea un grupo se deduce del Lema 1.2. Así, al considerar la familia de proyecciones canónicas $\{\pi_U : G \to G/U\}_{U \in \mathcal{U}}$, que es claramente compatible con la familia de morfismos $\{\phi_{UV}\}_{U \leq V}$, la propiedad universal del límite implica que existe un único morfismo de grupos topológicos $f : G \to \varprojlim_{U \in \mathcal{U}} G/U$ tal que para todo $U \in \mathcal{U}$, $p_U \circ f = \pi_U$. Además, como en la familia $\{\pi_U : G \to G/U\}_{U \in \mathcal{U}}$ todos los elementos son suprayectivos y los dominios y codominios correspondientes son espacios compactos y Hausdorff, entonces $f$ es suprayectiva. Para concluir se observa que como $\bigcap \mathcal{U} = \{e\}$, entonces $\operatorname{nuc}(\pi) = \{e\}$, lo que muestra que $f$ es un isomorfismo de grupos. Más aún, como $G$ es compacto y el codominio de $f$ es un espacio Hausdorff, entonces $f$ es un homeomorfismo, lo que muestra que $f$ es de hecho un isomorfismo de grupos topológicos. $\square$

Para futuras referencias vale la pena enunciar el siguiente corolario cuya prueba es directa del Lema 1.2 y del teorema anterior.

Corolario 1.4. *En un grupo profinito los subgrupos abiertos son precisamente los subgrupos cerrados de índice finito.*

El siguiente resultado muestra como obtener de forma abstracta grupos profinitos a partir de la estructura algebraica y topológica de un grupo profinito dado.

Proposición 1.5. *Sea $G$ un grupo profinito y $H \subseteq G$ un subgrupo.*

1. *Si $H$ es abierto o cerrado en $G$, entonces $H$ es profinito.*
2. *Si $H$ es cerrado y normal en $G$, entonces $G/H$ es profinito.*

Demostración. Para 1 primero supóngase que $H$ es cerrado en $G$. Dado que $G$ es compacto, la hipótesis implica que $H$ también lo es. Además como las propiedades de ser Hausdorff y totalmente disconexo se heredan a subespacios, entonces $H$ es compacto, Hausdorff y totalmente disconexo, por lo que es un grupo profinito.

En el caso en el que $H$ es abierto el corolario anterior implica que $H$ es cerrado y con índice finito en $G$, luego es un grupo profinito por el caso anterior.

Respecto a 2 sea $H$ un subgrupo de $G$ cerrado y normal. Estas propiedades implican que $G/H$ es un grupo topológico Hausdorff. Por otro lado la proyección canónica $p : G \to G/H$ es continua y suprayectiva, así que como $G$ es compacto entonces $G/H$ es compacto. Para concluir si $\{U_\alpha\}_{\alpha\in\Lambda}$ es un sistema fundamental de vecindades del neutro, entonces $\{p(U_\alpha)\}_{\alpha\in\Lambda}$ es un sistema fundamental de vecindades del neutro de $G/H$. Así, por el teorema anterior $G/H$ es un grupo profinito. □

Ahora se presentan algunos de los ejemplos más representativos de grupos profinitos.

Ejemplo 1.6. *Si $G$ es un grupo finito, entonces $G$ es un grupo profinito pues es límite del sistema inverso $(\{G_0\}, \{\phi_{00}\})$ donde $G_0 = G$ y $\phi_{00} = 1_G$.*

EJEMPLO 1.7. *Para $G$ un grupo sea $P_G = \{H \trianglelefteq G \mid [G:H] < \aleph_0\}$. Al considerar a $P_G$ con el orden dado por la contención inversa dicho conjunto adquiere estructura de orden parcial, con lo que se tiene un sistema inverso donde las funciones de transición $\phi_{HK} : G/K \to G/H$ son la función cambio de clase para $H \leq K$. El límite inverso de dicho sistema se conoce como la* ***completación profinita*** *de $G$ y se denota por $\hat{G}$.*

*Por la propiedad universal del límite existe un morfismo de grupos $\eta : G \to \hat{G}$ inducido por la familia de proyecciones canónicas en los elementos de $P_G$. Dicho morfismo tiene como núcleo $\bigcap_{H \in P_G} H$ y tiene imagen densa en $\hat{G}$. Así, este morfismo es inyectivo si y sólo si $\bigcap_{H \in P_G} H = \{e\}$. Cuando un grupo $G$ cumple esta última propiedad se dice que es* ***residualmente finito****.*

EJEMPLO 1.8. *Sea $G = \mathbb{Z}$. Como $G$ es abeliano entonces todo subgrupo de $G$ es normal. Además, $H \subseteq G$ es un subgrupo si y sólo si existe $n \in \mathbb{N}$ tal que $H = n\mathbb{Z}$. Con la notación del ejemplo anterior $P_G = \{n\mathbb{Z} \mid n \in \mathbb{N}^+\}$ y $\hat{\mathbb{Z}} := \varprojlim_{n \in \mathbb{N}^+} \mathbb{Z}/n\mathbb{Z}$ es la completación profinita de $\mathbb{Z}$. Nótese que como $\mathbb{Z}$ es residualmente finito entonces $\mathbb{Z}$ se encaja en su completación profinita y así $\mathbb{Z}$ es denso en $\hat{\mathbb{Z}}$.*

*Además, dado que para todo $n \in \mathbb{N}^+$, $\mathbb{Z}/n\mathbb{Z}$ es un anillo conmutativo unitario, $\hat{\mathbb{Z}}$ tiene estructura de anillo conmutativo unitario al definir para $([x_n])_n, ([y_n])_n \in \hat{\mathbb{Z}}$, $([x_n])_n \cdot ([y_n])_n := ([x_n y_n])_n$. Al anillo $\hat{\mathbb{Z}}$ se le conoce como el* ***anillo de números de Hensel****.*

EJEMPLO 1.9. *Sea $p \in \mathbb{N}$ un primo. Se considera como conjunto dirigido a $\mathbb{N}^+$ con su orden canónico. Así, el conjunto $\{\mathbb{Z}/p^n\mathbb{Z} \mid n \in \mathbb{N}^+\}$ forma un sistema inverso con la familia de funciones de transición $\{\phi_{nm} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}\}_{n \leq m}$ dadas por el cambio de clase. Sea $\mathbb{Z}_p := \varprojlim_{n \in \mathbb{N}^+} \mathbb{Z}/p^n\mathbb{Z}$ el grupo profinito definido por el sistema inverso considerado, y de manera análoga al ejemplo anterior la estructura de anillo conmutativo unitario de los grupos que definen al sistema inverso dan una estructura de anillo conmutativo unitario a $\mathbb{Z}_p$. A este anillo se le conoce como el* ***anillo de números $p$-ádicos****. Un grupo que es límite inverso de un sistema de $p$-grupos se conoce como* ***pro $p$-grupo****. Así, como para todo $n \in \mathbb{N}^+$, $\mathbb{Z}/p^n\mathbb{Z}$ es un $p$-grupo, entonces $\mathbb{Z}_p$ es un pro $p$-grupo.*

OBSERVACIÓN 1.10. *Como consecuencia del teorema chino del residuo se puede probar que $\hat{\mathbb{Z}} \cong \prod_{p \in \mathbb{N}^+,\ p\ primo} \mathbb{Z}_p$ como anillos conmutativos unitarios.*

EJEMPLO 1.11. *Para un grupo topológico $G$ se define su **dual**, $G^*$, como el espacio $\textbf{\textit{TopGrp}}(G, \mathbb{Q}/\mathbb{Z})$ con la topología compacto-abierta, donde $\mathbb{R}/\mathbb{Z}$ tiene la topología cociente dada por la proyección canónica $\mathbb{R} \to \mathbb{R}/\mathbb{Z}$. Es un resultado básico de la teoría de grupos topológicos que $G^*$ es un grupo topológico abeliano. Además, bajo estas hipótesis se puede definir un morfismo de grupos topológicos $\alpha_G : G \to G^{**}$ mediante la regla de correspondencia $\alpha_G(x)(\varphi) = \varphi(x)$, donde $x \in G$ y $\varphi \in G^*$. Es muy sencillo ver que la familia de morfismos de grupos topológicos $\alpha = \{\alpha_G : G \to G^{**}\}_{G \in \textbf{\textit{TopGrp}}}$ es una transformación natural entre los funtores $1_{\textbf{\textit{TopGrp}}}, (\_)^{**} : \textbf{\textit{TopGrp}} \to \textbf{\textit{TopGrp}}$. Más aún, para el caso abeliano se tiene el siguiente resultado cuya prueba puede encontrarse en el Teorema 2.9.9 del Capítulo 2 en* [**RZ**, pp 64–65].

TEOREMA 1.12. *(Dualidad de Pontryagin para grupos abelianos profinitos)*

1. *Si $G$ es un grupo abeliano profinito o abeliano discreto de torsión, entonces $G^* \cong \textbf{\textit{TopGrp}}(G, \mathbb{Q}/\mathbb{Z})$.*
2. *El dual de un grupo abeliano profinito es un grupo abeliano discreto de torsión y visceversa.*
3. *Para cada grupo abeliano profinito o abeliano discreto de torsión $\alpha_G : G \to G^{**}$ es un isomorfismo de grupos topológicos.*

*De la segunda afirmación del teorema anterior se deduce que el funtor que a cada grupo topológico le asigna su dual se restringe a un funtor de la categoría de grupos abelianos profinitos en la categoría de grupos abelianos discretos de torsión. Además, esta misma afirmación también dice que este funtor se restrige a un funtor de la categoría de grupos abelianos discretos de torsión en la categoría de grupos abelianos profinitos. Más aún, por la tercera afirmación la composición de estos funtores es naturalmente isomorfa a la identidad correspondiente al orden en que se componen. Para concluir nótese que las categorías de grupos abelianos discretos de torsión y la categoría de grupos abelianos de torsión son isomorfas. Por lo tanto se concluye que el teorema de dualidad de Pontryagin establece una antiequivalencia entre las categorías de grupos abelianos profinitos y de grupos abelianos de torsión.*

## 2. La versión para extensiones no necesariamente finitas

LEMA 1.13. *Sea $K|k$ una extensión de Galois. Entonces toda subextensión finita se encaja en una subextensión de Galois finita de $K|\,k$.*

Demostración. Sea $L|\,k$ una subextensión finita de $K|\,k$. Como $K|\,k$ es de Galois, entonces $K|\,k$ es separable y así $L|\,k$ es separable. Luego, por el teorema del elemento primitivo existe $a \in L$ tal que $L = k(a)$. Si $f$ denota el polinomio mínimo de $a$ con coeficientes en $k$, entonces el campo de descomposición de $f$, $k(f)$, tiene una copia de $L = k(a)$, y dicho campo de descomposición es una subextensión de Galois de $K|\,k$ finita pues $f$ es separable. □

El resultado anterior se puede interpretar diciendo que cada extensión de Galois de un campo $k$ se puede ver como la unión de extensiones de Galois finitas de $k$. De hecho esto también se puede expresar diciendo que estas son límite directo de sus subextensiones de Galois finitas.

Considérese una extensión de Galois $K|\,k$. Denótese por $\mathcal{S}_{K|\,k}$ al conjunto de subcampos de $K$ que son extensiones de Galois finitas de $k$. Este es un conjunto dirigido con la contención. Así, si $L, M \in \mathcal{S}_{K|\,k}$ son tales que $L \leq M$, entonces al considerar la función $\phi_{LM} : \mathrm{Gal}(M|k) \to \mathrm{Gal}(L|k)$ dada por $\phi_{LM}(\sigma) = \sigma|_L$, esta asignación está bien definida y además es suprayectiva por el TFTG. Más aún, en la situación de que $L, M, N \in \mathcal{S}_{K|\,k}$ son tales que $L \leq M \leq N$, claramente se tiene que $\phi_{MN} \circ \phi_{LM} = \phi_{LN}$. Estas observaciones muestran que $(\{\mathrm{Gal}(L|k)\}_{L\in\mathcal{S}_{K|\,k}}, \{\phi_{LM}\}_{L\leq M})$ es un sistema inverso de grupos finitos y entonces puede obtenerse su límite $(\varprojlim_{L\in\mathcal{S}_{K|\,k}} \mathrm{Gal}(L|\,k), \{p_L\}_{L\in\mathcal{S}_{K|\,k}})$. Esto motiva el siguiente resultado:

Proposición 1.14. *Si $K|k$ es una extensión de Galois, entonces $\mathrm{Gal}(K|k)$ tiene estructura de grupo profinito.*

Demostración. Con la notación de la discusión previa al resultado se afirma que $\mathrm{Gal}(K|\,k) \cong \varprojlim_{L\in\mathcal{S}_{K|\,k}} \mathrm{Gal}(L|\,k)$ en la categoría de grupos.

En efecto, para cada $L|\,k$ de Galois finita se define la función $r_L : \mathrm{Gal}(K|\,k) \to \mathrm{Gal}(L|\,k)$ mediante $r_L(\sigma) = \sigma|_L$. Esta función está bien definida pues al ser $L|\,k$ de Galois, $\sigma(L) \subseteq L$, y es claro que esta es un morfismo de grupos. Además, para $L|\,k$ y $M|\,k$ de Galois finitas tales que $M \leq L$, se tiene que claramente $\phi_{ML} \circ r_L = r_M$. Así, por la propiedad universal del límite en la categoría de grupos existe un único morfismo de grupos $r : \mathrm{Gal}(K|\,k) \to \varprojlim_{L\in\mathcal{S}_{K|\,k}} \mathrm{Gal}(L|\,k)$ tal que para toda $L|\,k$ de Galois finita, $p_L \circ r = r_L$. Así, la afirmación que se quiere probar es equivalente a ver que el morfismo $r$ es un isomorfismo en la categoría de grupos, y de hecho en este caso, esto es equivalente a probar que $r$ es una función inyectiva y suprayectiva.

Para la inyectividad de $r$ sea $\sigma \in \mathrm{nuc}(r)$. Para cada $L|\,k$ de Galois finita $\sigma|_L = r_L(\sigma) = p_L r(\sigma) = p_L(e) = 1_L$, con $e \in \varprojlim_{L\in\mathcal{S}_{K|\,k}} \mathrm{Gal}(L|\,k)$ el neutro en dicho grupo. Esto muestra que para cada extensión de Galois finita la restricción de $\sigma$ a dicha extensión es el neutro, por lo tanto $\sigma = 1_K$, lo que prueba la contención no trivial en la igualdad $\mathrm{nuc}(r) = \{1_K\}$, que es equivalente a que $r$ sea inyectiva.

Respecto a la suprayectividad sea $(\sigma_L)_{L\in\mathcal{S}_{K|\,k}} \in \varprojlim_{L\in\mathcal{S}_{K|\,k}} \mathrm{Gal}(L|\,k)$. Dado $a \in K$, se tiene por el Lema 1.13 que existe $L|\,k$ de Galois finita tal que $k(a) \subseteq L$. Así, se define $\sigma(a) = \sigma_L(a)$, si $L \in \mathcal{S}_{K|\,k}$ tal que $k(a) \subseteq L$. La asignación $\sigma$ es una función por la condición de compatibilidad que satisfacen los elementos en el límite inverso y por construcción es un elemento de $\mathrm{Gal}(K|\,k)$. Para ver que $r(\sigma) = (\sigma_L)_{L\in\mathcal{S}_{K|\,k}}$ nótese que dada $M \in \mathcal{S}_{K|\,k}$ se tiene que $p_M r(\sigma) = r_M(\sigma) = \sigma|_M := \sigma_M$. $\square$

Ahora se presentarán algunos ejemplos de grupos de Galois para extensiones infinitas.

Ejemplo 1.15. *Sea $p \in \mathbb{N}$ un primo, $k = \mathbb{F}_p$ el campo con $p$ elementos y $k_s$ la **clausura separable** de $k$. Lo que se busca determinar es el **grupo de Galois absoluto** de $k$,* $\mathrm{Gal}(k_s\,|\,k)$.[1]

*De acuerdo a la proposición anterior* $\mathrm{Gal}(k_s\,|\,k) \cong \varprojlim_{L\in\mathcal{S}_{k_s\,|\,k}} \mathrm{Gal}(L|\,k)$. *Sin embargo, por un resultado clásico respecto a campos finitos se sabe que* $\mathcal{S}_{k_s\,|\,k} = \{\mathbb{F}_{p^n} \mid n \in \mathbb{N}^+\}$ *y además,* $\mathrm{Gal}(\mathbb{F}_{p^n}|\,k) \cong \mathbb{Z}/n\mathbb{Z}$, *donde un generador para* $\mathrm{Gal}(\mathbb{F}_{p^n}|\,k)$ *es el morfismo de Frobenius* $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *cuya regla de correspondencia es* $\varphi(x) = x^p$.

*Ahora, si $n, m \in \mathbb{N}^+$ son tales que $n|m$, entonces el morfismo* $\varphi_{mn} : \mathrm{Gal}(\mathbb{F}_{p^m}|\,k) \to \mathrm{Gal}(\mathbb{F}_{p^n}|\,k)$ *corresponde por el isomorfismo de los grupos de Galois a los grupos cíclicos al morfismo* $\hat{\varphi_{mn}} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ *dado por el cambio de clase.*

*Por lo tanto,*

$$\mathrm{Gal}(k_s\,|\,k) \cong \varprojlim_{n\in\mathbb{N}^+} \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}.$$

[1] Dado que la clausura separable de un campo está bien definida salvo isomorfismo, lo mismo sucede con el grupo de Galois absoluto.

Ejemplo 1.16. *Sea $p \in \mathbb{N}$ un primo. Considérese la clausura algebraica de $\mathbb{Q}$ que es subcampo de $\mathbb{C}$, y se denota por $\mu_{p^n}$ al conjunto de raíces $p^n$-ésimas de la unidad para $n \in \mathbb{N}^+$. Además, $\mu_{p^\infty} := \bigcup_{n=1}^{\infty} \mu_{p^n}$.*

*Nótese que para cada $n \in \mathbb{N}^+$, $\mathbb{Q}(\mu_{p^n}) \subseteq \mathbb{Q}(\mu_{p^{n+1}})$ y además $\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{p^n})$. De esto se deduce que*

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q}) \cong \varprojlim_{n \in \mathbb{N}^+} \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})|\mathbb{Q}).$$

*Pero se recuerda que para $m > 2$ si $\omega \in \mathbb{C}$ es una raíz m-ésima primitiva de la unidad, entonces $\mathbb{Q}(\omega)|\mathbb{Q}$ es de Galois y $\mathrm{Gal}(\mathbb{Q}(\omega)|\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, con $(\mathbb{Z}/m\mathbb{Z})^\times$ el grupo de unidades del anillo $\mathbb{Z}/m\mathbb{Z}$.*

*Así, como para cada $n \in \mathbb{N}^+$, $\mathbb{Q}(\mu_{p^n})$ es el campo de descomposición de una $p^n$-ésima raíz primitiva de la unidad $w_{p^n}$, entonces $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})|\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. Luego,*

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q}) \cong \varprojlim_{n \in \mathbb{N}^+} (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times.$$

*Vale la pena mencionar que en el Teorema 2 del Capítulo 2 de* [**Se73**, pp 17] *se puede encontar una descripción más explícita del grupo de unidades de los enteros p-ádicos $\mathbb{Z}_p^\times$.*

Ejemplo 1.17. *De manera análoga a los ejemplos anteriores se puede ver que si $\mu = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^+(z^n = 1)\}$, entonces:*

$$\mathrm{Gal}(\mathbb{Q}(\mu)|\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times.$$

Como se mencionó en la introducción del capítulo, la diferencia fundamental entre el teorema fundamental de la teoría Galois para extensiones infinitas y finitas, es que en el primero se necesita introducir una noción topológica, mientras que en el segundo esta se puede ignorar. Dicho resultado será estudiado a continuación. Para esto si $G$ es un grupo topológico, se denota por $\mathcal{CS}(G)$ al conjunto de subgrupos cerrados de $G$. Para una extensión $K|\,k$, $\mathcal{E}_{K|\,k}$ denota el conjunto de subcampos de $K$ que son extensiones de $k$.

Teorema 1.18. *(Krull) Sea $K|\,k$ una extensión de Galois.*

1. *Si $L \in \mathcal{E}_{K|\,k}$, entonces $\mathrm{Gal}(K|L)$ es un subgrupo cerrado de $\mathrm{Gal}(K|\,k)$.*

2. *Las funciones*

$$\begin{aligned} \mathrm{Gal}(K|\_\ ) : \mathcal{E}_{K|\,k} &\to \mathcal{CS}(\mathrm{Gal}(K|\,k)) \\ L &\mapsto \mathrm{Gal}(K|L) \end{aligned}$$

$$\begin{aligned} K^{\_} : \mathcal{CS}(\mathrm{Gal}(K|\,k)) &\to \mathcal{E}_{K|\,k} \\ H &\mapsto K^H := \{a \in K \mid \forall \sigma \in H(\sigma(a) = a)\} \end{aligned}$$

   *Son inversas una de la otra y establecen una correspondencia biyectiva que invierte el orden entre* $\mathcal{E}_{K|\,k}$ *y* $\mathcal{CS}(\mathrm{Gal}(K|\,k))$.
3. *Una subextensión* $L|\,k$ *es de Galois si y sólo si* $\mathrm{Gal}(K|L) \trianglelefteq \mathrm{Gal}(K|\,k)$*, y en tal caso se tiene un isomorfismo canónico* $\mathrm{Gal}(L|\,k) \cong \mathrm{Gal}(K|\,k)/\,\mathrm{Gal}(K|L)$.

Demostración. La primera afirmación se va a probar en dos pasos. El primero es suponer que la extensión $L|\,k$ es finita y separable. Así, por el Lema 1.13 existe una extensión de Galois $M|\,k$ finita tal que $L \subseteq M$. Luego, $\mathrm{Gal}(M|\,k)$ es uno de los elementos del sistema inverso con el que se puede construir $\mathrm{Gal}(K|\,k)$ y además este contiene a $\mathrm{Gal}(M|L)$ como subgrupo.

Ahora se considera la proyección canónica $p_M : \mathrm{Gal}(K|\,k) \to \mathrm{Gal}(M|\,k)$ y sea $U := p_M^{-1}(\mathrm{Gal}(M|L))$. Como $p_M$ es continua y $\mathrm{Gal}(M|\,k)$ tiene la topología discreta, $U$ es un subgrupo cerrado de $\mathrm{Gal}(K|\,k)$. Se afirma que $U = \mathrm{Gal}(K|L)$, y nótese que al probar esto se concluye la afirmación para este caso.

En efecto, es claro que $U \subseteq \mathrm{Gal}(K|L)$ pues si $\sigma \in U$, entonces $\sigma|_M = p_M(\sigma) \in \mathrm{Gal}(M|L)$, luego, $\sigma|_L = 1_L$. Respecto a la otra contención nótese que $p_M(\mathrm{Gal}(K|L)) \subseteq \mathrm{Gal}(M|L)$. Al aplicar la imagen inversa a esta contención se tiene que $\mathrm{Gal}(K|L) \subseteq p_M^{-1} p_M(\mathrm{Gal}(K|L)) \subseteq p_M^{-1}(\mathrm{Gal}(M|L)) = U$, lo que muestra la segunda contención y concluye la prueba de la afirmación.

Para el caso de una extensión $L|\,k$ arbitraria, $L$ se puede escribir como unión de subextensiones finitas y separables $L_\alpha|\,k$ para $\alpha \in \Lambda$ con $\Lambda$ un conjunto de índices. Por lo ya demostrado $\mathrm{Gal}(K|L_\alpha)$ es un subgrupo cerrado de $\mathrm{Gal}(K|\,k)$ para cada $\alpha \in \Lambda$. Dado que por construcción $\mathrm{Gal}(K|L) = \bigcap_{\alpha\in\Lambda} \mathrm{Gal}(K|L_\alpha)$, entonces $\mathrm{Gal}(K|L)$ es una intersección de cerrados en $\mathrm{Gal}(K|\,k)$ y por lo tanto es un cerrado.

La prueba de la segunda afirmación se va a omitir pues es completamente análoga a la del teorema para el caso de extensiones finitas.

Continuando con esta afirmación sean $H \in \mathcal{CS}(\mathrm{Gal}(K|\,k))$ y $L := K^H$ la extensión que fija dicho subgrupo. Por construcción se tiene que $H \subseteq \mathrm{Gal}(K|L)$ y se afirma que de hecho se tiene igualdad en esta contención. Para esto sea $\sigma \in \mathrm{Gal}(K|L)$ y $U_M \subseteq \mathrm{Gal}(K|\,k)$ un subgrupo abierto, el cual corresponde a una extensión finita $M|L$, lo cual puede hacerse por el Teorema 1.3. Al aplicar $p_M$ a la contención de $H$ en $\mathrm{Gal}(K|L)$ se tiene que $p_M(H) \subseteq \mathrm{Gal}(M|L)$. Pero si esta contención es propia, entonces por el TFTG para extensiones finitas se tiene que el subgrupo $p_M(H)$ debe fijar una subextensión de $M|L$ estrictamente mayor a $L$, lo que contradice el hecho de que cada elemento de $M \setminus L$ se mueve por un elemento de $H$, así, se tiene que dar la igualdad. En particular un elemento de $H$ debe ir al mismo elemento en $\mathrm{Gal}(M|L)$ que $\sigma$, de donde $H \cap \sigma U_M \neq \emptyset$. Ahora, como la vecindad fue tomada de forma arbitraria esto implica que $\sigma \in \overline{H}$ y dado que $H$ es cerado, $\sigma \in H$, lo que prueba la igualdad que se queria, es decir, $H = \mathrm{Gal}(K|K^H)$.

Sea $L \in \mathcal{E}_{K|\,k}$. Por definición es claro que $L \subseteq K^{\mathrm{Gal}(K|L)}$. Para ver que la otra contención se cumple sea $a \in K^{\mathrm{Gal}(K|L)}$. Considérese $M$ una extensión de Galois finita de $L$ contenida en $K$ tal que $a \in M$. Dado que por la proposición A.1 todo automorfismo de $M$ que fija a $L$ se obtiene como restricción de un automorfismo de $K$ que fija a $L$, entonces se observa que el hecho de que $a \in K^{\mathrm{Gal}(K|L)}$ implica que $a \in M^{\mathrm{Gal}(M|L)}$. Pero como $M|L$ es finita, por el TFTG se tiene que $M^{\mathrm{Gal}(M|L)} = L$, lo que implica que $a \in L$ y demuestra la contención que se quería. Así, $L = K^{\mathrm{Gal}(K|L)}$.

En la ida de la tercera afirmación supóngase que $L|\,k$ es una extensión de Galois y se considera $r_L : \mathrm{Gal}(K|\,k) \to \mathrm{Gal}(L|\,k)$ el morfismo restricción. Se observa que $\sigma \in \mathrm{nuc}(r_L)$ si y sólo si $\sigma|_L = r_L(\sigma) = 1_L$, es decir, $\sigma \in \mathrm{Gal}(K|L)$. Esto muestra que $\mathrm{nuc}(r_L) = \mathrm{Gal}(K|L)$ y como $\mathrm{nuc}(r_L) \trianglelefteq \mathrm{Gal}(K|\,k)$ se tiene el primer resultado. Para la segunda afirmación en esta implicación nótese que como $r_L$ es suprayectiva entonces el primer teorema de isomorfismo implica que $\mathrm{Gal}(K|\,k)/\mathrm{Gal}(K|L) = \mathrm{Gal}(K|\,k)/\mathrm{nuc}(r_L) \cong r_L(\mathrm{Gal}(K|\,k)) = \mathrm{Gal}(L|\,k)$.

En el regreso de la tercera afirmación para aligerar la notación sean $G := \mathrm{Gal}(K|\,k)$ y $H = \mathrm{Gal}(K|L)$. Dado que $G/H$ es un grupo por la normalidad de $H$ en $G$, entonces se tiene una asignación $\cdot : G/H \times L^H \to L^H$ dada por $\sigma H \cdot a := \cdot(\sigma H, a) = \sigma(a)$. Esta asignación es una función pues si $\sigma H = \tau H$ y $a \in L^H$, entonces $\tau^{-1} \circ \sigma \in H$. Así, $\tau^{-1}\sigma(a) = a$, de donde $\tau(a) = \sigma(a)$. Además esta función está bien definida pues si $\sigma H \in G/H$ y $a \in L^H$, entonces para probar que $\sigma(a) \in L^H$ sea $\tau \in H$. Como $H \trianglelefteq G$ se tiene que $\sigma^{-1} \circ \tau \circ \sigma \in H$, de donde, $\sigma^{-1}\tau\sigma(a) = a$, por lo que $\tau\sigma(a) = \sigma(a)$. Como $\tau \in H$ fue arbitrario esto concluye la afirmación.

Por otro lado es claro que la función definida es una acción. Además, $L^G = (L^H)^{G/H} = k$, lo que prueba que $L|\,k$ es de Galois. $\square$

Una observación muy importante es que en el caso infinito no todo subgrupo del grupo de Galois de la extensión corresponde al grupo de Galois de una extensión intermedia.

EJEMPLO 1.19. *Como se vio en el Ejemplo 1.15 para* $k = \mathbb{F}_p$, $p \in \mathbb{N}$ *primo,* $\mathrm{Gal}(k_s \,|\, k) \cong \hat{\mathbb{Z}}$. *Se recuerda que como* $\mathbb{Z}$ *es un subgrupo denso de* $\hat{\mathbb{Z}}$, *entonces* $\mathbb{Z}$ *no puede ser el grupo de Galois de algún elemento en* $\mathcal{E}_{k_s \,|\, k}$.

Vale la pena mencionar que el primer ejemplo de que en el caso de extensiones infinitas no cualquier subgrupo del grupo de Galois de la extensión corresponde a una extesión intermedia fue dado por Dedekind, y este se obtiene al analizar la extensión $\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q}$ del Ejemplo 1.16. Sin embargo, Krull encontró una forma general de construir un subgrupo no cerrado del grupo de Galois de cualquier extensión infinita (ver [**K**]).

Nótese también que cuando la extensión de Galois $K|\,k$ es finita, entonces $\mathrm{Gal}(K|\,k)$ es finito y la topología de este grupo coincide con la discreta. Luego, la versión para extensiones infinitas incluye la versión para extensiones finitas.

## 3. Acciones del grupo de Galois absoluto en conjuntos finitos

LEMA 1.20. *Sean* $G$ *un grupo topológico y* $X$ *un espacio discreto. Entonces, una acción* $G \times X \to X$ *es continua si y sólo si para todo* $x \in X$ *el estabilizador de* $x$, $G_x$, *es abierto en* $G$.

DEMOSTRACIÓN. $\Rightarrow$) Si se denota por $m$ a la acción continua dada y se considera $x \in X$, entonces se observa que la función $\iota_x : G \to G \times X$ cuya regla de correspondencia es $\iota_x(g) = (g, x)$ es continua. Más aún, $g \in (m \circ \iota_x)^{-1}(\{x\})$ si y sólo si $m(g, x) = x$, es decir, $g \in G_x$. Esto prueba que $G_x = (m \circ \iota_x)^{-1}(\{x\})$. Como $X$ tiene la topología discreta $\{x\}$ es abierto y dado que $m \circ \iota_x$ es una función continua por ser composición de dos funciones continuas, se concluye que $G_x$ es abierto.

$\Leftarrow$) Como $X$ tiene la topología discreta para probar la afirmación basta con ver que $m^{-1}(\{x\})$ es abierto en $G \times X$ donde $x \in X$.

Para esto se observa que $m^{-1}(\{x\}) = \{(g, y) \in G \times X \mid g \cdot y = x\} = \bigcup_{y \in X} \{(g, y) \in G \times \{y\} \mid g \cdot y = x\}$. Si $X_y := \{(g, y) \in G \times \{y\} \mid g \cdot y = x\}$, entonces nótese que al suponer que $X_y \neq \emptyset$ se tiene una función $\alpha_y : G_x \to X_y$ definida mediante $\alpha_y(g) = (gh, y)$, donde $h \in X_y$ está fijo.

Se observa que $\alpha_y$ está bien definida pues para $g \in G_x$, $(gh) \cdot y = g \cdot (h \cdot y) = g \cdot x = x$. Además, nótese que $\alpha_y$ es continua pues si $U \subseteq G$ es un abierto, entonces $g \in \alpha_y^{-1}(U \times \{y\})$ si y sólo si $gh \in U$. Pero esta última afirmación es equivalente a decir que $g \in Uh^{-1}$, de donde $\alpha_y^{-1}(U \times \{y\}) = Uh^{-1} \cap G_x$. Como toda traslación por derecha en un grupo topológico es un homeomorfismo y entonces en particular es una función abierta, entonces $Uh^{-1}$ es un abierto en $G$ y así $Uh^{-1} \cap G_x$ es un abierto relativo en $G_x$, lo que muestra la continuidad.

Por otro lado $\alpha_y$ es abierta pues si $U \subseteq G$ es un abierto, entonces $(g, y) \in \alpha_y(U \cap G_x)$ si y sólo si existe $g' \in U \cap G_x$ tal que $g = g'h$. Pero esto último es equivalente a que $g \in (U \cap G_x)h$. Así, $\alpha_y(U \cap G_x) = ((U \cap G_x)h \times \{y\}) \cap X_y$. Como $G_x$ es un abierto por hipótesis entonces $U \cap G_x$ es abierto en $G$ y luego $(U \cap G_x)h$ también es abierto, por lo que $((U \cap G_x)h \times \{y\}) \cap X_y$ es un abierto relativo en $X_y$, lo que prueba que $\alpha_y$ es abierta.

Además, $\alpha_y$ es inyectiva pues si $\alpha_y(g) = \alpha_y(g')$, entonces $gh = g'h$, lo que implica que $g = g'$. Mientras que $\alpha_y$ es suprayectiva pues dado $(g, y) \in X_y$ se observa que $gh^{-1} \in G_x$ pues $(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot y = x$. Además, $\alpha(gh^{-1}) = (gh^{-1}h, y) = (g, y)$.

El argumento anterior prueba que $\alpha_y$ es un homeomorfismo entre $G_x$ y $X_y$ en el caso en que $X_y \neq \emptyset$. Así, $m^{-1}(\{x\})$ es una unión de abiertos en $G \times X$ y por lo tanto es un abierto. $\square$

NOTACIÓN 1.21. *Para $k$ un campo,* $\mathrm{Gal}(k)$ *denota el grupo de Galois absoluto* $\mathrm{Gal}(k_s \,|\, k)$.

Sea $L|\,k$ una extensión finita separable. Luego, $L$ tiene una cantidad finita de morfismos de $k$-álgebras con codominio la clausura algebraica de $k$, $\overline{k}$. Sin embargo, nótese que las imágenes de estos morfismos están contenidos en $k_s$. Así, el conjunto $\mathrm{Hom}_k(L, k_s)$ es finito. Más aún, se define una función $\cdot : \mathrm{Gal}(k) \times \mathrm{Hom}_k(L, k_s) \to \mathrm{Hom}_k(L, k_s)$ mediante $\sigma \cdot \varphi := \cdot(\sigma, \varphi) = \sigma \circ \varphi$. Es sencillo ver que esta función es una acción de grupos y que de hecho esta tiene sentido incluso si la extensión no es finita. Más aún se tiene lo siguiente:

PROPOSICIÓN 1.22. *Sea $L|\,k$ una extensión separable finita. Entonces,*

1. *La acción de* $\mathrm{Gal}(k)$ *en* $\mathrm{Hom}_k(L, k_s)$ *es continua y transitiva.*
2. $\mathrm{Hom}_k(L, k_s)$ *es isomorfo como* $\mathrm{Gal}(k)$*-conjunto con el conjunto de clases laterales izquierdas de algún subgrupo abierto de* $\mathrm{Gal}(k)$.

3. *Si $L|\, k$ es de Galois, entonces el conjunto de clases laterales del inciso anterior es cociente por un subgrupo abierto normal.*

Demostración. Para 1 se observa primero que dado $\phi \in \mathrm{Hom}_k(L, k_s)$ se tiene que $\mathrm{Gal}(k)_\phi = \mathrm{Gal}(k_s\,|\phi(L))$, que es un subgrupo abierto de $\mathrm{Gal}(k)$ pues si $\{x_1, ..., x_n\}$ es una base como $k$-espacio vectorial de $\phi(L)$ y $L_i$ es el subcampo de $\phi(L)$ generado por $x_i$, entonces se observa que la extensión $L_i|\, k$ es finita. Así, se pueden considerar los morfismos canónicos $p_{L_i} : \mathrm{Gal}(k) \to \mathrm{Gal}(L_i|\, k)$. Se afirma que $\mathrm{Gal}(k_s\,|\phi(L)) = \bigcap_{i=1}^n p_{L_i}^{-1}(\{1_{L_i}\})$, y nótese que al probar esta igualdad se tiene la conclusión que se quiere pues al tener $\mathrm{Gal}(L_i|\, k)$ la topología discreta y ser $p_{L_i}$ continua, $p_{L_i}^{-1}(\{1_{L_i}\})$ es un abierto de $\mathrm{Gal}(k)$. Por lo tanto la igualdad dice que $\mathrm{Gal}(k_s\,|\phi(L))$ es una intersección finita de abiertos en $\mathrm{Gal}(k)$ y así dicho conjunto es un abierto en $\mathrm{Gal}(k)$.

En efecto, si $\sigma \in \mathrm{Gal}(k_s\,|\phi(L))$, entonces dado $i \in \{1, ..., n\}$, se tiene que $p_{L_i}(\sigma) = \sigma|_{L_i} = 1_{L_i}$ pues $L_i$ es subcampo de $\phi(L)$. Así, esto prueba que $\sigma \in p_{L_i}^{-1}(\{1_{L_i}\})$, y como esto no depende de $i$, se concluye que $\sigma \in \bigcap_{i=1}^n p_{L_i}^{-1}(\{1_{L_i}\})$. El argumento anterior prueba que $\mathrm{Gal}(k_s\,|\phi(L)) \subseteq \bigcap_{i=1}^n p_{L_i}^{-1}(\{1_{L_i}\})$, y respecto a la otra contención dado $\sigma \in \bigcap_{i=1}^n p_{L_i}^{-1}(\{1_{L_i}\})$, se tiene que como para todo $i \in \{1, ..., n\}$, $\sigma|_{L_i} = 1_{L_i}$, entonces al ser $\{x_1, ..., x_n\}$ base de $\phi(L)$ esto implica que $\sigma|_{\phi(L)} = 1_{\phi(L)}$. Esto prueba la contención que se queria y así la igualdad mencionada.

Dado que se ha probado que $\mathrm{Gal}(k)_\phi$ es abierto en $\mathrm{Gal}(k)$ para $\phi \in \mathrm{Hom}_k(L, k_s)$, y como este resultado no depende del elemento $\phi$, se concluye que la acción definida es continua por el lema anterior.

Por otro lado como la extensión $L|\, k$ es finita y separable, el teorema del elemento primitivo implica que existe $a \in L$ tal que $L = k(a)$. Sea $f$ el polinomio mínimo de $a$ con coeficientes en $k$. Así, cada elemento de $\mathrm{Hom}_k(L, k_s)$ se construye al mandar a $a$ en una raíz de $f$ en $k_s$. Como $\mathrm{Gal}(k)$ permuta tales raíces de manera transitiva, entonces se sigue la transitividad de la acción y con esto se concluye la prueba de 1.

Respecto a la segunda afirmación sea $\phi \in \mathrm{Hom}_k(L, k_s)$. Para definir una función $\alpha : \mathrm{Hom}_k(L, k_s) \to \mathrm{Gal}(k)/\,\mathrm{Gal}(k)_\phi$ se usa el hecho de que la acción de $\mathrm{Gal}(k)$ en $\mathrm{Hom}_k(L, k_s)$ es transitiva y así se define $\alpha(\sigma \circ \phi) = \sigma\,\mathrm{Gal}(k)_\phi$. Dado que $\mathrm{Gal}(k)_\phi$ es abierto en $\mathrm{Gal}(k)$, se afirma que $\alpha$ establece la correspondencia biyectiva que se desea.

En efecto, es claro que esta función es suprayectiva. Para la inyectividad supóngase que $\alpha(\sigma\circ\phi) = \alpha(\tau\circ\phi)$ con $\sigma, \tau \in \mathrm{Gal}(k)$. De la definición de $\alpha$ la igualdad anterior implica que $\sigma\,\mathrm{Gal}(k)_\phi = \tau\,\mathrm{Gal}(k)_\phi$, lo que ocurre si y sólo si $\tau^{-1} \circ \sigma \in \mathrm{Gal}(k)_\phi$, es decir, $(\tau^{-1} \circ \sigma) \cdot \phi = \phi$. De esto se sigue que $\sigma \circ \phi = \tau \circ \phi$, de donde $\alpha$ es una función inyectiva, por lo tanto una biyección y se concluye la prueba de 2.

Para concluir, si la extensión $L|\, k$ es de Galois, por el Teorema 1.18 se tiene que $\operatorname{Gal}(k_s\,|L) \trianglelefteq \operatorname{Gal}(k)$. Así, como $\operatorname{Gal}(k_s\,|L) \cong \operatorname{Gal}(k_s\,|\phi(L)) = \operatorname{Gal}(k)_\phi$, se tiene que $\operatorname{Gal}(k)_\phi \trianglelefteq \operatorname{Gal}(k)$ y entonces $\operatorname{Gal}(k)/\operatorname{Gal}(k)_\phi$ es un grupo y este es de hecho el conjunto de clases laterales del subgrupo abierto $\operatorname{Gal}(k)_\phi$ de $\operatorname{Gal}(k)$. $\square$

Sea $\mathbf{FSep}(k)$ la categoría de extensiones finitas separables de $k$ y $\operatorname{Gal}(k)-\mathbf{FSet_t}$ la categoría de $\operatorname{Gal}(k)$-conjuntos finitos con la topología discreta cuya acción es continua y transitiva. El inciso 1 en la proposición anterior dice que para $L \in \mathbf{FSep}(k)$, $\operatorname{Hom}_k(L, k_s) \in \operatorname{Gal}(k) - \mathbf{FSet_t}$.

Además, si $\phi \in \mathbf{FSep}(k)(L, M)$, entonces se puede definir la función

$$\phi^* : \operatorname{Hom}_k(M, k_s) \to \operatorname{Hom}_k(L, k_s)$$

mediante $\phi^*(\psi) = \psi \circ \phi$. Esta respeta la acción de $\operatorname{Gal}(k)$ pues si $\sigma \in \operatorname{Gal}(k)$ y $\psi \in \operatorname{Hom}_k(M, k_s)$, entonces se tiene que $\phi^*(\sigma \cdot \psi) = (\sigma \cdot \psi) \circ \phi = \sigma \circ (\psi \circ \phi) = \sigma \cdot \phi^*(\psi)$, lo que muestra que $\phi^* \in \operatorname{Gal}(k) - \mathbf{FSet_t}(\operatorname{Hom}_k(M, k_s), \operatorname{Hom}_k(L, k_s))$.

La discusión anterior aunado a un sencillo cálculo que se va a omitir pues es estándar, dice que se tiene un funtor:

$$\operatorname{Hom}_k(\_, k_s) : \mathbf{FSep}(k)^{op} \longrightarrow \operatorname{Gal}(k) - \mathbf{FSet_t}$$

El funtor definido establece el siguiente importante resultado.

TEOREMA 1.23. *Sea $k$ un campo y fíjese una clausura separable de $k$, $k_s$. El funtor*

$$\operatorname{Hom}_k(\_, k_s) : \boldsymbol{FSep}(k)^{op} \longrightarrow \operatorname{Gal}(k) - \boldsymbol{FSet_t}$$

*establece una antiequivalencia entre las categorías de extensiones de $k$ finitas separables y de $\operatorname{Gal}(k)$-conjuntos finitos cuya acción es continua y transitiva. En esta equivalencia las extensiones de Galois finitas de $k$ dan lugar a $\operatorname{Gal}(k)$-conjuntos isomorfos a algún cociente finito de $\operatorname{Gal}(k)$.*

Demostración. Para la afirmación de la equivalencia se va a probar que el funtor $\mathrm{Hom}_k(\_, k_s) : \mathbf{FSep}(k)^{op} \to \mathrm{Gal}(k) - \mathbf{Set_t}$ es fiel, pleno y esencialmente suprayectivo.

Respecto a la propiedad de ser fiel y pleno sean $L, M \in \mathbf{FSep}(k)$. Se quiere ver que hay una biyección entre $\mathbf{FSep}(k)(L, M)$ y $\mathrm{Gal}(k) - \mathbf{FSet_t}(\mathrm{Hom}_k(M, k_s), \mathrm{Hom}_k(L, k_s))$ inducida por $\mathrm{Hom}_k(\_, k_s)$. Para esto se observa que por ser $\mathrm{Hom}_k(M, k_s)$ un $\mathrm{Gal}(k)$-conjunto transitivo, un morfismo $f : \mathrm{Hom}_k(M, k_s) \to \mathrm{Hom}_k(L, k_s)$ está determinado por la imagen de $\phi \in \mathrm{Hom}_k(M, k_s)$. Así, se observa que dado $\phi \in \mathrm{Hom}_k(M, k_s)$ se tiene que $\mathrm{Gal}(k)_\phi \subseteq \mathrm{Gal}(k)_{f(\phi)}$ para todo morfismo $\mathrm{Gal}(k)$-equivariante $f : \mathrm{Hom}_k(M, k_s) \to \mathrm{Hom}_k(L, k_s)$. Luego, por el TFTG de Krull, $f(\phi)(L) = k_s^{\mathrm{Gal}(k)_{f(\phi)}} \subseteq k_s^{\mathrm{Gal}(k)_\phi} = \phi(M)$. Si $\psi : \phi(M) \to M$ es la inversa de la correstricción de $\phi$, entonces $\psi \circ f(\phi) \in \mathrm{Hom}_k(L, M)$ pues de la contención anterior $\psi f(\phi)(L) \subseteq \psi\phi(M) = M$.

Además se observa que $(\psi \circ f(\phi))^* = f$ y por la transitividad de la acción basta ver que esta igualdad se da al evaluar en $\phi$. En efecto, pues $(\psi \circ f(\phi))^*(\phi) = \phi \circ (\psi \circ f(\phi)) = f(\phi)$, lo que prueba la suprayectividad de $\mathrm{Hom}_k(\_, k_s)$.

Para la inyectividad se observa que si $\eta \in \mathbf{FSep}(k)(L, M)$ es tal que $\eta^* = f$, entonces $\phi \circ \eta = \eta^*(\phi) = f(\phi)$. Así, $\eta = \psi \circ f(\phi)$, lo que concluye la prueba de esta afirmación.

Respecto a la suprayectividad esencial de $\mathrm{Hom}_k(\_, k_s)$ sea $S$ un $\mathrm{Gal}(k)$-conjunto finito cuya acción es transitiva y continua. Al tomar $s \in S$, el Lema 1.20 implica que el estabilizador $\mathrm{Gal}(k)_s$ es un subgrupo abierto de $\mathrm{Gal}(k)$. Así, por el Corolario 1.4 $\mathrm{Gal}(k)_s$ es cerrado y de índice finito por lo que el TFTG de Krull implica que este fija una extensión finita y separable $L$ de $k$. Si $\iota : L \to k_s$ es el morfismo inclusión, se define la función $\alpha : \mathrm{Hom}_k(L, k_s) \to S$ mediante $\alpha(\sigma \circ \iota) = \sigma \cdot s$, donde $\sigma \in \mathrm{Gal}(k)$ y nótese que esta definición se está usando que la acción de $\mathrm{Gal}(k)$ en $\mathrm{Hom}_k(L, k_s)$ es transitiva.

Se afirma que $\alpha$ es un isomorfismo. Para probar esto lo primero que se observa es que como los conjuntos involucrados tienen la topología discreta, la afirmación es equivalente a probar que $\alpha$ es una biyección $\mathrm{Gal}(k)$-equivariante. En efecto, si $\sigma, \tau \in \mathrm{Gal}(k)$, entonces $\alpha(\tau \circ (\sigma \circ \iota)) = \alpha((\tau \circ \sigma) \circ \iota) = (\tau \circ \sigma) \cdot s = \tau \cdot (\sigma \cdot s) = \tau \cdot \alpha(\sigma \circ \iota)$, lo que establece la propiedad de equivariancia.

Para la inyectividad nótese que por construcción $\mathrm{Gal}(k)_s = \mathrm{Gal}(k)_\iota$. Así, si $\alpha(\sigma \circ \iota) = \alpha(\tau \circ \iota)$ para $\sigma, \tau \in \mathrm{Gal}(k)$, entonces $\sigma \cdot s = \tau \cdot s$, de donde, $\tau^{-1} \circ \sigma \in \mathrm{Gal}(k)_s$ y así, $\tau^{-1} \circ \sigma \in \mathrm{Gal}(k)_\iota$, lo que implica que $\sigma \circ \iota = \tau \circ \iota$. Respecto a la suprayectividad dado $t \in S$ se tiene por transitividad de la acción que existe $\sigma \in \mathrm{Gal}(k)$ tal que $\sigma \cdot s = t$. Así, $\alpha(\sigma \circ \iota) = t$.

Para concluir se observa que si la extensión $L|\, k$ es de Galois, entonces para $\phi \in \mathrm{Hom}_k(L, k_s)$ se tiene que $\mathrm{Hom}_k(L, k_s) \cong \mathrm{Gal}(k)/\mathrm{Gal}(k)_\phi$ (Proposición 1.22). Además como se vio en la prueba de dicha proposición $\mathrm{Gal}(k)_\phi$ es abierto en $\mathrm{Gal}(k)$, así este subgrupo tiene índice finito en $\mathrm{Gal}(k)$ y por lo tanto $|\mathrm{Gal}(k)/\mathrm{Gal}(k)_\phi| < \aleph_0$. □

El último resultado de esta sección dice que el funtor contravariante representado por $k_s$, permite recuperar el grupo de Galois absoluto del campo en cuestión.

PROPOSICIÓN 1.24. *Para $k$ campo considérese el funtor* $\mathrm{Hom}_k(\_, k_s) : \boldsymbol{Sep}(k)^{op} \to \mathrm{Gal}(k) - \boldsymbol{Set}$. *Entonces,* $\mathrm{Gal}(k) \cong \mathrm{Aut}(\mathrm{Hom}_k(\_, k_s))$ *como grupos.*

DEMOSTRACIÓN. Se define $\alpha : \mathrm{Gal}(k) \to \mathrm{Aut}(\mathrm{Hom}_k(\_, k_s))$ donde para $\sigma \in \mathrm{Gal}(k)$ y $L|\, k$ es una extensión separable, $\alpha_k(\sigma)_L : \mathrm{Hom}_k(L, k_s) \to \mathrm{Hom}_k(L, k_s)$ tiene por regla de correspondencia $\alpha_k(\sigma)_L(f) = \sigma \circ f$. Lo primero que se observa es que dado que $f$ y $\sigma$ son $k$-morfismos, entonces su composición lo es, por lo que $\alpha(\sigma)_L$ está bien definida.

Por otro lado $\alpha$ también está bien definida pues para $\sigma \in \mathrm{Gal}(k)$, se tiene que $\alpha(\sigma) \circ \alpha(\sigma^{-1}) = \alpha(\sigma^{-1}) \circ \alpha(\sigma) = 1_{\mathrm{Hom}(\_, k_s)}$. Además, es un cálculo de rutina ver que $\alpha$ respeta composiciones. Así, $\alpha$ es un morfismo de grupos.

Para ver que $\alpha$ es un isomorfismo, dada la caracterización de los isomorfismos en la categoría de grupos, resta ver que $\alpha$ es una función biyectiva. Así, lo primero que se va a probar es que esta función es inyectiva. Pero esto es equivalente a probar que el núcleo de este morfismo es el neutro. En efecto, si $\sigma \in \mathrm{Gal}(k)$ es tal que $\alpha(\sigma) = 1_{\mathrm{Hom}_k(\_, k_s)}$, entonces dado $a \in k_s$, se considera la extensión separable $k(a)|\, k$. Sea $\iota \in \mathrm{Hom}_k(k(a), k_s)$ el $k$-morfismo inclusión. Entonces $\alpha(\sigma)_{k(a)}(\iota)(a) = \iota(a)$, de lo que se deduce que $\sigma(a) = a$. Como el elemento $a \in k_s$ tomado fue arbitrario, se concluye que $\sigma = 1_{k_s}$, y esto prueba la contención no trivial de la igualdad $\mathrm{nuc}(\alpha) = \{1_{k_s}\}$. Por lo tanto $\alpha$ es inyectiva.

Respecto a la suprayectividad sea $\eta \in \mathrm{Aut}(\mathrm{Hom}_k(\_, k_s))$. Nótese que dada $L|\, k$ una extensión separable y $f \in \mathrm{Hom}_k(L, k_s)$, se tiene por naturalidad de $\eta$ la conmutatividad del siguiente diagrama:

$$\begin{tikzcd}
\mathrm{Hom}_k(k_s, k_s) \arrow[r, "h_{k_s}(f)"] \arrow[d, "\eta_{k_s}"'] & \mathrm{Hom}_k(L, k_s) \arrow[d, "\eta_L"] \\
\mathrm{Hom}_k(k_s, k_s) \arrow[r, "h_{k_s}(f)"'] & \mathrm{Hom}_k(L, k_s)
\end{tikzcd}$$

Entonces se considera $L = k_s$ y $f = \eta_{k_s}^{-1}(1_{k_s}) \in \mathrm{Hom}_k(k_s, k_s)$. La conmutatividad del diagrama dice que $\eta_{k_s} \circ h_{k_s}(\eta_{k_s}^{-1}(1_{k_s}))(1_{k_s}) = h_{k_s}(\eta_{k_s}^{-1}(1_{k_s})) \circ \eta_{k_s}(1_{k_s})$, lo que implica que $\eta_{k_s}(1_{k_s}) \circ \eta_{k_s}^{-1}(1_{k_s}) = \eta_{k_s}(\eta_{k_s}^{-1}(1_{k_s})) = 1_{k_s}$. Este argumento prueba que $\eta_{k_s}(1_{k_s})$ es un epimorfismo que escinde, y un argumento análogo usando la naturalidad de $\eta^{-1}$ muestra que este morfismo es también un monomorfismo que escinde. Por lo tanto se concluye que $\eta_{k_s}(1_{k_s})$ es un isomorfismo, es decir, que $\eta_{k_s}(1_{k_s}) \in \mathrm{Gal}(k)$

Así, se afirma que $\alpha(\eta_{k_s}(1_{k_s})) = \eta$. En efecto, dada $L|\,k$ una extensión separable y $f \in \mathrm{Hom}_k(L, k_s)$, la conmutatividad del diagrama anterior implica que al evaluar en $1_{k_s}$, $\eta_L(f) = \eta_{k_s}(1_{k_s}) \circ f$. Luego, como $\alpha(\eta_{k_s}(1_{k_s}))_L(f) = \eta_{k_s}(1_{k_s}) \circ f$, se tiene que $\alpha(\eta_{k_s}(1_{k_s}))_L(f) = \eta_L(f)$, lo que prueba la afirmación. $\square$

## 4. La versión de Grothendieck

La idea de esta sección es liberar el Teorema 1.23 para el caso en que la acción del grupo de Galois absoluto en un conjunto finito no sean transitivas necesariamente. El resultado correspondiente es lo que se conoce como la versión de Grothendieck del TFTG y para este es necesario definir el concepto algebraico que suplirá a las extensiones finitas separables, para establecer la equivalencia que se quiere.

DEFINICIÓN 1.25. *Una $k$-álgebra $A$ de dimensión finita es* ***étale*** *(sobre $k$) si es isomorfa a un producto finito de extensiones separables de $k$.*

Vale la pena mencionar que el nombre de álgebra étale proviene del hecho de que una $k$-álgebra conmutativa de dimensión finita $A$ es étale si y sólo si el morfismo de esquemas $\mathrm{Spec}(A) \to \mathrm{Spec}(k)$ es étale (ver Ejemplo 3.23 del Capítulo 3).

Es claro que toda extensión finita y separable de $k$ es una $k$-álgebra étale. Sin embargo, como sucede con el concepto de grupo profinito, en la mayoria de los casos es difícil de la definición saber si una $k$-álgebra finitamente dimensional dada es étale.

Para esto se busca un teorema de caracterización de este tipo de álgebras, al menos para el caso conmutativo. En esta dirección se requiere de un resultado previo.

LEMA 1.26. *Sea $A$ una $k$-álgebra de dimensión finita. Entonces, $A$ es isomorfa a un producto de extensiones de campo de $k$ finitas si y sólo si $A$ es reducida.*

DEMOSTRACIÓN. $\Rightarrow$) Es claro.

$\Leftarrow$) Supóngase que $A$ es reducida. Por el teorema de Krull-Remak-Schmidt, $A \cong \prod_{i=1}^{n} A_i$ donde cada $A_i$ es una $k$-álgebra inescindible. Esta descomposición implica que cada $A_i$ tiene dimensión finita sobre $k$ y es reducida. Así, el resultado se sigue si se prueba que toda $k$-álgebra inescindible de dimensión finita reducida es un campo.

En efecto, sea $B$ una de tales $k$-álgebras. Así, los únicos idempotentes de $B$ son 0 y 1 pues en otro caso $B \cong Be \times B(1-e)$ para $e \in B$ un idempotente distinto de cero y uno, lo que contradice el hecho de que $B$ es inescindible pues $Be \neq 0$ y $B(1-e) \neq 0$.

Para ver que $B$ es un campo sea $x \in B$ con $x \neq 0$. Entonces se considera la cadena descendente de ideales $(x) \supseteq (x^2) \supseteq ....$ Como $B$ es un $k$-espacio vectorial de dimensión finita entonces $B$ tiene longitud finita, por lo que existe $N \in \mathbb{N}^+$ tal que $(x^N) = (x^{N+1})$. Así, existe $y \in B$ tal que $x^N = x^{N+1}y$. Pero esta igualdad implica que $x^N = x^{2N}y^N$ y entonces $x^N y^N = x^{2N}y^{2N} = (x^N y^N)^2$, es decir, que $x^N y^N$ es idempotente en $B$. Luego, por lo demostrado antes se tiene que $x^N y^N = 0$ ó $x^N y^N = 1$. Sin embargo, si $x^N y^N = 0$, entonces se tiene que $x^N = x^{2N} y^N = 0$. Dado que $x \neq 0$, entonces $x$ es un nilpotente no trivial, lo que contradice el hecho de que $B$ es reducida. Así, $x^N y^N = 1$, y como $N \geq 1$, $x(x^{N-1}y^N) = 1$, es decir, $x \in B^\times$. Además, como el elemento no cero tomado fue arbitrario se concluye que todo elemento no cero de $B$ es una unidad, es decir, que $B$ es un campo. $\square$

Un resultado que vale la pena mencionar se muestra a continuación.

COROLARIO 1.27. *Sea $A$ una $k$-álgebra de dimensión finita conmutativa con $k$ perfecto. Entonces, $A$ es étale si y sólo si $A$ es reducida.*

DEMOSTRACIÓN. $\Rightarrow$) Es claro de la ida en el lema anterior.

$\Leftarrow$) Si $A$ es reducida entonces por el lema anterior $A \cong \prod_{\alpha \in \Lambda} L_\alpha$ con $L_\alpha | \, k$ finitas. Por ser $A$ de dimensión finita, $|\Lambda| < \aleph_0$. Además, cada extensión $L_\alpha$ es algebraica y por ser $k$ perfecto la extensión $L_\alpha | \, k$ es separable, lo que concluye la prueba. $\square$

PROPOSICIÓN 1.28. *Sea $A$ una $k$-álgebra finitamente generada conmutativa. Son equivalentes:*

1. *$A$ es étale.*
2. *$A \otimes_k \overline{k}$ es isomorfa a un producto finito de $\overline{k}$.*
3. *$A \otimes_k \overline{k}$ es reducida.*

DEMOSTRACIÓN. Es claro que $2 \Rightarrow 3$. Además, como $A \otimes_k \overline{k}$ es una $\overline{k}$-álgebra tal que $\dim_{\overline{k}}(A \otimes_k \overline{k}) = \dim_k(A)$ y $\overline{k}$ es algebraicamente cerrado, al suponer 3 el lema 1.26 implica que $A \otimes_k \overline{k} \cong \prod_{i=1}^n L_i$ para $L_i|\overline{k}$ finita. Así, la extensión $L_i|\overline{k}$ es algebraica y por definición de la clausura algebraica $L_i = \overline{k}$, lo que muestra que $3 \Rightarrow 2$.

$1 \Rightarrow 2$) Para esta implicación basta con ver que para toda extensión separable $L|\, k$ se tiene que $L \otimes_k \overline{k}$ es isomorfa a un producto finito de $\overline{k}$.

En efecto, si $L|\, k$ es una de tales extensiones, entonces existe $f \in k[x]$ tal que $L \cong k[x]/(f)$, y $f$ se descompone en factores lineales distintos con coeficientes en $k$, digamos $f = (x - a_1) \cdot ... \cdot (x - a_n)$ con $a_1, ..., a_n \in k$. Así,

$$L \otimes_k \overline{k} \cong \overline{k}[x]/(f) \cong \prod_{i=1}^{n} \overline{k}[x]/(x - a_i) \cong \prod_{i=1}^{n} \overline{k},$$

donde el segundo isomorfismo se da por el teorema chino del residuo.

Esto concluye la prueba en esta dirección.

$2 \Rightarrow 1$) Sea $A_r = A/N(A)$ la $k$-álgebra reducida asociada a $A$, donde $N(A)$ es el nilradical de $A$. Al tener $A_r$ dimensión finita el Lema 1.26 implica que $A_r$ es producto de extensiones de campo de $k$ finitas. Como $\overline{k}$ es una $k$-álgebra reducida, la propiedad universal de $A_r$ implica que cada morfismo $A \to \overline{k}$ se factoriza a través de un único morfismo de $k$-álgebras $A_r \to \overline{k}$. Además, la asignación que a cada $k$-morfismo $A \to \overline{k}$ le asocia su morfismo $A_r \to \overline{k}$ es lineal, por lo que se tiene un un isomorfismo de $k$-espacios $\mathrm{Hom}_k(A, \overline{k}) \cong \mathrm{Hom}_k(A_r, \overline{k})$. Dado que $\dim_k(A) < \aleph_0$ y $\dim_k(A_r) < \aleph_0$, entonces se tienen isomorfismos de $k$-espacios vectoriales $\mathrm{Hom}_k(A, \overline{k}) \cong \overline{k}^{\dim_k(A)}$ y $\mathrm{Hom}_k(A_r, \overline{k}) \cong \overline{k}^{\dim_k(A_r)}$. Esto implica que $\dim_k(A) = \dim_k(A_r)$ y así, $A \cong A_r$.

Para concluir, lo que se tiene que probar es que si $A_r \cong \prod_{i=1}^n L_i$, entonces la extensión $L_i|\, k$ es separable. En efecto, cada morfismo en $\mathrm{Hom}_k(A, \overline{k})$ da lugar a un único encaje de alguno de los $L_i$ en $\overline{k}$. Así,

$$|\,\mathrm{Hom}_k(A, \overline{k})| \leq \sum_{i=1}^{n} |\,\mathrm{Hom}_k(L_i, \overline{k})| \leq \sum_{i=1}^{n} [L_i : k] = \dim_k(A),$$

donde la segunda desigualdad se da por la Proposición A.2.

Para ver que la desigualdad anterior es de hecho igualdad, nótese que se tiene una biyección entre los conjuntos $\mathrm{Hom}_k(A,\overline{k})$ y $\mathrm{Hom}_{\overline{k}}(A\otimes_k \overline{k},\overline{k})$ pues dado $f\in \mathrm{Hom}_k(A,\overline{k})$ se tiene que $f\otimes 1_{\overline{k}}\in \mathrm{Hom}_{\overline{k}}(A\otimes_k \overline{k},\overline{k}\otimes_k \overline{k})$. Si $\mu:\overline{k}\otimes_k \overline{k}\to \overline{k}$ es el morfismo inducido por la multiplicación en $\overline{k}$, entonces $\mu\circ(f\otimes 1_{\overline{k}})\in \mathrm{Hom}_{\overline{k}}(A\otimes_k\overline{k},\overline{k})$. Así, se define $\alpha:\mathrm{Hom}_k(A,\overline{k})\to \mathrm{Hom}_{\overline{k}}(A\otimes_k \overline{k},\overline{k})$ mediante $\alpha(f)=\mu\circ(f\otimes 1_{\overline{k}})$. Para definir la función inversa de $\alpha$, $\beta:\mathrm{Hom}_{\overline{k}}(A\otimes_k \overline{k},\overline{k})\to \mathrm{Hom}_k(A,\overline{k})$, se observa que dado $g\in \mathrm{Hom}_{\overline{k}}(A\otimes_k \overline{k},\overline{k})$, se tiene que como la inclusión $\iota:k\to\overline{k}$ induce $1_A\otimes\iota\in \mathrm{Hom}_{\overline{k}}(A\otimes_k k, A\otimes_k \overline{k})$, entonces $g\circ(1_A\otimes\iota)\in \mathrm{Hom}_k(A\otimes_k k,\overline{k})$, y este se compone con el isomorfismo $A\cong A\otimes_k k$. Por construcción es claro que $\alpha$ y $\beta$ son inversas entre sí.

El argumento anterior aunado al hecho de que $\mathrm{Hom}_{\overline{k}}(A\otimes_k \overline{k},\overline{k})$ tiene $\dim_{\overline{k}}(A\otimes_k \overline{k})$ elementos, y esta dimensión es igual a $\dim_k(A)$, implican que $|\mathrm{Hom}_k(A,\overline{k})| = \dim_k(A)$. Como para cada $i\in\{1,...,n\}$ se tiene que $|\mathrm{Hom}_k(L_i,\overline{k})|\leq [L_i:k]$, entonces para cada $i$ se tiene que $|\mathrm{Hom}_k(L_i,\overline{k})|\leq [L_i:k]$. Pero por la Proposición A.2 esto implica que $L_i|\,k$ es separable. $\square$

Con la proposición anterior se tiene un criterio más sencillo para saber si una $k$-álgebra de dimensión finita es étale como se ve a continuación.

Ejemplo 1.29. *La $\mathbb{R}$-álgebra conmutativa $\mathbb{R}[x]/(x^2)$ no es étale pues $\mathbb{R}[x]/(x^2)\otimes_{\mathbb{R}} \overline{\mathbb{R}}\cong \overline{\mathbb{R}}[x]/(x^2)\cong \mathbb{C}[x]/(x^2)$. Así, $\overline{x}\in\mathbb{C}[x]/(x^2)$ es un nilpotente no trivial, por lo que $\mathbb{R}[x]/(x^2)\otimes_{\mathbb{R}}\overline{\mathbb{R}}$ no es reducida.*

Regresando al problema inicial sea $A$ una $k$-álgebra finita étale y supóngase que $A=\prod_{i=1}^n L_i$ con $L_i|\,k$ finitas y separables. Dado que se tiene el isomorfismo de $k$-espacios vectoriales entre $\mathrm{Hom}_k(A,k_s)$ y $\prod_{i=1}^n \mathrm{Hom}_k(L_i,k_s)$, entonces $|\mathrm{Hom}_k(A,k_s)| = \prod_{i=1}^n |\mathrm{Hom}_k(L_i,k_s)|$. Pero por la Proposición A.2 para cada $i\in\{1,...,n\}$, $|\mathrm{Hom}_k(L_i,k_s)|\leq [L_i:k]$, de lo que se deduce que $|\mathrm{Hom}_k(A,k_s)|\leq \prod_{i=1}^n [L_i:k] < \aleph_0$.

Al identificar $\mathrm{Hom}_k(A,k_s)$ con $\prod_{i=1}^n \mathrm{Hom}_k(L_i,k_s)$ y dado que $\mathrm{Hom}_k(L_i,k_s)$ es un $\mathrm{Gal}(k)$-conjunto con acción continua al considerarlo como espacio discreto, entonces $\mathrm{Hom}_k(A,k_s)$ es un $\mathrm{Gal}(k)$-conjunto. De hecho se tiene el siguiente resultado:

Proposición 1.30. *Sea $A$ una $k$-álgebra étale. Entonces $\mathrm{Hom}_k(A,k_s)$ es un $\mathrm{Gal}(k)$-conjunto finito cuya acción es continua.*

Demostración. Con la notación de la discusión previa lo único que falta probar es la continuidad de la acción. Para esto sea $\phi = (\phi_i)_{i\in\{1,\ldots,n\}} \in \prod_{i=1}^{n} \mathrm{Hom}_k(L_i, k_s)$. Nótese que $\mathrm{Gal}(k)_\phi = \bigcap_{i=1}^{n} \mathrm{Gal}(k)_{\phi_i}$. Así, dado que cada $\mathrm{Hom}_k(L_i, k_s)$ tiene la topología discreta y la acción de $\mathrm{Gal}(k)$ es continua, entonces $\mathrm{Gal}(k)_{\phi_i} \subseteq \mathrm{Gal}(k)$ es un subgrupo abierto. Luego, $\mathrm{Gal}(k)_\phi$ es una intersección finita de subgrupos abiertos, por lo que es un subgrupo abierto. Además, dado que el elemento $\phi$ tomado fue arbitrario se concluye que todos los estabilizadores son abiertos. Más aún, como $\mathrm{Hom}_k(A, k_s)$ tiene la topología discreta, el Lema 1.20 permite concluir que la acción es continua. □

En este momento se disponen de todas las herramientas para probar la versión de Grothendieck del Teorema Fundamental de la Teoría de Galois. Lo único que falta mencionar es que la **categoría de $k$-álgebras étale** es la subcategoría plena de la categoría de $k$-álgebras finitamente generadas. Esta categoría se va a denotar por $\mathbf{\acute{E}tAlg}(k)$.

Teorema 1.31. *(Grothendieck) Sea $k$ un campo. El funtor que a cada $k$-álgebra finitamente generada étale le asocia* $\mathrm{Hom}_k(A, k_s)$ *establece una antiequivalencia entre las categorías de $k$-álgebras de dimensión finita étales y de* $\mathrm{Gal}(k)$*-conjuntos cuya acción es continua.*

Demostración. Siguiendo la estrategia del Teorema 1.23 se va a probar que el funtor

$$\mathrm{Hom}_k(\_, k_s) : \mathbf{\acute{E}tAlg}(k)^{op} \to \mathrm{Gal}(k) - \mathbf{FSet}$$

es fiel, pleno y esencialmente suprayectivo.

Para ver que es fiel y pleno sean $A$ y $B$ dos $k$-álgebras étale finitas con digamos $A = \prod_{i=1}^{n} L_i$ y $B = \prod_{j=1}^{m} M_j$. Dado que se tiene la correspondencia biyectiva:

$$\mathrm{Hom}_k(A, B) \cong \prod_{i=1}^{n}\prod_{j=1}^{m} \mathrm{Hom}_k(L_i, M_j)$$

y por el Teorema 1.23 para cualesquiera $i \in \{1, ..., n\}$ y $j \in \{1, ..., m\}$ se tiene una biyección $\mathrm{Hom}_k(L_i, M_j) \cong \mathrm{Gal}(k) - \mathbf{FSet_t}(\mathrm{Hom}_k(M_j, k_s), \mathrm{Hom}_k(L_i, k_s))$, entonces

$$\begin{aligned}\mathrm{Hom}_k(A, B) &\cong \mathrm{Gal}(k) - \mathbf{FSet}\left(\prod_{i=1}^{n} \mathrm{Hom}_k(L_i, k_s), \prod_{j=1}^{m} \mathrm{Hom}_k(M_j, k_s)\right)\\ &\cong \mathrm{Gal}(k) - \mathbf{FSet}(\mathrm{Hom}_k(B, k_s), \mathrm{Hom}_k(A, k_s)).\end{aligned}$$

Respecto a la propiedad de ser esencialmente suprayectivo sea $S \in \mathrm{Gal}(k)-\mathbf{FSet}$. Así, existe $\Lambda \subseteq S$ finito tal que $S = \bigcup_{x\in\Lambda} \mathcal{O}(x)$, con $\mathcal{O}(x)$ la órbita de $x$. Como cada órbita es un conjunto finito cuya acción es continua, por ser restricción de la acción de $S$, y es trastitiva, entonces para cada $x \in \Lambda$ existe $L_x |\, k$ finita y separable tal que $\mathrm{Hom}_k(L_x, k) \cong \mathcal{O}(x)$. Así, $S \cong \mathrm{Hom}_k(\prod_{x\in\Lambda} L_s, k_s)$. $\square$

Capítulo 2

# Sobre la teoría de aplicaciones cubrientes

En este capítulo se introducen y estudian algunas propiedades básicas de un tipo especial de aplicaciones cubrientes conocidas como de Galois. Entre los resultados claves se demuestra que estas tienen teoremas análogos al Teorema Fundamental de la Teoría de Galois de Krull (Teorema 1.2 del Capítulo 1) y de Grothendieck (Teorema 1.4 del Capítulo 1). El capítulo concluye con dos caracterizaciones de la categoría de aplicaciones cubrientes sobre un espacio topológico $X$ con ciertas hipótesis de conexidad sobre este.

## 1. Propiedades básicas

A lo largo de este capítulo $X$ será un espacio topológico. Para establecer notación se recuerdan los siguientes conceptos.

DEFINICIÓN 2.1. *La categoría rebanada* ***Top*** $/X$ *se conoce como la categoría de haces sobre* $X$*.*

DEFINICIÓN 2.2. *Dado* $p : Y \to X$ *un haz sobre* $X$*, se dice que* $p$ *es una* ***aplicación cubriente*** *si para cada* $x \in X$*, existe una vecindad abierta de* $x$*,* $V \subseteq X$*, tal que* $p^{-1}(V) = \coprod_{i\in I} U_i$*, donde para cada* $i \in I$*,* $U_i \subseteq Y$ *es un abierto y* $p|_{U_i} : U_i \to V$ *es un homeomorfismo.*[1]

Para $p : Y \to X \in$ **Top** $/X$ una aplicación cubriente, a $X$ se le denomina como el **espacio base** y a $Y$ como el **espacio cubriente** de la aplicación $p$. Dado $x \in X$, al conjunto $p^{-1}(x)$ se le denomina como la **fibra** en el punto $x$. Una vecindad $V \subseteq X$ de $x \in X$ como en la definición de aplicación cubriente se dice que está **cubierta parejamente** por la familia de abiertos $\{U_i \mid i \in I\}$. A los abiertos $\{U_i \mid i \in I\}$ se les llama **hojas**. Se denota por **Cov(X)** a la subcategoría plena de **Top**$/X$ cuyos objetos son las aplicaciones cubrientes.

[1] En esta definición $\coprod$ denota la unión ajena de conjuntos, que de hecho es el objeto en el coproducto de estos para las categorías **Set** y **Top**.

Es directo de la definición probar las siguientes propiedades topológicas básicas:

PROPOSICIÓN 2.3. *Sea* $p : Y \to X \in \boldsymbol{Cov(X)}$. *Entonces,*

1. $p$ *es un homeomorfismo local.*
2. *Todas las fibras de* $p$ *son no vacías y discretas. En particular* $p$ *es suprayectiva.*
3. $p$ *es una función abierta. Más aún, una identificación.*
4. *Si* $X$ *es conexo, entonces todas las fibras tienen la misma cardinalidad. Más aún, cualesquiera dos fibras son homeomorfas.*

En el caso de $X$ conexo se define la **multiplicidad** de la aplicación cubriente como la cardinalidad de cualquier fibra. Esta está bien definida por el inciso 4 de la proposición anterior.

Una forma simple de producir ejemplos de aplicaciones cubrientes se obtiene al considerar $F$ un espacio discreto. Así, la función proyección en la primera coordenada, $p_1 : X \times F \to X$, conocida como **haz trivial** sobre $X$, es una aplicación cubriente. A esta aplicación cubriente se le conoce como la **aplicación cubriente trivial**. Una discusión más amplia de este tipo de aplicaciones cubrientes se encuentra en el Ejemplo 2.27. Por otro lado, no toda aplicación cubriente es isomorfa a una aplicación cubriente trivial (ver Ejemplo 2.33). Sin embargo, el siguiente resultado dice que de manera local todas las aplicaciones cubrientes son haces triviales.

PROPOSICIÓN 2.4. *Sea* $p : Y \to X$ *un haz sobre* $X$. *Entonces,* $p \in \boldsymbol{Cov(X)}$ *si y sólo si para cada* $x \in X$ *existe* $V \subseteq X$ *una vecindad abierta de* $x$ *tal que* $p|_{p^{-1}(V)} : p^{-1}(V) \to V$ *es isomorfo a un cubriente trivial en* $\boldsymbol{Top}/V$.

DEMOSTRACIÓN. $\Rightarrow$) Como $p \in \mathbf{Cov(X)}$, dado $x \in X$ existe $V \subseteq X$ una vecindad abierta de $x$ cubierta parejamente por la familia de abiertos $\{U_i \mid i \in I\}$ en $X$. Al considerar al conjunto $I$ como espacio discreto, se puede considerar $p_1 : V \times I \to V$ la aplicación cubriente trivial sobre $V$. Se afirma que $p|_{p^{-1}(V)} \cong p_1$ en $\mathbf{Top}/V$. Así, para probar la afirmación se observa que para $y \in p^{-1}(V)$, dado que existe un único $i_y \in I$ tal que $y \in U_{i_y}$, se define $f : p^{-1}(V) \to V \times I$ mediante la regla de correspondencia $f(y) = (p(y), i_y)$. De la definición es claro que $p_1 \circ f = p|_{p^{-1}(V)}$.

Respecto a la continuidad de $f$, al ser $I$ discreto, basta con ver que la imagen inversa de $A \times \{i\} \subseteq V \times I$ es un abierto, donde $A$ es un abierto no vacío en $V$ e $i \in I$. En efecto, $y \in f^{-1}(A \times \{i\})$ si y sólo si $i_y = i$ y $p(y) \in A$, es decir, $y \in U_i \cap p^{-1}(A)$. Así, $f^{-1}(A \times \{i\}) = U_i \cap p^{-1}(A)$, que es un abierto en $p^{-1}(V)$. Además, $f$ es abierta pues si $A \subseteq p^{-1}(V)$ es un abierto no vacío, entonces dado $a \in A$, se tiene que existe un único $i_0 \in I$ tal que $a \in U_{i_0}$. Nótese que $f(a) = (p(a), i_0) \in p(A \cap U_{i_0}) \times \{i_0\}$ y que $p(A \cap U_{i_0}) \times \{i_0\} \subseteq X \times I$ es un abierto. Más aún, $p(A \cap U_{i_0}) \times \{i_0\} \subseteq f(A)$, lo que prueba que $f(A)$ es abierto.

Por otro lado sean $y_1, y_2 \in p^{-1}(V)$ tales que $f(y_1) = f(y_2)$. Así, $p(y_1) = p(y_2)$, y como $y_1, y_2 \in U_{i_{y_1}}$, al ser $p$ un homeomorfismo, al restringirse a dicha hoja, se concluye que $y_1 = y_2$, lo que prueba que $p$ es inyectiva. Por otro lado, dado $(x, i) \in V \times I$, al ser $p|_{U_i}$ un homeomorfismo se tiene que $(p|_{U_i})^{-1}(x) \in U_i$, de donde $f((p|_{U_i})^{-1}(x)) = (p((p|_{U_i})^{-1}(x)), i) = (x, i)$. Esto prueba que $f$ es también suprayectiva y por lo tanto un homeomorfismo.

$\Leftarrow$) Dado $x \in X$ sea $V$ la vecindad abierta de $x$ tal que $p|_{p^{-1}(V)}$ es isomorfa a un cubriente trivial sobre $V$ en la categoría **Top** $/V$. En particular $p^{-1}(V) \cong V \times I$ para $I$ un espacio discreto. Así, $p^{-1}(V) \cong \coprod_{i \in I} V \times \{i\}$, cada uniendo es un abierto y $V \times \{i\} \cong V$. Esto prueba el resultado. $\square$

A continuación se van a probar dos lemas técnicos que se utilizarán en el desarrollo del presente capítulo.

Lema 2.5. *Sean $p : Y \to X \in$ **Cov(X)** con $X$ localmente conexo, $Z \in$ **Top** conexo y $f, g : Z \to Y$ funciones continuas tales que $p \circ f = p \circ g$. Si existe $z_0 \in Z$ tal que $f(z_0) = g(z_0)$, entonces $f = g$.*

Demostración. Se define el conjunto $A = \{z \in Z \mid f(z) = g(z)\}$. Nótese que si se prueba que este conjunto es abierto y cerrado en $Z$, la conexidad de $Z$ implica que $A = Z$ dado que $z_0 \in A$, lo que concluye la prueba.

Para ver que $A$ es abierto; sea $z \in A$. Si se pone $x := pf(z) = pg(z)$, entonces existe $V \subseteq X$ una vecindad abierta conexa de $x$ cubierta parejamente por una familia de abiertos en $Y$, $\{U_i \mid i \in I\}$, donde la conexidad de $V$ se tiene pues $X$ es localmente conexo. Dado que $f(z) \in p^{-1}(V)$, existe un único $i_0 \in I$ tal que $f(z) \in U_{i_0}$. Al ser $p$ abierta, suprayectiva, $V = \coprod_{i \in I} p(U_i)$ y $V$ conexo, lo anterior implica que $V = p(U_{i_0})$. Así, como $(p \circ f)^{-1}(V) \subseteq Z$ es un abierto y $z \in (p \circ f)^{-1}(V)$, si se prueba que $(p \circ f)^{-1}(V) \subseteq A$, se concluye que $A$ es abierto. En esta dirección, dado $a \in (p \circ f)^{-1}(V)$ se tiene que $pf(a), pg(a) \in V$. Como $p(U_{i_0}) = V$ y $p|_{U_{i_0}}$ es biyectiva, esto implica que $f(a) = g(a)$, de donde $a \in A$.

Respecto a la propiedad de ser $A$ cerrado, se va a probar que $Z \setminus A$ es abierto. Así, dado $z \in Z \setminus A$, se observa que al considerar $V \subseteq Y$ una vecindad abierta de $pf(z) = pg(z)$ cubierta parejamente por la familia de hojas $\{U_i \mid i \in I\}$; como $f(z) \in U_{i_0}$ y $g(z) \in U_{i_1}$, se observa que $i_0 \neq i_1$ pues en caso contrario al ser $p|_{U_{i_0}}$ un homeomorfismo, la igualdad $p(f(z)) = p(g(z))$ implica que $f(z) = g(z)$, lo que es una contradicción. Luego, se considera el conjunto $f^{-1}(U_{i_0}) \cap g^{-1}(U_{i_1}) \subseteq Z$, que es abierto por ser $f$ y $g$ funciones continuas. Además es claro que $z \in f^{-1}(U_{i_0}) \cap g^{-1}(U_{i_1})$. Si se prueba que $f^{-1}(U_{i_0}) \cap g^{-1}(U_{i_1}) \subseteq Z \setminus A$ se concluye la prueba. Pero esto es claro pues si $a \in f^{-1}(U_{i_0}) \cap g^{-1}(U_{i_1})$, entonces $f(a) \in U_{i_0}$ y $g(a) \in U_{i_1}$. Luego, $f(a) \neq g(a)$ pues $U_{i_0} \cap U_{i_1} = \emptyset$. □

LEMA 2.6.

1. *Sean $p : Y \to X \in$ **Cov(X)** y $q : Z \to Y \in$ **Cov(Y)** con $X$ es localmente conexo y localmente simplemente conexo. Entonces $p \circ q : Z \to X \in$ **Cov(X)**.*
2. *Sean $p : Y \to X \in$ **Cov(X)** con $X$ localmente conexo y $q : Z \to Y$ una función continua con $Y$ conexo tales que $p \circ q : Z \to X \in$ **Cov(X)**. Entonces $q : Z \to Y \in$ **Cov(Y)**.*

DEMOSTRACIÓN. Para la primera afirmación, sea $x \in X$. Las hipótesis sobre $X$ aunadas al hecho de que $p$ es una aplicación cubriente implican por la Proposición 2.4 que existe una vecindad abierta de $x$ simplemente conexa tal que $p|_{p^{-1}(V)} : p^{-1}(V) \to V$ es isomorfo a un haz trivial sobre $V$. Además, al aplicar el mismo argumento sobre cada una de las componentes conexas de $p^{-1}(V)$, se tiene que $q$ debe ser trivial al restringirste a un abierto en cada una de ellas por la Proposición 2.4, luego, $p \circ q$ debe ser trivial sobre cada uno de dichos abiertos. Así, al usar nuevamente la Proposición 2.4 se deduce que $p \circ q \in \mathbf{Cov(X)}$.

Respecto a la segunda afirmación, sea $y \in Y$. Dado que $p(y) \in X$ y al ser $p$ y $p \circ q$ aplicaciones cubrientes, existe una vecindad abierta de $p(y)$ conexa, $V \subseteq X$, cubierta parejamente por las familias de abiertos $\{U_i \mid i \in I\}$ y $\{W_j \mid j \in J\}$ para $p$ y $p \circ q$ respectivamente. Sea $i_0 \in I$ el único indice tal que $y \in U_{i_0}$. Ahora se define el conjunto $J_0 = \{j \in J \mid q(W_j) \subseteq U_{i_0}\}$, el cual es distinto del vacío pues $q$ es continua y $W_j$ es siempre conexo. Se afirma que $q^{-1}(U_{i_0}) = \coprod_{j \in J_0} W_j$. En efecto, dado $j \in J_0$ se tiene que para $z \in W_j$, $q(z) \in U_{i_0}$, de lo que se concluye que $\coprod_{j \in J_0} W_j \subseteq q^{-1}(U_{i_0})$. Por otro lado, si $z \in q^{-1}(U_{i_0})$, entonces $q(z) \in U_{i_0}$, de donde $pq(z) \in p(U_{i_0}) = V$, luego existe un único $j_0 \in J$ tal que $z \in W_{j_0}$. Por continuidad de $q$ se tiene que $q(W_{j_0}) \subseteq U_{i_0}$ y así $z \in \coprod_{j \in J_0} W_j$, lo que prueba la segunda contención.

En lo que respecta a ver que para cada $j \in J_0$ se tiene que $q|_{W_j} : W_j \to U_{i_0}$ es un homeomorfismo, se observa que el siguiente diagrama claramente conmuta para cada uno de tales índices.

$$
\begin{tikzcd}
W_j \arrow[rr, "q|_{W_j}"] \arrow[dr, "p\circ q|_{W_j}"'] & & U_{i_0} \arrow[dl, "p|_{U_{i_0}}"] \\
& V &
\end{tikzcd}
$$

Dado que $p \circ q|_{W_j}$ y $p|_{U_{i_0}}$ son homeomorfismos, entonces $q|_{W_j}$ también lo es, lo que concluye la prueba de que $q$ es una aplicación cubriente. $\square$

Para $p : Y \to X \in \mathbf{Cov(X)}$, sea $\mathrm{Aut}(p)$ el conjunto de automorfismos de $p$. Nótese que este conjunto tiene estructura de grupo con la composición de funciones como operación y neutro la función identidad en $Y$.

DEFINICIÓN 2.7. *Dado $p : Y \to X \in$ **Cov(X)**, al grupo* $\mathrm{Aut}(p)$ *se le conoce como el **grupo de transformaciones cubrientes** de $p$.*

Muchos ejemplos interesantes de aplicaciones cubrientes en los que el cálculo del su grupo de transformaciones cubrientes es relativamete sencillo provienen de la teoría de grupos topológicos. En esta dirección se recuerdan la siguiente definición y el siguiente resultado:

DEFINICIÓN 2.8. *La acción (izquierda) de un grupo discreto $G$ en un espacio $X$ es **propiamente discontinua** si para cada $x \in X$, existe $V \subseteq X$ una vecindad abierta de $x$ tal que para todo $g \in G$ con $g \neq e$, $V \cap gV = \emptyset$.*

PROPOSICIÓN 2.9. *Si $G$ es un grupo topológico discreto que actúa de forma propiamente discontinua en un espacio $X$ conexo, entonces la proyección en el espacio de órbitas de la acción, $\pi_G : X \to X/G$, es una aplicación cubriente de multiplicidad $|G|$ con* $\mathrm{Aut}(\pi_G) \cong G$.

Una prueba del resultado anterior puede consultarse en la Proposición 4.20 de [**Sw**, pp 62]. Un ejemplo general y de carácter intesante para los fines de este trabajo se obtiene al notar que dado $p : Y \to X \in \mathbf{Cov(X)}$, se puede definir una acción de $\mathrm{Aut}(p)$ en $Y$ dada por $f \cdot y = f(y)$, donde $f \in \mathrm{Aut}(p)$ y $y \in Y$.

PROPOSICIÓN 2.10. *Sea $p : Y \to X \in$ **Cov(X)** con $X$ localmente conexo. La acción de* $\mathrm{Aut}(p)$ *como grupo discreto en $Y$ definida anteriormente es continua. Además, si $Y$ es conexo, entonces la acción es propiamente discontinua.*

Demostración. Respecto a la continuidad, sea $U \subseteq Y$ abierto no vacío y denótese por $\mu$ a la acción. Así, $(f, y) \in \mu^{-1}(U)$ si y sólo si $f(y) \in U$, condición que es equivalente a decir que $(f, y) \in \bigcup_{g \in \mathrm{Aut}(p)} \{g\} \times g^{-1}(U)$. Esto prueba que $\mu^{-1}(U) = \bigcup_{g \in \mathrm{Aut}(p)} \{g\} \times g^{-1}(U)$. Además, como cada uno de los uniendos es abierto en $\mathrm{Aut}(p) \times Y$ se concluye que $\mu^{-1}(U)$ también lo es, lo que prueba que la acción es continua.

Para ver que la acción es propiamente discontinua sea $y \in Y$. Al denotar $x := p(y)$, la definición de aplicación cubriente aunada al hecho de que $Y$ es conexo implican que existe $V \subseteq X$ una vecindad abierta conexa de $x$ cubierta parejamente por la familia de abiertos $\{U_i \mid i \in I\}$ en $Y$. Luego, existe un único $i_0 \in I$ tal que $y \in U_{i_0}$. Más aún, por ser $p$ suprayectiva $V = \coprod_{i \in I} p(U_i)$, y al ser $p$ abierta, la conexidad de $V$ implica que $V = p(U_{i_0})$.

Se afirma que para cada $f \in \mathrm{Aut}(p)$ con $f \neq 1_Y$, $U_{i_0} \cap fU_{i_0} = \emptyset$. En efecto, al proceder por contrapositiva, si existe $f \in \mathrm{Aut}(p)$ tal que $U_{i_0} \cap fU_{i_0} \neq \emptyset$, entonces existe $y_0 \in U_{i_0}$ tal que $y_0 = f(y_1)$ para $y_1 \in U_{i_0}$. Luego, $p(y_1) = pf(y_1) = p(y_0)$. Pero, $p|_{U_{i_0}} : U_{i_0} \to V$ es un homeomorfismo, de donde la igualdad anterior implica que $y_0 = y_1$. Así, $f(y_0) = y_0$, por lo que del Lema 2.5 se deduce que $f = 1_Y$. $\square$

De las dos proposiciones anteriores se deduce el siguiente resultado.

Corolario 2.11. *Para $p : Y \to X \in$ **Cov(X)** con $Y$ conexo y $X$ localmente conexo,* $\mathrm{Aut}(\pi_{\mathrm{Aut}(p)}) \cong \mathrm{Aut}(p)$.

Demostración. Dado que $Y$ es conexo, la proposición anterior implica que la acción de $\mathrm{Aut}(p)$ en $Y$ es propiamente discontinua. Así, la Proposición 2.9 implica que la proyección en el espacio de órbitas $\pi_{\mathrm{Aut}(p)} : Y \to Y/\mathrm{Aut}(p)$ es una aplicación cubriente y que $\mathrm{Aut}(\pi_{\mathrm{Aut}(p)}) \cong \mathrm{Aut}(p)$. $\square$

## 2. La acción de monodromía y el funtor fibra sobre un punto

En la sección anterior no se mencionaron dos de las propiedades más importantes de las aplicaciones cubrientes. Estas se muestran en el siguiente resultado:

Teorema 2.12. *Sean $p : Y \to X \in$ **Cov(X)** con $X$ localmente conexo, $x \in X$ y $y \in p^{-1}(x)$. Entonces se cumple lo siguiente:*

1. *Propiedad de Levantamiento de Trayectorias:* *Dada* $\sigma : [0,1] \to X$ *una trayectoria tal que* $\sigma(0) = x$*, existe una única trayectoria* $\tilde{\sigma} : [0,1] \to Y$ *tal que* $\tilde{\sigma}(0) = y$ *y* $p \circ \tilde{\sigma} = \sigma$*.*
2. *Propiedad de Levantamiento de Homotopías:* *Dadas* $f : Z \to X$ *una función continua y* $H : Z \times [0,1] \to X$ *una homotopía tales que* $p \circ f = H|_{Z\times\{0\}}$*, existe una homotopía* $\tilde{H} : Z \times [0,1] \to Y$ *tal que* $\tilde{H}|_{Z\times\{0\}} = f$ *y* $p \circ \tilde{H} = H$*.*

La prueba del resultado anterior puede encontrarse en [**S**, pp 35–36] Lema 3.3.2. En lo que sigue las siglas PLT y PLH denotan una abreviación para indicar el uso de la propiedad de levantamiento de trayectorías y homotopías, respectivamente. Se recuerda que una función continua que satisface PLH se conoce como una **fibración de Hurewicz**. Así, toda aplicación cubriente es una fibración de Hurewicz.

El siguiente resultado que se deduce del teorema anterior será bastante utilizado, por lo que vale la pena enunciarlo.

COROLARIO 2.13. *Sean* $p : Y \to X \in$ ***Cov(X)*** *y* $\sigma, \tau \in X^I$ *tales que* $\sigma \simeq \tau$ *relativas al* $\{0,1\}$*. Entonces* $\tilde{\sigma}(1) = \tilde{\tau}(1)$*.*

El siguiente resultado es una aplicación más del teorema anterior.

PROPOSICIÓN 2.14. *Toda aplicación cubriente de un espacio simplemente conexo y localmente conectable por trayectorias es trivial.*

DEMOSTRACIÓN. Sea $p : Y \to X$ una de tales aplicaciones cubrientes. Además, puede suponerse sin pérdida de generalidad que $Y$ es conexo. Se afirma que $p$ es inyectiva. En efecto, sean $y_0, y_1 \in Y$ tales que $p(y_0) = p(y_1)$. Así, como $p$ es un homeomorfismo local y $X$ tiene una base de vecindades abiertas conectables por trayectorias, se tiene que $Y$ es localmente conectable por trayectorias, de donde se deduce que $Y$ es conectable por trayectorias. Como existe una trayectoria $\sigma \in Y^I$ tal que $\sigma(0) = y_0$ y $\sigma(1) = y_1$, al ser $p\circ\sigma \in X^I$ un lazo en $p(y_0)$, se tiene que $p\circ\sigma \simeq c_{p(y_0)}$. Luego, por la PLH se tiene que $\sigma \simeq c_{y_0}$, de donde $y_1 = \sigma(1) = c_{y_0}(1) = y_0$.

Dado que $p$ es una función continua y biyectiva, existe su inversa en la categoría de conjuntos $p^{-1} : Y \to X$. Más aún, esta es continua por ser $p$ un homeomorfismo local. Esto prueba que $p$ es un homeomorfismo, con lo que se concluye la prueba. $\square$

Ahora se obtendrá un análogo a la acción de $\mathrm{Gal}(k)$ en $\mathrm{Hom}_k(A, k_s)$ para $A$ una $k$-álgebra finita étale presentada en el capítulo anterior, pero para el caso de aplicaciones cubrientes. Para esto, sean $p : Y \to X \in \mathbf{Cov(X)}$ y $x \in X$. Se denota por $\pi_1(\mathrm{X}, \mathrm{x})$ al grupo fundamental de $X$ en el punto de $x$. Se quiere definir una función $\pi_1(\mathrm{X}, \mathrm{x}) \times p^{-1}(x) \to p^{-1}(x)$. Así, dados $[\alpha] \in \pi_1(\mathrm{X}, \mathrm{x})$ y $y \in p^{-1}(x)$, se define $[\alpha] \cdot y = \tilde{\alpha}(1)$, donde $\tilde{\alpha}$ se obtiene por la PLT como la única trayectoria $\tilde{\alpha} \in Y^I$ tal que $\tilde{\alpha}(0) = y$ y $p \circ \tilde{\alpha} = \alpha$. Además se observa que esta asignación es una función por el Corolario 2.13 y es muy sencillo ver que esta función es una acción de grupo, a la que se le conoce como la **acción de monodromía** en la fibra $p^{-1}(x)$.

Vale la pena mencionar que el nombre de esta acción proviene del análisis complejo pues de hecho la PLH es una generalización del teorema de monodromía en análisis complejo, que básicamente es la prueba de unicidad para la continuación analítica a lo largo de una trayectoría de una función definida en un dominio complejo. Los detalles de esto pueden consultarse por ejemplo en [**BG**].

Ahora considérese $(X, x) \in \mathbf{Top}_*$. La acción de monodromía se puede interpretar mediante la existencia de una asignación que a toda $p : Y \to X \in \mathbf{Cov(X)}$, le asigna un $\pi_1(X, x)$-conjunto, a saber, la fibra en $x$ dada por $p$. Sea $\mathrm{Fib_x} : \mathbf{Cov(X)} \to \pi_1(X, x) - \mathbf{Set}$ dicha asignación. Para ver que esta es funtorial, sea $f : Y \to Z$ un morfismo entre las aplicaciones cubrientes $p : Y \to X$ y $q : Z \to X$. Dado $y \in p^{-1}(x)$, se tiene que $qf(y) = p(y) = x$, es decir, $f(y) \in q^{-1}(x)$. Así, se define $\mathrm{Fib_x}(f) : p^{-1}(x) \to q^{-1}(x)$ mediante $\mathrm{Fib_x}(f)(y) = f(y)$. Esta asignación define en efecto un morfismo de $\pi_1(\mathrm{X}, \mathrm{x})$-conjuntos pues dado $[\alpha] \in \pi_1(\mathrm{X}, \mathrm{x})$ y $y \in p^{-1}(x)$ se tiene que

$$\mathrm{Fib_x}(f)([\alpha] \cdot y) = \mathrm{Fib_x}(f)(\tilde{\alpha}(1)) = f(\tilde{\alpha}(1)),$$

donde $\tilde{\alpha} : I \to Y$ es la única trayectoria tal que $\tilde{\alpha}(0) = y$ y $p \circ \tilde{\alpha} = \alpha$. Pero estas condiciones implican que $f \circ \tilde{\alpha} : I \to Z$ es una trayectoria con $q \circ (f \circ \tilde{\alpha}) = \alpha$ y $(f \circ \tilde{\alpha})(0) = f(y)$, lo que dice que este es el único levantamiento por $q$ de la trayectoria $\alpha$. Así, $[\alpha] \cdot f(y) = f(\tilde{\alpha}(1))$. Pero de esta igualdad es claro entonces que $\mathrm{Fib_x}(f)([\alpha] \cdot y) = [\alpha] \cdot \mathrm{Fib_x}(f)(y)$.

Un cálculo de rutina prueba el siguiente resultado.

PROPOSICIÓN 2.15. *Dado $(X, x) \in \boldsymbol{Top}_*$, la asignación*

$$\mathrm{Fib_x} : \boldsymbol{Cov(X)} \to \pi_1(X, x) - \boldsymbol{Set}$$

*es un funtor.*

Los espacios conexos, localmente conexos y localmente simplemente conexos son muy especiales pues para estos se puede construir siempre un espacio cubriente que se conoce como el **cubriente universal**. A continuación se recordará la construcción de dicho espacio y sus principales propiedades pues será útil en lo que sigue. Para esto supóngase que $X$ es uno de tales espacios. Dado $x \in X$, se define el conjunto $\tilde{\mathrm{X}}_{\mathrm{x}}$ como aquél formado por clases de homotopía relativas al $\{0,1\}$ de trayectorias $\sigma : I \to X$, tales que $\sigma(0) = x$. Nótese que hay un elemento canónico $[c_x] \in \tilde{\mathrm{X}}_{\mathrm{x}}$, que es la clase del lazo constante en $x$. Así, se puede definir una función $p_x : \tilde{\mathrm{X}}_{\mathrm{x}} \to X$ mediante la regla de correspondencia $p_x([\sigma]) := \sigma(1)$, donde $[\sigma] \in \tilde{\mathrm{X}}_{\mathrm{x}}$. Esta asignación es una función pues las homotopías consideradas tienen los mismos extremos por definición.

Para dar una topología a $\tilde{\mathrm{X}}_{\mathrm{x}}$, dados $[\sigma] \in \tilde{\mathrm{X}}_{\mathrm{x}}$ y $U$ una vecindad abierta de $\sigma(1)$ simplemente conexa, se define $U_{[\sigma]} = \{[\sigma * \tau] \mid \tau \in X^I,\ \tau(0) = \sigma(1) \text{ y } \tau([0,1]) \subseteq U\}$. Puede probarse que la familia de conjuntos $\{U_{[\sigma]} \mid [\sigma] \in \tilde{\mathrm{X}}_{\mathrm{x}}\}$ satisfacen los axiomas de una base para una topología en $\tilde{\mathrm{X}}_{\mathrm{x}}$ con la que dicho espacio es conexo (ver por ejemplo el Lema 2.4.2 [**S**, pp 40]). Además, con esta topología $p_x$ resulta ser una aplicación cubriente (ver por ejemplo [**H**, pp 64–65]).

La razón por la cual $\tilde{\mathrm{X}}_{\mathrm{x}}$ se conoce como el cubriente universal de $X$ proviene del hecho de que $p_x$ es una objeto inicial en la categoría de aplicaciones cubrientes con base $X$ y espacio cubriente conexo. Los detalles de esta afirmación pueden consultarse en [**R**, pp 288] Teorema 10.17.

OBSERVACIÓN 2.16. *Hay una acción derecha de* $\pi_1(\mathrm{X},\mathrm{x})$ *en* $\tilde{\mathrm{X}}_{\mathrm{x}}$ *pues dados* $[\sigma] \in \tilde{\mathrm{X}}_{\mathrm{x}}$ *y* $[\alpha] \in \pi_1(\mathrm{X},\mathrm{x})$*, puede considerarse* $[\alpha * \sigma] \in \tilde{\mathrm{X}}_{\mathrm{x}}$*. Así,* $[\sigma] \cdot [\alpha] := [\alpha * \sigma]$*, y esta asignación es función por la propiedad de que si* $\alpha \simeq \alpha'$ *y* $\sigma \simeq \sigma'$ *relativas al* $\{0,1\}$*, entonces* $\alpha * \sigma \simeq \alpha' * \sigma'$ *relativa al* $\{0,1\}$*.*

Regresando a la analogía que se dio entre el funtor de fibra en un punto y la formulación de Grothendieck del Teorema Fundamental de la Teoría de Galois, se tiene el siguiente resultado que muestra que la relación entre estos es más que una analogía, pues el espacio cubriente universal juega un papel similar a la clausura separable de un campo.

PROPOSICIÓN 2.17. *Sea* $(X,x) \in \boldsymbol{Top}_*$ *con* $X$ *conexo, localmente conexo y localmente simplemente conexo. Entonces, el funtor* $\mathrm{Fib}_{\mathrm{x}}$ *es representable.*

DEMOSTRACIÓN. De las hipótesis se deduce que para $X$ existe su cubriente universal $p_x : \tilde{\mathrm{X}}_{\mathrm{x}} \to X$. Se afirma que $\mathrm{Fib}_{\mathrm{x}} \cong \mathbf{Cov(X)}(p_x, \_)$.

En efecto, sea $p : Y \to X \in \mathbf{Cov(X)}$. Para construir $\varphi_p : \mathrm{Fib_x}(p) \to \mathbf{Cov(X)}(p_x, p)$ se observa que dado $y \in p^{-1}(x)$ y $[\sigma] \in \tilde{\mathrm{X}}_{\mathrm{x}}$, existe una única trayectoria $\tilde{\sigma} : I \to Y$ tal que $\tilde{\sigma}(0) = y$ y $p \circ \tilde{\sigma} = \sigma$. Entonces se define $\varphi_p(y)([\sigma]) = \tilde{\sigma}(1)$. Por el Corolario 2.13 $\varphi_p(y)$ está bien definida. Además es claro de la construcción que $p \circ \varphi_p(y) = p_x$ y dado que $p$ es un homeomorfismo local y $p_x$ es continua, esta igualdad implica que $\varphi_p(y)$ es continua.

Para ver que $\varphi_p$ es inyectiva, sean $y_0, y_1 \in p^{-1}(x)$ tales que $\varphi_p(y_0) = \varphi_p(y_1)$. Al considerar el elemento canónico $[c_x] \in \tilde{\mathrm{X}}_{\mathrm{x}}$ se tiene que $\varphi_p(y_0)([c_x]) = \varphi_p(y_1)([c_x])$, de donde $y_1 = \tilde{c_x}(1) = y_2$. Respecto a la suprayectividad sea $f \in \mathbf{Cov(X)}(p_x, p)$. Lo primero que se observa es que $pf([c_x]) = p_x([c_x]) = x$ y así se afirma que $\varphi_p(f[c_x]) = f$. Para probar esto nótese que $p \circ \varphi_p(f[c_x]) = p_x = p \circ f$, y que $\varphi_p(f[c_x])[c_x] = \tilde{\sigma}(1)$ con $\tilde{\sigma} : I \to Y$ la única trayectoria tal que $\tilde{\sigma}(0) = f[c_x]$ y $p \circ \tilde{\sigma} = c_x$. Así, $\tilde{\sigma} = c_{f[c_x]}$ y entonces $\varphi_p(f[c_x])(c_x) = f([c_x])$. Dado que $\tilde{\mathrm{X}}_{\mathrm{x}}$ es conexo y $X$ localmente conexo, el Lema 2.5 implica la igualdad que se quería.

Para ver que el isomorfismo es natural, se quiere probar que el siguiente diagrama conmuta donde $f \in \mathbf{Cov(X)}(p, q)$ para $p : Y \to X$ y $q : Z \to X$ aplicaciones cubrientes sobre $X$.

$$\begin{tikzcd}
\mathrm{Fib_x}(p) \arrow[r, "\varphi_p"] \arrow[d, "\mathrm{Fib_x}(f)"'] & \mathbf{Cov(X)}(p_x, p) \arrow[d, "f_*"] \\
\mathrm{Fib_x}(q) \arrow[r, "\varphi_q"'] & \mathbf{Cov(X)}(p_x, q)
\end{tikzcd}$$

Así, dados $y \in p^{-1}(x)$ y $[\sigma] \in \tilde{\mathrm{X}}_{\mathrm{x}}$ se tiene que

$$(\varphi_q \circ \mathrm{Fib_x}(f))(y)\,[\sigma] = \varphi_q(f(y))\,[\sigma] = \tilde{\sigma}(1),$$

donde $\tilde{\sigma} : I \to Z$ es la única trayectoria tal que $q \circ \tilde{\sigma} = \sigma$ y $\tilde{\sigma}(0) = f(y)$.

Por otro lado se tiene que

$$(f_* \circ \varphi_p)(y)\,[\sigma] = (f \circ \varphi_p(y))([\sigma]) = f\tilde{\sigma'}(1),$$

donde $\tilde{\sigma'} : I \to Y$ es la única trayectoria tal que $p \circ \tilde{\sigma'} = \sigma$ y $\tilde{\sigma'}(0) = y$.

Pero se observa que $f \circ \tilde{\sigma'} : I \to Z$ es una trayectoria, $q \circ (f \circ \tilde{\sigma'}) = \sigma$ y $(f \circ \tilde{\sigma'})(0) = f(y)$. Luego, la unicidad en el levantamiento dice que $\tilde{\sigma} = f \circ \tilde{\sigma'}$, de donde se deduce la igualdad que se quiere. $\square$

Se recuerda que cuando un funtor es representable se puede hablar de un **elemento universal**, que es el que corresponde al morfismo identidad. Así, al considerar las hipótesis del resultado anterior, se observa que como $\mathrm{Fib_x}(p_x) \cong \mathbf{Cov(X)}(p_x, p_x)$ y dado que $[c_x] \in \mathrm{Fib_x}(p_x)$, $p_{[c_x]}([c_x]) = [c_x]$, $p_x \circ p_{[c_x]} = p_x$, del Lema 2.5 se tiene que $p_{[c_x]} = 1_{\tilde{\mathrm{X}}_\mathrm{x}}$. Así, el elemento canónico en la fibra $p_x^{-1}(x)$ es de hecho el elemento universal en la representabilidad del funtor $\mathrm{Fib_x}$.

Además, si $p : Y \to X \in \mathbf{Cov(X)}$ con $X$ satisfaciendo las hipótesis del resultado anterior, entonces para $x \in X$ y $y \in p^{-1}(x)$, se sabe que a este elemento corresponde un único $p_y \in \mathbf{Cov(X)}(p_x, p)$. La naturalidad de la representabilidad del funtor de fibras implica que $p_y([c_x]) = y$.

Observación 2.18. *Continuando con las hipótesis del resultado anterior nótese que se puede definir una acción derecha de* $\mathrm{Aut}(p_x)$ *en* $\boldsymbol{Cov(X)}(p_x, p)$ *cuya regla de correspondencia es* $g \cdot f := g \circ f$ *para* $f \in \mathrm{Aut}(p_x)$ *y* $g \in \boldsymbol{Cov(X)}(p_x, p)$*. De la representabilidad del funtor* $\mathrm{Fib_x}$*, esto da lugar a una acción derecha de* $\mathrm{Aut}(p_x)$ *en* $p^{-1}(x)$ *definida mediante* $y \cdot f =: \varphi_p^{-1}(p_y \circ f)$*, donde* $y \in p^{-1}(x)$ *y* $f \in \mathrm{Aut}(p_x)$*.*

## 3. Aplicaciones cubrientes de Galois

A lo largo de esta sección $X$ será siempre localmente conexo.

Sea $p : Y \to X \in \mathbf{Cov(X)}$ con $Y$ conexo. Por el Corolario 2.11 $\pi_{\mathrm{Aut}(p)}$ es una aplicación cubriente, y se tiene una factorización en **Top** para $p$ de la forma:

$$\begin{tikzcd} Y \arrow[rr, "p"] \arrow[dr, "\pi_{\mathrm{Aut}(p)}"'] & & X \\ & Y/\mathrm{Aut}(p) \arrow[ur, "\overline{p}_{\mathrm{Aut}(p)}"'] & \end{tikzcd}$$

donde $\overline{p}_{\mathrm{Aut}(p)}(\mathrm{Aut}(p)y) := p(y)$. Además, es claro de la definición que $\overline{p}_{\mathrm{Aut}(p)} \circ \pi_{\mathrm{Aut}(p)} = p$.

Para ver que el diagrama anterior está en **Top** lo único que restaría checar es la continuidad de $\overline{p}_{\mathrm{Aut}(p)}$. Así, si $V \subseteq X$ es un abierto, para ver que $\overline{p}_{\mathrm{Aut}(p)}^{-1}(V) \subseteq Y/\mathrm{Aut}(p)$ es abierto, dado que $Y/\mathrm{Aut}(p)$ tiene la topología cociente, esta afirmación es equivalente a probar que $\pi_{\mathrm{Aut}(p)}^{-1}\overline{p}_{\mathrm{Aut}(p)}^{-1}(V) \subseteq X$ es abierto. Sin embargo esto es claro pues de la conmutatividad $\pi_{\mathrm{Aut}(p)}^{-1}\overline{p}_{\mathrm{Aut}(p)}^{-1}(V) = p^{-1}(V)$ y $p$ es continua.

DEFINICIÓN 2.19. *Dado $p : Y \to X \in$* ***Cov(X)*** *con $Y$ conexo, se dice que $p$ es un* ***cubriente de Galois*** *si $\overline{p}_{\mathrm{Aut}(p)}$ es un homeomorfismo.*

La idea de la definicion anterior es que los cubrientes de Galois son aquellos que son isomorfos a proyecciones en espacios de órbitas, donde el grupo en cuestión actúa de forma propiamente discontinua. Un hecho que justifica el nombre de este tipo de aplicaciones cubrientes se da en el contexto de la geometría algebraica compleja, pues en este caso puede probarse que una aplicación cubriente entre superficies de Riemann conexas $p : Y \to X$ es de Galois si y sólo si el campo de funciones meromorfas $\mathcal{M}(Y)$ es una extensión de Galois de $\mathcal{M}(X)$. Además de que en este caso $\mathrm{Gal}(\mathcal{M}(Y)|\mathcal{M}(X)) \cong \mathrm{Aut}(p)$ y así, $Y/\mathrm{Gal}(\mathcal{M}(Y)|\mathcal{M}(X)) \cong X$ (Ver capítulo 3 de [**S**]).

Ahora, dado que la definición dada es impráctica, se tiene el siguiente resultado de caracterización.

PROPOSICIÓN 2.20. *Sea $p : Y \to X \in$* ***Cov(X)*** *con $Y$ conexo. Son equivalentes:*

1. *$p$ es de Galois.*
2. $\mathrm{Aut}(p)$ *actúa de manera transitiva en todas las fibras de $p$.*
3. $\mathrm{Aut}(p)$ *actúa de manera transitiva en alguna fibra de $p$.*

DEMOSTRACIÓN. $1 \Rightarrow 2$) Sean $x \in X$ así como $y_0, y_1 \in p^{-1}(x)$. Dado que $p(y_0) = p(y_1)$, la factorización de $p$ aunada al hecho de que $\overline{p}_{\mathrm{Aut}(p)}$ es un homeomorfismo implican que $\pi_{\mathrm{Aut}(p)}(y_0) = \pi_{\mathrm{Aut}(p)}(y_1)$. Sin embargo, esta igualdad implica que $\mathrm{Aut}(p)y_0 = \mathrm{Aut}(p)y_1$, de donde se tiene el resultado.

$2 \Rightarrow 3$) Es claro.

$3 \Rightarrow 1$) Sea $p^{-1}(x)$ la fibra en la que la acción de $\mathrm{Aut}(p)$ es transitiva. Para definir una función inversa de $\overline{p}_{\mathrm{Aut}(p)}$, $f : X \to Y/\mathrm{Aut}(p)$, se observa que dados $x \in X$ y $y_0, y_1 \in p^{-1}(x)$, la hipótesis implica que $\mathrm{Aut}(p)y_0 = \mathrm{Aut}(p)y_1$, por transitividad de la acción. Luego, la asignación $f(x) = \mathrm{Aut}(p)y$ si $y \in p^{-1}(x)$, es una función. Lo primero que se observa es que esta función es la inversa de $\overline{p}_{\mathrm{Aut}(p)}$ en la categoría de conjuntos, pues para $x \in X$ y $y \in p^{-1}(x)$, $\overline{p}_{\mathrm{Aut}(p)}(f(x)) = \overline{p}_{\mathrm{Aut}(p)}(\mathrm{Aut}(p)y) = p(y) = x$. Por otro lado, dado $\mathrm{Aut}(p)y \in Y/\mathrm{Aut}(p)$, se tiene que $f\overline{p}_{\mathrm{Aut}(p)}(\mathrm{Aut}(p)y) = f(p(y)) = \mathrm{Aut}(p)y$.

Para concluir la prueba, se va a ver que $f$ es la inversa de $\overline{p}_{\mathrm{Aut}(p)}$ en **Top**, para lo que falta probar que $f$ es continua. En efecto, dado $U \subseteq Y/\mathrm{Aut}(p)$ abierto, dado que $p$ es una identificación, $f^{-1}(A) \subseteq X$ es abierto si y sólo si $p^{-1}f^{-1}(A) \subseteq Y$ es abierto.

Pero $f \circ p = (f \circ \overline{p}_{\mathrm{Aut}(p)}) \circ \pi_{\mathrm{Aut}(p)} = \pi_{\mathrm{Aut}(p)}$. Por lo que $p^{-1}f^{-1}(A) = \pi^{-1}_{\mathrm{Aut}(p)}(A)$, y la afirmación que se quiere probar es consecuencia de la continuidad $\pi_{\mathrm{Aut}(p)}$. □

Corolario 2.21. *Todo endomorfismo en un cubriente de Galois es un automorfismo.*

Demostración. Sea $p : Y \to X \in \mathbf{Cov(X)}$ de Galois y $f \in \mathbf{Cov(X)}(p, p)$. Si $y \in Y$, entonces $p(f(y)) = p(y)$, por lo que al ser la acción de $\mathrm{Aut}(p)$ en las fibras de $p$ transitiva, existe $g \in \mathrm{Aut}(p)$ tal que $f(y) = g \cdot y = g(y)$. Como $p \circ f = p = p \circ g$, $X$ es localmente conexo y $Y$ conexo, el Lema 2.5 implica que $f = g$, lo que concluye la prueba. □

Uno de los usos básicos de las aplicaciones cubrientes es el cálculo de grupos de homotopía. Un conocido resultado afirma que para $p : Y \to X \in \mathbf{Cov(X)}$; dados $x \in X$ y $y \in p^{-1}(x)$, se tiene que para cada $n \geq 2$, $\pi_n(p) : \pi_n(Y, y) \to \pi_n(X, x)$ es un isomorfismo. Con las mismas hipótesis, y como consecuencia de PLT, en el caso del grupo fundamental se concluye que $\pi_1(p) : \pi_1(Y, y) \to \pi_1(X, x)$ es un monomorfismo de grupos. Así, en este caso no se puede a priori concluir nada. Sin embargo, se tiene el siguiente resultado.

Proposición 2.22. *Sea $p : Y \to X \in \boldsymbol{Cov(X)}$ de Galois con $X$ y $Y$ localmente conectables por trayectorias. Dados $x_0 \in X$ y $y_0 \in p^{-1}(x_0)$, se tiene una sucesión exacta corta*

$$\{e\} \longrightarrow \pi_1(Y, y_0) \xrightarrow{\pi_1(p)} \pi_1(X, x_0) \longrightarrow \mathrm{Aut}(p) \longrightarrow \{e\}$$

Demostración. Para definir una asignación $\psi : \pi_1(X, x_0) \to \mathrm{Aut}(p)$ se observa que dado $[\alpha] \in \pi_1(X, x_0)$ y $y \in Y$, por la PLT existe una única $\tilde{\alpha} \in Y^I$ tal que $p \circ \tilde{\alpha} = \alpha$ y $\tilde{\alpha}(0) = y$. Nótese que $p\tilde{\alpha}(1) = \alpha(1) = x_0 = \alpha(0) = p\tilde{\alpha}(0) = py$, luego como $p$ es de Galois, existe $f_\alpha \in \mathrm{Aut}(p)$ tal que $f_\alpha(\tilde{\alpha}(1)) = y$. De hecho, como $X$ es localmente conexo y $Y$ es conexo, el Lema 2.5 implica que $f_\alpha$ es el único automorfismo con esta propiedad. Así, se define $\psi([\alpha])(y) = f_\alpha(y)$. Además por el Corolario 2.13 esta asignación es una función y por construcción está bien definida. Para ver que es un morfismo de grupos sean $[\alpha], [\beta] \in \pi_1(X, x_0)$. Dado $y \in Y$, se tiene que $f_{\alpha * \beta} \in \mathrm{Aut}(p)$ es el único automorfismo de $p$ tal que $f_{\alpha*\beta}(\widetilde{(\alpha * \beta)}(1)) = y$ con $\widetilde{\alpha * \beta} \in Y^I$ la única trayectoria tal que $\widetilde{(\alpha * \beta)}(0) = y$ y $p \circ \widetilde{(\alpha * \beta)} = \alpha * \beta$. Así, se tiene que

$$f_\alpha f_\beta(\widetilde{(\alpha * \beta)}(1)) = f_\alpha f_\beta(\tilde{\beta}(1)) = f_\alpha(\tilde{\beta}(0)) = f_\alpha(\tilde{\alpha}(1)) = y,$$

donde la primera igualdad se da pues $\widetilde{\alpha * \beta} = \tilde{\alpha} * \tilde{\beta}$, la segunda por definición de $f_\beta$, la tercera pues $\tilde{\alpha}(1) = \tilde{\beta}(0)$ y la última por definición de $f_\alpha$.

Dado que $f_\alpha \circ f_\beta \in \mathrm{Aut}(p)$, el cálculo anterior prueba que $f_{\alpha*\beta}(y) = (f_\alpha \circ f_\beta)(y)$ y de esto se sigue que $\psi$ es un morfismo de grupos.

Para ver que $\psi$ es un epimorfismo en la categoría de grupos, lo que resta probar es que esta función es suprayectiva. Así, sea $g \in \mathrm{Aut}(p)$. Al ser $Y$ conexo y localmente conectable por trayectorias, $Y$ es conectable por trayectorias. Así, existe $\alpha \in Y^I$ tal que $\alpha(0) = g(y_0)$ y $\alpha(1) = y_0$. Esto implica que $p \circ \alpha \in X^I$ y además como $pg(y_0) = p(y_0) = x_0$, entonces $p \circ \alpha \in \Omega_{x_0}(X)$. Como $\widetilde{p \circ \alpha} = \alpha$, entonces $g(\widetilde{(p \circ \alpha)}(1)) = g(\alpha(1)) = g(y_0)$ y $f_{p\circ\alpha}(\widetilde{(p \circ \alpha)}(1)) = \alpha(0) = g(y_0)$. Como $X$ es localmente conexo y $Y$ conexo, el Lema 2.5 implica que $g = f_{p\circ\alpha}$, lo que muestra la suprayectividad de $\psi$.

Lo que resta probar es la exactitud en $\pi_1(X, x_0)$. Así, dado $[\beta] \in \pi_1(Y, y_0)$, se tiene que $\psi\pi_1(p)([\beta]) = \psi([p \circ \beta])$. Como $\widetilde{p \circ \beta} = \beta$, entonces $f_{p\circ\beta}(y_0) = y_0$, lo que implica por el Lema 2.5 que $f_{p\circ\beta} = 1_Y$, y así $\mathrm{im}(\pi_1(p)) \subseteq \mathrm{nuc}(\psi)$. Respecto a la otra contención sea $[\alpha] \in \mathrm{nuc}(\psi)$. Por la PLT existe una única $\tilde{\alpha} \in Y^I$ tal que $\tilde{\alpha}(0) = y_0$ y $p \circ \tilde{\alpha} = \alpha$. Además, la hipótesis dice que $\psi([\alpha]) = 1_Y$, lo que implica que $f_\alpha = 1_Y$ y dado que $f_\alpha(\tilde{\alpha}(1)) = y_0$, se concluye que $\tilde{\alpha}(1) = y_0$ y así, $\tilde{\alpha} \in \Omega_{y_0}(Y)$. Para concluir, $\pi_1(p)([\tilde{\alpha}]) = [p \circ \tilde{\alpha}] = [\alpha]$, lo que prueba que $[\alpha] \in \mathrm{im}(\pi_1(p))$ y termina la prueba. $\square$

El siguiente resultado justifica por completo el nombre de estas aplicaciones cubrientes tan especiales. Este puede considerarse como el análogo a la versión de Krull del TFTG, pero para aplicaciones cubrientes. Para su formulación sean $\mathrm{Sub}(\mathrm{Aut}(p))$ la retícula de subgrupos de $\mathrm{Aut}(p)$ y SCov(p) el conjunto de clases de isomorfismo de aplicaciones cubrientes sobre $X$ tales que $p$ se factoriza a través de estas.

TEOREMA 2.23. *(Correspondencia de Galois para aplicaciones cubrientes)* *Sea $p : Y \to X \in$ **Cov(X)** de Galois. Dado un subgrupo $H \subseteq \mathrm{Aut}(p)$, $p$ induce una aplicación cubriente canónica $\overline{p}_H : Y/H \to X$. Por otro lado, si $q : Z \to X \in$ **Cov(X)** con $Z$ conexo tal que existe $f$ continua que hace conmutar el siguiente diagrama*

$$\begin{tikzcd}
Y \arrow[rr, "p"] \arrow[dr, "f"'] & & X \\
& Z \arrow[ur, "q"'] &
\end{tikzcd}$$

*entonces* $f \in$ ***Cov(Z)*** *de Galois y* $Z \cong Y/H$ *para algún subgrupo* $H \subseteq \mathrm{Aut}(p)$.

*Así, las funciones*

$$\begin{aligned} \overline{p}_{\_} : \mathrm{Sub}(\mathrm{Aut}(p)) &\to \mathrm{SCov(p)} \\ H &\mapsto (\overline{p}_H : Y/H \to X) \end{aligned}$$

$$\begin{aligned} \mathrm{Aut}(\_) : \mathrm{SCov(p)} &\to \mathrm{Sub}(\mathrm{Aut}(p)) \\ (q : Z \to X) &\mapsto \mathrm{Aut}(q) \end{aligned}$$

*son mutuamente inversas.*

*Además,* $q : Z \to X \in$ ***Cov(X)*** *es de Galois si y sólo si* $\mathrm{Aut}(f)$ *es un subgrupo normal de* $\mathrm{Aut}(p)$ *y* $\mathrm{Aut}(p)/\mathrm{Aut}(f) \cong \mathrm{Aut}(q)$.

Demostración. La primera afirmación se sigue que $p = \overline{p}_H \circ p_H$, $p$ es una aplicación cubriente y $p_H$ un homeomorfismo local.

Respecto a la segunda afirmación sea $f$ como en las hipótesis. Como $Y$ es conexo, $X$ localmente conexo y $q \circ f$ es una aplicación cubriente, el Lema 2.6 implica que $f \in$ **Cov(Z)**. Dado que $Y$ es conexo, para ver que $f$ es de Galois, por la Proposición 2.20 se puede probar que $\mathrm{Aut}(f)$ actúa de manera transitiva en una fibra de $f$. En efecto, dado $z \in Z$, se consideran $y_0, y_1 \in f^{-1}(z)$. Como para todo $i \in \{0,1\}$, $p(y_i) = qf(y_i) = q(z) \in X$, dado que $p$ es de Galois, existe $g \in \mathrm{Aut}(p)$ tal que $g(y_0) = y_1$. Si se prueba que $g \in \mathrm{Aut}(f)$, esto concluye la afirmación. En efecto, nótese que $f \circ g, f : Y \to Z$, $Y$ es conexo y $q \circ (f \circ g) = p \circ g = p = q \circ f$. Además, $(f \circ g)(y_0) = f(y_1) = z = f(y_0)$. Luego, como $X$ es localmente conexo, por el Lema 2.5 se concluye que $f \circ g = f$, lo que prueba la afirmación.

Dado que $f$ es de Galois, entonces $\overline{f}_{\mathrm{Aut}(f)} : Y/\mathrm{Aut}(f) \to Z$ es un homeomorfismo, de lo que se deduce que $Z \cong Y/\mathrm{Aut}(f)$ y además, claramente $\mathrm{Aut}(f) \subseteq \mathrm{Aut}(p)$ es un subgrupo.

La parte de que las funciones dadas son mutuamente inversas es análoga a lo que se hizo en la prueba del Teorema 1.2.

Para la última afirmación, respecto a la ida sean $g \in \mathrm{Aut}(p)$ y $h \in \mathrm{Aut}(f)$. Si $y \in Y$, entonces $pg(y) = p(y)$. Esto implica que $q(fg(y)) = q(f(y)) \in X$, por lo que al ser $q$ de Galois, existe $l \in \mathrm{Aut}(q)$ tal que $l(f(y)) = fg(y)$. Además, se observa que $f \circ g, l \circ f : Y \to Z$ y que $Y$ es conexo, luego, el Lema 2.5 implica que $f \circ g = l \circ f$. Más aún, el Lema 2.5 permite concluir que de hecho existe una única

$l \in \operatorname{Aut}(q)$ con la propiedad de que $f \circ g = l \circ f$, lo que dice que se tiene una función $\varphi : \operatorname{Aut}(p) \to \operatorname{Aut}(q)$. Más aún es claro que esta es un morfismo de grupos y es claro que $\operatorname{nuc}(\varphi) = \operatorname{Aut}(f)$. Esto muestra que $\operatorname{Aut}(f) \trianglelefteq \operatorname{Aut}(p)$ y además que existe un morfismo de grupos inyectivo $\overline{\varphi} : \operatorname{Aut}(p)/\operatorname{Aut}(f) \to \operatorname{Aut}(q)$. Dado que $f$ y $p$ son de Galois $Y/\operatorname{Aut}(f) \cong Z$ y $Y/\operatorname{Aut}(p) \cong X$, de donde

$$Z/(\operatorname{Aut}(p)/\operatorname{Aut}(f)) \cong (Y/\operatorname{Aut}(f))/(\operatorname{Aut}(p)/\operatorname{Aut}(f)) \cong Y/\operatorname{Aut}(p) \cong X.$$

Por la biyección esto implica que $\operatorname{Aut}(p)/\operatorname{Aut}(f) \cong \operatorname{Aut}(q)$ pues $q$ es de Galois.

Respecto al regreso de la afirmación al ser $f$ de Galois, $Y/\operatorname{Aut}(f) \cong Z$ y así se tiene que $Z/\operatorname{Aut}(q) \cong (Y/\operatorname{Aut}(f))/(\operatorname{Aut}(p)/\operatorname{Aut}(f)) \cong Y/\operatorname{Aut}(p) \cong X$, donde el último homeomorfismo se da pues $p$ es de Galois. □

El siguiente resultado da uno de los ejemplos más importantes de cubrientes de Galois.

PROPOSICIÓN 2.24. *Sea $X$ conexo, localmente conexo y localmente simplemente conexo. Entonces,*

1. *La aplicación cubriente $p_x : \tilde{\mathrm{X}}_{\mathrm{x}} \to X$ es un cubriente de Galois tal que* $\operatorname{Aut}(p_x) \cong \pi_1(\mathrm{X}, \mathrm{x})^{op}$.
2. *Para cada $p : Y \to X \in$ **Cov(X)**, la acción izquierda de* $\operatorname{Aut}(p_x)^{op}$ *en* $\operatorname{Fib}_{\mathrm{x}}(p)$ *dada en la Observación 2.18 corresponde a la acción de monodromía.*

DEMOSTRACIÓN. Para la primera afirmación, dado que $\tilde{\mathrm{X}}_{\mathrm{x}}$ es conexo, por la Proposición 2.20, la afirmación es equivalente a probar que dado $x \in X$, $\operatorname{Aut}(p_x)$ actúa de forma transitiva en $p_x^{-1}(x)$. En efecto, si $[\sigma], [\tau] \in p_x^{-1}(x)$, por representabilidad del funtor $\operatorname{Fib}_{\mathrm{x}}$, existen morfismos de aplicaciones cubrientes $p_{[\sigma]}, p_{[\tau]} \in \mathbf{Cov(X)}(p_x, p_x)$ tales que $p_{[\sigma]}([c_x]) = [\sigma]$ y $p_{[\tau]}([c_x]) = [\tau]$. Nótese que dado $[\sigma'] \in p_{[\sigma]}^{-1}([c_x])$, se tiene que $p_x p_{[\sigma]}([\sigma']) = p_x([c_x]) = x$, lo que dice que $[\sigma'] \in (p_x \circ p_{[\sigma]})^{-1}(x)$. Luego, como $p_x \circ p_{[\sigma]} : \tilde{\mathrm{X}}_{\mathrm{x}} \to X$ es una aplicación cubriente, la representabilidad del funtor $\operatorname{Fib}_{\mathrm{x}}$ implica que existe un único $p_{[\sigma']} \in \mathbf{Cov(X)}(p_x, p_x \circ p_{[\sigma]})$ tal que $p_{[\sigma']}([c_x]) = [\sigma']$. Ahora se observa que $(p_{[\sigma]} \circ p_{[\sigma']})([c_x]) = p_{[\sigma]}([\sigma']) = [c_x]$ y que $p_x \circ (p[\sigma] \circ p_{[\sigma']}) = p_x$. Luego, como $X$ localmente conexo y $\tilde{\mathrm{X}}_{\mathrm{x}}$ conexo, el Lema 2.5 implica que $p_{[\sigma]} \circ p_{[\sigma']} = 1_{\tilde{\mathrm{X}}_{\mathrm{x}}}$, de donde $p_{[\sigma']}$ es un homeomorfismo y por lo tanto $p_{[\sigma]} \in \operatorname{Aut}(p_x)$. Además se observa que el argumento anterior dependió simplemente de que $[\sigma] \in p_x^{-1}(x)$, lo que implica que $p_{[\tau]} \in \operatorname{Aut}(p_x)$. Así, $p_{[\tau]} p_{[\sigma]}^{-1}([\sigma]) = p_{[\tau]}([c_x]) = [\tau]$, lo que prueba la transitividad de la acción.

Para ver que $\mathrm{Aut}(p_x) \cong \pi_1(\mathrm{X},\mathrm{x})^{op}$, nótese que la acción de la Observación 2.16 da lugar a un morfismo de grupos $\rho : \pi_1(\mathrm{X},\mathrm{x})^{op} \to \mathrm{Aut}(\tilde{\mathrm{X}}_{\mathrm{x}})$. Lo primero que se observa es que de hecho el codominio puede restringirse a $\mathrm{Aut}(p_x)$ pues para $[\alpha] \in \pi_1(\mathrm{X},\mathrm{x})$ y $[\sigma] \in \tilde{\mathrm{X}}_{\mathrm{x}}$, $p_x\rho([\alpha])([\sigma]) = p_x([\alpha * \sigma]) = (\alpha * \sigma)(1) = \sigma(1) = p_x([\sigma])$. Así, abusando de la notación se tiene un morfismo $\rho : \pi_1(\mathrm{X},\mathrm{x})^{op} \to \mathrm{Aut}(p_x)$. Luego, para probar la afirmación se va a ver que este es un isomorfismo, pero en la categoría de grupos esto es equivalente a probar que es inyectivo y suprayectivo.

Respecto a la inyectividad se va a ver que $\rho$ tiene núcleo trivial. Para esto sea $[\alpha] \in \mathrm{nuc}(\rho)$. Así, $\rho([\alpha]) = 1_{\tilde{\mathrm{X}}_{\mathrm{x}}}$, por lo que al evaluar en $[c_x] \in \tilde{\mathrm{X}}_{\mathrm{x}}$ se tiene que $[\alpha] = [\alpha * c_x] = [c_x]$, de donde se tiene el resultado deseado.

En lo que concierne a la suprayectividad sea $f \in \mathrm{Aut}(p_x)$. Así, $f([c_x]) \in \tilde{\mathrm{X}}_{\mathrm{x}}$, por lo que existe $\sigma \in X^I$ con $\sigma(0) = x$, tal que $f([c_x]) = [\sigma]$. Dado que $\sigma(1) = p_x([\sigma]) = p_x f([c_x]) = p_x([c_x]) = c_x(1) = x$, entonces $\sigma \in \Omega_x(X)$. Así, se considera $\rho([\sigma]) \in \mathrm{Aut}(p_x)$ y se afirma que $\rho([\sigma]) = f$. En efecto, lo primero que se observa es que $\rho([\sigma])([c_x]) = [\sigma * c_x] = [\sigma] = f([c_x])$. También que $p_x \circ \rho[\sigma] = p_x = p_x \circ f$ y, dado que $\tilde{\mathrm{X}}_{\mathrm{x}}$ es conexo y localmente conexo, por el Lema 2.5 se concluye que $\rho[\sigma] = f$.

Para la última afirmación se observa que la acción derecha de la Observación 2.18 $p^{-1}(x) \times \mathrm{Aut}(p_x) \to p^{-1}(x)$ es equivalente a la acción izquierda $\mathrm{Aut}(p_x)^{op} \times p^{-1}(x) \to p^{-1}(x)$ dada por $(g, y) \mapsto y \cdot g$. Además, por el isomorfismo demostrado esta es equivalente a una acción $\pi_1(\mathrm{X},\mathrm{x}) \times p^{-1}(x) \to p^{-1}(x)$ definida mediante $[\alpha] \cdot y = \rho([\alpha]) \cdot y := \varphi_p^{-1}(p_y \circ \rho([\alpha]))$. Así, lo que se tiene que probar es que $\tilde{\alpha}(1) = \varphi_p^{-1}(p_y \circ \rho([\alpha]))$ con $\tilde{\alpha} \in Y^I$ la única trayectoria tal que $p \circ \tilde{\alpha} = \alpha$ y $\tilde{\alpha}(0) = y$. De hecho nótese que la igualdad que se quiere es equivalente a probar que $p_{\tilde{\alpha}(1)} = p_y \circ \rho([\alpha])$. Así, como ambas son funciones con dominio $\tilde{\mathrm{X}}_{\mathrm{x}}$ y codominio $Y$, $p \circ (p_y \circ \rho([\alpha])) = p \circ p_{\tilde{\alpha}(1)}$, $(p_y \circ \rho([\alpha]))([c_x]) = p_y([\alpha * c_x]) = p_y([\alpha]) = \tilde{\alpha}(1) = p_{\tilde{\alpha}(1)}([c_x])$. El hecho de que $\tilde{\mathrm{X}}_{\mathrm{x}}$ es conexo y $X$ localmente conexo implican por el Lema 2.5 la igualdad que se quiere. □

La interpretación de los resultados probados en esta sección tiene como consecuencia directa la prueba del siguiente importante resultado.

Teorema 2.25. *Sea $X$ conexo, localmente conexo y localmente simplemente conexo. El funtor* $\mathrm{Fib}_{\mathrm{x}}$ *es una equivalencia de categorías. En esta equivalencia los cubrientes conexos corresponden a* $\pi_1(\mathrm{X},\mathrm{x})$*-conjuntos con acción transitiva y los cubrientes de Galois a cocientes por un subgrupo normal.*

Demostración. Para ver que este funtor es una equivalencia de categorías se va a ver que este es fiel, pleno y esencialmente suprayectivo.

Para ver que es fiel y pleno sean $p : Y \to X, q : Z \to X \in \mathbf{Cov(X)}$. Además, puede suponerse sin pérdida de generalidad que $Y$ y $Z$ son conexos. Luego, sea $f \in \pi_1(X,x) - \mathbf{Set}(\mathrm{Fib_x}(p), \mathrm{Fib_x}(q))$. Al considerar $y \in p^{-1}(x)$, tómese el morfismo $p_y : \tilde{X}_x \to Y$ correspondiente usando la representabilidad del funtor $\mathrm{Fib_x}$. Al usar el teorema de correspondencia de Galois para aplicaciones cubrientes, $p_y$ induce un isomorfismo $f_y : Y \to \tilde{X}_x/H$, donde $H = \mathrm{Aut}(p_y)$, que es el estabilizador de $y$. Como $f$ define una función inyectiva de $H$ en el estabilizador de $f(y)$, el morfismo $p_{f(y)} : \tilde{X}_x \to Z$ induce un morfismo $\tilde{X}_x/H \to Z$, por lo que al componer este con $f_y$ se obtiene una función continua $Y \to Z$ tal que al aplicar $\mathrm{Fib_x}$ se obtiene $f$.

La suprayectividad esencial puede nuevamete tratarse sin pérdida de generalidad para el caso conexo, y esta es sencilla pues del resultado anterior uno de tales cubrientes se obtiene como el cociente de $\tilde{X}_x$ con el estabilizador de un punto. Además, las correspondencias dadas en la equivalencia se obtienen nuevamente del resultado anterior claramente. □

Además, también se tiene el siguiente resultado inmediato del anterior.

Corolario 2.26. *Con las mismas hipótesis del teorema anterior, el funtor* $\mathrm{Fib_x}$ *induce una equivalencia entre las categorías de aplicaciones cubrientes finitas sobre* $X$, ***FCov(X)***, *y la categoría de conjuntos finitos con la topología discreta y una acción continua de* $\pi_1(\hat{X},x)$. *En esta equivalencia las aplicaciones cubrientes conexas corresponden a* $\pi_1(\hat{X},x)$*-conjuntos finitos con acción transitiva y las aplicaciones cubrientes de Galois a cocientes por subgrupos abiertos y normales.*

Demostración. Es claro del resultado anterior notando que los elementos en $\mathbf{FCov(X)}$ tienen fibras finitas y discretas; observación que aunada al hecho de que las categorías $G - \mathbf{FSet}$ y $\hat{G} - \mathbf{FSet}$ son isomorfas si $G$ es discreto, dan el resultado que se busca al considerar el caso particular de $G = \pi_1(X,x)$. □

## 4. Ejemplos

Se recuerda que para $X$ un espacio topológico conectable por trayectorias dados $x_0, x_1 \in X$, $\pi_1(X,x_0) \cong \pi_1(X,x_1)$. Así, en tal caso no hay ambigüedad al escribir $\pi_1(X)$ para el grupo fundamental del espacio $X$ con cualquier punto base.[2]

[2]Ver el final de la Sección 2.5.

EJEMPLO 2.27. *Considérese una aplicación cubriente trivial $p_1 : X \times F \to X$. Nótese que si $|F| \geq 2$, entonces $X \times F$ no puede ser conexo, luego, esta aplicación no es en general de Galois. Además se observa que $f \in \mathrm{Aut}(p_1)$ si y sólo si $f = 1_X \times \overline{f}$ con $\overline{f} : F \to F$ un homeomorfismo. Sin embargo, al ser $F$ discreto, esta última condición es equivalente a que $\overline{f} : F \to F$ sea biyectiva. Esto prueba que $\mathrm{Aut}(p_1) \cong S_F$, el grupo de permutaciones sobre $F$. Es claro que la acción de $\mathrm{Aut}(p_1)$ en $F$ es transitiva.*

EJEMPLO 2.28. *Sea $n \in \mathbb{N}^+$. Considérese la acción de $\mathbb{Z}^n$ en $\mathbb{R}^n$ dada por traslación. Esta acción es continua y de hecho es propiamente discontinua. Así, por la Proposición 2.9 se concluye que $\pi_{\mathbb{Z}^n} : \mathbb{R}^n \to \mathbb{R}^n/\mathbb{Z}^n$ es una aplicación cubriente con $\mathrm{Aut}(\pi_{\mathbb{Z}^n}) \cong \mathbb{Z}^n$ y multiplicidad infinita numerable. Dado que $\mathbb{R}^n/\mathbb{Z}^n \cong \mathbb{T}^n$, el $n$-toro, esto dice que de hecho $\mathbb{Z}^n$ es una retícula geométrica en $\mathbb{R}^n$. Además, la aplicación cociente es de Galois pues $\mathbb{R}^n$ es cubriente universal de $\mathbb{T}^n$ ya que $\mathbb{T}^n$ es conectable por trayectorias y simplemente conexo, así como $\mathbb{R}^n$ es simplemente conexo. Así, por la Proposición 2.22 aunada al hecho de que $\pi_1(\mathbb{R}^n) = 0$, se concluye que $\pi_1(\mathbb{T}^n) \cong \mathbb{Z}^n$.*

EJEMPLO 2.29. *Sea $n \in \mathbb{N}^+$. La acción antípoda $\mathbb{Z}/2\mathbb{Z} \times \mathbb{S}^n \to \mathbb{S}^n$ es propiamente discontinua pues es una acción de un grupo discreto en un espacio Hausdorff sin puntos fijos. Así, por la Proposición 2.9 se concluye que $\pi_{\mathbb{Z}/2\mathbb{Z}} : \mathbb{S}^n \to \mathbb{S}^n/(\mathbb{Z}/2\mathbb{Z})$ es una aplicación cubriente con dos hojas y $\mathrm{Aut}(\pi_{\mathbb{Z}/2\mathbb{Z}}) \cong \mathbb{Z}/2\mathbb{Z}$. Esta aplicación es de Galois pues es el cubriente universal de $\mathbb{RP}^n \cong \mathbb{S}^n/(\mathbb{Z}/2\mathbb{Z})$. Dado que para $n \geq 2$, $\pi_1(S^n) = 0$, entonces la Proposición 2.22 implica que $\pi_1(\mathbb{RP}^n) \cong \mathbb{Z}/2\mathbb{Z}$. En el caso de $n = 1$ dicha proposición se convierte en un problema de extensión $Ext^1_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$. Pero como $\mathbb{RP}^1 \cong \mathbb{S}^1$, en este caso el ejemplo anterior permite concluir que $\pi_1(\mathbb{RP}^1) \cong \mathbb{Z}$.*

EJEMPLO 2.30. *Considérese la acción de $\mathbb{Z}$ en $\mathbb{R}^2$ definida por $n \cdot (x_1, x_2) = (x_1 + n, (-1)^n x_2)$. Esta es la acción de un grupo discreto que es propiamente discontinua. Así, la Proposición 2.9 implica que $\pi_{\mathbb{Z}} : \mathbb{R}^2 \to \mathbb{R}^2/\mathbb{Z}$ es una aplicación cubriente con multiplicidad numerable y $\mathrm{Aut}(\pi_{\mathbb{Z}}) \cong \mathbb{Z}$. Se recuerda que puede probarse que en este caso $\mathbb{R}^2/\mathbb{Z} \cong E(\gamma_1^1)$, donde $E(\gamma_1^1)$ es la banda de Möbius abierta. Además, esto es un cubriente universal, por lo que esta aplicación es de Galois. Dado que $\pi_1(\mathbb{R}^2) \cong 0$, la Proposición 2.22 implica que $\pi_1(E(\gamma_1^1)) \cong \mathbb{Z}$.*

Ejemplo 2.31. *Considérense las transformaciones rigidas* $T, S : \mathbb{R}^2 \to \mathbb{R}^2$ *cuya regla de correspondencia son* $T(x_1, x_2) = (x_1 + 1, x_2)$ *y* $S(x_1, x_2) = (-x_1, x_2 + 1)$. *Sea* $G$ *el subgrupo de* $E(2)$, *el grupo de transformaciones rigidas de* $\mathbb{R}^2$, *generado por* $T$ *y* $S$. *Nótese que* $G$ *actúa en* $\mathbb{R}^2$ *de manera propiamente discontinua. Así,* $\pi_G : \mathbb{R}^2 \to \mathbb{R}^2/G$ *es una aplicación cubriente con multiplicidad* $|G|$ *y* $\mathrm{Aut}(\pi_G) \cong G$. *Puede probarse que* $\mathbb{R}^2/G \cong K$, *la botella de Klein, y por lo tanto de la Proposición 2.22 se tiene que* $\pi_1(K) \cong G$.

Ejemplo 2.32. *Sea* $p : \mathbb{C} \to \mathbb{C}^\times$ *la función exponencial compleja* $p(z) = e^z$. *Esta es una aplicación cubriente con multiplicidad infinita numerable. Se observa que si* $f \in \mathrm{Aut}(p)$, *entonces* $e^{f(0)} = pf(0) = p(0) = 1$, *lo que implica que existe un único* $n \in \mathbb{Z}$ *tal que* $f(0) = 2\pi i n$. *Así,* $\mathrm{Aut}(p) \cong \mathbb{Z}$. *Esta aplicación cubriente es claramente de Galois pues la acción en una fibra siempre es transitiva. Por otro lado, la proposición 2.22 aunada al hecho de que* $\pi_1(\mathbb{C}) = 0$ *implican que* $\pi_1(\mathbb{C}^\times) \cong \mathbb{Z}$.

Ejemplo 2.33. *Para* $n \in \mathbb{N}^+$, *sea* $p : \mathbb{C}^\times \to \mathbb{C}^\times$ *la función elevar a la* $n$. *Esta resulta ser una aplicación cubriente de* $n$ *hojas que es una aplicación de Galois. En este caso es sencillo probar que* $\mathrm{Aut}(p) \cong \mathbb{Z}/n\mathbb{Z}$.

## 5. Dos caracterizaciones para Cov(X)

La motivación de esta sección es caracterizar de dos formas la categoría de aplicaciones cubrientes sobre un espacio con ciertas hipótesis de conexidad sobre la base.

**5.1. Caracterización con gavillas.** Un conocido resultado dice que la categoría de gavillas sobre un espacio topológico $X$ es equivalente a la categoría de homeomorfismos locales sobre dicho espacio (ver por ejemplo el Capítulo 2 de [**MM**, pp 90]). En la primera proposición de este capítulo se mencionó que toda aplicación cubriente sobre $X$ es un homeomorfismo local sobre dicho espacio, así que una pregunta natural es si se puede caracterizar la categoría de aplicaciones cubrientes con una subcategoría de la categoría de gavillas. La respuesta a esta pregunta afirmativa y se tratará en esta sección.

En lo que sigue $\mathcal{O}(X)$ denota la categoría de abiertos del espacio $X$. La categoría de gavillas sobre $X$ se denota por **Sh(X)**.

Definición 2.34.

1. *Si $F$ es un espacio discreto, la gavilla de funciones continuas con valores en $F$, $\mathcal{C}(\_, F) : \mathcal{O}(X)^{op} \to$ **Set**, se conoce como **gavilla constante**.*
2. *$\mathcal{F} \in$ **Sh(X)** es **localmente constante**, si para cada $x \in X$ existe $U \subseteq X$ vecindad abierta de $x$ e $I_x$ un espacio discreto, tales que $\mathcal{F}|_U$ es isomorfo a $\mathcal{C}(\_, I_x)|_U$, como gavillas sobre $U$.*

Para $p : Y \to X \in \mathbf{Top}/X$ sea $\Gamma_p : \mathcal{O}(X)^{op} \to \mathbf{Set}$ el funtor que a nivel de objetos se define mediante $\Gamma_p(U) := \{s : U \to Y \mid s \text{ es continua y } p \circ s = 1_U\}$ y, en morfismos como la restricción al abierto más pequeño. Como las funciones continuas satisfacen la "condición de pegado", es sencillo ver que $\Gamma_p \in$ **Sh(X)**, y a esta se le conoce como la **gavilla de secciones (transversales)** de $p$. De hecho se tiene el siguiente resultado.

Proposición 2.35. *Sea $p : Y \to X \in$ **Top**$/X$ con $X$ localmente conexo. Entonces,*

1. *Si $p \in$ **Cov(X)**, entonces $\Gamma_p$ es localmente constante.*
2. *Si $p \in$ **Cov(X)**, entonces $\Gamma_p$ es constante si y sólo si $p$ es trivial.*

Demostración. Respecto a la primera afirmación sea $x \in X$. La Proposición 2.4 implica que existe $V \subseteq X$ una vecindad abierta de $x$ tal que $p^{-1}(V) \cong V \times I$ con $I \in \mathbf{Top}$ discreto. Así, se afirma que $\Gamma_p|_V \cong \mathcal{C}(\_, I)|_V$ como gavillas sobre $V$.

En efecto, dado $U \in \mathcal{O}(X)$ se define $\psi_U : \Gamma_p(U \cap V) \to \mathcal{C}(U \cap V, I)$, donde para $s \in \Gamma_p(U \cap V)$, $\psi_U(s) = \pi_2 \circ f \circ s$, con $\pi_2 : V \times I \to I$ la proyección en la segunda coordenada y $f : p^{-1}(V) \to V \times I$ un homeomorfismo en $\mathbf{Top}/V$. Para ver que esta función es un isomorfismo en **Set** se va a probar que esta es inyectiva y suprayectiva. Para la inyectividad, dadas $s, t \in \Gamma_p(U \cap V)$ tales que $\psi_U(s) = \psi_U(t)$, es decir, $\pi_2 \circ f \circ s = \pi_2 \circ f \circ t$, se observa que $\pi_1 \circ f \circ s = p \circ s = 1_{U \cap V} = p \circ t = \pi_1 \circ f \circ t$, por lo que de la propiedad universal del producto $f \circ s = f \circ t$. Además, $f$ es un homeomorfismo, luego $s = t$. Respecto a la suprayectividad, sea $g \in \mathcal{C}(U \cap V, I)$. Considérese la función inducida por la propiedad universal del producto topológico $(\iota, g) : U \cap V \to V \times I$, donde $\iota : U \cap V \to V$ es la inclusión. Luego, $f^{-1} \circ (\iota, g) : U \cap V \to p^{-1}(V) \subseteq Y$ es una función continua. Además, $p \circ (f^{-1} \circ (\iota, g)) = \pi_1(\iota, g) = \iota$, lo que dice que $f^{-1} \circ (\iota, g) \in \Gamma_p(U \cap V)$ y también $\psi_U(f^{-1} \circ (\iota, g)) = \pi_2 \circ f \circ (f^{-1} \circ (\iota, g)) = g$.

Lo único que resta ver en esta parte es la naturalidad del isomorfismo. Sin embargo esto es claro pues las restricciones son restricciones de funciones de conjuntos.

Para la segunda afirmación la ida es consecuencia de que una aplicación cubriente con una sección global es un homeomorfismo, así $p$ es trivial. El regreso es claro pues si $p = p_1 : X \times I \to X$ una aplicación cubriente trivial, un argumento análogo al de la primera parte para $V = X$ prueba que $\Gamma_p \cong \mathcal{C}(\_, I)$. □

La proposición anterior se puede interpretar diciendo que existe una asignación a nivel de objetos entre las categorías de aplicaciones cubrientes sobre $X$ y de gavillas localmente constantes sobre dicho espacio. Para ver que esta asignación es funtorial se observa que si $f \in \mathbf{Cov(X)}(p, q)$, entonces $\Gamma(f) : \Gamma_p \to \Gamma_q$ se define para que en cada $U \subseteq X$ abierto, $\Gamma(f)_U(s) = f \circ s$. Es muy sencillo ver que $\Gamma_p(f)$ es una transformación natural y que de hecho esta $\Gamma$ da lugar a un funtor de la categoría de aplicaciones cubrientes sobre $X$ a la categoría de gavillas localmente constantes sobre $X$, la que se va a denotar mediante $\mathbf{LCSh(X)}$. Lo que se va a probar es que cuando $X$ es un espacio localmente conexo, el funtor definido es una equivalencia, y para probar esto se va a construir un funtor en la otra dirección.

Definición 2.36. *Sea $\mathcal{F} \in$ **Sh(X)**. Dado $x \in X$, se define el **tallo** de $\mathcal{F}$ en $x$ como el conjunto $\mathcal{F}_x = \varinjlim_{U \in \mathcal{O}(X)\ x \in U} \mathcal{F}(U)$.*

Al ser el tallo un colímite, la propiedad universal de este le da carácter funtorial a esta construcción. Por otro lado, la categoría $\mathcal{O}(X)$ es filtrante, así que en este caso es un resultado general de la teoría de categorías que se puede dar otra caracterización como objeto al tallo de $\mathcal{F}$ en $x$ como sigue:

$$\mathcal{F}_x = \coprod_{U \in \mathcal{O}(X)\ x \in U} \mathcal{F}(U)/\sim,$$

donde $(s \in \mathcal{F}(U)) \sim (t \in \mathcal{F}(V))$ si existe $W \in \mathcal{O}(X)$ con $x \in W$ y $W \subseteq U \cap V$, tal que $s|_W = t|_W$.

Así, un elemento en $\mathcal{F}_x$ es una clase de equivalencia $[s \in \mathcal{F}(U)]_x$ para $U \in \mathcal{O}(X)$ con $x \in U$, y a estos de les conoce como **gérmenes** en $x$. Entonces sea $X_{\mathcal{F}} = \coprod_{x \in X} \mathcal{F}_x$ y nótese que se tiene una función canónica $p_{\mathcal{F}} : X_{\mathcal{F}} \to X$ definida mediante $p_{\mathcal{F}}([s \in \mathcal{F}(U)]_x) = x$.

Para dar una topología a $X_{\mathcal{F}}$, se observa que para $U \in \mathcal{O}(X)$ y $s \in \mathcal{F}(U)$, se puede definir una función $\tilde{s} : U \to X_{\mathcal{F}}$ mediante $\tilde{s}(x) = [s \in \mathcal{F}(U)]_x$.

Proposición 2.37. *La familia $\{\tilde{s}(U) \mid U \in \mathcal{O}(X),\ s \in \mathcal{F}(U)\}$ satisface los axiomas de una base para la topología de $X_{\mathcal{F}}$. Con esta topología $p_{\mathcal{F}}$ es continua así como cada función $\tilde{s}$. Más aún, estas son secciones de $p_{\mathcal{F}}$.*

Demostración. Para la primera afirmación sean $U, V \in \mathcal{O}(X)$, $s \in \mathcal{F}(U)$ y $t \in \mathcal{F}(V)$ tales que $\tilde{s}(U) \cap \tilde{t}(V) \neq \emptyset$. Luego, existe $x \in U \cap V$ tal que $[s \in \mathcal{F}(U)]_x = [t \in \mathcal{F}(V)]_x$. Por definición esta igualdad implica que existe $W \in \mathcal{O}(X)$ con $W \subseteq U \cap V$ y $x \in W$ tal que $s|_W = t|_W$. Así es claro que $(\widetilde{s|_W})(W) \subseteq \tilde{s}(U) \cap \tilde{t}(V)$ y $[s \in \mathcal{F}(U)]_x \in (\widetilde{s|_W})(W)$, lo que prueba la afirmación.

Para ver que $p_{\mathcal{F}}$ es continua sea $U \subseteq X$ un abierto no vacío. Si $[s \in \mathcal{F}(U)]_x \in \mathcal{F}(U)$, entonces se tiene que $\tilde{s}(U) \subseteq p_{\mathcal{F}}^{-1}(U)$ y que $[s \in \mathcal{F}(U)]_x \in \tilde{s}(U)$, lo que prueba que $p_{\mathcal{F}}^{-1}(U) \subseteq X_{\mathcal{F}}$ es un abierto.

Para concluir, si $U \in \mathcal{O}(X)$ y $s \in \mathcal{F}(U)$, para ver que $\tilde{s} : U \to X_{\mathcal{F}}$ es continua sea $t \in \mathcal{F}(V)$ con $V \in \mathcal{O}(X)$. Dado que $x \in \tilde{s}^{-1}(\tilde{t}(V))$ si y sólo si $x \in V$ y $[s \in \mathcal{F}(U)]_x = [t \in \mathcal{F}(V)]_x$, y esto último es equivalente a decir que existe $W \in \mathcal{O}(X)$ con $W \subseteq U \cap V$ y $x \in W$ tales que $s|_W = t|_W$, se tiene que $W \subseteq \tilde{s}^{-1}(\tilde{t}(V))$, por lo que $\tilde{s}^{-1}(\tilde{t}(V)) \subseteq U$ es abierto.

Además es claro que para $s \in \mathcal{F}(U)$, $p_{\mathcal{F}} \circ \tilde{s} = 1_U$. □

La proposición anterior dice que se tiene una asignación a nivel de objetos entre las categorías **Sh(X)** y **Top** $/X$.

Proposición 2.38. *Si $\mathcal{F} \in$ **Sh(X)** es localmente constante con $X$ localmente conexo, entonces $p_{\mathcal{F}} \in$ **Cov(X)**. Además, esta asignación da lugar a un funtor $\Lambda :$ **LCSh(X)** $\to$ **Cov(X)**.*

Demostración. Supóngase que $\mathcal{F} \in$ **Sh(X)** es localmente constante. Como $X$ es localmente conexo, dado $x \in X$ existe $V \subseteq X$ vecindad abierta y conexa de $x$ tal que $\mathcal{F}|_V \cong \mathcal{C}(\_, I)|_V$ como gavillas sobre $V$ con $I \in$ **Top** discreto. Dado que $p_{\mathcal{F}}^{-1}(V) = \coprod_{x \in V} \mathcal{F}_x$ y como para $x \in V$ se tiene que $\mathcal{F}_x \cong I$, entonces $p_{\mathcal{F}}^{-1}(V) \cong \coprod_{x \in V} I \cong V \times I$, que por la Proposición 2.4 implica que $p_{\mathcal{F}}$ es una aplicación cubriente.

Respecto a la funtorialidad nótese que la primera parte de esta proposición es la asignación a nivel de objetos. En lo que respecta a morfismos sea $\varphi : \mathcal{F} \to \mathcal{G}$ una transformación natural con $\mathcal{F}, \mathcal{G} \in$ **LCSh(X)**. Así, para definir $\Lambda(\varphi) \in$ **Cov(X)**$(p_{\mathcal{F}}, p_{\mathcal{G}})$ se observa que dado $[s \in \mathcal{F}(U)]_x \in X_{\mathcal{F}}$, $[\varphi_U(s) \in \mathcal{G}(U)]_x \in X_{\mathcal{G}}$. Así, $\Lambda(\varphi)([s \in \mathcal{F}(U)]_x) := [\varphi_U(s) \in \mathcal{G}(U)]_x$. Es claro de la definición que $p_{\mathcal{G}} \circ \Lambda(\varphi) = p_{\mathcal{F}}$. Para la continuidad sean $U \in \mathcal{O}(X)$ y $s \in \mathcal{G}(U)$. Para probar que $\Lambda(\varphi)^{-1}(\tilde{s}(U)) \subseteq X_{\mathcal{F}}$ es un abierto sea $[t \in \mathcal{F}(V)]_x \in \Lambda(\varphi)^{-1}(\tilde{s}(U))$. Esto implica que $[\varphi_V(t) \in \mathcal{G}(V)]_x \in \tilde{s}(U)$, lo que es equivalente a decir que $x \in V$ y $[\varphi_V(t) \in \mathcal{G}(V)]_x = [s \in \mathcal{G}(U)]_x$. Esta última igualdad es equivalente a decir que existe $W \in \mathcal{O}(X)$ con $W \subseteq U \cap V$ y $x \in W$ tal que $\varphi_W(t|_W) = \varphi_V(t)|_W = s|_W$, donde la primera igualdad se obtiene del hecho de que $\varphi$ es natural. Así, es claro que $[t \in \mathcal{F}(V)]_x \in (\widetilde{t|_W})(W)$ y además $(\widetilde{t|_W})(W) \subseteq \Lambda(\varphi)^{-1}(\tilde{s}(U))$ pues dado $y \in W$, $\Lambda(\varphi)([t|_W \in \mathcal{F}(W)]_y) = [\varphi_W(t|_W) \in \mathcal{G}(W)]_y = [\varphi_V(t)|_W \in \mathcal{G}(W)]_y = [s|_W \in \mathcal{G}(W)]_y = [s \in \mathcal{G}(U)]_y \in \tilde{s}(U)$. Esto concluye la prueba de la continuidad.

Para terminar, nótese que es claro de la definición que $\Lambda$ manda composiciones en composiciones e identidades en identidades, lo que prueba que es en efecto un funtor. $\square$

Teorema 2.39. *Si $X$ localmente conexo, entonces **Cov(X)** es equivalente a la categoría **LCSh(X)**. En esta equivalencia las aplicaciones cubrientes triviales corresponden a las gavillas constantes.*

Demostración. Sea $X \in \mathbf{Top}$ un espacio localmente conexo. Lo que se quiere probar es que $\Lambda \circ \Gamma \cong 1_{\mathbf{Cov(X)}}$ y $\Gamma \circ \Lambda \cong 1_{\mathbf{LCSh(X)}}$.

Respecto a la primera afirmación dado $p : Y \to X \in \mathbf{Cov(X)}$, se define $f_p : X_{\Gamma_p} \to Y$ mediante la regla de correspondencia $f_p([s \in \Gamma_p(U)]_x) = s(x)$. Es claro de la definición que $p \circ f_p = p_{\Gamma_p}$. Para la continuidad sea $U \subseteq Y$ un abierto no vacío. Si $[s \in \Gamma_p(V)]_x \in f_p^{-1}(U)$, entonces $s(x) \in U$, lo que es equivalente a que $x \in s^{-1}(U)$. Dado que $s^{-1}(U) \subseteq X$ es un abierto y $s|_{V \cap s^{-1}(U)} \in \Gamma_p(V \cap s^{-1}(U))$, se observa que $(\widetilde{s|_{V\cap s^{-1}(U)}})(V \cap s^{-1}(U)) \subseteq f_p^{-1}(U)$ y que $[s \in \Gamma_p(V)]_x \in (\widetilde{s|_{V\cap s^{-1}(U)}})(V \cap s^{-1}(U))$, lo que prueba la continuidad de $f_p$.

Además, si $f \in \mathbf{Cov(X)}(p, q)$ con digamos $p : Y \to X$ y $q : Z \to X$, es claro que el siguiente diagrama conmuta pues todos los triángulos lo hacen.

$$\begin{tikzcd}
X_{\Gamma_p} \arrow[rr, "\Lambda\Gamma(f)"] \arrow[dr, "p_{\Gamma_p}"] \arrow[dd, "f_p"'] & & X_{\Gamma_q} \arrow[dl, "p_{\Gamma_q}"'] \arrow[dd, "f_q"] \\
& X & \\
Y \arrow[ur, "p"] \arrow[rr, "f"'] & & Z \arrow[ul, "q"']
\end{tikzcd}$$

Para concluir la prueba de esta afirmación, por la Proposición 2.4 basta con mostrar que se tiene dicho isomorfismo para $p = p_1 : X \times F \to X$ una aplicación cubriente trivial. En efecto, dados $U \subseteq X$ abierto y $s \in \Gamma_p(U)$, de la definición se tiene que $f_p(\tilde{s}(U)) = s(U)$, y dado que $s(U) = U \times p_2 s(U)$, con $p_2 : X \times F \to F$ la proyección en la segunda coordenada, se concluye que $f_p(\tilde{s}(U)) \subseteq X \times F$ es un abierto. Por definición de la topología en $X_{\Gamma_p}$ esto implica que $f_p$ es una función abierta. La inyectividad de $f_p$ se sigue del hecho de que si $f_p([s \in \Gamma_p(U)]_x) = f_p([t \in \Gamma_p(V)]_y)$, entonces $s(x) = t(y)$, lo que implica que $x = y$ y así, $s(x) = t(x)$. La continuidad de las secciones implica que existe $W \subseteq U \cap V$ abierto con $x \in W$ tal que $s|_W = t|_W$, lo que por definición implica que $[s \in \Gamma_p(U)]_x = [t \in \Gamma_p(V)]_y$. Lo único que resta probar es que $f_p$ es suprayectiva. Para esto dado $y \in Y$ se tiene que para $x := p(y) \in X$ existe $V \subseteq X$ vecindad abierta de $x$ cubierta parejamente por la familia de abiertos en $Y$, $\{U_i \mid i \in I\}$. Sea $i_0 \in I$ el único índice tal que $y \in U_{i_0}$. Dado que $p|_{U_{i_0}} : U_{i_0} \to V$ es un homeomorfismo, se tiene que $(p|_{U_{i_0}})^{-1} \in \Gamma_p(V)$. Así, $[(p|_{U_{i_0}})^{-1} \in \Gamma_p(V)]_{p(y)} \in X_{\Gamma_p}$ y además, $f_p([(p|_{U_{i_0}})^{-1} \in \Gamma_p(V)]_{p(y)}) = (p|_{U_{i_0}})^{-1}(p(y)) = y$, lo que prueba lo que se quería y así, $f_p$ es un homeomorfismo natural.

En lo que respecta a la segunda afirmación, sea $\mathcal{F} \in$ **Sh(X)** y nótese que se puede definir $\tau^{\mathcal{F}} : \mathcal{F} \to \Gamma_{p_{\mathcal{F}}}$, donde para $U \subseteq X$ un abierto, $\tau^{\mathcal{F}}_U : \mathcal{F}(U) \to \Gamma_{p_{\mathcal{F}}}(U)$ tiene por regla de correspondencia $\tau^{\mathcal{F}}_U(s) = \tilde{s}$. Para ver que $\tau^{\mathcal{F}}$ define en efecto una transformación natural sean $U \subseteq V$ abiertos en $X$. Lo que se quiere ver es que el siguiente diagrama conmuta

$$\begin{tikzcd}
\mathcal{F}(V) \arrow[r, "\tau^{\mathcal{F}}_V"] \arrow[d, "(_)|_U"'] & \Gamma_{p_{\mathcal{F}}}(V) \arrow[d, "(_)|_U"] \\
\mathcal{F}(U) \arrow[r, "\tau^{\mathcal{F}}_U"'] & \Gamma_{p_{\mathcal{F}}}(U)
\end{tikzcd}$$

Lo que es equivalente a probar que para todo $s \in \mathcal{F}(V)$, $\widetilde{(s|_U)} = \tilde{s}|_U$, afirmación que es clara.

Para ver que $\tau$ es un isomorfismo natural, lo primero que se observa es que si $\varphi \in$ **LCSh(X)**$(\mathcal{F}, \mathcal{G})$ y $U \in \mathcal{O}(X)$, entonces el siguiente diagrama conmuta

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\tau^{\mathcal{F}}_U"] \arrow[d, "\varphi_U"'] & \Gamma_{p_{\mathcal{F}}}(U) \arrow[d, "\Gamma\Lambda(\varphi)_U"] \\
\mathcal{G}(U) \arrow[r, "\tau^{\mathcal{G}}_U"'] & \Gamma_{p_{\mathcal{G}}}(U)
\end{tikzcd}$$

Pues si $s \in \mathcal{F}(U)$, entonces $(\Gamma\Lambda(\varphi)_U \circ \tau_U^{\mathcal{F}})(s) = \Gamma\Lambda(\varphi)_U(\tilde{s}) = \Lambda(\varphi) \circ \tilde{s}$. Así, si $x \in U$, $(\Gamma\Lambda(\varphi)_U \circ \tau_U^{\mathcal{F}})(s)(x) = \Lambda(\varphi)([s \in \mathcal{F}(U)]_x) = [\varphi_U(s) \in \mathcal{G}(U)]_x = \varphi_U([s \in \mathcal{F}(U)]_x) = \varphi_U\tilde{s}(x) = (\varphi_U \circ \tau_U^{\mathcal{G}})(s)(x)$.

Respecto a la prueba de que esta transformación natural define en efecto un isomorfismo, por definición de gavilla localmente constante basta con probar el resultado suponiendo que $\mathcal{F}$ es constante y así, sea $\mathcal{F} = \mathcal{C}(\_, F)$, con $F \in$ **Top** discreto. Luego, la afirmación es equivalente a probar que dado $U \subseteq X$ abierto, $\tau_U^{\mathcal{F}} : \mathcal{F}(U) \to \Gamma_{p_{\mathcal{F}}}(U)$ es una función biyectiva. Pero si $s, t \in \mathcal{F}(U)$ son tales que $\tau_U^{\mathcal{F}}(s) = \tau_U^{\mathcal{F}}(t)$, entonces $\tilde{s} = \tilde{t}$. Luego, dado $x \in U$ existe $W_x \subseteq U$ vecindad abierta de $x$ tal que $s|_{W_x} = t|_{W_x}$. En particular $s(x) = t(x)$ y dado que el elemento $x \in U$ fue arbitario, se concluye que $s = t$. Para la suprayectividad sea $s \in \Gamma_{p_{\mathcal{F}}}(U)$. Dado $x \in U$, se tiene que $s(x) = [s_x \in \mathcal{F}(U_x)]_x$. El axioma de gavillas implica que existe una única $t \in \mathcal{F}(U)$ tal que $t|_{U_x} = s_x$ para todo $x \in U$. Así, $\tau_U^{\mathcal{F}}(t)(x) = \tilde{t}(x) = [t \in \mathcal{F}(U)]_x = [t|_{U_x} \in \mathcal{F}(U_x)]_x = [s_x \in \mathcal{F}(U_x)]_x = s(x)$, lo que prueba que $\tau_U^{\mathcal{F}}(t) = s$ y concluye la prueba de esta afirmación.

La correspondencia para las aplicaciones cubrientes triviales se sigue de la Proposición 2.11. $\square$

**5.2. Caracterización con el grupoide fundamental.** La equivalencia que se va a obtener en esta sección proviene del hecho de que la acción de monodromía se puede interpretar funtorialmente de una segunda forma. Para esto se recuerda que el **grupoide fundamental** en $X$, $\pi_{\leq 1}(\mathrm{X})$, es la categoría cuyos objetos son los puntos de $X$, y para $x, y \in X$, $\pi_{\leq 1}(\mathrm{X})(x, y)$ consta de las clases de homotopía relativas al $\{0, 1\}$ de trayectorías cuyo extremo inicial y final son $x$ y $y$ respectivamente.

Se recuerda que un grupoide es una categoría en la que todo morfismo es isomorfismo. Luego, nótese que $\pi_{\leq 1}(\mathrm{X})$ es en efecto un grupoide en sentido categórico. Asimismo, en un grupoide todas las familias de automorfismos en un objeto tienen estructura de grupo. En el caso del grupoide fundamental nótese que si $x \in X$, entonces $\pi_{\leq 1}(\mathrm{X})(x, x) = \pi_1(\mathrm{X}, \mathrm{x})$. Además, la colección de clases de isomorfismo de $\pi_{\leq 1}(\mathrm{X})$ coincide con el conjunto de componentes por trayectorias de $X$, $\pi_0(X)$. Estas últimas dos observaciones justifican la notación para el grupoide fundamental de un espacio $X$ pues como se ve esta categoría contiene información de los grupos fundamentales del espacio en cuestión así como de su conjunto de componentes por trayectorias.

Ahora considérese $p : Y \to X \in$ **Cov(X)** y nótese que se puede definir una asignación entre categorías, $T_p : \pi_{\leq 1}(\mathrm{X}) \to$ **Set**, que a nivel de objetos tiene por regla

$T_p(x) = p^{-1}(x)$, donde $x \in X$. Además, si $[\sigma] \in \pi_{\leq 1}(\mathrm{X})(x,y)$, entonces $T_p([\sigma])(z) = \tilde{\sigma}(1)$, donde $\tilde{\sigma} \in Y^I$ es el único levantamiento tal que $\tilde{\sigma}(0) = z$, $p \circ \tilde{\sigma} = \sigma$ y $z \in p^{-1}(x)$.

Es sencillo ver que $T_p$ es un funtor, al que se le conoce como el **funtor de transporte**. Más aún, esto da lugar a un funtor $T : \mathbf{Cov(X)} \to \mathbf{Fun}(\pi_{\leq 1}(\mathrm{X}), \mathbf{Set})$, donde para $f \in \mathbf{Cov(X)}(p,q)$ con digamos $p : Y \to X$ y $q : Z \to Y$, se tiene que $T(f) : T_p \to T_q$ tiene por componentes a $T(f)_x : p^{-1}(x) \to q^{-1}(x)$ cuya regla de correspondencia es $T(f)_x(y) = f(y)$, donde $x \in X$. Un cálculo de rutina prueba que $T(f)$ es una transformación natural entre $T_p$ y $T_q$.

El teorema que se va a probar afirma que cuando $X$ es conectable por trayectorias, localmente conectable por trayectorias y semilocalmente simplemente conexo, $T$ es una equivalencia de categorías. Para esto se va a construir un funtor en la otra dirección.

Dado $F \in \mathbf{Fun}(\pi_{\leq 1}(\mathrm{X}), \mathbf{Set})$, considérese el conjunto $X_F := \coprod_{x \in X} F(x)$. Al considerar para cada $x \in X$ la función constante con valor $x$, $C_x : F(x) \to X$, la propiedad universal del coproducto en la categoría de conjuntos implica que existe una única función $p_F : X_F \to X$ tal que $p_F|_{F(x)} = C_x$. Si además $X$ es conectable por trayectorias, localmente conectable por trayectorias y semilocalmente simplemente conexo, entonces la familia de subconjuntos abiertos de $X$ simplemente conexos es no vacía y denótese a esta por $\mathcal{U}$. De hecho $\mathcal{U}$ es una cubierta abierta de $X$. Luego, dados $U \in \mathcal{U}$ así como $x \in U$, se define una asignación $\varphi_{U,x} : U \times F(x) \to p_F^{-1}(U)$ donde para $(u,z) \in U \times F(x)$, se considera $\sigma \in U^I$ tal que $\sigma(0) = x$ y $\sigma(1) = u$. Dicha trayectoría existe pues $U$ es conectable por trayectorias. Así, $F([\sigma]) : F(x) \to F(u)$ y entonces $\varphi_{U,x}(u,z) := F([\sigma])(z)$. Nótese que esta asignación es una función pues al ser $U$ simplemente conexo cualesquiera dos trayectorias con los mismos extremos son homotópicas. Además nótese que $p_F(\varphi_{U,x}(u,z)) = u \in U$, por lo que la función está bien definida.

Ahora se observa que la función $\varphi_{U,x} : U \times F(x) \to p_F^{-1}(U)$ es biyectiva. Para esto si $(u_0, z_0), (u_1, z_1) \in U \times F(x)$ son tales que $\varphi_{U,x}(u_0, z_0) = \varphi_{U,x}(u_1, z_1)$, entonces $F([\sigma])(z_0) = F([\tau])(z_1)$ con $\sigma, \tau \in U^I$ tales que $\sigma(0) = \tau(0) = x$, $\sigma(1) = u_0$ y $\tau(1) = u_1$. Dado que $\varphi_{U,x}(u_0, z_0) \in F(u_0)$ y $\varphi_{U,x}(u_1, z_1) \in F(u_1)$, la igualdad de estos elementos implica que $u_0 = u_1$. Así, por ser $U$ simplemente conexo $[\sigma] = [\tau]$, lo que implica que $F([\sigma])(z_0) = F([\tau])(z_1)$. Pero dado que $\pi_1(\mathrm{X}, \mathrm{x})$ es un grupoide, $[\sigma]$ es un isomorfismo, así $F$ preserva isomorfismos y entonces $F([\sigma])$ es una función biyectiva, por lo que la última igualdad implica que $z_0 = z_1$ y concluye la prueba de la inyectividad. Respecto a la suprayectividad sea $b \in p_F^{-1}(U)$. Dado que $p_F(b) \in U$ y $U$ es conectable por trayectorias, existe $\sigma \in U^I$ tal que $\sigma(0) = x$ y $\sigma(1) = p_F(b)$. Además, por definición $b \in F(p_F(b))$ y $F([\sigma]) : F(x) \to F(p_F(b))$ es una función biyectiva, por lo que existe un único $z \in F(x)$ tal que $F([\sigma])(z) = b$. Así, es claro que $\varphi_{U,x}(p_F(b), z) = b$.

En resumen se ha probado que se tiene una familia de funciones biyectivas $\{\varphi_{U,x} : U \times F(x) \to p_F^{-1}(U) \mid U \in \mathcal{U},\ x \in U\}$. A los conjuntos de la imagen de $F$ se les da la topología discreta, los dominios de cada función son espacios topológicos y al dotar a cada $p_F^{-1}(U)$ con la topología final, dichas funciones se vuelven homeomorfismos. Sin embargo, para poder definir una topología en $X_F$ usando esta familia, tiene que probarse que hay compatibilidad en las intersecciones de abiertos no vacías, es decir, que para cualesquiera $U, V \in \mathcal{U}$ tales que $U \cap V \neq \emptyset$, se tiene que $\varphi_{V,x_1}^{-1} \circ \varphi_{U,x_0} : (U \cap V) \times F(x_0) \to (U \cap V) \times F(x_1)$ es un homeomorfismo. Sin embargo esto es claro de la definición de la topología. Así, se tiene el siguiente resultado.

Lema 2.40. *Con las condiciones y notación de antes existe una topología en $X_F$ que hace a cada uno de los elementos de la familia $\{\varphi_{U,x} : U \times F(x) \to p_F^{-1}(U) \mid U \in \mathcal{U},\ x \in U\}$ un homeomorfismo. Con esta topología la función $p_F$ resulta ser una aplicación cubriente.*

Demostración. Por la discusión previa lo único que falta probar es que $p_F : X_F \to X$ es en efecto una aplicación cubriente. Para esto se va a usar el Lema 2.4 pues nótese que dado $x \in X$ existe $U \in \mathcal{U}$ tal que $x \in U$. Así, $\varphi_{U,x} : U \times F(x) \to p_F^{-1}(U)$ es un homeomorfismo. Además, se afirma que el siguiente diagrama conmuta

$$\begin{tikzcd} U \times F(x) \arrow[rr, "\varphi_{U,x}"] \arrow[dr, "p_1"'] & & p_F^{-1}(U) \arrow[dl, "(p_F)|_{p_F^{-1}(U)}"] \\ & U & \end{tikzcd}$$

Sin embargo, esta afirmación es clara pues para $(u, z) \in U \times F(x)$ sea $\sigma \in U^I$ tal que $\sigma(0) = x$ y $\sigma(1) = u$. Dado que $F([\sigma])(z) \in F(u)$, entonces $((p_F)|_{p_F^{-1}(U)} \circ \varphi_{U,x})(u, z) = u = p_1(u, z)$. Esto prueba que $\varphi_{U,x}$ es un isomorfismo en la categoría **Top** $/U$ y concluye la prueba. $\square$

Teorema 2.41. *Sea $X$ un espacio conectable por trayectorias, localmente conectable por trayectorias y semilocalmente simplemente conexo. Entonces las categorías* ***Cov(X)*** *y* ***Fun***$(\pi_{\leq 1}(\mathrm{X}), \textbf{\textit{Set}})$ *son equivalentes.*

Demostración. Se afirma que el funtor $T : \mathbf{Cov(X)} \to \mathbf{Fun}(\pi_{\leq 1}(\mathrm{X}), \mathbf{Set})$ es una equivalencia. Para probar esto se va a ver que este es fiel, pleno y esencialmente suprayectivo.

En esta dirección sean $p, q \in \mathbf{Cov(X)}$ con digamos $p : Y \to X$ y $q : Z \to X$. Se quiere ver que la asignación inducida por $T$, $\mathbf{Cov(X)}(p, q) \to \mathbf{Fun}(\pi_{\leq 1}(\mathrm{X}), \mathbf{Set})(T(p), T(q))$, es una biyección. Respecto a la inyectividad si $f, g \in \mathbf{Cov(X)}$ son tales que $T(f) = T(g)$, entonces sea $y \in Y$ y defina $x := p(y)$. Así, $y \in p^{-1}(x)$ y dado que $T(f)_x = T(g)_x$, entonces $f(y) = T(f)_x(y) = T(g)_x(y) = g(y)$. Dado que el elemento $y \in Y$ fue arbitrario, se concluye que $f = g$.

Para la suprayectividad sea $\varphi \in \mathbf{Fun}(\pi_{\leq 1}(\mathrm{X}), \mathbf{Set})(T(p), T(q))$. Se define $f : Y \to Z$ donde para $y \in Y$, $f(y) = \varphi_{p(y)}(y)$. Es claro por construcción que $p \circ f = q$. Además, la continuidad se sigue de la definición y es claro que $T(f) = \alpha$.

En lo que respecta a la suprayectividad escencial dado $F \in \mathbf{Fun}(\pi_{\leq 1}(\mathrm{X}), \mathbf{Set})$ considérese $p_F : X_F \to X$ la aplicación cubriente del lema anterior. Nótese que dado $x \in X$, $p_F^{-1}(x) = F(x)$. Así, se tiene que $T(p_F) = F$. $\square$

Para concluir el capítulo se va a tratar el problema de la dependencia del punto base en el grupo fundamental. El resultado que se busca probar es que cuando el espacio $X$ es conectable por trayectorias, cualesquiera dos grupos fundamentales con distintos puntos base son isomorfos. Sin embargo, y aunque la prueba clásica no es complicada pues el isomorfismo se obtiene al tomar la clase del lazo que se obtiene al conjugar con la trayectoria que une los puntos base, el tratamiento que se quiere dar es categórico y apovecha la teoría desarrollada hasta este momento. En esta dirección se recuerda lo siguiente:

Definición 2.42. *Una categoría $\mathcal{C}$ es* ***conexa*** *si para cualesquiera dos objetos $C_0, C_n \in \mathcal{C}$, existe un diagrama de forma zig-zag:*

$$\begin{tikzcd}
C_0 \arrow[dr, "f_0"'] & & C_2 \arrow[dl, "f_1"] & \dots & C_{n-2} \arrow[dr, "f_{n-2}"'] & & C_n \arrow[dl, "f_{n-1}"] \\
& C_1 & & & & C_{n-1} &
\end{tikzcd}$$

Nótese que si $\mathcal{C}$ es un grupoide, entonces la condición de ser conexa es equivalente a la existencia de un morfismo entre cualesquiera dos objetos. Además, se observa que si $X$ es un espacio conectable por trayectorias, entonces $\pi_{\leq 1}(X)$ es un grupoide conexo. Luego, el resultado que se busca es consecuencia directa del siguiente resultado.

PROPOSICIÓN 2.43. *Supóngase que $\mathcal{C}$ es un grupoide conexo. Entonces, $\mathcal{C}$ es equivalente a la categoría asociada al grupo de automorfismos de cualquier objeto de $\mathcal{C}$.*

DEMOSTRACIÓN. Sea $C \in \mathcal{C}$ y denótese por $B\operatorname{Aut}(C)$ al grupo $\operatorname{Aut}(C)$ como categoría con un único objeto. Así, se define una asignación $F : B\operatorname{Aut}(C) \to \mathcal{C}$ mediante $F(*) = C$ y, para cada $f \in \operatorname{Aut}(C)$, $F(f) = f$. Es claro de la definición que $F$ es un funtor y que este es fiel y pleno. Para ver que este es esencialmente suprayectivo sea $D \in \mathcal{C}$. Dado que $\mathcal{C}$ es un grupoide conexo, existe un morfismo $f : C \to D$ que es necesariamente un isomorfismo. Así, $F(*) = C \cong D$. □

COROLARIO 2.44. *Si $X$ es un espacio conectable por trayectorias, entonces para cualesquiera $x_0, x_1 \in X$, $\pi_1(X, x_0) \cong \pi_1(X, x_1)$.*

DEMOSTRACIÓN. Se deduce del hecho de que por el resultado anterior $B\operatorname{Aut}(x_0) \simeq \pi_{\leq 1}(X)$ y $B\operatorname{Aut}(x_1) \simeq \pi_{\leq 1}(X)$, por lo que $B\operatorname{Aut}(x_0) \simeq B\operatorname{Aut}(x_1)$. Esto implica que $\operatorname{Aut}(x_0) \cong \operatorname{Aut}(x_1)$ y de esto se deduce el resultado deseado pues $\operatorname{Aut}(x_i) = \pi_1(X, x_i)$ para $i \in \{0, 1\}$. □

Para concluir este capítulo se va a presentar una segunda prueba del Teorema 2.41, que es mucho más categórica. Lo que se va a usar en esta es un conocido resultado que se deduce del lema de Yoneda cuando se prueba el teorema de Cayley. Este afirma que para $G$ un grupo, si $BG$ denota al grupo visto como categoría con un sólo objeto, entonces $\mathbf{Fun}(BG, \mathbf{Set}) \simeq G - \mathbf{Set}$.

Así, para $X$ satisfaciendo las hipótesis del Teorema 2.41, se tiene del corolario anterior que dado $x \in X$, $\pi_{\leq 1}(X) \simeq B\pi_1(X, x)$. Luego, $\mathbf{Fun}(\pi_{\leq 1}(X), \mathbf{Set}) \simeq \mathbf{Fun}(B\pi_1(X, x), \mathbf{Set})$, que al usar el resultado mencionado en el párrafo anterior es equivalente a $\pi_1(X, x) - \mathbf{Set}$. Pero como se vio anteriormente esta categoría es equivalente a $\mathbf{Cov(X)}$.

Capítulo 3

# Morfismos étale finitos y el grupo fundamental algebraico

El presente capítulo comienza dando una nueva caracterización del concepto de $k$-álgebra finita étale a partir de los módulos de diferenciales de Kähler, que agrega una equivalencia más a las dadas en la Proposición 1.28. También, se muestra que esto da lugar a un funtor, que se conoce como el funtor cotangente relativo, y se estudian algunas propiedades de éste.

Posteriormente, se introduce el concepto de cubriente étale finito de un esquema y se estudian algunas propiedades básicas de dichos morfismos, los cuales son el sustituto, para el caso de esquemas, del concepto de aplicación cubriente estudiado en el capítulo anterior. Además, se muestra que existe una subclase de dichos cubrientes para los cuales se tiene un teorema de Galois como sucedía para el caso de las aplicaciones cubrientes. Los elementos de dicha clase se conocen como cubrientes étale finitos de Galois.

Con la teoría desarrollada es posible definir un objeto, que se conoce como el grupo fundamental algebraico de un esquema (sobre un punto geométrico), del cual se estudian algunas propiedades básicas. El capítulo concluye con un par de ejemplos que muestran que este objeto puede considerarse como una generalización del grupo de Galois absoluto de un campo, así como del grupo fundamental de un espacio topológico bajo ciertas condiciones.

## 1. Módulos de diferenciales de Kähler

A lo largo de este capítulo todos los anillos serán conmutativos y unitarios a no ser que se diga lo contrario.

Definición 3.1. *Sean $A$ un anillo y $M$ un $A$-módulo. Un morfismo de grupos abelianos $d : A \to M$ es una* ***derivación*** *si se satisface la siguiente propiedad conocida como la* ***regla de Leibniz****: Para cualesquiera $a_1, a_2 \in A$, $d(a_1a_2) =$*

$a_1d(a_2) + a_2d(a_1)$. *Para $A$ una $R$-álgebra una derivación es $R$-**lineal** si es un morfismo de $R$-módulos. En este caso, el conjunto de derivaciones $R$-lineales se denota por* $\mathrm{Der_R}(A, M)$

Para $A$ una $R$-álgebra y $M$ un $R$-módulo, $\mathrm{Der_R}(A, M)$ tiene estructura de $R$-módulo al definir la suma de manera puntual y la acción de $R$ en dicho grupo como $(r \cdot d)(a) = rd(a)$, donde $r \in R$ y $a \in A$.

PROPOSICIÓN 3.2. *Sea $A$ una $R$-álgebra y $d : A \to A$ una derivación. Entonces,*

1. $d(1) = 0$.
2. $d \in \mathrm{Der_R}(A, A)$ *si y sólo si* $R \subseteq \mathrm{nuc}(d)$.

DEMOSTRACIÓN. Para la primera afirmación $d(1) = d(1 \cdot 1) = d(1) + d(1)$, donde en la última igualdad se usó la regla de Leibniz. El resultado se obtiene de la propiedad de cancelación respecto a la suma.

Respecto a la segunda afirmación, para la ida, sea $a \in R$. Entonces, $d(a) = d(a \cdot 1) = ad(1) = 0$. Dado que el elemento fue arbitrario se concluye que $R \subseteq \mathrm{nuc}(d)$. Respecto al regreso sean $a_1, a_2 \in A$ y $r \in R$. Así, $d(ra_1 + a_2) = d(ra_1) + d(a_2) = rd(a_1) + a_1d(r) + d(a_2) = rd(a_1) + d(a_2)$, lo que muestra que $d$ es $R$-lineal. $\square$

Una construcción que permite entender de manera complementaria la idea de derivación se encuentra en el siguiente resultado.

PROPOSICIÓN 3.3. *Sea $A$ una $R$-álgebra. Entonces, existe un único $A$-módulo (salvo isomorfismo), $\Omega_{A/R}$, con una derivación $R$-lineal $d_A : A \to \Omega_{A/R}$ tales que cualquier $A$-módulo $M$ y $d' \in \mathrm{Der_R}(A, M)$, existe un único morfismo de $A$-módulos $f : \Omega_{A/R} \to M$ tal que $f \circ d_A = d'$. En otras palabras, existe una corresondencia biyectiva entre* $\mathrm{Der_R}(A, M) \cong A - \boldsymbol{Mod}(\Omega_{A/R}, M)$.

DEMOSTRACIÓN. Considérense $N$ el $A$-módulo libre con base el conjunto $\{d(a) \mid a \in A\}$ y $N'$ el submódulo generado por el conjunto $\{d(r), d(a_1+a_2)-d(a_1)-d(a_2), d(a_1a_2)-a_1d(a_2) - a_2d(a_1)\}_{r\in R,\ a_1,a_2\in A}$. Luego, se definen $\Omega_{A/R} := N/N'$ y una función $d_A : A \to \Omega_{A/R}$ mediante la regla de correspondencia $d_A(a) = d(a)$.

Nótese que por construcción $d_A \in \mathrm{Der_R}(A, \Omega_{A/R})$. Ahora, sean $M$ un $A$-módulo y $\hat{d} \in \mathrm{Der_R}(A, M)$. Así, se define $g : N \to M$ como el único morfismo $A$-lineal tal que para cada $a \in A$, $g(d(a)) = \hat{d}(a)$. Dado que por definición $g$ anula a los generadores de $N'$, entonces este induce un único morfismo de $A$-módulos $f : \Omega_{A/R} \to M$ tal que para cada $a \in A$, $f(d(a) + N') = \hat{d}(a)$. Así, $f$ satisface la propiedad que se quería y de este argumento se deduce la biyección entre $\mathrm{Der}_{\mathrm{R}}(A, M)$ y $\mathrm{Hom}_{\mathbf{A\text{-}Mod}}(\Omega_{A/R}, M)$ al asociar a $\hat{d} \in \mathrm{Der}_{\mathrm{R}}(A, M)$ el morfismo $f \in \mathrm{Hom}_{\mathbf{A\text{-}Mod}}(\Omega_{A/R}, M)$.

Además, la unicidad requerida para $\Omega_{A/R}$ se obtiene de un argumento canónico en teoría de categorías y se deduce de la biyección probada, por lo tanto esta se va a omitir. □

Definición 3.4. *Para $A$ una $R$-álgebra, al $A$-módulo $\Omega_{A/R}$ se conoce como el* ***módulo de diferenciales de Kähler*** *de $A$ sobre $R$. A la derivación $R$-lineal $d_A : A \to \Omega_{A/R}$ se le conoce como* ***derivación universal*** *de $A$ en $\Omega_{A/R}$. Además, al resultado anterior se le conoce como la* ***propiedad universal del módulo de diferenciales de Kähler*** *$\Omega_{A/R}$.*

Ejemplo 3.5. *Considérese $A = R[x_1, ..., x_n]$ el anillo de polinomios con coeficientes en $R$ y $n$ indeterminadas. Dado que para cada $i \in \{1, ..., n\}$ se tiene que $\frac{\partial}{\partial x_i} \in \mathrm{Der}_{\mathrm{R}}(A, A)$, entonces por la propiedad universal del módulo de diferenciales de Kähler para cada $i \in \{1, ..., n\}$, existe $\partial_i \in \mathrm{Hom}_{\boldsymbol{A\text{-}Mod}}(\Omega_{A/R}, A)$ tal que $\partial_i(dx_j) = \delta_{ij}$, con $\delta_{ij}$ la delta de Kronecker. Esto permite definir un morfismo de $A$-módulos $(\partial_1, ..., \partial_n) : \Omega_{A/R} \to A^n$, que es claramente el inverso del morfismo de $A$-módulos $A^n \to \Omega_{A/R}$ que en la base de $A^n$ satisface que $e_i \mapsto dx_i$. Dado que $\{x_1, ..., x_n\}$ son generadores de $A$ como $R$-álgebra, entonces $\{dx_1, ..., dx_n\}$ son generadores de $\Omega_{A/R}$ como $A$-módulo, de lo que se deduce que $\Omega_{A/R} \cong \bigoplus_{i=1}^{n} A dx_i$.*

El siguiente resultado dice como asociar a un morfismo de $R$-álgebras una sucesión exacta de módulos de diferenciales de Kähler. Vale la pena mencionar que esta no es la única forma de asociar una sucesión exacta a este tipo de morfismos pues existe también la conocida sucesión cotangente relativa, la cual no se encuentra dentro del material expuesto pues no es necesaria para los fines de este trabajo, pero puede ser consultada en la Proposición 16.2 de [**E**, pp 386].

Proposición 3.6. *(Sucesión conormal) Sea $f : A \to B$ un morfismo suprayectivo de $R$-álgebras. Al considerar $I = \mathrm{nuc}(f)$, existe una sucesión exacta de $B$-módulos de la forma*

$$I/I^2 \xrightarrow{\delta} B \otimes_A \Omega_{A/R} \xrightarrow{\beta} \Omega_{B/R} \longrightarrow 0.$$

Demostración. Por el primer teorema de isomorfismo para $R$-álgebras se tiene que $A/I \cong B$. De este isomorfismo resulta claro que hay una acción de $B$ en $I/I^2$ y en el resto de la prueba se identificará $B$ con $A/I$.

Nótese que el morfismo $\alpha : I \to B \otimes_A \Omega_{A/R}$ definido mediante $\alpha(a) = 1 \otimes d_A(a)$ satisface que $\alpha(I^2) = 0$. Por lo tanto este induce un morfismo de $B$-módulos $\delta : I/I^2 \to B \otimes_A \Omega_{A/R}$ cuya regla de correspondencia es $\delta(x + I^2) = \alpha(x)$.

Por otro lado, al usar la propiedad universal del producto tensorial en la función $A$-bilineal $B \times \Omega_{A/R} \to \Omega_{B/R}$ cuya regla de correspondencia es $(b, d_A(a)) \mapsto bd_B(a+I)$, se induce un morfismo de $B$-módulos $\beta : B \otimes_A \Omega_{A/R} \to \Omega_{B/R}$.

Es claro que $\beta$ es suprayectiva. Además, para $x \in I$ se tiene que $\beta\delta(x + I^2) = \beta(1 \otimes d_A(x)) = \beta(0) = 0$, por lo que al ser dicho elemento arbitario $\mathrm{im}(\delta) \subseteq \mathrm{nuc}(\beta)$. Para ver que esta contención es de hecho una igualdad, por el lema de Yoneda basta con ver que para cada $B$-módulo la siguiente sucesión es exacta

$$\mathrm{Hom}_B(I/I^2, M) \xleftarrow{\delta^*} \mathrm{Hom}_B(B \otimes_A \Omega_{A/R}, M) \xleftarrow{\beta^*} \mathrm{Hom}_B(\Omega_{B/R}, M)$$

En efecto, sea $g \in \mathrm{Hom}_B(B \otimes_A \Omega_{A/R}, M)$ tal que $\delta^*(g) = 0$. Nótese que por la adjunción del funtor producto tensorial con el funtor hom, el hecho de que $\mathrm{Hom}_B(B, M) \cong B$ y la propiedad universal de las diferenciales de Kähler se tienen biyecciones $\mathrm{Hom}_B(B \otimes_A \Omega_{A/R}, M) \cong \mathrm{Hom}_A(\Omega_{A/R}, M) \cong \mathrm{Der}_{\mathrm{R}}(A, M)$, donde $g \mapsto \varphi_g \circ d_A$ con $\varphi_g : \Omega_{A/R} \to M$ definido mediante $\varphi_g(d_A(a)) = g(1 \otimes d_A(a))$ para cada $a \in A$. Se observa que si $a \in I$, entonces $\varphi_g d_A(a) = g(1 \otimes d_A(a)) = 0$, por lo que existe $\hat{g} : B \to M$ un morfismo de $B$-módulos definido por $\hat{g}(a + I) = \varphi_g(d_A(a))$, y de hecho este es una derivación $R$-lineal. Luego, por la propiedad universal de $\Omega_{B/R}$ existe un único morfismo de $B$-módulos $h : \Omega_{B/R} \to M$ tal que $h \circ d_B = \hat{g}$. Así, se afirma que $\beta^*(h) = g$, es decir, que $h \circ \beta = g$. Para probar esto basta con checar dicha igualdad en elementos de la forma $b \otimes d_A(a) \in B \otimes_A \Omega_{A/R}$. En efecto pues

$$h(\beta(b \otimes d_A(a))) = h(bd_B(a+I)) = bh(d_B(a+I)) = b\hat{g}(a+I) = bg(1 \otimes d_A(a)) = g(b \otimes d_A(a)),$$

lo que concluye la prueba. □

Para varios resultados subsecuentes en esta sección se va a usar la regla de correspondencia de los morfismos $\delta$ y $\beta$ definidos en el resultado anterior. Por ejemplo, el siguiente resultado estudia el problema de la inyectividad de $\delta$, aunque de hecho dice algo más fuerte.

Proposición 3.7. *Sea $f : A \to B$ un morfismo suprayectivo de $R$-álgebras y considérese la sucesión conormal definida por $f$*

$$I/I^2 \xrightarrow{\delta} B \otimes_A \Omega_{A/R} \xrightarrow{\beta} \Omega_{B/R} \longrightarrow 0.$$

*Entonces $\delta$ es un monomorfismo que se escinde si y sólo si existe un morfismo de $R$-álgebras $\tau : B \to A/I^2$ que escinde al morfismo cambio de clase $p : A/I^2 \to B$.*

Demostración. $\Rightarrow$) Como antes se va a escribir $B = A/I$. Además, nótese que a lo largo de toda la prueba puede suponerse sin pérdida de generalidad que $I^2 = 0$, pues al considerar la sucesión conormal para el morfismo $A \twoheadrightarrow B \twoheadrightarrow B/I^2$, esta implica que $\Omega_{(A/I^2)/R}$ se obtiene de $\Omega_{A/R}$ al factorizar por $I^2\Omega_{A/R}$ y $\delta(I^2)$. Sin embargo, $\delta(I^2) \subseteq I\Omega_{A/R}$ y así, $B \otimes_A \Omega_{(A/I^2)/R} \cong B \otimes_A \Omega_{A/R}$.

Ahora, supóngase que $\delta$ se escinde por el morfismo de $B$-módulos $\sigma : B \otimes_A \Omega_{A/R} \to I$, es decir, que $\sigma \circ \delta = 1_I$. Sea $\gamma : \Omega_{A/R} \to B \otimes_A \Omega_{A/R}$ el morfismo inducido por $f \otimes 1_{\Omega_{A/R}} : A \otimes_A \Omega_{A/R} \to B \otimes_A \Omega_{A/R}$ usando el isomorfismo canónico $A \otimes_A \Omega_{A/R} \cong \Omega_{A/R}$. Luego, al definir el morfismo $D = \sigma \circ \gamma \circ d_A : A \to A$, se tiene que $D \in \mathrm{Der_R}(A, A)$ y que $\mathrm{im}(D) \subseteq I$. Así, $1_A - D : A \to A$ es un morfismo de $R$-álgebras. Además, si $a \in I$, entonces $D(a) = \sigma\gamma d_A(a) = \sigma(f \otimes 1_{\Omega_{A/R}})(1 \otimes d_A(a)) = \sigma(1 \otimes d_A(a)) = \sigma\delta(a) = a$, lo que muestra que $I \subseteq \mathrm{nuc}(1_A - D)$. Luego, existe $\tau : A/I \to A$ un morfismo de $R$-álgebras tal que $\tau(a + I) = (1_A - D)(a) = a - D(a)$. Para ver que este morfismo es el buscado nótese que como $D(a) \in I$, entonces $pD(a) = 0$. Así, $(p \circ \tau)(a + I) = p(a - D(a)) = p(a) = a + I$, lo que prueba que $p \circ \tau = 1_B$.

$\Leftarrow$) Supóngase que $\tau : B \to A/I^2$ es un morfismo de $R$-álgebras tal que $p \circ \tau = 1_B$. Si se define $D : A \to A$ mediante $D = 1_A - \tau \circ p$, entonces nótese que $\mathrm{im}(D) \subseteq \mathrm{nuc}(p) = I$. Dado que $I^2 = 0$, se tiene que $D \in \mathrm{Der_R}(A, I)$. Luego, por la propiedad universal del módulo de diferenciales de Kähler $D$ induce un único $\varphi_D \in \mathrm{Hom}_{\mathbf{A\text{-}Mod}}(\Omega_{A/R}, I)$. Además, dado que $I^2 = 0$, $\varphi_D$ se factoriza a través de $\sigma : \Omega_{A/R} \otimes_A B \to I$. De donde en particular para cada $a \in A$,

$$\sigma(d_A(a) \otimes 1) = \varphi_D(d_A(a)) = D(a).$$

Para concluir la prueba se afirma que $\sigma \circ \delta = 1_I$. En efecto, dado $a \in I$, como $\mathrm{nuc}(p) = I$, se tiene que

$$\sigma\delta(a) = \sigma(1 \otimes d_A(a)) = D(a) = a - \tau p(a) = a.$$

□

Del resultado anterior se deduce el siguiente importante resultado de álgebra conmutativa. Se recuerda que para $(A, \mathfrak{m})$ un anillo local, un **campo de coeficientes** es un subcampo $k \subseteq A$ que es isomorfo a un subcampo de $A/\mathfrak{m}$ mediante la proyección canónica $A \to A/\mathfrak{m}$.

Corolario 3.8. *Sea $(A, \mathfrak{m})$ un anillo local y supóngase que $k \subseteq A$. Sea $\delta : \mathfrak{m} / \mathfrak{m}^2 \to A/\mathfrak{m} \otimes_k \Omega_{A/\mathfrak{m}}$ el morfismo de la sucesión conormal asociada a $f : A \to A/\mathfrak{m}$. Entonces $\delta$ es un monomorfismo si y sólo si existe un campo de coeficientes para $A/\mathfrak{m}^2$ que contiene a $k$. En particular, $\delta$ es un monomorfismo cuando $A/\mathfrak{m}$ es una extesión separable sobre $k$.*

Demostración. Para la primera afirmación considérese el morfismo de $k$-álgebras suprayectivo $A \to A/\mathfrak{m}$ dado por la proyección canónica. Como $\delta$ es un morfismo de $A/\mathfrak{m}$-módulos, es decir, de $A/\mathfrak{m}$-espacios vectoriales, entonces $\delta$ es un monomorfismo si y sólo si es un monomorfismo que escinde, y la existencia del campo de coeficientes se deduce del resultado anterior.

Si la extensión $(A/\mathfrak{m})| \, k$ es separable, entonces por el Teorema 7.8 de [**E**, pp 190] se tiene que $A/\mathfrak{m}$ tiene un campo de coeficientes que contiene a $k$. Lo que implica por la primera parte de la proposición que $\delta$ es un monomorfismo. $\square$

El siguiente resultado establece, entre otras cosas, propiedades de funtorialidad para el módulo de diferenciales de Kähler.

Proposición 3.9.

1. *Si $A$ es una $R$-álgebra finitamente generada, entonces $\Omega_{A/R}$ es un $A$-módulo finitamente generado.*
2. *Todo morfismo de $R$-álgebras $f : A \to B$ induce un morfismo de $A$-módulos, $f_* : \Omega_{A/R} \to \Omega_{B/R}$.*
3. *Si $f : A \to B$ y $g : B \to C$ son morfismos de $R$-álgebras, entonces $(g \circ f)_* = g_* \circ f_*$.*
4. *Para $A$ una $R$-álgebra, $(1_A)_* = 1_{\Omega_{A/R}}$.*

Demostración. Para la primera afirmación supóngase que $A$ es generado como $R$-álgebra por el conjunto $\{a_1, ..., a_n\}$. Entonces, se sigue que las clases de equivalencia del conjunto $\{d_A(a_1), ..., d_A(a_n)\}$ generan a $\Omega_{A/R}$ como $A$-módulo, lo que concluye la prueba de esta afirmación.

Respecto a la segunda afirmación primero nótese que $f$ da una estructura de $A$-módulo a $\Omega_{B/R}$. Ahora, considérese la función $d_B \circ f : A \to \Omega_{B/R}$. Esta función es un morfismo de $R$-módulos pues es composición de dos morfismos de $R$-módulos. Además, esta satisface la regla de Leibniz pues

$$(d_B \circ f)(a_1a_2) = d_B(f(a_1)f(a_2)) = f(a_1)(d_B \circ f)(a_2) + f(a_2)(d_B \circ f)(a_1).$$

Así, por la propiedad universal de $\Omega_{A/R}$ existe un único morfismo de $A$-módulos, $f_* : \Omega_{A/R} \to \Omega_{B/R}$, tal que $f_* \circ d_A = d_B \circ f$, lo que concluye la prueba de esta afirmación.

Para concluir, dado que el morfismo asociado a un morfismo de $R$-álgebras se obtiene a partir de una propiedad universal, el que esta asignación respete composiciones e identidades es inmediato. $\square$

Para dar la definición de $\Omega_{\text{-}/R}$ como un funtor, con la misma terminología de [**EGA1**], se recuerda que la categoría de **dimódulos**, que se denotará por **DMod**, tiene por objetos parejas $(A, M)$ con $A$ un anillo unitario (no necesariamente conmutativo) y $M$ un $A$-módulo. Los morfismos son parejas de flechas $(\varphi, f) : (A, M) \to (B, M)$ con $\varphi : A \to B$ un morfismo de anillos y $f : M \to N$ morfismo de grupos abelianos tales que para cualesquiera $a \in A$ y $m \in M$, $f(am) = \varphi(a)f(m)$, es decir, $f$ es un morfismo de $A$-módulos al dotar a $N$ con la estructura de $A$-módulo inducida por $\varphi$.

La proposición anterior y la discusión previa justifican lo siguiente.

Definición 3.10. *A la asignación $\Omega_{\text{-}/R} : R - \textbf{\textit{Alg}} \to \textbf{\textit{DMod}}$ se le conoce como **funtor cotangente relativo**.*

Las siguientes propiedades generales del funtor cotangente relativo serán fundamentales para el resultado principal de esta sección. La primera de estas dice que dicho funtor preserva productos finitos.

Proposición 3.11. *Sean $A_1, ..., A_n$ una familia de $R$-álgebras y considérese $A = \prod_{i=1}^n A_i$. Entonces $\Omega_{A/R} \cong \prod_{i=1}^n \Omega_{A_i/R}$ como $A$-módulos.*

Demostración. Sean $A_1, ..., A_n$ una familia de $R$-álgebras y considérese $A = \prod_{i=1}^n A_i$. Dado que la familia de proyecciones $\{\pi_i : A \to A_i\}_{i\in\{1,...,n\}}$ da una estructura de $A$-álgebra a cada $\Omega_{A_i/R}$, lo que se va a probar es que el $A$-módulo $\prod_{i=1}^n \Omega_{A_i/R}$ satisface la propiedad universal que define a $\Omega_{A/R}$. Para esto, si $d_i : A_i \to \Omega_{A_i/R}$ es la derivación universal de $A_i$, entonces al considerar la familia de morfismos de $R$-módulos $\{\pi_i \circ d_i : A \to \Omega_{A_i/R}\}_{i\in\{1,...,n\}}$, esta induce un morfismo de $R$-módulos

$D : A \to \prod_{i=1}^n \Omega_{A_i/R}$. Además, por la construcción de $D$ es sencillo ver que este satisface la regla de Leibniz.

Sea ahora $M$ un $R$-módulo y $d \in \mathrm{Der}_{\mathrm{R}}(A, M)$. Para definir $f : \prod_{i=1}^n \Omega_{A_i/R} \to M$ un morfismo de $A$-módulos, basta con definir para cada $i \in \{1, ..., n\}$ un morfismo de $A_i$-módulos $f_i : \Omega_{A_i/R} \to M$. Para esto se observa que dado $i \in \{1, ..., n\}$, se tiene que $d \circ \iota_j : A_j \to M$ es una derivación $R$-lineal, con $\iota_j : A_j \to A$ la $j$-ésima inclusión. Luego, la propiedad universal de $\Omega_{A_j/R}$ permite obtener el morfismo de $A_j$-módulos que se quiere.

Además, la unicidad de $f$ se sigue de su definición y esto concluye la prueba. $\square$

Respecto al coproducto se tiene el siguiente resultado, que de hecho generaliza el cálculo mostrado en el Ejemplo 3.5.

Proposición 3.12. *Sea $B$ el coproducto de una familia de $R$-álgebras $\{A_i\}_{i\in I}$. Entonces, $\Omega_{B/R} \cong \bigoplus_{i\in I}(B \otimes_{A_i} \Omega_{A_i/R}) \cong \bigoplus_{i\in I}((\coprod_{j\neq i} A_j) \otimes_R \Omega_{A_i/R})$.*

Demostración. Para $i \in I$ nótese que $B \otimes_{A_i} \Omega_{A_i/R} \cong (\coprod_{j\neq i} A_i) \otimes_R (A_i \otimes_{A_i} \Omega_{A_i/R}) \cong (\coprod_{j\neq i} A_j) \otimes_R \Omega_{A_i/R}$, de donde se deduce el segundo isomorfismo. Para el isomorfismo que falta probar escríbase $B_i = (\coprod_{j\neq i} A_j) \otimes_R \Omega_{A_i/R}$. Luego, lo que se va a probar es que $\Omega_{B/R} \cong \bigoplus_{i\in I} B_i$ construyendo un morfismo de $B$-módulos y su inversa. Así, construir un morfismo de $B$-módulos $f : \Omega_{B/R} \to \bigoplus_{i\in I} B_i$, es equivalente a construir una derivación $R$-lineal $B \to \bigoplus_{i\in I} B_i$. Pero al considerar $i \in I$ fija, nótese que $B \cong (\coprod_{j\neq i} A_j) \otimes_R A_i$, así que se tiene el morfismo $1_{\coprod_{j\neq i} A_j} \otimes d_i : B \to B_i$, el cual es una derivación $R$-lineal pues $d_i : A_i \to \Omega_{A_i/R}$ denota la derivación universal de $A_i$. Por lo tanto se tiene el morfismo que se busca al componer con la inclusión de $B_i$ en $B$.

Por otro lado, para definir $g : \bigoplus_{i\in I}(B \otimes_{A_i} \Omega_{A_i/R}) \to \Omega_{B/R}$, por la propiedad universal del coproducto en $B - \mathbf{Mod}$, esto es equivalente a definir para $i \in I$ morfismos de $B$-módulos, $B \otimes_{A_i} \Omega_{A_i/R} \to \Omega_{B/R}$. Dicho morfismo se define con la regla de correspondencia $1 \otimes d_i a \mapsto d_B(\iota_i(a))$, donde $d_B : B \to \Omega_{B/R}$ es la derivación universal e $\iota_i : A_i \to B$ la inclusión de $A_i$ en el coproducto. Además, por construcción es claro que los morfismos son mutuamente inversos. $\square$

Corolario 3.13. *Sea $A$ una $R$-álgebra y $B = A[x_1, ..., x_n]$. Entonces, $\Omega_{B/R} \cong (B \otimes_A \Omega_{A/R}) \oplus (\bigoplus_{i=1}^n B dx_i)$.*

Demostración. Si se define $C = R[x_1, ..., x_n]$, entonces se tiene que $B \cong A \otimes_R C$. Luego, de la proposición anterior se deduce que $\Omega_{B/R} \cong (B \otimes_A \Omega_{A/R}) \oplus (B \otimes_C \Omega_{C/R})$. Por lo tanto, si se prueba que $B \otimes_C \Omega_{C/R} \cong \bigoplus_{i=1}^n Bdx_i$, entonces se tiene el resultado deseado. Sin embargo, por el ejemplo 3.5 se tiene que $\Omega_{C/R} \cong \bigoplus_{i=1}^n Cdx_i$, por lo que $B \otimes_C \Omega_{C/R} \cong \bigoplus_{i=1}^n B \otimes_C Cdx_i \cong \bigoplus_{i=1}^n Bdx_i$, que es lo que se quería probar. □

El siguiente resultado se puede interpretar como una propiedad de preservación de conúcleos para el funtor $\Omega_{\text{-}/R}$, y es consecuencia directa de la existencia de la sucesión conormal.

Corolario 3.14. *Sea $f : A \to B$ un morfismo de $R$-álgebras y $t : B \to C$ su conúcleo. Entonces se tiene una sucesión exacta de $C$-módulos*

$$C \otimes_A \Omega_{A/R} \longrightarrow C \otimes_B \Omega_{B/R} \longrightarrow \Omega_{C/R} \longrightarrow 0.$$

Demostración. Dado que $t$ es un morfismo de $R$-álgebras suprayectivo, al considerar $I = \text{nuc}(t)$, existe la sucesión conormal

$$I/I^2 \xrightarrow{\delta} C \otimes_B \Omega_{B/R} \xrightarrow{\beta} \Omega_{C/R} \longrightarrow 0$$

Así, $\Omega_{C/R} \cong (C \otimes_B \Omega_{B/R})/\,\text{nuc}(\beta)$. Pero nótese que por construcción de $\delta$ se tiene que $\text{nuc}(\beta) = \langle\{1 \otimes d_B f(a) \mid a \in A\}\rangle$. Además se cumple que el morfismo inducido por $f$, $f_* : \Omega_{A/R} \to \Omega_{B/R}$, cumple que $f_* \circ d_A = d_B \circ f$, de lo que es claro que $\text{nuc}(t) = \text{im}(1_C \otimes f_*)$, y se tiene la exactitud deseada. □

De los últimos dos resultados se obtiene la siguiente importante propiedad categórica, que dice que el funtor cotangente relativo preserva una familia muy especial de colímites.

Corolario 3.15. *Sea $D$ un diagrama en la categoría de $R$-álgebras y $A = \varinjlim_i D_i$. Entonces, $\Omega_{A/R} \cong \varinjlim_i A \otimes_{D_i} \Omega_{D_i/R}$.*

Demostración. Es claro pues se deduce de que $\Omega_{\text{-}/R}$ preserva coproductos y conúcleos, y con estos objetos de puede construir el límite directo de cualquier diagrama de $A$-álgebras. □

Corolario 3.16. *(Propiedad de Localización) Sea $A$ una $R$-álgebra y $S \subseteq A$ un conjunto multiplicativo. Entonces, $\Omega_{A[S^{-1}]/R} \cong A[S^{-1}] \otimes_A \Omega_{A/R}$.*

Demostración. Dado que el módulo de fracciones $A[S^{-1}] \cong \varinjlim_{f\in S} A_f$ y por el resultado anterior el funtor cotangente relativo preserva límites directos, entonces basta con probar el resultado al tomar $S$ el conjunto multiplicativo formado por las potencias de $f \in A$. En efecto, como $A_f \cong A[x]/\langle fx-1\rangle$ por el lema de Rabinowitsch, al usar el Corolario 3.14 en el morfismo inclusión $\langle fx-1\rangle \hookrightarrow A[x]$ cuyo conúcleo es la proyección canónica $A[x] \to A_f$, se deduce que $\Omega_{A_f/R} \cong (A_f \otimes_{A[x]} \Omega_{A[x]/R})/\langle 1 \otimes d_{A[x]}(fx-1)\rangle$. Nótese que por 3.13 se tiene que $\Omega_{A[x]/R} \cong (A[x] \otimes_A \Omega_{A/R}) \oplus A[x]dx$, por lo que $A_f \otimes_{A[x]} \Omega_{A[x]/R} \cong (A_f \otimes_A \Omega_{A/R}) \oplus A_f dx$. Más aún, $d_{A[x]}(fx-1) = fd_{A[x]}x + xd_{A[x]}f$ y $f \in A_f$ es unidad, de lo que se deduce que $\Omega_{A_f/R} \cong A_f \otimes_A \Omega_{A/R}$. □

En este momento se disponen de todas las propiedades básicas del funtor cotangente relativo que nos serán de utilidad. Así, para hallar la conexión del módulo de diferenciales de Kähler con las $k$-álgebras finitamente generadas étale, se requiere el siguiente resultado de la teoría de campos.

Lema 3.17. *Sean $k \to L$ un morfismo de campos y $K|L$ una extensión algebraica separable. Entonces $\Omega_{K|\,k} \cong K \otimes_k \Omega_{L/\,k}$.*

Demostración. Dado que los funtores $\Omega_{\_/L}$ y $K \otimes_L \_$ conmutan con límites directos por la Proposición 3.15 y por ser un adjunto izquierdo, respectivamente, basta con probar la afirmación para el caso en que la extensión $K|L$ es finita. Luego, por el teorema del elemento primitivo existe $a \in K$ tal que $K = L(a)$. Además, si $f \in L[x]$ es el polinomio mínimo de $a$, entonces $K = L[x]/(f)$, de donde la sucesión conormal de $k$-álgebras asociada al morfismo suprayectivo $L[x] \to K$ tiene la forma:

$$(f)/(f^2) \longrightarrow K \otimes_{L[x]} \Omega_{L[x]/\,k} \longrightarrow \Omega_{K/\,k} \longrightarrow 0$$

Dado que por el Corolario 3.13 se tiene que $\Omega_{L[x]/\,k} \cong (L[x] \otimes_L \Omega_{L/\,k}) \oplus L[x]dx$, entonces $K \otimes_{L[x]} \Omega_{L[x]/\,k} \cong (K \otimes_L \Omega_{L/\,k}) \oplus Kdx$. Además, como mediante este isomorfismo al elemento $1 \otimes d_{L[x]}(f)$ le corresponde el elemento $f'(a)dx$ en $Kdx$, del hecho de que $K|L$ es separable se tiene que $f'(a) \neq 0$, por lo que $f'(a)dx$ genera a $Kdx$. De esto se deduce que $\Omega_{K/\,k} \cong K \otimes_L \Omega_{L/\,k}$. □

Con todas las herramientas desarrolladas se puede probar ahora el siguiente resultado, que es uno de los más importantes de esta sección.

Teorema 3.18. *Sea $A$ una $k$-álgebra finitamente generada. Entonces $A$ es étale si y sólo si $\Omega_{A/\,k} = 0$.*

Demostración. Si $A$ es una $k$-álgebra finitamente generada étale, entonces $A = \prod_{i=1}^{n} L_i$ con $L_i|\, k$ una extensión finita y separable para cada $i \in \{1, ..., n\}$. Por la Proposición 3.11 se deduce que $\Omega_{A/\,k} \cong \prod_{i=1}^{n} \Omega_{L_i/\,k}$ como $A$-módulos. Así, lo que se tiene que probar es que para cada $i \in \{1, ..., n\}$, $\Omega_{L_i/\,k} = 0$. Sin embargo, esto es claro del Lema 3.17.

Para el regreso supóngase que $\Omega_{A/\,k} = 0$. Como $\dim_k(A)$ es finita, entonces $A$ es artiniano. Así, por el teorema de estructura para anillos artinianos se tiene que $A$ es producto de una cantidad finita de anillos artinianos locales. Por lo tanto, para probar la afirmación se puede suponer que $A$ es un anillo artiniano local. Entonces sea $\mathfrak{m} \subseteq A$ el ideal máximo de $A$. Luego, se puede considerar la sucesión conormal:

$$\mathfrak{m}/\mathfrak{m}^2 \longrightarrow A/\mathfrak{m} \otimes_A \Omega_{A/\,k} \longrightarrow \Omega_{(A/\mathfrak{m})/\,k} \longrightarrow 0.$$

Así, la hipótesis implica que $\Omega_{(A/\mathfrak{m})/\,k} = 0$. Más aún, esto implica que la extensión $(A/\mathfrak{m})|\, k$ es finita y separable. Luego, el morfismo $\mathfrak{m}/\mathfrak{m}^2 \to A/\mathfrak{m} \otimes_A \Omega_{A/\,k}$ es inyectivo por el Corolario 3.8 y así, $\mathfrak{m}/\mathfrak{m}^2 = 0$. El lema de Nakayama implica que $\mathfrak{m} = 0$ y esto concluye la prueba pues entonces $A|\, k$ es una extensión finita y separable. □

## 2. Morfismos étale finitos

En esta sección se comenzará por recordar algunos conceptos y resultados básicos relativos a la teoría de esquemas. En esta dirección se comienza por recordar que para $f : X \to Y$ una función continua y $\mathcal{F} \in \mathbf{ASh(X)}$, se define la **imagen directa** de $\mathcal{F}$ mediante $f$, denotada por $f_* \mathcal{F}$, como la pregavilla que para $V \in \mathcal{O}(X)$ tiene por regla de correspondencia $(f_* \mathcal{F})(V) = \mathcal{F}(f^{-1}(V))$. Además, para $V, W \in \mathcal{O}(Y)$ con $V \subseteq W$, $\mathrm{res}_V^W(f_* \mathcal{F}) = \mathrm{res}_{f^{-1}(V)}^{f^{-1}(W)}(\mathcal{F})$. Puede probarse que de hecho esto da lugar a un funtor $f_* : \mathbf{ASh(X)} \to \mathbf{ASh(Y)}$ y que este tiene un adjunto izquierdo conocido como el funtor imagen inversa, $f^{-1}$.

Dado $M \in$ **A-Mod**, a este se le puede asociar un $\mathcal{O}_{\mathrm{X}}$-módulo, con $X = \operatorname{Spec} A$, que se denota por $\tilde{M}$, tal que en los abiertos básicos para la topología de Zariski de $X$, $X_f$ para $f \in A$, $\tilde{M}(X_f) = M_f$. Esta construcción, que se conoce como **construcción "tilde"**, define un funtor entre las categorías **A-Mod** y $\mathcal{O}_X - \mathbf{Mod}$, que de hecho establece una equivalencia de categorías con su imagen. Además, este funtor preserva sucesiones exactas.

Definición 3.19. *Sea $X$ un esquema y $\mathcal{F}$ un $\mathcal{O}_X$-módulo. Se dice que:*

1. *$\mathcal{F}$ es una gavilla* ***casi-coherente*** *(sobre $X$) si existe una cubierta afín de $X$, $\{U_i = \operatorname{Spec}(A_i)\}_{i\in I}$, tal que para cada $i \in I$, $\mathcal{F}|_{U_i} \cong \tilde{M}_i$ para $M_i$ un $A_i$-módulo.*
2. *$\mathcal{F}$ es una gavilla* ***coherente*** *(sobre $X$) si existe una cubierta afín de $X$, $\{U_i = \operatorname{Spec}(A_i)\}_{i\in I}$, tal que para cada $i \in I$, $\mathcal{F}|_{U_i} \cong \tilde{M}_i$ para $M_i$ un $A_i$-módulo finitamente generado.*
3. *$\mathcal{F}$ es* ***localmente libre*** *(sobre $X$) si existe una cubierta afín de $X$, $\{U_i = \operatorname{Spec}(A_i)\}_{i\in I}$, tal que para cada $i \in I$, $\mathcal{F}|_{U_i} \cong \tilde{M}_i$ para $M_i$ un $A_i$-módulo libre. Si en este caso resulta que todos los módulos tienen rango constante $r$, se dice que $\mathcal{F}$ es* ***localmente libre de rango*** *$r$.*

En la busqueda de dar la definición de los morfismos de esquemas que son los equivalentes a las aplicaciones cubrientes en topología, se recuerdan las siguientes definiciones básicas.

Definición 3.20. *Sea $\phi : Y \to X$ un morfismo de esquemas afín. Se dice que dicho morfismo es:*

1. ***finito*** *si para todo $U \subseteq X$ abierto, $\phi_*\mathcal{O}_Y(U)$ es un $\mathcal{O}_X(U)$-módulo finito.*
2. ***localmente libre de rango finito*** *si es finito y la gavilla $\phi_*\mathcal{O}_Y$ es localmente libre de rango finito.*

Entre las propiedades básicas de los morfismos finitos y localmente libres de rango de finito se encuentra que estos son cerrados bajo composición. Así, la última definición que se requiere recordar se encuentra en la siguiente discusión.

Sean $\phi : Y \to X$ un morfismo de esquemas y $x \in X$. Para $U \subseteq X$ un abierto afín, con $U = \operatorname{Spec} A$, tal que $x \in U$, se tiene que a $x$ le corresponde un ideal primo $\mathfrak{p}_x \subseteq A$. . Si se pone $k(x) := A_{\mathfrak{p}_x}/\,\mathfrak{p}_x A_{\mathfrak{p}_x}$ para el **campo de residuos** en el punto $x$, el morfismo de anillos canónico $A \to k(x)$ induce un morfismo de esquemas $\overline{x} : \operatorname{Spec} k(x) \to X$. Con esta notación se define la **fibra** de $\phi$ en $x$, $Y_x$, mediante el siguiente producto fibrado en la categoría de esquemas

$$\begin{tikzcd} Y_x = Y \times_X \operatorname{Spec} k(x) \arrow[r] \arrow[d] & Y \arrow[d, "\phi"] \\ \operatorname{Spec} k(x) \arrow[r, "\overline{x}"'] & X \end{tikzcd}$$

Vale la pena mencionar que aunque es sabido que el espacio topológico subyacente al producto fibrado de dos esquemas no es el producto fibrado de los espacios topológicos subyacentes en cada uno de los esquemas, esta anomalía no se tiene para el caso de fibras pues de hecho para cada $x \in X$, $\phi^{-1}(x)$ y el espacio subyacente al esquema $Y_x$ resultan ser homeomorfos. También, se recuerda que a los morfismos $\operatorname{Spec}(k) \to X$ cuando $k$ es algebraicamente cerrado se les conoce como **puntos geométricos** del esquema $X$.

La definición que se busca se presenta a continuación.

DEFINICIÓN 3.21. *Sea $\phi : Y \to X$ un morfismo finito de esquemas. Se dice que el morfismo $\phi$ es:*

1. ***étale finito*** *si es localmente libre y toda fibra de $\phi$, $Y_x$, es el espectro de una $k(x)$-álgebra finita étale.*
2. ***cubriente étale finito*** *si es un morfismo étale finito suprayectivo.*

EJEMPLO 3.22. *Sea $n \in \mathbb{N}$ con $n \geq 2$. Considérese el morfismo de $k$-álgebras $k[t] \to k[t]$ tal que $t \mapsto t^n$, y sea $\phi : \mathbb{A}^1_k \to \mathbb{A}^1_k$ el morfismo afín inducido. Nótese que $\phi$ es finito y localmente libre. Sin embargo, este morfismo no es étale pues su fibra en $0$, $(\mathbb{A}^1_k)_0$, es isomorfa al espectro de un punto no reducido simple.*

EJEMPLO 3.23. *Como se mencionó en el Capítulo 1, la definición de $k$-álgebra étale tiene una parte geométrica, que como es de esperarse se encuentra contenida en los morfismos étale. Para ver esto, sea $L|\,k$ una extensión de campos finita. El morfismo de esquemas afín inducido por la inclusión $\phi : \operatorname{Spec} L \to \operatorname{Spec} k$ es finito y localmente libre. Además, este es étale si y sólo si $L|\,k$ es separable. Más generalmente, para $A$ una $k$-álgebra finita, se tiene que el morfismo de esquemas $\phi : \operatorname{Spec} A \to \operatorname{Spec} k$ es étale si y sólo si $A$ es una $k$-álgebra finita étale.*

EJEMPLO 3.24. *Sea $\phi : Y \to X$ el morfismo de esquemas afines inducido por el morfismo de anillos canónico $A \to B$, donde $B = A[t]/(f)$ con $f \in A[t]$ un polinomio mónico de grado d. Dado que $B$ es un $A$-módulo finitamente generado por el conjunto $\{\bar{1}, \bar{t}, ..., \bar{t}^{d-1}\}$, entonces $\phi$ es un morfismo finito y localmente libre. Más aún, si mcd$(f, f') = 1$ en $A[t]$, entonces dado $x \in X$ se tiene que $Y_x = \operatorname{Spec}(B \otimes_A k(x))$, y dado que $B \otimes_A k(x) \cong k(x)[t]/(\overline{f})$, el que $f$ tenga raíces simples implica que $k(x)[t]/(\overline{f})$ es una $k(x)$-álgebra finita étale. Por lo tanto, bajo estas condiciones $\phi : Y \to X$ es un morfismo étale finito.*

Ejemplo 3.25. *Sea $\phi : Y \to X$ un morfismo de esquemas afines con $X$ neteriano y normal de dimensión 1. Si $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$ y $\phi$ es inducido por una inclusión $A \subseteq B$, entonces $A$ y $B$ son anillos de Dedekind y los puntos en la fibra $\mathfrak{p} \in X$ corresponden a factores primos $\mathfrak{p}_i$ en la descomposición $\mathfrak{p}B = \mathfrak{p}_1^{k_1} \cdot ... \cdot \mathfrak{p}_n^{k_n}$. En particular, $Y_{\mathfrak{p}}$ es espectro de una $k(\mathfrak{p})$-álgebra finitamente generada étale si y sólo si $k_i = 1$ para todo $i \in \{1, ..., n\}$.*

*Un caso particularmente interesante que conecta se da cuando se considera una torre de extensiones finitas $L|\,k\,|\mathbb{Q}$. Luego, al considerar $A$ la cerradura entera de $\mathbb{Z}$ en $k$ y $B$ la cerradura entera de $\mathbb{Z}$ en $L$, se tiene que el morfismo de esquemas afines $\phi : \operatorname{Spec} B \to \operatorname{Spec} A$ es finito y suprayectivo. Así, en este ejemplo $\phi$ es un cubriente étale si y sólo si la extensión $L|\,k$ es **no ramificada**. Más aún, un famoso teorema de Minkowski afirma que toda extensión no trivial $\mathbb{Q}$ se ramifica (ver por ejemplo Teorema 2.18* [**Neu**, pp 207]*). Por lo tanto, el teorema de Minkowski puede interpretarse diciendo que* $\operatorname{Spec} \mathbb{Z}$ *no tiene cubrientes étale finitos no triviales.*

Ejemplo 3.26. *Un encaje cerrado es étale si y sólo si es un encaje abierto y cerrado (Ver Proposición 5.17* [**L**, pp 74–75]*).*

Ahora se discutirán algunas propiedades relativas a la clase especial de morfismos que se muestran en la Definición 3.21.

Proposición 3.27. *Sea $X$ un esquema afín. El funtor $F : (\boldsymbol{AfSm}/X)^{op} \to$ **qCoh(**$\mathcal{O}_{\mathrm{X}}$ **−Alg)** que a nivel de objetos se define como $(\phi : Y \to X) \mapsto \phi_*(\mathcal{O}_Y)$, es una equivalencia de categorías.*

Demostración. Lo primero que se observa es que por definición de morfismo de esquemas $F$ está bien definido, es decir, que dado $\phi : Y \to X \in (\mathbf{AfSm}/X)^{op}$, se tiene que $\phi_*(\mathcal{O}_Y)$ es un $\mathcal{O}_X$-módulo y que además dado $U = \operatorname{Spec} A \subseteq X$ un abierto afín, como $\phi^{-1}(U) = \operatorname{Spec} B$, se tiene que al considerar a $B$ como un $A$-módulo se satisface que $\phi_*(\mathcal{O}_Y)|_U \cong \tilde{B}$. También se observa que para $\psi \in (\mathbf{AfSm}/X)^{op}(\varphi : Z \to X, \phi : Y \to X) = \mathbf{AfSm}/X(\phi : Y \to X, \varphi : Z \to X)$, $F(\psi) = \varphi_*\psi^\sharp$, con $\psi^\sharp : \mathcal{O}_Z \to \psi_*\mathcal{O}_Y$.

Para probar la afirmación que se quiere se va a construir un funtor

$$G : \mathbf{qCoh(}\,\mathcal{O}_{\mathrm{X}}\,\mathbf{-Alg)} \to (\mathbf{AfSm}/X)^{op}$$

tal que $F \circ G \cong 1_{\mathbf{qCoh(}\,\mathcal{O}_{\mathrm{X}}\,\mathbf{-Alg)}}$ y $G \circ F \cong 1_{(\mathbf{AfSm}/X)^{op}}$. Así, dada $\mathcal{A} \in \mathbf{qCoh(}\,\mathcal{O}_{\mathrm{X}}\,\mathbf{-Alg)}$, considérense abiertos distinguidos de $X$, $U = \operatorname{Spec} A$ y $V = \operatorname{Spec} B$. Si estos son tales que $U \cap V \neq \emptyset$, entonces se cubre por abiertos distinguidos a dicha intersección y sea $W = \operatorname{Spec} C$ uno de tales abiertos distinguidos. Dado que $W \subseteq U$, se tiene el siguiente diagrama conmutativo:

$$\begin{tikzcd}
\mathcal{A}(U) \arrow[r, "\mathrm{res}^U_W(\mathcal{A})"] & \mathcal{A}(W) \\
\mathcal{O}_X(U) \arrow[u, "r_U"] \arrow[r, "\mathrm{res}^U_W(\mathcal{O}_X)"'] & \mathcal{O}_X(W) \arrow[u, "r_W"']
\end{tikzcd}$$

Dado que $C$ es una localización de $A$ y $B$, entonces $\mathcal{A}(W)$ es una localización de $\mathcal{A}(U)$ y $\mathcal{A}(V)$, por lo que se pueden identificar $\mathcal{A}(U)$ y $\mathcal{A}(V)$ a lo largo de $\mathcal{A}(W)$. Además, los morfismos de anillos $r_U : A \to \mathcal{A}(U)$ y $r_V : B \to \mathcal{A}(V)$ inducen los morfismos de esquemas afines $(\phi_{\mathcal{A}})_U : \operatorname{Spec} \mathcal{A}(U) \to U$ y $(\phi_{\mathcal{A}})_V : \operatorname{Spec} \mathcal{A}(V) \to V$. Pero los isomorfismos dados por los abiertos distinguidos que cubren a $U \cap V$ permiten definir un isomorfismo de esquemas afines $(\phi_{\mathcal{A}})_U^{-1}(U \cap V) \cong (\phi_{\mathcal{A}})_V^{-1}(U \cap V)$. Sin embargo, como estos isomorfismos son definidos mediante los morfismos de restricción de una gavilla, estos definen globalmente un morfismo $\phi_{\mathcal{A}} : Y \to X$, el cual es por construcción afín. Notacionalmente se escribe $Y = \operatorname{Spec}(\mathcal{A})$.

La construcción anterior permite definir $G(\mathcal{A}) = \phi_{\mathcal{A}}$. Además, como para cada abierto afín $U \subseteq X$ se tiene que $(\phi_{\mathcal{A}})_*(\mathcal{O}_Y)(U) = \mathcal{O}_Y(\phi_{\mathcal{A}}^{-1}(U)) \cong \mathcal{O}_Y(\operatorname{Spec} \mathcal{A}(U)) \cong \mathcal{A}(U)$, se deduce que $FG(\mathcal{A}) = F(\phi_{\mathcal{A}}) = (\phi_{\mathcal{A}})_* \mathcal{O}_Y \cong \mathcal{A}$.

Por otro lado, dado $\phi : Y \to X \in (\mathbf{AfSm}/X)^{op}$ y al ser $\phi_* \mathcal{O}_Y \in \mathbf{qCoh}(\mathcal{O}_X{-}\mathbf{Alg})$, de la construcción se tiene que $Y \cong \operatorname{Spec}(\phi_* \mathcal{O}_Y)$ en $\mathbf{Sm}/X$. Entonces $GF(\phi) = G(\phi_* \mathcal{O}_Y) = \phi_{\phi_* \mathcal{O}_Y} \cong \phi$, de lo que se deduce la afirmación. □

Del resultado anterior y de la definición de morfismos finitos étale se obtiene el siguiente resultado de manera inmediata.

Corolario 3.28. *Definir un morfismo localmente libre sobre un esquema $X$ es equivalente a definir una $\mathcal{O}_{\mathrm{X}}$-álgebra casi-coherente de rango finito como $\mathcal{O}_{\mathrm{X}}$-módulo. Además, los morfismos étale finitos corresponden a $\mathcal{O}_{\mathrm{X}}$-álgebras $\mathcal{A}$ tales que $\mathcal{A}_x \otimes_{\mathcal{O}_{X,x}} k(x)$ es una $k(x)$-álgebra finita étale para cada $x \in X$.*

Proposición 3.29. *Un morfismo finito de esquemas $\phi : Y \to X$ es localmente libre si y sólo si $\phi_* \mathcal{O}_Y$ es una gavilla plana de $\mathcal{O}_X$-módulos.*

Demostración. Se deduce del hecho de que sobre un anillo local $(R, \mathfrak{m})$, un $R$-módulo es libre si y sólo si es plano. □

Proposición 3.30. *La imagen de un morfismo finito y localmente libre es abierta y cerrada.*

Demostración. Sea $\phi : Y \to X$ un morfismo finito y localmente libre. Dado que todo morfismo finito entre esquemas afines es cerrado, se deduce que $\phi(Y)$ es cerrado en $X$. Para la segunda afirmación se recuerda que $\phi(Y) = \operatorname{supp}(\phi_* \mathcal{O}_Y)$, por lo que si $\phi(y) \in \phi(Y)$, entonces por definición de soporte se tiene que $(\phi_* \mathcal{O}_Y)_{\phi(y)} \neq 0$. La definición de tallo implica que existe $U \subseteq X$ abierto tal que $\phi(y) \in U$ y $(\phi_* \mathcal{O}_Y)(U) \neq 0$, de lo que se deduce que $U \subseteq \phi(Y)$ y así, $\phi(Y)$ es abierto en $X$. □

En dirección de buscar una estructura categórica para los morfismos étale finitos, nótese que la identidad sobre un esquema es un morfismo étale finito. También se tiene lo siguiente.

Proposición 3.31. *Sean $\phi : Y \to X$ y $\psi : Z \to Y$ morfismos de esquemas étale finitos. Entonces, $\phi \circ \psi : Z \to X$ es un morfismo étale finito.*

Demostración. La composición de morfismos finitos y localmente libres es finito y localmente libre. Así, sea $x \in X$ y considérese el siguiente diagrama donde cada uno de los cuadrados en un producto fibrado.

$$\begin{tikzcd} Z \times_Y Y_x \arrow[r] \arrow[d] & Z \arrow[d, "\psi"] \\ Y_x \arrow[r] \arrow[d] & Y \arrow[d, "\phi"] \\ \operatorname{Spec} \overline{k(x)} \arrow[r, "\overline{x}"'] & X \end{tikzcd}$$

Como el cuadrado exterior es un producto fibrado, entonces $Z_x \cong Z \times_Y Y_x$. Al ser $\phi$ étale finito, se tiene que $Y_x \cong \operatorname{Spec}(\prod_{i=1}^n L_i)$ con $L_i |\, k(x)$ extensión finita y separable para cada $i \in \{1, ..., n\}$. Además, dado que $Z \times_Y Y_x \cong \coprod_{i=1}^n Z \times_Y \operatorname{Spec} L_i$, al ser $\psi$ étale finito, para cada $i \in \{1, ..., n\}$ existe $A_i$ una $L_i$-álgebra finita étale tal que $Z \times_Y \operatorname{Spec} L_i \cong \operatorname{Spec}(A_i)$. Así, $Z \times_Y Y_x \cong \operatorname{Spec}(\prod_{i=1}^n A_i)$ y por lo tanto $Z_x \cong \operatorname{Spec}(\prod_{i=1}^n A_i)$. Nótese que $\prod_{i=1}^n A_i$ es una $k(x)$-álgebra finita étale pues cada $A_i$ es étale finita sobre $L_i$ y $L_i |\, k(x)$ es una extensión separable. □

El siguiente resultado también tiene una interpretación categórica pues tiene que ver con la preservación de la propiedad de ser étale finito bajo productos fibrados, es decir, de la existencia de un funtor cambio de base.

PROPOSICIÓN 3.32. *Sean $\phi : Y \to X$ un morfismo étale finito y $\psi : Z \to X$ un morfismo de esquemas. Si el siguiente diagrama representa el producto fibrado de $\phi$ a lo largo de $\psi$*

$$\begin{tikzcd} Y \times_X Z \arrow[r, "p_1"] \arrow[d, "p_2"'] & Y \arrow[d, "\phi"] \\ Z \arrow[r, "\psi"'] & X, \end{tikzcd}$$

*entonces $p_2 : Y \times_X Z \to Z$ es un morfismo étale finito.*

DEMOSTRACIÓN. Se sabe que con estas hipótesis $p_2$ es un morfismo localmente libre de rango finito. Así, lo que resta probar es la condición sobre las fibras. Para esto sean $z \in Z$ y $\overline{z} : \operatorname{Spec} K \to Z$ un punto geométrico que define dicho elemento. Entonces considérese el siguiente diagrama:

$$\begin{tikzcd} (Y \times_X Z)_z \arrow[r, "q_1"] \arrow[d, "q_2"'] & Y \times_X Z \arrow[r, "p_1"] \arrow[d, "p_2"'] & Y \arrow[d, "\phi"] \\ \operatorname{Spec} K \arrow[r, "\overline{z}"'] & Z \arrow[r, "\psi"'] & X, \end{tikzcd}$$

Dado que ambos cuadrados son productos fibrados, entonces el cuadrado completo es un producto fibrado, lo que prueba que $(Y \times_X Z)_z \cong Y_{\psi \circ \overline{z}}$. Pero al ser $\phi$ un morfismo finito étale, esto implica que $Y_{\psi \circ \overline{z}}$ es isomorfo al espectro de una $K$-álgebra finita étale, de lo que se deduce que $(Y \times_X Z)_z$ es isomorfa a una $K$-álgebra finita étale y concluye la prueba de la afirmación. $\square$

Una vez que ya se tienen las propiedades básicas de los morfismos étale finitos, lo que se busca es un teorema de caracterización de dichos morfismos. Para esto se requiere un resultado algebraico, por lo que considérese $A$ una $R$-álgebra. Dado que el producto en $A$ es una función $R$-bilineal, esta induce un morfismo de $A$-módulos $m : A \otimes_R A \to A$. Luego, escríbase $I = \operatorname{nuc} m$. Nótese que $I = \langle \{1 \otimes a - a \otimes 1 \mid a \in A\} \rangle$ como $A \otimes_R A$-módulo pues para la conteción no trivial, dado $\sum_{i=1}^n a_i \otimes b_i \in \operatorname{nuc} m$, se tiene que $\sum_{i=1}^n a_i b_i = 0$. Así que,

$$\sum_{i=1}^{n} (a_i \otimes 1)(1 \otimes b_i - b_i \otimes 1) = \sum_{i=1}^{n} a_i \otimes b_i - \sum_{i=1}^{n} a_i b_i \otimes 1 = \sum_{i=1}^{n} a_i \otimes b_i.$$

LEMA 3.33. *Sean $A$ una $R$-álgebra e $I$ el núcleo del morfismo inducido por el producto $m : A \otimes_R A \to A$. Entonces, existe un isomorfismo canónico de $A$-módulos entre $\Omega_{A/R}$ e $I/I^2$.*

DEMOSTRACIÓN. Por la propiedad universal del módulo de diferenciales de Kähler, el definir un morfismo de $A$-módulos $\phi : \Omega_{A/R} \to I/I^2$ es equivalente a definir una $R$-derivación $d : A \to I/I^2$. Así, se define $d(a) = (1 \otimes a - a \otimes 1) + I^2$, la cual es sencillo ver que es en efecto una $R$-derivación. Por lo tanto, esta define un morfismo de $A$-módulos tal que para cada $a \in A$, $\phi(d_A a) = (1 \otimes a - a \otimes 1) + I^2$. Para ver que este $\phi$ es un isomorfismo, se va a construir su inversa. En esta dirección se considera la estructura estándar de grupo abeliano en el conjunto $A \times \Omega_{A/R}$, y se define el producto $(a, x)(b, y) = (ab, ay + bx)$. Luego, se considera $g : A \otimes_R A \to A \times \Omega_{A/R}$ definida por la propiedad universal del producto tensorial mediante el morfismo $R$-bilineal $A \times A \to A \times \Omega_{A/R}$ tal que $(a, b) \mapsto (ab, ad_A(b))$. Nótese que $g(1 \otimes a - a \otimes 1) = (0, da)$, por lo que $g$ induce el morfismo buscado en la otra dirección al definir $\overline{g} : I/I^2 \to \Omega_{A/R}$ dado por $\overline{g}(x + I^2) = \pi_2 g(x)$. Esta es una función pues $g(I^2) = 0$ por construcción del producto en $A \times \Omega_{A/R}$.

Para concluir se observa que $(g \circ \phi)(d_A(a)) = (0, d_A a)$, por lo que $\overline{g} \circ \phi = 1_{\Omega_{A/R}}$. Por otro lado, si $x \in I$ tiene la forma $x = \sum_{i=1}^n a_i \otimes b_i$, entonces

$$\phi \circ \overline{g}(x + I^2) = \phi(\sum_{i=1}^n a_i d_A(b_i)) = \sum_{i=1}^n a_i \phi(d_A(b_i)) = \sum_{i=1}^n (a_i \otimes b_i + a_i b_i \otimes 1) + I^2 = x + I^2,$$

pues $\sum_{i=1}^n a_i b_i = 0$. $\square$

LEMA 3.34. *(Cambio de base de las diferenciales de Kähler) Sean $A$ y $B$ $R$-álgebras. Entonces $\Omega_{(A \otimes_R B)/A} \cong A \otimes_R \Omega_{B/R}$.*

DEMOSTRACIÓN. Considérese el morfismo $1_A \otimes d_B : A \otimes_R B \to A \otimes_R \Omega_{B/R}$, el cual define una $A$-derivación. Así, por la propiedad universal de las diferenciales de Kähler este induce un morfismo de $(A \otimes_R B)$-módulos $f : \Omega_{(A \otimes_R B)/A} \to A \otimes_R \Omega_{B/R}$ tal que para cada $a \in A$ y $b \in B$, $f(d_{(A \otimes_R B)}(a \otimes b)) = a \otimes d_B(b)$.

Por otro lado, la propiedad universal del módulo de diferenciales de Kähler permite definir un morfismo de $B$-módulos, $\Omega_{B/R} \to \Omega_{(A \otimes_R B)/A}$, tal que $d_B(b) \mapsto d_{(A \otimes_R B)}(1 \otimes b)$. Esto permite definir un morfismo $A \times \Omega_{B/R} \to \Omega_{A \otimes_R B/R}$ tal que $(a, d_B(b)) \mapsto d_{A \otimes_R B}(a \otimes b)$. Es claro que este es $R$-bilineal, por lo que este induce un morfismo $g : A \otimes_R \Omega_{B/R} \to \Omega_{(A \otimes_R B)/R}$ tal que $g(a \times d_B(b)) = d_{A \otimes_R B}(a \otimes b)$. Es claro que $g$ resulta ser la inversa de $f$. $\square$

Sea $\phi : Y \to X$ un morfismo separado de esquemas. Para $\Delta_\phi : Y \to Y \times_X Y$, denótese por $\mathcal{I}$ al núcleo del morfismo de gavillas asociado $\Delta_\phi^\sharp : \mathcal{O}_{Y\times_X Y} \to (\Delta_\phi)_*\mathcal{O}_Y$. Como sucede en el caso afín, esto da estructura a $\mathcal{I}/\mathcal{I}^2$ de $\mathcal{O}_{Y\times_X Y}/\mathcal{I}$-módulo. Por definición $\Delta_\phi(Y) \subseteq Y \times_X Y$ es un subesquema cerrado y además la gavilla $\mathcal{I}/\mathcal{I}^2$ es cero fuera de $\Delta_\phi(Y)$, por lo que puede identificarse con $\mathcal{O}_{\Delta_\phi(Y)}$.

DEFINICIÓN 3.35. *La **gavilla de diferenciales relativas** $\Omega_{Y/X}$ es el $\mathcal{O}_Y$-módulo definido por el producto fibrado del $\mathcal{O}_{\Delta_\phi(Y)}$-módulo $\mathcal{I}/\mathcal{I}^2$ vía el isomorfismo $Y \cong \Delta_\phi(Y)$.*

PROPOSICIÓN 3.36. *Sea $\phi : Y \to X$ un morfismo finito y localmente libre. Son equivalentes:*

1. *$\phi$ es étale.*
2. *$\Omega_{Y/X} = 0$.*
3. *El morfismo diagonal $\Delta_\phi : Y \to Y \times_X Y$ es un isomorfismo de $Y$ con un subesquema abierto-cerado de $Y \times_X Y$.*

DEMOSTRACIÓN. $1 \Rightarrow 2$) Como $\phi$ es finito, entonces es separado y por lo tanto $\Omega_{Y/X}$ está definida. Además, como se quiere probar una condición local, puede suponerse que $\phi$ es un morfismo entre esquemas afines y por la propiedad de localización, cambio de base y la versión geométrica del lema de Nakayama, todo se reduce a probar que para cada $x \in X$, $Y_x$ es el espectro de una $k(x)$-álgebra finita étale si y sólo si $\Omega_{Y_x|\operatorname{Spec} k(x)} = 0$, condición que se satisface por el Teorema 3.18.

$2 \Rightarrow 3$) Dado que $\phi$ es un morfismo finito, entonces es separado y así, el morfismo diagonal $\Delta_\phi : Y \to Y \times_X Y$ es una inmersión cerrada. Luego, a esta corresponde una gavilla de ideales $\mathcal{I}$ de $Y \times_X Y$. Así, la restricción de $\mathcal{I}/\mathcal{I}^2$ a $\Delta_\phi(Y)$ es isomorfa a $\Omega_{Y|X}$, que es cero por hipótesis. Al usar la versión geométrica del lema de Nakayama se deduce que el tallo de $\mathcal{I}$ es trivial en todos los puntos de $\Delta_\phi(Y)$. Además, como $\mathcal{I}$ es coherente, se tiene que $\mathcal{I} = 0$ en un abierto de $Y \times_X Y$, por lo que $\Delta_\phi(Y)$ es un abierto cerrado en $Y \times_X Y$.

$3 \Rightarrow 1$) Sea $\overline{x} : \operatorname{Spec} \overline{k(x)} \to X$ un punto geométrico y considérese el morfismo diagonal inducido por $\phi$, $\Delta_\phi : Y \to Y \times_X Y$. Luego, sea el siguiente cuadrado conmutativo, que es un producto fibrado en la categoría de esquemas.

$$\begin{tikzcd}
Y_x \arrow[r, "p_1"] \arrow[dd, "p_2"'] & Y \arrow[d, "\Delta_\phi"] \\
 & Y \times_X Y \arrow[d] \\
\operatorname{Spec} \overline{k(x)} \arrow[r, "\overline{x}"'] & X
\end{tikzcd}$$

Nótese que $Y_x \times_X Y \cong (Y \times_X \operatorname{Spec} \overline{k(x)}) \times_{\operatorname{Spec} \overline{k(x)}} (\operatorname{Spec} \overline{k(x)} \times_X Y) \cong Y_x \times_{\operatorname{Spec} \overline{k(x)}} Y_x$. Así, el morfismo $\Delta_x : Y_x \to Y_x \times_X Y$ inducido establece un isomorfismo de $Y_x$ con un subesquema abierto-cerrado de $Y_x \times_{\operatorname{Spec} \overline{k(x)}} Y_x$. Dado que $Y_x = \operatorname{Spec} A$ con $A$ una $\overline{k(x)}$-álgebra finitamente generada, entonces $Y_x$ tiene una cantidad finita de puntos, todos ellos con campos de residuos $\overline{k(x)}$ por ser este campo algebraicamente cerrado. Así, si se toma $\overline{y} : \operatorname{Spec} \overline{k(x)} \to Y_x$ uno de tales puntos, entonces al realizar un cambio de base a través de $\overline{y}$ se obtiene un morfismo $\operatorname{Spec} \overline{k(x)} \to Y_x$, que es un isomorfismo con un subesquema abierto-cerrado de $Y_x$. Como $\operatorname{Spec} \overline{k(x)}$ es conexo, dicho subesquema debe ser una componente conexa. Luego, se ha probado que $Y_x$ es una unión finita de puntos como subesquema, lo que prueba la afirmación. $\square$

Vale la pena mencionar que en el teorema anterior las dos primeras implicaciones dan un buen criterio para ver si un morfismo finito y localmente libre es étale, el cual pone en manifiesto que dicha propiedad tiene un trasfondo diferencial. Para ver esto supóngase que se tiene un abierto afín de $X$, $U = \operatorname{Spec} A$, tal que $\phi^{-1}(U) = \operatorname{Spec} A[x_1, ..., x_n]/\langle f_1, ..., f_n\rangle$ con los polinomios $f_i$ mónicos. Si sobre todos estos abiertos afines el determinante del jacobiano $(\partial_i f_j)_{i,j}$ va a una unidad en $A[x_1, ..., x_n]/\langle f_1, ..., f_n\rangle$, entonces $\Omega_{Y/X} = 0$, y así $\phi$ es étale. A esto se le conoce como el **criterio del Jacobiano** y para una discusión mucho más amplia del tema se recomiendan las secciones 5 y 10 del Capítulo 3 en [**M**].

Para concluir esta sección se va presentar un resultado más. Nótese que este es un análogo, para el caso de esquemas, de la Proposición 2.4, que se podía interpretar como una condición de trivialidad local para aplicaciones cubrientes pues decía que dichas funciones continuas eran localmente haces triviales, y que de hecho eso las caracterizaba.

Definición 3.37. *Un cubriente étale finito $\phi : Y \to X$ es* ***trivial*** *si $Y$ es isomorfo a una unión finita disjunta de copias de $X$ en* $\boldsymbol{Sm}/X$ *y, $\phi$ se restringe a la identidad en cada componente.*

Proposición 3.38. *Sea $\phi : Y \to X$ un morfismo de esquemas suprayectivo con $X$ conexo. Entonces, $\phi$ es un cubriente étale finito si y sólo si existe un morfismo $\psi : Z \to X$ finito, localmente libre y suprayectivo tal que $Y \times_X Z$ es cubriente trivial de $Z$.*

Demostración. $\Rightarrow$) Considérse $\phi$ como en las hipótesis. Dado que $X$ es conexo, entonces las fibras de $\phi$ tienen todas la misma cardinalidad y sea esta $n$. Luego, la prueba se va a realizar por inducción sobre $n$.

El paso base $n = 1$ es claro. Así, suponiendo que el resultado es válido para morfismos con fibras de cardinalidad $n-1$, supóngase que $\phi$ tiene fibras con cardinalidad $n$. Luego, de la tercera afirmación del Teorema 3.36 se deduce que $\Delta_\phi : Y \to Y \times_X Y$ induce una sección para $p_2 : Y \times_X Y \to Y$. De hecho nótese que esto dice que $Y \times_X Y \cong Y \coprod Y'$ con $Y'$ subesquema abierto y cerrado. Así, del Ejemplo 3.26 se deduce que la inclusión $\iota : Y' \to Y \times_X Y$ es un morfismo étale finito. Por otro lado, de la Proposición 3.32 se deduce que $p_2$ es un morfismo étale finito, por lo que $p_2 \circ \iota : Y' \to Y$ es un morfismo étale finito. Luego, al aplicar la hipótesis de inducción se deduce que existe $\psi' : Z \to Y$ tal que el morfismo $q_2 : Y' \times_Y Z \to Z$ es finito, localmente libre, suprayectivo y trivial. Luego, el morfismo $\psi : Z \to X$ definido por $\psi = \phi \circ \psi'$ permite concluir lo mismo respecto a $\phi$.

$\Leftarrow$) Lo primero que se va a probar es que $\phi$ es finito y localmente libre. Para esto nótese que si $U = \mathrm{Spec}(A)$ es un abierto afín, por hipótesis $\phi$ se restringe a un morfismo $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$. Por otro lado, la hipótesis implica que el morfismo $\psi$ se restringe a un morfismo $\mathrm{Spec}(C) \to \mathrm{Spec}(A)$ con $C$ un $A$-módulo libre finitamente generado, así, $B \otimes_A C$ es un $C$-módulo libre finitamente generado. Más aún, $B \otimes_A C$ es un $A$-módulo libre y finitamente generado. Pero como $C \cong A^n$ para algún $n \in \mathbb{N}^+$, se tiene que $B \otimes_A C \cong B^n$, por lo que la última observación implica que $B$ debe ser un $A$-módulo libre finitamente generado.

Respecto a la propiedad de ser $\phi$ étale finito, considérese $\overline{z} : \mathrm{Spec}\, K \to Z$ un punto geométrico de $Z$. Dado que $Y_{\psi \circ \overline{z}} \cong (Y \times_X Z)_{\overline{z}}$ y de la hipótesis de trivialidad $(Y \times_X Z)_{\overline{z}} \cong \coprod_{i \in F} \mathrm{Spec}\, K$ para $F$ finito, esto implica que la fibra $Y_{\psi \circ \overline{z}}$ es finita, es decir, es el espectro de una $K$-álgebra finita étale. Así, el resultado se concluye del hecho de que $\psi$ es suprayectiva. $\square$

## 3. Cubrientes étale finitos de Galois

Para comenzar esta sección se requiere del siguiente resultado que es el análogo del Lema 2.6 para el caso de esquemas, y que muestra nuevamente la analogía entre los cubrientes étale finitos y las aplicaciones cubrientes.

LEMA 3.39. *Sean $\phi : Y \to X$ y $\psi : Z \to Y$ morfismos de esquemas tales que $\phi \circ \psi : Z \to X$ y $\phi$ son étale finitos, entonces $\psi$ también lo es.*

DEMOSTRACIÓN. Considérese el siguiente diagrama donde el cuadrado es el producto fibrado de $\phi \circ \psi$ a lo largo de $\phi$. Se recuerda que en teoría de categorías este diagrama representa la construcción de la gráfica de $\psi$, que es el morfismo $\Gamma_\psi$.

$$\begin{tikzcd}
Z \arrow[drr, "1_Z"] \arrow[dr, dashed, "\Gamma_\psi"] \arrow[ddr, "\psi"'] & & \\
& Z \times_X Y \arrow[r, "p_1"] \arrow[d, "p_2"] & Z \arrow[d, "\phi\circ\psi"] \\
& Y \arrow[r, "\phi"'] & X
\end{tikzcd}$$

Nótese que por construcción $p_2 \circ \Gamma_\psi = \psi$ y además $p_2$ es un morfismo étale finito por la Proposición 3.32. Así, si se prueba que $\Gamma_\psi$ es un morfismo étale finito, entonces $\psi$ es composición de dos morfismos étale finitos y por lo tanto es uno de tales morfismos, lo que concluiría la prueba. Por lo tanto, lo que se tiene que probar es que $\Gamma_\psi$ es un morfismo étale finito.

En efecto, se sabe que la gráfica de $\psi$ también puede ser construida como el morfismo cambio de base de $\Delta_\phi$ a lo largo de $\psi \times_X 1_Y$. Luego, por la Proposición 3.36 se tiene que la inmesión $\Delta_\phi$ establece un isomorfismo entre $Y$ y un subesquema abierto-cerrado de $Y \times_X Y$ por ser $\phi$ étale finito, lo que implica que $\Delta_\phi$ es un morfismo étale. Por lo tanto la Proposición 3.32 implica que $\Gamma_\psi$ es un morfismo étale finito. $\square$

PROPOSICIÓN 3.40. *Sean $\phi : Y \to X$ un cubriente étale finito y $s : X \to Y$ una sección de $\phi$. Entonces, $s$ induce un isomorfismo entre $X$ y un subesquema abierto-cerrado de $Y$. En particular, si $X$ es conexo, entonces $s(X)$ es isomorfo a una componente conexa de $Y$.*

Demostración. Dado que $1_X$ y $\phi$ son morfismos étale finitos y $\phi \circ s = 1_X$, el lema anterior implica que $s$ también es étale finito. Luego, por la Proposición 3.30 se deduce que $s(X)$ es isomorfo a un subesquema abierto-cerrado de $Y$, lo que prueba la primera afirmación.

La segunda afirmación se deduce del hecho de que para $X$ conexo, $s(X)$ es un conexo y por lo tanto se encuetra contenido en una componente conexa de $Y$. Al ser este conjunto un abierto-cerrado no vacío, tiene que ser igual a toda la componente conexa. $\square$

Del resultado anterior se deduce el siguiente corolario que es un análogo del Lema 2.5 que fue muy útil para probar distintos resultados a lo largo del capítulo anterior.

Corolario 3.41. *Sean $\psi : Y \to X$ y $\varphi : Z \to X$ morfismos de esquemas con $Y$ conexo y $\varphi$ étale finito, así como $\phi_1, \phi_2 : Y \to Z$ tales que $\varphi \circ \phi_1 = \varphi \circ \phi_2 = \psi$ y existe un punto geométrico $\overline{y} : \operatorname{Spec} \overline{k(y)} \to Y$ con la propiedad de que $\phi_1 \circ \overline{y} = \phi_2 \circ \overline{y}$. Entonces, $\phi_1 = \phi_2$.*

Demostración. Considérese el siguiente diagrama donde el cuadrado es un producto fibrado e $i \in \{1, 2\}$.

$$\begin{tikzcd}
Y \arrow[drr, "\phi_i"] \arrow[dr, dashed, "\hat{\phi}_i"] \arrow[ddr, "1_Y"'] & & \\
& Z \times_X Y \arrow[r, "p_1"] \arrow[d, "p_2"] & Z \arrow[d, "\varphi"] \\
& Y \arrow[r, "\psi"'] & X
\end{tikzcd}$$

Dado que $\varphi$ es étale, entonces $p_2$ es étale. Además, nótese que para $i \in \{1, 2\}$ se tiene que $p_2 \circ \hat{\phi}_i = 1_Y$, es decir, $\hat{\phi}_1$ y $\hat{\phi}_2$ son secciones de $p_2$. Así, de la proposición anterior se deduce que estas inducen un isomorfismo de $Y$ con alguna componente conexa de $Z \times_X Y$. Pero como por hipótesis $\phi_1 \circ \overline{y} = \phi_2 \circ \overline{y}$, entonces la componente debe ser la misma y por lo tanto $\hat{\phi}_1 = \hat{\phi}_2$, de lo que se deduce el resultado. $\square$

Para el siguiente resultado se requiere de una discusión previa cuyo objetivo es obtener un análogo del grupo de transformaciones cubrientes para un esquema. Sean $\phi : Y \to X$ un morfismo de esquemas y $\operatorname{Aut}(Y|X)$ el conjunto cuyos elementos son los automorfismos de $Y$ que fijan $\phi$. Es claro que este conjunto es de hecho un grupo con operación la composición.

Por otro lado, dado un punto geométrico de $X$, $\overline{x}$, nótese que por la propiedad universal que define a la fibra geométrica existe una biyección entre los conjuntos $\mathbf{Sm}/\operatorname{Spec}\overline{k(x)}(\operatorname{Spec}\overline{k(x)}, Y_x)$ y $\mathbf{Sm}/X(\operatorname{Spec}\overline{k(x)}, Y)$, es decir, entre puntos geométricos de la fibra en $x$ de $\phi$, y puntos geométricos de $Y$.

$$
\begin{tikzcd}
\operatorname{Spec}\overline{k(x)} \arrow[dr, dashed] \arrow[drr] \arrow[ddr, "1_{\operatorname{Spec}\overline{k(x)}}"'] & & \\
& Y_x \arrow[r, "p_1"] \arrow[d, "p_2"'] & Y \arrow[d, "\phi"] \\
& \operatorname{Spec}\overline{k(x)} \arrow[r, "\overline{x}"'] & X
\end{tikzcd}
$$

Denótese por $F_{\overline{x}}(\phi) := \mathbf{Sm}/X(\operatorname{Spec}\overline{k(x)}, Y)$. Más aún, nótese que $\operatorname{Aut}(Y|X)$ actúa en $F_{\overline{x}}(\phi)$ pues si $\overline{y} : \operatorname{Spec}\overline{k(x)} \to Y$ es un punto geométrico de $Y$ en la categoría $\mathbf{Sm}/X$ y $\psi \in \operatorname{Aut}(Y|X)$, entonces se define $\psi \cdot \overline{y} := \psi \circ \overline{y}$. Como es claro que $\psi \cdot \overline{y} : \operatorname{Spec}\overline{k(x)} \to Y$ y además $\phi \circ (\psi \cdot \overline{y}) = (\phi \circ \psi) \circ \overline{y} = \phi \circ \overline{y}$, entonces $\psi \cdot \overline{y} \in F_{\overline{x}}(\phi)$.

Proposición 3.42. *Sea $\phi : Y \to X$ un cubriente étale conexo finito. Los elementos no triviales de* $\operatorname{Aut}(Y|X)$ *actúan sin puntos fijos en cada fibra geométrica. Más aún,* $\operatorname{Aut}(Y|X)$ *es finito.*

Demostración. La primera afirmación se sigue inmediatamente del corolario anterior. Para la segunda afirmación, sea $x \in X$. Luego, se construye la función $f : \operatorname{Aut}(Y|X) \to F_{\overline{x}}(\phi)$ mediante la regla de correspondencia $f(\psi) = \psi \cdot \overline{x}$. El corolario anterior implica nuevamente que $f$ es inyectiva, por lo que $|\operatorname{Aut}(Y|X)| \leq |F_{\overline{x}}(\phi)|$. Sin embargo, al ser $\phi$ un cubriente étale finito, existen $L_1, ..., L_n$ extensiones separables finitas de $k(x)$ tales que $Y_x = \operatorname{Spec}(\prod_{i=1}^n L_i)$. Pero como el funtor Spec manda productos en uniones ajenas, $Y_x \cong \coprod_{i=1}^n \operatorname{Spec}(L_i)$, de donde $|Y_x| = n$. La afirmación se sigue del hecho de que $|Y_x| = |F_{\overline{x}}(\phi)|$. $\square$

Nótese que el resultado anterior puede considerarse un análogo de la acción de monodromía estudiada en el capítulo anterior. Además, al tener una acción en el conjunto de fibras geométricas, una pregunta inmediata es si existe un análogo a la Proposición 2.9 pues además de que esta proporciona distintos ejemplos de aplicaciones cubrientes, la definición de aplicación cubriente de Galois está inspirada en saber si una aplicación cubriente puede ser pensada como una proyección en un espacio de órbitas. En esta dirección, lo que sigue es estudiar cocientes de esquemas por la acción de subgrupos de su grupo de automorfismos. Luego, considérese $\phi : Y \to X$ un morfismo de esquemas afín suprayectivo y $G \subseteq \mathrm{Aut}(Y|X)$ un subgrupo finito. A nivel de espacios topológicos se tiene que la proyección en el espacio de órbitas $\pi_G : Y \to Y/G$ permite dotar a $Y/G$ con la topología cociente.

Además, dado que para cada $g \in G$, $(\pi_G)_*\mathcal{O}_Y = (\pi_G)_* g_* \mathcal{O}_Y$, entonces existe una acción derecha canónica de $G$ en $(\pi_G)_*\mathcal{O}_Y$. Así, se define $\mathcal{O}_{Y/G}$ como la gavilla de secciones $G$-invariantes de $(\pi_G)_*\mathcal{O}_Y$, con lo que se obtiene un espacio anillado $(Y/G, \mathcal{O}_{Y/G})$.

Proposición 3.43. *El espacio anillado* $(Y/G, \mathcal{O}_{Y/G})$ *es un esquema y el morfismo* $\pi_G : Y \to Y/G$ *es afín y suprayectivo. Además,* $\phi : Y \to X$ *se factoriza a través de* $\pi_G$ *mediante un morfismo afín* $\psi : Y/G \to X$.

Demostración. Como $\phi : Y \to X$ es un morfismo afín, supóngase que $X = \operatorname{Spec} A$ y $Y = \operatorname{Spec} B$. Luego, el morfismo $\phi$ es inducido por un morfismo de anillos $f : A \to B$. Así, la acción de $G$ en $Y$ induce una acción de $G$ en $B$ y sea $B^G$ el anillo de $G$-invariantes de $B$. Además, el hecho de que $G \subseteq \mathrm{Aut}(Y|X)$ implica que $f$ tiene una factorización a través de $B^G$, es decir, existen morfismos de anillos que hacen el siguiente diagrama conmutativo.

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\hat{f}"'] & & B \\ & B^G \arrow[ur, "\iota"'] & \end{tikzcd}$$

Así, al aplicar el funtor Spec se tiene que $\phi = \mathrm{Spec}(f) = \mathrm{Spec}(\hat{f}) \circ \mathrm{Spec}(\iota)$, donde $\mathrm{Spec}(\iota) : Y \to \mathrm{Spec}(B^G)$ y $\mathrm{Spec}(\hat{f}) : \mathrm{Spec}(B^G) \to X$, por lo que al tomar $\pi_G = \mathrm{Spec}(\iota)$ y $\psi = \mathrm{Spec}(\hat{f})$, $\phi = \psi \circ \pi_G$ con $\psi$ y $\pi_G$ afines.

Lo siguiente que se va a probar es que $\pi_G$ es suprayectivo. Para esto se observa que $B$ es entero sobre $B^G$ pues dado $b \in B$ se tiene que al considerar $p \in B^G[x]$ definido por $p = \sum_{\psi \in G}(x - \psi(b))$, este polinomio es mónico y satisface que $p(b) = 0$. Entonces, por el teorema del ascenso, dado $\mathfrak{p} \in \mathrm{Spec}(B^G)$, existe $\mathfrak{q} \in \mathrm{Spec}(B)$ tal que $\mathfrak{q} \cap B^G = \mathfrak{p}$, condición que implica que $\pi_G(\mathfrak{q}) = \mathfrak{p}$.

Para concluir la prueba se afirma que $Y/G \cong \mathrm{Spec}(B^G)$. En efecto, para aligerar la notación denótese por $Y_G = \mathrm{Spec}(B^G)$. Así, lo primero que se observa es que para identificar los espacios subyacentes de $Y/G$ y $Y_G$, basta con identificarlos como conjuntos pues un conjunto de la forma $V(I) \subseteq Y$ da lugar a uno de la forma

$V(I^G) \subseteq Y_G$. Además, como se acaba de ver la suprayectividad de $\pi_G : Y \to Y_G$, lo que se quiere probar es que las fibras de dicho morfismo son $G$-órbitas de $\operatorname{Spec} B$. Para esto supóngase que dos $G$-órbitas $\{\sigma(P) \mid \sigma \in G\}$ y $\{\sigma(Q) \mid \sigma \in G\}$ de puntos de $B$, provienen del mismo punto $P^G \in \operatorname{Spec}(B^G)$. Dado que la fibra $Y_{k(P)}$ es cero dimensional, entonces $\sigma(P)$ y $\sigma(Q)$ inducen ideales máximos $\sigma(\overline{P})$ y $\sigma(\overline{Q})$ del anillo $B \otimes_{B^G} k(P^G)$ con $\bigcap \sigma(\overline{P}) = \bigcap \sigma(\overline{Q}) = 0$. Así, al usar el teorema chino del residuo se encuentra $\overline{b} \in \overline{B}$ tal que $\overline{b} \in \sigma(\overline{P})$ y $\overline{b} \notin \sigma(\overline{Q})$ para cada $\sigma \in G$, lo que es una contradicción. Para concluir, se observa que para probar que $((\pi_G)_* \mathcal{O}_Y)^G \cong \mathcal{O}_{Y_G}$, la primera gavilla es casi-coherente y proviene del núcleo del morfismo de gavillas casi-coherentes

$$\pi_* \mathcal{O}_Y \to \bigoplus_{\sigma \in G} \pi_* \mathcal{O}_Y,$$
$$g \mapsto (, ..., \sigma(g) - g, ...).$$

Esto implica que es suficiente con checar el isomorfismo en los anillos de secciones sobre $Y_G$, que es $B^G$ es ambos casos. □

El siguiente resultado dice que si de hecho $\phi : Y \to X$ tiene estructura de cubriente étale finito conexo, esta se hereda a $\pi_G$.

Proposición 3.44. *Sea $\phi : Y \to X$ un cubriente étale finito conexo y $G \subseteq \operatorname{Aut}(Y|X)$ un subgrupo. Entonces $\pi_G : Y \to Y/G$ es un cubriente étale finito de $Y/G$ y el morfismo afín $\psi : Y/G \to X$ también lo es.*

Demostración. Basta con probar que $\psi : Y/G \to X$ es un cubriente étale finito pues $\pi_G$ ya lo es al ser $\phi$ étale finito. Así, al aplicar la Proposición 3.38, se obtiene un cambio de base $Y \times_X Z \to Z$ tal que $Y \times_X Z$ es una unión finita disjunta de copias de $Z$. Por otro lado, existe una acción canónica de $G$ en $Y \times_X Z$ que viene del cambio de base de $Y$, la cual induce un isomorfismo $(Y \times_X Z)/G \cong F/G \times Y$, con $F$ el conjunto finito tal que $Y \times_X Z \cong Z \times F$. Ahora se observa que $(Y \times_X Z)/G \cong Y/G \times_X Z$, por lo que se tiene un morfismo canónico de comparación $Y \times_X Z \to Y/G \times_X Z$ que es constante en $G$-órbitas. Así, para ver que este induce un isomorfismo se va a trabajar sobre una vecindad afín $U = \operatorname{Spec} A$ en cada punto de $X$, con preimagen $\operatorname{Spec} B$ y $\operatorname{Spec} C$ en $Y$ y $Z$, respectivamente. Pero como existe un isomorfismo $B^G \otimes_A C \to (B \otimes_A C)^G$ para $U$ tal que $C$ es un $A$-módulo libre con acción trivial de $G$, entonces esto define un isomorfismo $Y/G \times_X Z \cong F/G \times Y$, que es nuevamente una unión finita ajena de copias de $Z$. Luego, al usar nuevamente la Proposición 3.38 se tiene el resultado deseado. □

Con el resultado anterior se tiene el primer ingrediente que se quiere para formular un teorema fundamental de la teoría de Galois en el caso de esquemas. El ingrediente restante será definir los morfismos en los cuales dicho teorema será válido. En esta dirección se tiene el siguiente resultado.

PROPOSICIÓN 3.45. *Sea $\phi : Y \to X$ un cubriente étale finito conexo. Las siguientes afirmaciones son equivalentes:*

1. $|\operatorname{Aut}(Y|X)| = |F_{\overline{x}}(\phi)|$.
2. $\operatorname{Aut}(Y|X)$ *actúa de forma transitiva en toda fibra geométrica de un punto $\overline{x}$ de $X$.*
3. $\operatorname{Aut}(Y|X)$ *actúa de forma transitiva en alguna fibra geométrica de un punto $\overline{x}$ de $X$.*

DEMOSTRACIÓN. $1 \Rightarrow 2$) Considérese la función $f : \operatorname{Aut}(Y|X) \to F_{\overline{x}}(\phi)$ definida por $f(\psi) = \psi \cdot \overline{y}$, para $\overline{y} \in F_{\overline{x}}(\phi)$. Como se vio en la prueba de la Proposición 3.42 esta función es inyectiva. Como por hipótesis el dominio y codominio tienen la misma cardinalidad y esta es finita por la Proposición 3.42, entonces esta función es suprayectiva. Para concluir, nótese que la suprayectividad implica la transitividad en fibras geométricas.

$2 \Rightarrow 3$) Es claro.

$3 \Rightarrow 1$) Sea $f : \operatorname{Aut}(Y|X) \to F_{\overline{x}}(\phi)$ la función inyectiva usada en la primera implicación de la prueba. Luego, la transitividad es equivalente a la suprayectividad de esta función, lo que establece la biyección deseada. $\square$

La proposición anterior es un claro análogo de la Proposición 2.20 del capítulo anterior. Por lo tanto, es de esperarse que se tenga lo siguiente.

DEFINICIÓN 3.46. *Un morfismo de esquemas que cumple una, y por lo tanto todas las afirmaciones equivalentes del resultado anterior se conoce como un* ***cubriente étale finito de Galois****. Además, a la cardinalidad de $|F_{\overline{x}}(\phi)|$ se le conoce como el* ***grado*** *del morfismo $\phi$ en el punto $\overline{x}$.*

EJEMPLO 3.47. *Sea $L|\,k$ una extensión de campos finita. Entonces, el morfismo de esquemas afines inducido por la inclusión $\operatorname{Spec} L \to \operatorname{Spec} k$ es un cubriente étale finito de Galois si y sólo si la extensión $L|\,k$ es de Galois. El grado de dicho morfismo es $[L : k]$.*

Ejemplo 3.48. *Para $k$ campo sea $A = k[t, t^{-1}]$, el anillo de polinomios de Laurent con coeficientes en $k$ en una indeterminada. Para $n \in \mathbb{Z} \setminus \{0\}$ sea $f_n : A \to A$ el morfismo de anillos tal que $f_n(t) = t^n$. Así, dicho morfismo induce un morfismo de esquemas afines $\phi_n : \operatorname{Spec} A \to \operatorname{Spec} A$ finito, localmente libre y suprayectivo. Si $n > 0$ y $\operatorname{car} k \nmid n$, entonces $f_n$ es isomorfo al morfismo canónico $g_n : A \to A[x]/\langle x^n - t\rangle$. Dado que $\frac{d}{dx}(x^n - t) = nx^{n-1}$, la hipótesis sobre la característica implica que mcd$(x^n - t, \frac{d}{dx}(x^n - t)) = 1$ en $A[x]$. Luego, por lo visto en el Ejemplo 3.24 $\phi_n$ es un morfismo étale finito. Además, nótese que el grado de este es $n$ en todo punto y que si $n < 0$, con las mismas hipótesis un argumento análogo muestra que $\phi_n$ es un morfismo étale finito de grado $-n$.*

*Por otro lado nótese que $\operatorname{Aut}(A|A)$ es isomorfo al grupo de raíces $n$-ésimas de la unidad en $k$ mediante el morfismo que a cada $\phi \in \operatorname{Aut}(A|A)$ le asigna $\frac{\phi(t)}{t}$. De esto se concluye que el correspondiente cubriente étale conexo finito es de Galois si y sólo si $k$ tiene una raíz $n$-ésima de la unidad.*

En este momento puede enunciarse el teorema que se buscaba y que es el claro análogo del Teorema 2.23. Además, como a lo largo de esta sección se buscaron los análogos de cada uno de los conceptos involucrados en dicho teorema, la prueba se va a omitir pues es esencialmente la misma y no requiere de algún argumento especial de la teoría de esquemas.

Teorema 3.49. *(Teorema de correspondencia de Galois para cubrientes étale finitos) Sea $\phi : Y \to X$ un cubriente étale finito de Galois. Si $\psi : Z \to X$ es un cubriente étale finito conexo tal que el siguiente diagrama conmuta*

$$\begin{tikzcd} Y \arrow[r, "\phi"] \arrow[dr, "\pi"'] & X \\ & Z \arrow[u, "\psi"'] \end{tikzcd}$$

*entonces $\pi$ es un cubriente étale finito de Galois y $Z \cong Y/H$ para algún subgrupo $H \subseteq \operatorname{Aut}(Y|X)$. En este caso se tiene una biyección entre subgrupos de $\operatorname{Aut}(Y|X)$ y cubrientes sobre $Z$ en los cuales se factoriza $\phi$. Más aún, en esta correspondencia $\psi : Z \to X$ es de Galois si y sólo si su subgrupo asociado $H$, es normal en $\operatorname{Aut}(Y|X)$ y se satisface que $\operatorname{Aut}(Z|X) \cong \operatorname{Aut}(Y|X)/H$.*

El último resultado que se va a presentar es un análogo del Lema 1.13 para el caso de cubrientes étales finitos y se debe a Serre. De hecho, para el caso de morfismos de esquemas afines que son espectros de campos, la prueba de este resultado es precisamente dicho lema, de ahí el nombre que recibe el resultado. Por otro lado, nótese que este dice que todo cubriente étale finito se puede cubrir por un cubriente étale finito de Galois, en un sentido que se va a hacer preciso en la siguiente sección (ver prueba de la Proposición 3.54). La prueba de este se va a posponer para el siguiente capítulo donde se usarán argumentos más categóricos.

PROPOSICIÓN 3.50. *(Clausura de Galois de un cubriente étale finito) Sea $\phi : Y \to X$ un cubriente étale finito con $Y$ conexo. Entonces existe $\psi : Z \to Y$ un morfismo de esquemas tal que $\phi \circ \psi : Z \to X$ es un cubriente étale finito de Galois. Más áun, cualquier morfismo sobre $X$ de un cubriente de Galois de $Y$ se factoriza a través $\psi$.*

## 4. Definición del grupo fundamental algebraico

Sea $\mathbf{F\acute{E}t(X)}$ la subcategoría plena de la categoría rebanada $\mathbf{Sm}/X$, cuyos objetos son los cubrientes étale finitos de $X$. Luego, dado $x \in X$ se define una asignación $F_{\overline{x}} : \mathbf{F\acute{E}t(X)} \to \mathbf{Set}$ como sigue: A nivel de objetos dado $\phi : Y \to X$ un cubriente étale finito, $F_{\overline{x}}(\phi) := \mathbf{F\acute{E}t(X)}(\mathrm{Spec}\,\overline{k(x)}, Y)$. Para morfismos si $\phi : Y \to X$ y $\psi : Z \to X$ son cubrientes étale finitos y $\varphi \in \mathbf{F\acute{E}t(X)}(\phi, \psi)$, entonces $\mathrm{F}_{\overline{\mathrm{x}}}(\varphi) : \mathrm{F}_{\overline{\mathrm{x}}}(\phi) \to \mathrm{F}_{\overline{\mathrm{x}}}(\psi)$ tiene por regla de correspondencia $\mathrm{F}_{\overline{\mathrm{x}}}(\varphi)(\overline{y}) = \varphi \circ \overline{y}$.

La prueba del siguiente resultado es de rutina, por lo que esta se va a omitir.

PROPOSICIÓN 3.51. *La asignación $\mathrm{F}_{\overline{\mathrm{x}}} : \boldsymbol{F\acute{E}t(X)} \to \boldsymbol{Set}$ es un funtor y a este se le conoce como el funtor **fibra** en el punto geométrico $\overline{x}$.*

Para la primera propiedad del funtor definido se recuerda la siguiente definición de la teoría de categorías.

DEFINICIÓN 3.52. *Sea $F : \mathcal{C} \to \boldsymbol{Set}$ un funtor. Se dice que $F$ es **pro-represetable** si existe un sistema inverso en $\mathcal{C}$, $(\{P_\alpha\}_{\alpha\in\Lambda}, \{\phi_{\alpha\beta} : P_\beta \to P_\alpha\}_{\alpha\leq\beta})$, tal que $F \cong \varinjlim_\alpha \mathcal{C}(P_\alpha, \_)$.*

EJEMPLO 3.53. *El funtor $\mathrm{Hom}_k(\_, k_s) : \boldsymbol{FSep}(k)^{op} \to \boldsymbol{Set}$ es pro-representable pues $k_s$ es el límite directo de las extensiones finitas y separables de $k$ y en conjuntos el funtor $\mathrm{Hom}_k(L, \_)$ preserva límites directos. Se recomienda ver la Sección 5.1 de este capítulo para entender el trasfondo de este ejemplo.*

Proposición 3.54. *El funtor* $\mathrm{F}_{\overline{\mathrm{x}}} : \boldsymbol{F\acute{E}t(X)} \to \boldsymbol{Set}$ *es pro-representable.*

Demostración. Considére $\Lambda = \{\phi : Y \to X \mid \phi$ es cubriente étale finito de Galois$\}$. Luego, se define una relación de orden en $\Lambda$ en la cual $(\phi : Y \to X) \leq (\psi : Z \to X)$ si existe $\varphi \in \mathbf{F\acute{E}t(X)}(\psi, \phi)$. Nótese que la antisimetría de $\leq$ viene del hecho de que los endomorfismos de cubrientes de Galois son automorfismos.

Para ver que $(\Lambda, \leq)$ es un conjunto dirigido sean $\phi : Y \to X$ y $\psi : Z \to X$ elementos de $\Lambda$. Al considerar el producto fibrado de $\phi$ a lo largo de $\psi$, considére $Z$ una componente conexa de $Y \times_X Z$.

$$\begin{tikzcd}
Z \arrow[r, "\iota"] & Y \times_X Z \arrow[r, "p_1"] \arrow[d, "p_2"'] & Y \arrow[d, "\phi"] \\
& Z \arrow[r, "\psi"'] & X
\end{tikzcd}$$

Luego, al tomar $\phi \circ p_1 \circ \iota = \psi \circ p_2 \circ \iota : Z \to X$, la Proposición 3.50 implica que existe un morfismo de esquemas $\varphi : W \to Z$ tal que $(\phi \circ p_1 \circ \iota) \circ \varphi = (\psi \circ p_2 \circ \iota) \circ \varphi : W \to X$ es un cubriente étale finito de Galois, de lo que se deduce el resultado pues $\phi \leq \psi \circ p_2 \circ \iota \circ \varphi$ y $\psi \leq \psi \circ p_2 \circ \iota \circ \varphi$.

Para definir los morfismos de transición, para cada elemento de $\Lambda$, $\phi : Y \to X$, considérese $y_\phi \in \mathrm{F}_{\overline{\mathrm{x}}}(\phi)$ fijo. Entonces, dados $\phi, \psi \in \Lambda$ tales que $\phi \leq \psi$. por el Corolario 3.41 existe un único $\lambda : Z \to Z$ tal que $\psi \circ \lambda \circ y_\psi = y_\phi$. Así, se define $f_{\phi\psi} = \psi \circ \lambda$, y nótese que por construcción estas funciones son de transición.

Ahora, dado que se quiere definir una transformación natural $\eta : \varinjlim_{\phi \in \Lambda} \mathbf{F\acute{E}t(X)}(\phi, \_) \to \mathrm{F}_{\overline{\mathrm{x}}}$, entonces dado $\psi \in \mathbf{F\acute{E}t(X)}$, para definir $\eta_\psi : \varinjlim_{\phi \in \Lambda} \mathbf{F\acute{E}t(X)}(\phi, \psi) \to \mathrm{F}_{\overline{\mathrm{x}}}(\psi)$ se va a usar la propiedad universal del límite directo. Así, se considera el siguiente diagrama:

$$\begin{tikzcd}
\mathbf{F\acute{E}t(X)}(\phi, \psi) \arrow[rr, "f^*_{\phi\varphi}"] \arrow[dr, "\iota_\phi"] \arrow[ddr, "g_\phi"'] & & \mathbf{F\acute{E}t(X)}(\varphi, \psi) \arrow[dl, "\iota_\varphi"'] \arrow[ddl, "g_\varphi"] \\
& \varinjlim_{\phi \in \Lambda} \mathbf{F\acute{E}t(X)}(\phi, \psi) \arrow[d, dashed, "\eta_\psi"'] & \\
& \mathrm{F}_{\overline{\mathrm{x}}}(\psi) &
\end{tikzcd}$$

donde para $\phi \in \Lambda$, $g_\phi : \mathbf{FÉt(X)}(\phi, \psi) \to \mathrm{F}_{\overline{\mathrm{x}}}(\psi)$ tiene por regla de correspondencia $g_\phi(\alpha) = \mathrm{F}_{\overline{\mathrm{x}}}(\alpha)(y_\phi)$. Por definición de las funciones de transición el diagrama exterior conmuta y por lo tanto existe $\eta_\psi$. Además, nótese que dado que se definió $\eta_\psi$ usando la propiedad universal del límite directo, entonces $\eta$ es una transformación natural.

Para ver que $\eta$ es un isomorfismo, se va a construir su inversa. Para esto basta construir para cada $\psi \in \mathbf{FÉt(X)}$ una inversa para $\eta_\psi$. En esta dirección lo primero que se observa es que basta con probar esta afirmación bajo la hipótesis de que $X$ es conexo pues $X$ puede descomponerse en unión ajena de sus componentes conexas. Luego, por la Proposición 3.50 existe $\varphi : Z \to X$ un cubriente étale finito de Galois. Así, para cada $y \in \mathrm{F}_{\overline{\mathrm{x}}}(\psi)$ existe un único automorfismo sobre $X$, $\lambda$, tal que para cada $\mathrm{F}_{\overline{\mathrm{x}}}(\varphi \circ \lambda)(y_\phi) = y$ para $y_\phi \in \mathrm{F}_{\overline{\mathrm{x}}}(\phi)$ con $\phi \in \Lambda$. Al tomar la clase de $\varphi \circ \lambda$ en $\varinjlim_{\phi\in\Lambda} \mathbf{FÉt(X)}(\phi, \psi)$ se tiene el morfismo en la otra dirección que es el inverso de $\eta_\psi$. □

Corolario 3.55. *Todo automorfismo del funtor* $\mathrm{F}_{\overline{\mathrm{x}}}$ *se construye de un único automorfismo del sistema inverso construido en la prueba de proposición anterior.*

Demostración. Todo automorfismo de $\mathrm{F}_{\overline{\mathrm{x}}}$ manda al sistema construido en la proposición anterior en otro sistema, con objetos digamos $\{P'_\alpha\}$. Como $P_\alpha$ es de Galois, para cada $\alpha$ existe un único automorfismo $\lambda_\alpha \in \mathrm{Aut}(P_\alpha|X)$ que manda a $P_\alpha$ en $P'_\alpha$. Como para el primer sistema se tiene la condición de compatibilidad, esta se satiface para los morfismos $\lambda_\alpha$, de donde se deduce el resultado. □

Definición 3.56. *Sea $X$ un esquema y $x \in X$. El grupo de automorfismos del funtor* $\mathrm{F}_{\overline{\mathrm{x}}}$ *se conoce como el* ***grupo fundamental algebraico (étale o de Grothendieck)*** *del esquema $X$ en el punto geométrico $\overline{x}$. Este se denota por $\pi_1^{alg}(X, \overline{x})$.*

Corolario 3.57. *Los grupos de automorfismos* $\mathrm{Aut}(P_\alpha)^{op}$ *forman un sistema inverso cuyo límite inverso es $\pi_1^{alg}(X, \overline{x})$.*

Demostración. Nótese que si $(\phi : Y \to X) \leq (\psi : Z \to X)$ para $\phi, \psi \in \Lambda$, entonces al ser estos cubrientes étale finitos de Galois, se tiene que el morfismo inducido $\mathrm{Aut}(Z|X) \to \mathrm{Aut}(Y|X)$ es suprayectivo. Como los elementos del límite inverso son exactamente los automorfismos del sistema inverso $(\{P_\alpha\}, \{\phi_{\alpha\beta}\})$, que por el corolario anterior corresponden biyectivamente a automorfismos del funtor de fibras, el isomorfismo con el grupo opuesto proviene de considerar el funtor "Hom" contravariante. □

Ejemplo 3.58. *Como aplicación del teorema de Minkowski, para todo punto geométrico de* $\operatorname{Spec}\mathbb{Z}$ *se tiene que* $\pi_1^{alg}(\operatorname{Spec}\mathbb{Z},\overline{x})\cong\{0\}$.

Teorema 3.59. *(Grothendieck) Sea* $X$ *un esquema conexo y* $\overline{x}:\operatorname{Spec}\overline{k(x)}\to X$ *un punto geométrico. Entonces,*

1. *El grupo* $\pi_1^{alg}(X,\overline{x})$ *es profinito y su acción en* $\mathrm{F}_{\overline{x}}(\phi)$ *es continua para cada cubriente étale finito* $\phi:Y\to X$.
2. *El funtor* $\mathrm{F}_{\overline{x}}$ *induce una equivalencia de categorías entre* ***FÉt(X)*** *y* $\pi_1^{alg}(X,\overline{x})-$***FSet***. *En esta equivalencia los cubrientes conexos corresponden a* $\pi_1^{alg}(X,\overline{x})$*-conjuntos finitos con acción transitiva y, los cubrientes de Galois a cocientes de* $\pi_1^{alg}(X,\overline{x})$.

Demostración. Por la proposición anterior se puede considerar un sistema inverso $(\{P_\alpha\},\{\phi_{\alpha\beta}\})$ de cubrientes de Galois que pro-representan al funtor $\mathrm{F}_{\overline{x}}$. Dado que por un resultado previo $\operatorname{Aut}(P_\alpha|X)$ es finito, entonces el corolario anterior implica que $\pi_1^{alg}(X,\overline{x})$ es un grupo profinito. Además, un automorfismo del sistema inverso $(\{P_\alpha\},\{\phi_{\alpha\beta}\})$ induce un automorfismo de $\mathrm{F}_{\overline{x}}(Y)=\varinjlim_\alpha \mathbf{FÉt(X)}(P_\alpha,Y)$, donde hay una acción izquierda de $\pi_1(X,\overline{x})$ en $\mathrm{F}_{\overline{x}}(Y)$ para todo $Y\in$ **FÉt(X)**. Esta acción es continua pues un elemento $\overline{y}\in\mathrm{F}_{\overline{x}}(Y)$, proviene de una clase de $\mathbf{Fét(X)}(P_\alpha,Y)$ donde la acción de $\pi_1^{alg}(X,\overline{x})$ factoriza por $\operatorname{Aut}(P_\alpha|X)^{op}$, lo que concluye la prueba de la primera afirmación.

Respecto a la segunda afirmación, la prueba es similar a la del TFTG de Grothendieck presentada en el Capítulo 1. Lo único que se tratará es la suprayectividad esencial. En efecto, sea $E$ un $\pi_1^{alg}(X,\overline{x})$-conjunto finito. Además, dado que $E$ puede descomponerse en sus órbitas, puede suponerse que la acción sobre $E$ es transitiva. Así, el estabilizador de un punto $e\in E$ es un subgrupo abierto $U$ de $\pi_1^{alg}(X,\overline{x})$ y este contiene un subgrupo abierto normal $V_\alpha$ que viene del morfismo canónico $\pi_1^{alg}(X,\overline{x})\to\operatorname{Aut}(P_\alpha|X)^{op}$. Sea $\overline{U}$ la imagen de $U$ en $\operatorname{Aut}(P_\alpha|X)^{op}$. Si $Z$ es el cociente de $P_\alpha$ por la acción de $\overline{U}^{op}$, entonces $\mathrm{F}_{\overline{x}}(Z)\cong E$. □

## 5. Dos cálculos de $\pi_1^{alg}(X,\overline{x})$

El objetivo de esta sección es presentar de forma explícita el grupo fundamental algebraico para un $k$-esquema y para un esquema localmente de tipo finito sobre los complejos. La importancia de estas descripciones radica en el hecho de que estas permiten conectar respectivamente el grupo fundamental algebraico con el grupo de Galois absoluto de un campo y el grupo fundamental.

**5.1. Para $k$-esquemas.** Sea $X = \operatorname{Spec} k$ con $k$ campo. Por el Ejemplo 3.23 se sabe que un cubriente étale finito sobre $X$ corresponde al espectro de una $k$-álgebra finita étale. Así, si $\phi : Y \to X$ es uno de tales morfismos de esquemas y $\overline{x} : \operatorname{Spec} K \to X$ es su único punto geométrico, dado que $Y = \operatorname{Spec}(A)$ con $A = \prod_{i=1}^{n} L_i$ para $L_i|\, k$ extensiones fininitas separables, entonces la imagen de las componentes conexas de $Y$ mediante $F_x$, $\operatorname{Spec} L_i$, es el conjunto subyacente de $\operatorname{Spec}(L_i \otimes_k K)$, que es un conjunto finito indexado por $\operatorname{Hom}_k(L, K)$. Como de hecho la imagen de cada uno de estos morfismos está contenida en $k_s$ esto implica que $F_x(\phi|_{\operatorname{Spec} L_i}) \cong \operatorname{Hom}_k(L_i, k_s)$. Por lo tanto se deduce que $F_x \cong \operatorname{Hom}(\_, k_s)$ y de este isomorfismo de funtores es claro que se tiene el siguiente resultado.

Teorema 3.60. *Si $X = \operatorname{Spec} k$ con $k$ campo, entonces para el único punto geométrico de $X$, $\overline{x}$, existe un isomorfismo de grupos profinitos $\pi_1^{alg}(X,\overline{x}) \cong \operatorname{Gal}(k)$.*

La primera observación que vale la pena realizar es que el teorema anterior y el Teorema 3.59 tienen como consecuencia el Teorema 1.23, que fue probado con únicamente métodos de la teoría de campos.

Por otro lado, el teorema anterior permite obtener ejemplos más concretos de grupos fundametales algebraicos. A continuación se presentan algunos de ellos.

Ejemplo 3.61. *Si $k$ es algebraicamente cerrado, entonces $k_s = k$, por lo que $\operatorname{Gal}(k) \cong 0$. Así, del teorema anterior se deduce que para el único punto geométrico $\overline{x}$ de $\operatorname{Spec} k$, $\pi_1^{alg}(\operatorname{Spec} k,\overline{x}) \cong \{0\}$.*

Ejemplo 3.62. *Dado que $(\mathbb{R})_s \cong \mathbb{C}$, entonces $\operatorname{Gal}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. Así, para el único punto geométrico de $\operatorname{Spec}\mathbb{R}$, $\overline{x}$, se tiene que $\pi_1^{alg}(\operatorname{Spec}\mathbb{R},\overline{x}) \cong \mathbb{Z}/2\mathbb{Z}$.*

Ejemplo 3.63. *Sea $k$ un campo finito. Como se vio en el Ejemplo 1.15 $\operatorname{Gal}(k) \cong \hat{\mathbb{Z}}$. Así, para el único punto geométrico de $\operatorname{Spec}(k)$, $\overline{x}$, se tiene que $\pi_1^{alg}(\operatorname{Spec} k,\overline{x}) \cong \hat{\mathbb{Z}}$.*

Ejemplo 3.64. *Para el campo de funciones racionales de $\mathbb{C}[t]$, $\mathbb{C}(t)$, Douady demostró que $\operatorname{Gal}(\mathbb{C}(t)) \cong \hat{F}(\mathbb{C})$, donde $\hat{F}(\mathbb{C})$ es el grupo profinito libre con base $\mathbb{C}$ (Ver por ejemplo el Teorema 3.4.8 de* [**S**, pp 81–82]*). Por lo tanto, si $\overline{x}$ es el único punto geométrico de $\operatorname{Spec}\mathbb{C}(t)$, entonces $\pi_1^{alg}(\operatorname{Spec}\mathbb{C}(t),\overline{x}) \cong \hat{F}(\mathbb{C})$.*

**5.2. $\mathbb{C}$-esquemas localmente de tipo finito.** Para esta sección se requieren algunos resultados de geometría algebraica compleja. Los más técnicos se usarán sin dar una prueba, pero se indicará el lugar donde pueden consultarse pues el objetivo de estas sección es establecer una relación entre el grupo fundamental algebraico y el grupo fundamental. Además, **LFTSm** denota la categoría de esquemas localmente de tipo finito.

Sea $X$ un esquema localmente de tipo finito sobre $\mathbb{C}$. Es conocido que se tiene una biyección entre el conjunto de puntos $\mathbb{C}$-racionales de $X$, $X_{\mathbb{C}}$, y los puntos cerrados de $X$. Así, para asociar a $X$ un espacio topológico complejo se realiza lo siguiente: Si $X$ es un esquema afín, entonces nótese que para $\phi : X \hookrightarrow \mathbb{A}^n_{\mathbb{C}}$ un encaje cerrado, este induce una función $\phi_{\mathbb{C}} : X_{\mathbb{C}} \to \mathbb{C}^n$ mediante la cual se le da la topología que induce $\mathbb{C}^n$ en $X_{\mathbb{C}}$. Puede probarse que esta topología no depende del encaje. Además, si $X$ es un esquema arbitrario, entonces al tomar una cubierta afín de $X$ y realizar este proceso en cada uno de los abiertos afines de la cubierta, puede inducirse una topología en $X$. Al espacio topológico resultante se le denota por $X^{an}$ y se le conoce como la **analitificación** del esquema $X$.

La asignación anterior permite definir un funtor $A : \mathbf{LFTSm}/\mathbb{C} \to \mathbf{Top}$ que se le conoce como el **funtor de analitificación**.

PROPOSICIÓN 3.65. *Si $\phi : Y \to X$ es un morfismo finito étale, entonces $A(\phi) : Y^{an} \to X^{an}$ es una aplicación cubriente finita.*

Una prueba del resultado anterior puede darse usando una proposición de la teoría de aplicaciones cubrientes que dice que un homeomorfismo local $f : Y \to X$ separado con fibras finitas y grado localmente constante como función de $y \in Y$ es una aplicación cubriente. Así, lo que se hace es ver que $A(\phi)$ cumple las hipótesis de dicho teorema.

Nótese que el resultado anterior implica que el funtor de analitificación da lugar a un funtor $\mathbf{F\acute{E}t}/X \to \mathbf{FCov}/X^{an}$, el cual se va a denotar por $A$ y se llamará funtor de analitificación en un abuso de notación. Además, se tiene el siguiente profundo y nada trivial resultado:

TEOREMA 3.66. *El funtor $A : \boldsymbol{F\acute{E}t}/X \to \boldsymbol{FCov}/X^{an}$ es una equivalencia de categorias.*

DEMOSTRACIÓN. Ver [**GAGA**] ó [**Se58**] Proposiciones 19, corolario de la Proposición 20 y corolario del Teorema 3. ☐

Ahora sea $\overline{x}$ un punto geométrico del esquema $X$ y se considera el siguiente diagrama:

$$\begin{tikzcd}
\mathbf{F\acute{E}t}/X \arrow[r, "A"] \arrow[d, "F_{\overline{x}}"'] & \mathbf{FCov}/X^{an} \arrow[d, "T"] \\
\mathbf{Set} & \pi_1(\hat{X^{an}}, x) - \mathbf{FSet} \arrow[l, "U"]
\end{tikzcd}$$

En ese diagrama el funtor $T$ es la equivalencia de categorías del Teorema 2.25, mientras que $U$ es el funtor que olvida. Nótese que este diagrama conmuta pues en el contexto analítico las fibras geométricas y la fibra en un punto coinciden. Luego, como $T \circ A : \mathbf{F\acute{E}t}/X \to \pi_1(\hat{X^{an}}, x) - \mathbf{FSet}$ es una equivalencia, entonces se deduce que $\pi_1^{alg}(X, \overline{x}) \cong \mathrm{Aut}(U)$ como grupos. Pero más aún, se tiene lo siguiente:

PROPOSICIÓN 3.67. *Sean $G$ un grupo profinito y $U : G - \boldsymbol{FSet} \to \boldsymbol{Set}$ el funtor que olvida. Entonces existe un isomorfismo de grupos topológicos* $\mathrm{Aut}(U) \cong G$*.*

De la proposición anterior y la discusión anterior se obtiene de manera obvia el siguiente resultado.

TEOREMA 3.68. *Para $X$ un esquema conexo localmente finito sobre $\mathbb{C}$ y $x \in X$, existe un isomorfismo de grupos topológicos $\pi_1^{alg}(X, \overline{x}) \cong \pi_1(\hat{X^{an}}, x)$*

Como antes del resultado anterior pueden obtenerse algunos ejemplos concretos.

EJEMPLO 3.69. *Considérese $X = \mathbb{A}^1_{\mathbb{C}}$. Dado que $X^{an} \cong \mathbb{C}$ con su topología usual, entonces para cualquier $x \in \mathbb{A}^1_{\mathbb{C}}$ se tiene que $\pi_1(X^{an}, x) \cong \{0\}$. Como este grupo es finito entonces es profinito y así su completación profinita es él mismo. Por lo tanto, para cada $x \in \mathbb{A}^1_{\mathbb{C}}$, $\pi_1^{alg}(\mathbb{A}^1_{\mathbb{C}}, \overline{x}) \cong \{0\}$.*

EJEMPLO 3.70. *Sea $X = \mathbb{P}^1_{\mathbb{C}}$. Como $X^{an}$ es simplemente conexo, entonces para cada $x \in X$ se tiene que $\pi_1(X^{an}, x) \cong \{0\}$. Por lo tanto $\pi_1^{alg}(\mathbb{P}^1_{\mathbb{C}}, \overline{x}) \cong \{0\}$.*

EJEMPLO 3.71. *Sea $X = \mathbb{A}^1_{\mathbb{C}} \setminus \{0\} \subseteq \mathbb{A}^1_{\mathbb{C}}$. Luego, $X^{an} \cong \mathbb{C}^{\times}$ y como se vio en el Ejemplo 2.31 se tiene que $\pi_1(X^{an}, x) \cong \mathbb{Z}$ para cada $x \in X^{an}$. Por lo tanto, $\pi_1^{alg}(\mathbb{A}^1_{\mathbb{C}} \setminus \{0\}, \overline{x}) \cong \hat{\mathbb{Z}}$.*

Capítulo 4

# Categorías de Galois

En este capítulo se estudian algunas propiedades básicas relativas a las categorías de Galois, que son el lenguaje adecuado para tratar simultáneamente algunos aspectos de las teorías de álgebras étale de dimensión finita, aplicaciones cubrientes finitas y morfismos de esquemas étale finitos, pues con este formalismo se hace evidente que algunas propiedades análogas entre las teorías mencionadas tienen un trasfondo y forman parte de una teoría más general. En particular, un ejemplo de gran relevancia se encuentra en el hecho de que para cada una de estas existe un grupo distinguido que permite ver que cada una es equivalente a una categoría de conjuntos finitos dotados con la topología discreta, en la que actúa de manera continua dicho grupo. Este hecho sucede para cualquier categoría de Galois y de hecho se prueba que dicho grupo da lugar a una equivalencia de 2-categorías.

## 1. Definiciones y propiedades básicas

Para formular la definición de categoría de Galois se requieren de algunos conceptos previos provenientes de la teoría de categorías. El primero de ellos tiene que ver con una clase especial de morfismos y se presenta a continuación.

Definición 4.1. *Sea $\mathcal{C}$ una categoría. Un morfismo en $\mathcal{C}$, $f : Y \to X$ es un* ***epimorfismo estricto*** *si el producto fibrado de $f$ a lo largo de $f$ existe y además, si $p_1, p_2 : Y \times_X Y \to Y$ son sus morfismos canónicos, entonces para cada $Z \in \mathcal{C}$ la función inducida $f^* : \mathcal{C}(X,Z) \to \mathcal{C}(Y,Z)$ es una biyección entre $\mathcal{C}(X,Z)$ y $\{\beta \in \mathcal{C}(Y,Z) \mid \beta \circ p_1 = \beta \circ p_2\}$.*

Antes de mencionar algunos ejemplos se probará un resultado que compara el concepto de epimorfismo estricto con el de epimorfismo.

Proposición 4.2. *Sea $\mathcal{C}$ una categoría.*

1. *Todo epimorfismo estricto es un epimorfismo.*

2. *Un epimorfismo es estricto si y sólo si es el coigualador de un par de morfismos en $\mathcal{C}$.*

Demostración. Para la primera afirmación sean $f : Y \to X$ un epimorfismo estricto y $g, h : X \to Z$ morfismos tales que $g \circ f = h \circ f$. Nótese que $g \circ f \in \mathcal{C}(Y, Z)$ y que $(g \circ f) \circ p_1 = (g \circ f) \circ p_2$. Así, existe un único $k \in \mathcal{C}(X, Z)$ tal que $f^*(k) = g \circ f$, es decir, $k \circ f = g \circ f$. Como $g, h \in \mathcal{C}(X, Z)$ y se satisface por hipótesis que $g \circ f = h \circ f$, entonces $g = h = k$.

Respecto a la segunda afirmación, para la ida considérense los morfismos canónicos del producto fibrado de $f$ a lo largo de $f$, $p_1, p_2 : Y \times_X Y \to Y$. Es claro que $f$ es el coigualador de $p_1$ y $p_2$. Para el regreso supóngase que $f$ es el coigualador del par de morfismos $g, h : Z \to Y$. Esto implica que el producto fibrado de $f$ a través de sí mismo existe pues $Z \cong Y \times_X Y$, $p_1 = g$ y $p_2 = h$. Ahora, sea $f^* : \mathcal{C}(Z, X) \to \mathcal{C}(Z, Y)$ la función inducida para $Z \in \mathcal{C}$. La inyectividad de esta función es consecuencia de que $f$ es un epimorfismo y el hecho de que la imagen de $f^*$ es el conjunto de $\beta \in \mathcal{C}(Z, Y)$ tales que $\beta \circ p = \beta \circ q$ es consecuencia de que $f$ es coigualador de $g$ y $h$. Así, $f$ es un epimorfismo estricto. $\square$

Ejemplo 4.3. *Todo isomorfismo es un epimorfismo estricto.*

Ejemplo 4.4. *En la categoría de conjuntos o cualquier categoría conormal, los epimorfismos estrictos son precisamente los epimorfismos. En particular esto sucede en cualquier categoría abeliana.*

Ejemplo 4.5. *Considérese el morfismo de esquemas afines sobre un campo $k$, $\varphi : \operatorname{Spec} k[t] \to \operatorname{Spec} k[t^3, t^5]$, inducido por el morfismo inclusión de $k$-álgebras $k[t^3, t^5] \to k[t]$. Por tal razón, dicho morfismo es un epimorfismo. Lo que se afirma es que este no es estricto. Para esto se consideran $Z = \operatorname{Spec} k[t]$ y $\varphi^* : \boldsymbol{Sm}/\operatorname{Spec} k(\operatorname{Spec} k[t^3, t^5], \operatorname{Spec} k[t]) \to \boldsymbol{Sm}/\operatorname{Spec} k(\operatorname{Spec} k[t], \operatorname{Spec} k[t])$. Nótese que el morfismo de $k$-esquemas $\psi : \operatorname{Spec} k[t] \to \operatorname{Spec} k[t]$ inducido por el morfismo de $k$-álgebras $k[t] \to k[t]$ tal que $t \mapsto t^7$, satisface que $\psi \circ p_1 = \psi \circ p_2$ con $p_1$ y $p_2$ los morfismos canónicos del producto fibrado de $\varphi$ a través de sí mismo pues $(1 \otimes t)^7 = (t \otimes 1)^7$ en $k[t] \otimes_{k[t^3, t^5]} k[t]$. Sin embargo, $\psi \notin \operatorname{im}(\varphi^*)$ pues $t^7 \notin k[t^3, t^5]$.*

Ejemplo 4.6. *(Grothendieck) Un morfismo de esquemas $\phi : Y \to X$ que es fielmente plano, es decir, plano y suprayectivo, es un epimorfismo estricto (Ver Teorema 2.17 de* [**Mi**, pp 17–19]*).*

PROPOSICIÓN 4.7. *Sea $\mathcal{C}$ una categoría en la que todo morfismo tiene una factorización de la forma $u \circ e$ con $u$ un monomorfismo que escinde y $e$ un epimorfismo estricto. Entonces, la composición de epimorfismos estrictos es un epimorfismo estricto.*

DEMOSTRACIÓN. Sean $e : Y \to X$ y $f : Z \to Y$ epimorfismos estrictos. Así, considérese el morfismo $e \circ f : Z \to X$, el cual se puede escribir como $e \circ f = u \circ g$ con $g : Z \to W$ un epimorfismo estricto y $u : W \to X$ un monomorfismo que escinde. Dado que $f$ es un epimorfismo que estricto, si $p_1, p_2 : Y \times_X Y \to Y$ son los morfismos canónicos del producto fibrado de $f$ consigo mismo, se tiene que como $f \circ p_1 = f \circ p_2$, entonces $e \circ f \circ p_1 = e \circ f \circ p_2$, de donde $u \circ g \circ p_1 = u \circ g \circ p_2$. Dado que $u$ es en particular un monomorfismo, se deduce que $g \circ p_1 = g \circ p_2$. Por lo tanto, existe $h \in \mathcal{C}(Y, W)$ tal que para $f^* : \mathcal{C}(Y, W) \to \mathcal{C}(Z, W)$ se satisface que $f^*(h) = g$, es decir, $h \circ f = g$. Además, $u \circ h = e$ pues $(u \circ h) \circ f = u \circ g = e \circ f$ y dado que $f$ es un epimorfismo, se sigue el resultado deseado. Así, dado que $e$ es en particular un epimorfismo, entonces $u$ es un epimorfismo y, dado que es un monomorfismo que escinde, este es un isomofismo, de lo que se sigue que $e \circ f$ es un epimorfismo estricto. □

Para $\mathcal{C}$ una categoría se pone $\mathcal{M}$ la clase de todos los monomorfismos que escinden de $\mathcal{C}$ y $\mathcal{E}$ la clase de todos los epimorfismos estrictos de dicha categoría. Con esta notación se tiene el siguiente resultado.

PROPOSICIÓN 4.8. *Sea $\mathcal{C}$ una categoría en la que todo morfismo tiene una factorización con un monomorfismo que escinde seguido de un epimorfismo estricto. Entonces, la pareja $(\mathcal{M}, \mathcal{E})$ es un sistema de factorización en $\mathcal{C}$, es decir, se cumplen las siguientes propiedades:*

1. *Todo isomorfismo es elemento de $\mathcal{M} \cap \mathcal{E}$.*
2. *$\mathcal{M}$ y $\mathcal{E}$ son cerrados bajo composiciones.*
3. *Para cada $f : Y \to X$ morfismo en $\mathcal{C}$, existen $u \in \mathcal{M}$ y $e \in \mathcal{E}$ tales que $f = u \circ e$.*
4. *Considérese el siguiente cuadrado conmutativo donde $e \in \mathcal{E}$ y $u \in \mathcal{M}$.*

$$\begin{tikzcd} Z \arrow[r, "e"] \arrow[d, "g"'] & W \arrow[d, "f"] \\ Y \arrow[r, "u"'] & X \end{tikzcd}$$

*Entonces, existe un único morfismo $h : W \to Y$ tal que $h \circ e = g$ y $u \circ h = f$.*

Demostración. Nótese que 1 es claro del Ejemplo 4.3 y de que todo isomorfismo es un monomorfismo que escinde. Además, dado que los monomorfismos que escinden son cerrados bajo composición, de la hipótesis y la Proposición 4.7 se deduce que los epimorfismos estrictos también. Por lo tanto se cumple 2. Más aún, 3 se satisface trivialmente por hipótesis. Luego, lo que resta probar es 4. Para esto considérese los morfismos como en las hipótesis. Nótese que si $p_1, p_2 : Z \times_W Z \to Z$ son los morfismos canónicos del producto fibrado de $e$ a lo largo de sí mismo, entonces $g \circ p_1 = g \circ p_2$ pues $u \circ (g \circ p_1) = f \circ (e \circ p_1) = f \circ (e \circ p_2) = u \circ (g \circ p_2)$. De donde la igualdad que se quiere se obtiene del hecho de que $u$ es en particular un monomorfismo. Así, como $e \in \mathcal{E}$ se tiene que existe $h \in \mathcal{C}(W, Y)$ tal que $e^* : \mathcal{C}(W, Y) \to \mathcal{C}(Z, Y)$ cumple que $e^*(h) = g$, es decir, $h \circ e = g$. Para ver que $u \circ h = f$, nótese que $(u \circ h) \circ e = u \circ g = f \circ e$. Luego, como $e$ es en particular un epimorfismo, se sigue la igualdad que se quiere. Además, la unicidad de $h$ se obtiene de la ecuación $u \circ h = f$ y del hecho de que $u$ es en particular un monomorfismo. $\square$

El siguiente es un resultado general de la teoría de categorías respecto a sistemas de factorización cuya prueba se va omitir. Sin embargo, esta puede consultarse en la Proposición 5.3.3 de [**BJ**, pp 145–149].

Proposición 4.9. *Sea $(\mathcal{E}, \mathcal{M})$ un sistema de factorización en una categoría $\mathcal{C}$. Entonces,*

1. *Si $f \in \mathcal{M} \cap \mathcal{E}$, entonces $f$ es un isomorfismo.*
2. *La factorización de $f : Y \to X$ un morfismo en $\mathcal{C}$, $f = m \circ e$ con $m \in \mathcal{M}$ y $e \in \mathcal{E}$ es única salvo isomorfismo.*
3. *$u \in \mathcal{M}$ si y sólo si para cualquier cuadrado conmutativo de la forma*

$$\begin{tikzcd} Z \arrow[r, "e"] \arrow[d, "g"'] & W \arrow[d, "f"] \arrow[dl, dashed] \\ Y \arrow[r, "u"'] & X \end{tikzcd}$$

   *existe un único $h : W \to Y$ que hace conmutar ambos triángulos. Además, la afirmación correspondiente para elementos de $\mathcal{E}$ se cumple.*
4. *Si $f \circ g \in \mathcal{M}$ y $f \in \mathcal{M}$, entonces $g \in \mathcal{M}$. Dualmente, si $f \circ g \in \mathcal{E}$ y $g \in \mathcal{E}$, entonces $f \in \mathcal{E}$.*
5. *Si el siguiente diagrama es un producto fibrado con $u \in \mathcal{M}$,*

$$\begin{tikzcd} Z \arrow[r, "f"] \arrow[d] & W \arrow[d] \\ Y \arrow[r, "u"'] & X \end{tikzcd}$$

*entonces $f \in \mathcal{M}$. Además, la propiedad dual para morfismos en $\mathcal{E}$ es válida.*

COROLARIO 4.10. *Sea $\mathcal{C}$ una categoría en la que todo morfismo tiene una factorización con un monomorfismo que escinde seguido de un epimorfismo estricto. Entonces cada una de las afirmaciones de la proposición anterior se cumplen.*

Ahora, el siguiente concepto categórico a establecer es el de cociente de un objeto por un subgrupo de un grupo de automorfismos.

DEFINICIÓN 4.11. *Sea $\mathcal{C}$ un categoría. Dados $Y \in \mathcal{C}$ y $G \subseteq \mathrm{Aut}_{\mathcal{C}}(Y)$ un subgrupo, el **cociente de** $Y$ **por** $G$ consta de un objeto en $\mathcal{C}$, $Y/G$, junto con un morfismo $p : Y \to Y/G$ tales que para cada $\sigma \in G$, $p \circ \sigma = p$. Además, si $f : Y \to X$ es un morfismo en $\mathcal{C}$ tal que para cada $\sigma \in G$ cumple que $f \circ \sigma = f$, entonces existe un único morfismo en $\mathcal{C}$, $\hat{f} : Y/G \to X$ tal que $\hat{f} \circ p = f$.*

*Una categoría $\mathcal{C}$ tiene cocientes por subgrupos si para cualesquiera $Y \in \mathcal{C}$ y $G \subseteq \mathrm{Aut}_{\mathcal{C}}(Y)$ subgrupo, existe el cociente de $Y$ por $G$.*

EJEMPLO 4.12. *La categoría de conjuntos tiene cocientes donde dado $Y \in$ **Set** y $G \subseteq \mathrm{Aut}_{\boldsymbol{Set}}(Y)$, $Y/G$ es el espacio de órbitas de la acción de $G$ en $Y$. Además, $p : Y \to Y/G$ es la proyección en el conjunto de órbitas.*

EJEMPLO 4.13. *Del Resultado 2.9 y un sencillo cálculo para ver que la proyección en el espacio de óbitas satisface la propiedad universal de la definición anterior, se deduce que la categoría de aplicaciones cubrientes finitas sobre un espacio conexo tiene cocientes por grupos finitos.*

EJEMPLO 4.14. *Los resultados 3.43 y 3.44 dicen que la categoría de cubrientes étale finitos tienen cocientes por grupos finitos.*

Con la discusión previa se puede dar la definición que se buscaba.

DEFINICIÓN 4.15. *Una **categoría de Galois** consta de una pareja $(\mathcal{C}, F)$ donde $\mathcal{C}$ es una categoría y $F : \mathcal{C} \to$ **FSet** es un funtor, tales que:*

1. *$\mathcal{C}$ tiene límites directos finitos.*

2. *$\mathcal{C}$ tiene coproductos finitos y cocientes por grupos finitos de automorfismos de objetos en $\mathcal{C}$.*
3. *Todo morfismo en $\mathcal{C}$ tiene una factorización mediante un monomorfismo que escinde y un epimorfismo estricto.*
4. *$F$ conmuta con límites finitos.*
5. *$F$ conmuta con coproductos finitos, cocientes con subgrupos de automorfismos finitos y preserva epimorfismos estrictos.*
6. *$F$ refleja isomorfismos.*

*En tal caso se dice que $F$ es un* ***funtor de fibra*** *de $\mathcal{C}$. Además, cuando se diga que $\mathcal{C}$ es una categoría de Galois, se está diciendo que existe $F : \mathcal{C} \to$* ***FSet*** *un funtor tal que $(\mathcal{C}, F)$ es una categoría de Galois.*

La primera observación que vale la pena realizar es que en una categoría de Galois es válido el Corolario 4.10. Además, antes de dar algunos ejemplos vale la pena tener a la mano el siguiente resultado.

PROPOSICIÓN 4.16. *Sea $(\mathcal{C}, F)$ una categoría de Galois. Entonces,*

1. *$\mathcal{C}$ tiene objeto inicial, $0$, y objeto terminal $1$. Estos son preservados por el funtor $F$.*
2. *$\mathcal{C}$ tiene productos fibrados, igualadores y productos. El funtor $F$ preserva todos estos.*
3. *$F$ preserva monomorfismos.*

DEMOSTRACIÓN. Para 1 nótese que $0$ es el coproducto de una familia vacía y $1$ el límite de una familia vacía. Por tal razón $F$ preserva dichos objetos.

Respecto a 2 se observa que si $\mathcal{C}$ tiene límites finitos entonces tiene productos fibrados, igualadores y productos. Por tal razón $F$ preserva dichos objetos.

Para concluir, 3 se deduce del hecho de que $f : Y \to X$ un morfismo en $\mathcal{C}$ es un monomorfismo si y sólo si el siguiente diagrama es un producto fibrado

$$\begin{tikzcd} Y \arrow[r, "1_Y"] \arrow[d, "1_Y"'] & Y \arrow[d, "f"] \\ Y \arrow[r, "f"'] & X \end{tikzcd}$$

□

Ejemplo 4.17. *Para $k$ un campo, la categoría de $k$-álgebras finitas étale es una categoría de Galois con funtor de fibra* $\mathrm{Hom}_k(\_, k_s)$.

Ejemplo 4.18. *Para un espacio topológico $X$ conexo, localmente conexo y localmente simplemente conexo, la categoría de aplicaciones cubrientes finitas sobre $X$ es una categoría de Galois con funtor fibra cualquier funtor de fibras en un punto de $X$.*

Ejemplo 4.19. *La categoría de morfismos étale finitos sobre un esquema $X$ es de Galois, donde el funtor de fibra puede tomarse como el funtor de fibras sobre cualquier punto geométrico de $X$.*

Ejemplo 4.20. *Sea $G$ un grupo profinito. La categoría de $G$-conjuntos finitos (con la topología discreta) con acción continua de $G$ es una categoría de Galois con funtor de fibra el funtor que olvida $U : G - \boldsymbol{FSet} \to \boldsymbol{FSet}$.*

Nótese que de hecho los ejemplos 4.17, 4.18 y 4.19 son casos particulares del ejemplo anterior por las proposiciones 1.31, 2.26 y 3.59, respectivamente.

Para el siguiente resultado se recuerda que una categoría $\mathcal{C}$ es **artiniana** si para cada sucesión de objetos y morfismos en $\mathcal{C}$ de la forma:

$$\dots \longrightarrow C_3 \xrightarrow{f_3} C_2 \xrightarrow{f_2} C_1 \xrightarrow{f_1} C_0,$$

con cada $f_n$ monomorfismo, existe $N \in \mathbb{N}^+$ tal que para cada $n \geq N$, $f_n$ es un isomorfismo.

Proposición 4.21. *Toda categoría de Galois es artiniana.*

Demostración. Sea $(\mathcal{C}, F)$ una categoría de Galois y considérese la siguiente sucesión en $\mathcal{C}$ donde cada morfismo es un monomorfismo.

$$\dots \longrightarrow C_3 \xrightarrow{f_3} C_2 \xrightarrow{f_2} C_1 \xrightarrow{f_1} C_0$$

Al aplicar el funtor $F$ y dado que este preserva monomorfismos por la proposición anterior, se tiene la siguiente sucesión de conjuntos finitos con funciones inyectivas entre ellos

$$\dots \longrightarrow F(C_3) \xrightarrow{F(f_3)} F(C_2) \xrightarrow{F(f_2)} F(C_1) \xrightarrow{F(f_1)} F(C_0).$$

Como $F(C_0)$ es un conjunto finito, esto implica que existe $N \in \mathbb{N}^+$ tal que para cada $n \geq N$, $F(f_n)$ es una biyección. Pero como $F$ refleja isomorfismos, esto implica que para cada $n \geq N$, $f_n$ es un isomorfismo. $\square$

Proposición 4.22. *Sean $(\mathcal{C}, F)$ una categoría de Galois, $f : Y \to X$ un morfismo en $\mathcal{C}$ y $X_0 \in \mathcal{C}$. Entonces,*

1. *$F(f)$ es un epimorfismo si y sólo si $f$ es un epimorfismo estricto.*
2. *$F(f)$ es un monomorfismo si y sólo si $f$ es un monomorfismo.*
3. *$F(X_0) = \emptyset$ si y sólo si $X_0 = 0$.*
4. *$F(X_0) = \{*\}$ si y sólo si $X_0 = 1$.*

Demostración. Considérese una descomposición de $f$ de la forma $f = u \circ e$ con $u$ un monomorfismo que escinde y $e$ un epimorfismo estricto. Así, $F(f) = F(u) \circ F(e)$ y, dado que $F(f)$ es por hipótesis un epimorfismo, entonces $F(u)$ también lo es. Además, como $F$ preserva monomorfismos, $F(u)$ es un monomorfismo y por lo tanto $F(u)$ es una biyección. Así, dado que $F$ refleja isomorfismos se tiene que $u$ es un isomorfismo y por lo tanto $f$ es un epimorfismo estricto. La otra dirección se sigue de que $F$ preserva epimorfismos estrictos y que los epimorfismos estrictos en **Set** son precisamente los epimorfismos.

Respecto a la segunda propiedad, $F$ preserva monomorfismos por un resultado previo. Por otro lado, si $F(f)$ es un monomorfismo, entonces al escribir $f = u \circ e$ con $u$ un monomorfismo que escinde y $e$ un epimorfismo estricto, se tiene que $F(f) = F(u) \circ F(e)$, de donde $F(e)$ es inyectiva. Dado que $F(e)$ es suprayectiva, entonces es una biyección y como $F$ refleja isomofismos se deduce que $e$ es un isomorfismo. Así, $f$ es un monomorfismo que escinde y por lo tanto un monomorfismo.

Para la ida de 3 considérese el único morfismo en $\mathcal{C}$, $0 \to X_0$. Luego, al aplicar el funtor $F$ se tiene que $F(0) \to F(X_0)$ es una biyección pues $F(0) = \emptyset$. Así, como $F$ refleja isomorfismos se deduce que $0 \cong X_0$. El regreso es claro pues $F$ preseva el coproducto de una familia vacía, que es el objeto inicial en la categoría en cuestión.

La prueba de la afirmación 4 es análoga a la de 2, por lo tanto esta se va a omitir. $\square$

Corolario 4.23. *En toda categoría de Galois el objeto inicial es estricto, es decir, todo morfismo $X \to 0$ es un isomorfismo.*

Demostración. Sea $X \to 0$ un morfismo en una categoría de Galois $(\mathcal{C}, F)$. Entonces, $F(X) \to F(0)$ es una función y como $F(0) = \emptyset$, entonces $F(X) = \emptyset$. Así, del resultado anterior $X \cong 0$ y el isomorfismo está dado por el morfismo $X \to 0$. $\square$

Corolario 4.24. *En toda categoría de Galois los morfismos canónicos de un coproducto finito son monomorfismos.*

Demostración. Sea $(\mathcal{C}, F)$ una categoría de Galois. Para probar la afirmación basta con mostrar que esta es válida para el coproducto de dos objetos pues para el caso de una familia vacía el resultado se sigue del corolario anterior. Así, sean $X, Y \in \mathcal{C}$ y, $\iota_1 : X \to X \coprod Y$ e $\iota_2 : Y \to X \coprod Y$ los morfismos canónicos. Luego, $F(\iota_1) : F(X) \to F(X \coprod Y) \cong F(X) \sqcup F(Y)$. Pero en la categoría de conjuntos dicho morfismo es inyectivo, por lo que la proposición anterior implica que $\iota_1$ es un monomorfismo. Además, el argumento para $\iota_2$ se va a omitir pues es completamente análogo. $\square$

## 2. Objetos conexos y de Galois

El siguiente concepto es una adaptación del concepto de conexidad en topología.

Definición 4.25. *Sea $\mathcal{C}$ una categoría con coproductos finitos. Un objeto $X \in \mathcal{C}$ es* ***conexo*** *si $X \neq 0$ y siempre que $X = Y \coprod Z$ con $Y, Z \in \mathcal{C}$, entonces $Y = 0$ ó $Z = 0$.*

Lo primero que se busca es dar un resultado de caracterización de objetos conexos en una categoría de Galois a partir de morfismos. En esta dirección se requiere probar el siguiente resultado que tiene una hipótesis más débil que la afirmación 1 de la Proposición 4.9.

Lema 4.26. *Supóngase que $f : Y \to X$ es un morfismo en $\mathcal{C}$ que es simultáneamente un monomorfismo y un epimorfismo estricto. Entonces, $f$ es un isomorfismo.*

Demostración. Al ser $f$ un epimorfismo estricto se tiene que $f^* : \mathcal{C}(X, Y) \to \mathcal{C}(Y, Y)$ es una biyección de $\mathcal{C}(X, Y)$ con $\{\beta \in \mathcal{C}(Y, Y) \mid \beta \circ p_1 = \beta \circ p_2\}$, con $p_1, p_2 : Y \times_X Y \to Y$ los morfismos canónicos del producto fibrado. Así, como $f \circ p_1 = f \circ p_2$, al ser $f$ un monomorfismo se deduce que $p_1 = p_2$, de donde se deduce que $1_Y \circ p_1 = 1_Y \circ p_2$ y así, existe $g \in \mathcal{C}(X, Y)$ tal que $f^*(g) = 1_Y$, es decir, $g \circ f = 1_Y$. Esto prueba que $f$ es de hecho un monomorfismo que escinde y al ser $f$ un epimorfismo también, se deduce que es un isomorfismo. $\square$

Proposición 4.27. *Sea $X \in \mathcal{C}$ con $(\mathcal{C}, F)$ una categoría de Galois. Entonces, $X$ es conexo si y sólo si todo monomorfismo en $\mathcal{C}$, $Y \to X$ con $Y \neq 0$, es un isomorfismo.*

Demostración. $\Rightarrow$) Sea $f : Y \to X$ un monomorfismo en $\mathcal{C}$ con $Y \neq 0$ y $X$ conexo. Al considerar la factorización $f = u \circ e$ con $u : Z \to X$ monomorfismo que escinde y $e : Y \to Z$ epimorfismo estricto, se tiene que $X = Z \coprod W$ para algún $W \in \mathcal{C}$. Entonces, de la conexidad de $X$ se deduce que $Z = 0$ ó $W = 0$. Pero si $Z = 0$, entonces $Y = 0$ por ser el objeto inicial en $\mathcal{C}$ estricto, lo que es una contradicción. Luego $W = 0$ y así, $u$ es un isomorfismo. Por otro lado $e$ es un epimorfismo estricto y dado que $f$ es un monomorfismo $e$ también lo es. Por lo tanto, del lema anterior se deduce que $e$ es un isomorfismo y así, $f$ también lo es.

$\Leftarrow$) Supóngase que $X = Y \coprod Z$ y que $Y \neq 0$. Así, se tiene un monomorfismo $Y \to X$, que es la inclusión canónica, el cual es un isomorfismo por hipótesis. Luego, como $F(X) = F(Y) \sqcup F(Z)$, esto implica que $F(Z) = \emptyset$ y de una proposición anterior se deduce que $Z = 0$. □

Corolario 4.28. *Sea $X \in \mathcal{C}$ con $X \neq 0$. Entonces existen $X_1, ..., X_n \in \mathcal{C}$ conexos tales que $X = \coprod_{i=1}^{n} X_i$ y además, dicha descomposición es única salvo el orden de los factores.*

Demostración. Lo primero que se va a probar es la existencia de la descomposición. Así, dado que toda categoría de Galois es artiniana, entonces existe un monomorfismo $X_1 \xrightarrow{f_1} X$ con $X_1$ conexo. Si dicho morfismo en un isomorfismo, entonces se ha concluido la prueba. En caso contrario sea $f_1 = u_1 \circ e_1$ con $u_1 : Y \to X$ un monomorfismo que escinde y $e_1 : X_1 \to Y$ un epimorfismo estricto. Como $f_1$ es un monomorfismo entonces $e_1$ también lo es. Luego $e_1$ es un isomorfismo y así $Y$ es conexo y por lo tanto $X \cong X_1 \coprod Y_1$ para algún $Y_1 \in \mathcal{C}$. Así, al repetir el argumento anterior con $Y_1$, existe un objeto conexo $X_2 \in \mathcal{C}$ y un monomorfismo $f_2 : X_2 \to Y_1$. Por lo tanto $X \cong X_1 \coprod X_2 \coprod Y_2$ para algún $Y_2 \in \mathcal{C}$ y el argumento puede iterarse. Además, este se detiene pues como el funtor $F$ toma valores en conjuntos finitos y preserva coproductos, se requieren a lo más tantos pasos como $|F(X)|$ para obtener la descomposición deseada.

Respecto a la unicidad supóngase que $X = \coprod_{i=1}^{n} X_i = \coprod_{j=1}^{m} X'_j$ son descomposiciones de $X$ con objetos conexos y sin pérdida de generalidad que $n \leq m$. Al aplicar el funtor $F$ se tiene que $\sqcup_{i=1}^{n} F(X_i) = \sqcup_{j=1}^{m} F(X'_j)$. Así, para cada $i \in \{1, ..., n\}$ sea $\sigma(i) \in \{1, ..., m\}$ el único indice tal que $F(X_i) \cap F(X'_{\sigma(i)}) \neq \emptyset$. Luego, considérese el siguiente diagrama que es un producto fibrado.

$$\begin{tikzcd}
X_i \times_X X'_{\sigma(i)} \arrow[r, "p_1"] \arrow[d, "p_2"'] & X_i \arrow[d, "\iota_i"] \\
X'_{\sigma(i)} \arrow[r, "\iota'_{\sigma(i)}"'] & X
\end{tikzcd}$$

Dado que $\iota_i$ y $\iota'_{\sigma(i)}$ son monomorfismos, entonces también lo son $p_1$ y $p_2$. Luego, $F(X_i \times_X X'_{\sigma(i)}) \cong F(X_1) \cap F(X'_{\sigma(i)}) \neq \emptyset$ pues $F$ preserva monomorfismos. Así, se deduce por la Proposición 4.27 que $p_1$ y $p_2$ son isomorfismos. Por lo tanto $X_i \cong X_{\sigma(i)}$. Además, esto implica que $F(\coprod_{j\neq\sigma(i)} X'_j) = \emptyset$, de donde $n = m$ pues al ser cada objeto conexo no se puede tener que para algun índice $j \neq \sigma(i)$, $F(X'_j) = \emptyset$, pues esto implica que $X'_j = 0$, lo que es una contradicción. $\square$

El resultado anterior aunado a su análogo en topología general motivan lo siguiente.

DEFINICIÓN 4.29. *Los elementos de la descomposición de $X$ según el corolario anterior se conocen como las **componentes conexas** de $X$.*

Los siguientes resultados se refieren a propiedades respecto a morfismos donde al menos un objeto es conexo. Para estos resultados se requiere introducir la **categoría punteada** asociada a una categoría de Galois $(\mathcal{C}, F)$ que se denota por $\mathcal{C}_*$. Esta tiene por objetos parejas $(X, c)$ con $X \in \mathcal{C}$ y $c \in F(X)$. Un morfismo en $\mathcal{C}_*$, $f : (Y, c) \to (X, d)$, es un morfismo en $\mathcal{C}$, $f : Y \to X$ tal que $F(f)(c) = d$.

PROPOSICIÓN 4.30. *(Teorema de Rigidez) Sea $Y \in \mathcal{C}$ conexo con $d \in F(Y)$. Para todo $X \in \mathcal{C}$ con $X \neq 0$ y $c \in F(X)$, $|\mathcal{C}_*((Y, d), (X, c))| \leq 1$.*

DEMOSTRACIÓN. Supóngase que $f, g : (Y, d) \to (X, c)$ son morfismos en $\mathcal{C}_*$ y considérese $e : E \to Y$ el igualador de $f$ y $g$ en $\mathcal{C}$. Como $F(e) : F(E) \to F(Y)$ es el igualador de $F(f), F(g) : F(Y) \to F(X)$ y además por definición de $\mathcal{C}_*$ se tiene que $F(f)(d) = c = F(g)(d)$, entonces $d \in F(E)$, de lo que se deduce que $F(E) \neq \emptyset$. Así, $E \neq 0$ y dado que $e$ es siempre un monomorfismo, se tiene que $e$ es un isomorfismo por la Proposición 4.27. Por lo tanto $f = g$. $\square$

Vale la pena observar que el teorema de Rigidez es un análogo categórico del Lema 2.5 y del Corolario 3.41, que afirman que dos morfismos de aplicaciones cubrientes o morfismos étale finitos que coincidieran en un punto o punto geométrico respectivamente, tenían que ser iguales si el dominio es conexo. De hecho, la idea de considerar categorías punteadas es precisamente la de tener este tipo de resultados.

Para el siguiente resultado se recuerda que para $X, Y \in \mathcal{C}$ con $\mathcal{C}$ una categoría cualquiera, se dice que $X$ **domina** a $Y$, lo que se denota por $X \geq Y$, si existe al menos un morfismo $X \to Y$. Nótese que la relación de dominación es reflexiva y transitiva.

PROPOSICIÓN 4.31. *(Teorema de dominación por objetos conexos) Sea $(\mathcal{C}, F)$ una categoría de Galois. Para toda familia $\{(X_i, c_i)\}_{i=1}^n \subseteq \mathcal{C}_*$, existe $(X_0, c_0) \in \mathcal{C}_*$ con $X_0 \in \mathcal{C}$ conexo tal que para cada $i \in \{1, ..., n\}$, $(X_0, c_0) \geq (X_i, c_i)$.*

DEMOSTRACIÓN. Sea $\{(X_i, c_i)\}_{i=1}^n \subseteq \mathcal{C}_*$. Así, dado que existen las proyecciones canónicas $\pi_j : \prod_{i=1}^n X_i \to X_j$ y como $F(\prod_{i=1}^n X_i) \cong \prod_{i=1}^n F(X_i)$, entonces para cada $j \in \{1, ..., n\}$, $(\prod_{i=1}^n X_i, (c_1, ..., c_n)) \geq (X_j, c_j)$. Así, de acuerdo al argumento anterior, basta con probar que dado un objeto $(Y, d) \in \mathcal{C}_*$, este puede ser dominado por un objeto conexo.

En efecto, considérese la descomposición en componentes conexas de $Y$, $Y = \coprod_{i=1}^m Y_i$. Dado que $d \in F(Y)$ y $F(Y) = \sqcup_{i=1}^m F(Y_i)$, existe un único $i_0 \in \{1, ..., m\}$ tal que $d \in F(Y_{i_0})$. Luego, al considerar la inclusión canónica $\iota_{i_0} : Y_{i_0} \to Y$, esta satisface que $F(\iota_{i_0})(d) = d$ y por lo tanto $(Y_{i_0}, d) \geq (X, d)$ en $\mathcal{C}_*$. $\square$

COROLARIO 4.32. *Sea $(\mathcal{C}, F)$ una categoría de Galois. Para todo $X \in \mathcal{C}$ no inicial existe $(X_0, c_0) \in \mathcal{C}_*$ con $X_0$ conexo tal que la función $ev_{c_0} : \mathcal{C}(X_0, X) \to F(X)$ cuya regla de correspondencia es $ev_{c_0}(u) = F(u)(c_0)$, es biyectiva.*

DEMOSTRACIÓN. Sea $X \in \mathcal{C}$ con $X \neq 0$. Si $F(X) = \{c_1, ..., c_n\}$, entonces al considerar la familia $\{(X, c_i)\}_{i=1}^n \subseteq \mathcal{C}_*$, la proposición anterior implica que existe $(X_0, c_0) \in \mathcal{C}_*$ con $X_0$ conexo tal que $(X_0, C_0) \geq (X, c_i)$ para cada $i \in \{1, ..., n\}$ y, sea $f_i$ el morfismo testigo de la dominación. Por construcción es claro que $ev_{c_0}$ es suprayectiva. Más aún, la inyectividad se sigue de que si $g, h \in \mathcal{C}(X_0, X)$ son tales que $ev_{c_0}(g) = ev_{c_0}(h)$, entonces $F(g)(c_0) = F(h)(c_0)$. Luego, $g$ y $h$ inducen un morfismo en $\mathcal{C}_*((X_0, c_0), (X, F(g)(c_0)))$, que por el teorema de rigidez debe ser el mismo y así, $g = h$. $\square$

PROPOSICIÓN 4.33. *Sea $(\mathcal{C}, F)$ una categoría de Galois.*
1. *Si $X \in \mathcal{C}$ es conexo, entonces todo morfismo $f : Y \to X$ con $Y \neq 0$ es un epimorfismo estricto.*
2. *Todo endomorfismo de un objeto conexo es un automorfismo.*

3. *Si $f : Y \to X$ es un epimorfismo estricto y $Y$ es conexo, entonces $X$ es conexo.*

Demostración. Para 1 sea $f : Y \to X$ un morfismo con $X$ conexo y $Y \neq 0$. Al considerar la factorización de $f = u \circ e$ con $u : Z \to X$ un monomorfismo que escinde y $e : Y \to Z$ un epimorfismo estricto, dado que $X = Z \coprod W$ para algún $W \in \mathcal{C}$, si se supone que $W \neq 0$, entonces la conexidad implica que $Z = 0$. Luego, al ser 0 un objeto inicial estricto se tiene que $Y = 0$, lo que es una contradicción. De este argumento se concluye que $W = 0$ y así, $u$ es un isomorfismo. Por lo tanto $f$ es un epimorfismo estricto.

Respecto a 2 sea $f : X \to X$ un morfismo con $X$ conexo. Dado que $f = u \circ e$ con $u : Y \to X$ un monomorfismo que escinde y $e : X \to Y$ un epimorfismo estricto, se tiene que $X \cong Y \coprod W$ para algún $W \in \mathcal{C}$. La conexidad de $X$ implica que $W = 0$ pues en caso contrario $Y = 0$ y al ser el objeto inicial estricto $X = 0$, lo que es una contradicción. Por lo tanto $Y \cong X$ con un isomorfismo dado por $u$. Además, como en particular esto implica que $|F(X)| = |F(Y)|$ y además $F(e) : F(X) \to F(Y)$ es suprayectiva, entonces $F(e)$ es una biyección, lo que implica que $e$ es un isomorfismo. Por lo tanto $f$ es composición de dos isomorfismos y entonces es un isomorfismo.

En lo que respecta a 3 sea $f : Y \to X$ un epimorfismo estricto. Por hipótesis $Y \neq 0$, lo que implica que $X \neq 0$. Además existe una factorización de $f$, $f = u \circ e$ con $u : Z \to X$ un monomorfismo que escinde y $e : Y \to Z$ un epimorfismo estricto. Así, supóngase que $X = Z \coprod W$ y además que $Z \neq 0$. Luego, considérese el morfismo canónico $\iota : Z \to X$, $d \in F(Z)$ y tómense $c \in F(Y)$ tal que $d := F(f)(c)$. Luego, se tienen morfismos en la categoría $\mathcal{C}_*$, $f : (Y, c) \to (X, d)$ e $\iota : (Z, d) \to (X, d)$. Además, por el teorema de dominación por objetos conexos existe $(X_0, c_0) \in \mathcal{C}_*$ tal que $X_0$ es conexo, $(X_0, c_0) \geq (Y, c)$ con testigo $p$ y $(X_0, c_0) \geq (Z, d)$ con testigo $q$. Además, por la primera afirmación de esta proposición se tiene que $p$ y $q$ son epimorfismos estrictos. Como $f \circ p, \iota \circ q : (X_0, c_0) \to (X, c)$, el teorema de rigidez implica que $f \circ p = \iota \circ q$. Dado que $f \circ p$ es un epimorfismo estricto, entonces $\iota$ es un epimorfismo estricto y al ser $\iota$ un monomorfismo por el Corolario 4.24, entonces $\iota$ es un isomorfismo. Así, $F(X) \cong F(Z)$ y dado que $F(X) \cong F(Z) \sqcup F(W)$, entonces $F(W) = \emptyset$, de donde $W = 0$. Esto concluye la prueba de la conexidad de $X$. □

Para el siguiente resultado nótese que si $(\mathcal{C}, F)$ es una categoría de Galois y $X \in \mathcal{C}$ es conexo, entonces dado $c \in F(X)$ la función $ev_c : \mathrm{Aut}_{\mathcal{C}}(X) \to F(X)$ cuya regla de correspondencia es $ev_c(f) = F(f)(c)$ es inyectiva por el teorema de rigidez. Esto implica que $|\mathrm{Aut}_{\mathcal{C}}(X)| \leq |F(X)|$, por lo que el conjunto $\mathrm{Aut}_{\mathcal{C}}(X)$ es finito.

El siguiente resultado da condiciones equivalentes para ver cuando esta función es suprayectiva y por lo tanto una biyección.

Proposición 4.34. *Sea $X \in \mathcal{C}$ un objeto conexo en una categoría de Galois $(\mathcal{C}, F)$. Las siguientes afirmaciones son equivalentes:*

1. *La función $ev_c : \operatorname{Aut}_{\mathcal{C}}(X) \to F(X)$ es una biyección.*
2. *$\operatorname{Aut}_{\mathcal{C}}(X)$ actúa sin puntos fijos y de forma transitiva en $F(X)$.*
3. *$\operatorname{Aut}_{\mathcal{C}}(X)$ actúa de forma transitiva en $F(X)$.*
4. *$X/\operatorname{Aut}_{\mathcal{C}}(X) = 0$.*
5. *$|\operatorname{Aut}_{\mathcal{C}}(X)| = |F(X)|$*

Demostración. Dado que $ev_c$ es siempre inyectiva, entonces 1 y 5 son equivalentes. Además es claro que $1 \Rightarrow 2$, $2 \Rightarrow 3$, $3 \Rightarrow 4$ y que $4 \Rightarrow 5$. $\square$

Definición 4.35. *Un objeto conexo $X \in \mathcal{C}$ que cumple una de, y por lo tanto todas, las condiciones equivalentes de la proposición anterior se conoce como un **objeto de Galois**.*

El primer resultado que se va a estudiar es el análogo al probado por Serre para el caso de esquemas que se encuentra en el capítulo anterior. Este afirma que todo objeto conexo puede ser dominado de forma mínima por un objeto de Galois.

Proposición 4.36. *(Clausura de Galois) Para cada $X \in \mathcal{C}$ conexo existe $\hat{X} \in \mathcal{C}$ de Galois que lo domina y es mínimo respecto a esta propiedad.*

Demostración. Sea $X \in \mathcal{C}$ conexo. Por el Corolario 4.32 existe $(X_0, c_0) \in \mathcal{C}_*$ con $X_0 \in \mathcal{C}$ conexo tal que $ev_{c_0} : \mathcal{C}(X_0, X) \to F(X)$ es una biyección. Ahora supóngase que $\mathcal{C}(X_0, X) = \{f_1, ..., f_n\}$ y defínase para cada $i \in \{1, ..., n\}$, $c_i := F(f_i)(c_0)$. Luego, como $\mathcal{C}$ tiene productos finitos, por la propiedad universal existe un único morfismo $f : X_0 \to X^n$ tal que para cada $i \in \{1, ..., n\}$, $\pi_i \circ f = f_i$, con $\pi_i : X^n \to X$ la $i$-ésima proyección. Como $f = u \circ e$ con $u : \hat{X} \to X^n$ monomorfismo que escinde y $e : X_0 \to \hat{X}$ epimorfismo estricto, se tiene que la conexidad de $X_0$ implica que $\hat{X}$ es conexo. Lo que se afirma es que de hecho $\hat{X}$ es de Galois. Para esto sea $d \in F(\hat{X})$ definido por $d = F(e)(c_0)$. Se va a probar que $ev_d : \operatorname{Aut}_{\mathcal{C}}(\hat{X}) \to F(\hat{X})$ es una biyección, para lo que basta ver que esta función es suprayectiva pues es inyectiva por ser $\hat{X}$ conexo.

En efecto, sea $c \in F(\hat{X})$. Ahora considérense $(\hat{X}, c), (X_0, c_0) \in \mathcal{C}_*$. Al usar el teorema de dominación por objetos conexos se deduce que existe $(\overline{X_0}, \overline{c_0}) \in \mathcal{C}_*$, con

$\overline{X_0} \in \mathcal{C}$ conexo, tal que domina a los objetos considerados. Así, al reemplazar $(X_0, c_0)$ por $(\overline{X_0}, \overline{c_0})$, se puede suponer que hay un morfismo $g : (X_0, c_0) \to (\hat{X}, c)$.

Ahora se afirma que existe $\sigma \in \mathrm{Aut}_{\mathcal{C}}(\hat{X})$ tal que $\sigma \circ e = g$. Nótese que si esto pasa entonces $F(\sigma)(F(e)(c_0)) = F(\sigma \circ e)(c_0) = F(g)(c_0) = c$, lo que concluiría la prueba de la suprayectividad. Así, para probar la existencia de $\sigma \in \mathrm{Aut}_{\mathcal{C}}(\hat{X})$ con la propiedad mencionada nótese que para cada $i \in \{1, ..., n\}$ se tiene que $\pi_i \circ u \circ g : X_0 \to X$. Luego, se afirma que $\mathcal{C}(X_0, X) = \{\pi_i \circ u \circ g \mid i \in \{1, ..., n\}\}$. En dirección de probar esta igualdad, dado $i \in \{1, ..., n\}$ se tiene que $\pi_i \circ u \circ g = \pi_i \circ f = f_i$, por lo que $\{\pi_i \circ u \circ g \mid i \in \{1, ..., n\}\} \subseteq \mathcal{C}(X_0, X)$. Para probar la igualdad que se quiere basta con ver que el subconjunto tiene precisamente $n$ elementos. Para esto, si $i, j \in \{1, ..., n\}$ son tales que $\pi_i \circ u \circ g = \pi_j \circ u \circ g$, al ser $g$ en particular un epimorfismo se tiene que $\pi_i \circ u = \pi_j \circ u$. Esto implica que $\pi_i \circ f = \pi_j \circ f$ al componer con $e$, de donde $f_i = f_j$. Esto último implica que $i = j$, lo que concluye la prueba de la afirmación.

La igualdad de conjuntos implica que dado $i \in \{1, ..., n\}$ existe $\tau(i) \in \{1, ..., n\}$ tal que $f_i = \pi_{\tau(i)} \circ u \circ g$. De esto es claro que debe existir $\sigma \in \mathrm{Aut}_{\mathcal{C}}(\hat{X})$ tal que $\sigma \circ e = g$.

Respecto a la propiedad de minimalidad de $\hat{X}$ sea $q : Y \to X$ un morfismo con $Y$ de Galois. Así, para cada $i \in \{1, ..., n\}$ sea $d_i \in F(Y)$ tal que $F(q)(d_i) = c_i$, el cual existe pues $q$ es un epimorfismo estricto por ser $X$ conexo. Además, sea $\sigma_i \in \mathrm{Aut}_{\mathcal{C}}(Y)$ tal que $F(\sigma_i)(d_1) = d_i$, el cual existe pues $Y$ es de Galois. Dado que $q \circ \sigma_i : Y \to X$, por la propiedad universal del producto existe un único morfismo $k : Y \to X^n$ tal que $\pi_i \circ k = q \circ \sigma_i$, con $\pi_i : X^n \to X$ la $i$-ésima proyección. Así, al escribir $k = u' \circ e'$ con $u' : Z \to X^n$ monomorfismo que escinde y $e' : Y \to Z$ epimorfismo estricto, se deduce que $Z$ es conexo. Así, este es componente de $X^n$ y además, nótese que $F(k)(d_1) = (c_1, ..., c_n)$, por lo que $Z \cong \hat{X}$. Luego, existe un morfismo $Y \to \hat{X}$, lo que concluye la prueba. $\square$

Supóngase que $X = \coprod_{i=1}^{n} X_i$, con $X_i$ sus componentes conexas. Si $\iota_i : X_i \to X$ denota el morfismo canónico de $X_i$ en $X$, entonces dado $Y \in \mathcal{C}$ con $Y \neq 0$, estos inducen funciones $(\iota_i)_* : \mathcal{C}(Y, X_i) \to \mathcal{C}(Y, X)$. Luego, por la propiedad universal del coproducto en la categoría de conjuntos se tiene que estas funciones inducen una única función $\phi : \sqcup_{i=1}^{n} \mathcal{C}(Y, X_i) \to \mathcal{C}(Y, X)$ tal que $\phi|_{\mathcal{C}(Y, X_i)} = (\iota_i)_*$. Con la notación anterior se tiene el siguiente resultado.

LEMA 4.37. *La función $\phi$ es una biyección.*

Demostración. Para la inyectividad, sean $f, g \in \sqcup_{i=1}^{n} \mathcal{C}(Y, X_i)$ tales que $\phi(f) = \phi(g)$. Si $f \in \mathcal{C}(Y, X_j)$ y $g \in \mathcal{C}(Y, X_k)$, entonces esta igualdad dice que $\iota_j \circ f = (\iota_j)_*(f) = (\iota_k)_*(g) = \iota_k \circ g$. Luego, al ser $Y \neq 0$ y $X_j$ y $X_k$ conexos, se deduce que $f$ y $g$ son epimorfismos estrictos. Así, la igualdad que se tiene implica que el morfismo $\iota_j \circ f$ tiene dos descomposiciones a partir de un monomorfismo que escinde y un epimorfismo estricto, por lo que $X_j \cong X_k$ y así, $j = k$. De esto se deduce que $f = g$.

Respecto a la suprayectividad, sea $f \in \mathcal{C}(Y, X)$. Luego, supóngase que $f = u \circ e$ con $u : Z \to X$ un monomorfismo que escinde y $e : Y \to Z$ un epimorfismo estricto. Dado que $Y$ es conexo, entonces $Z$ también lo es, lo que implica que $Z$ es componente conexa de $X$. Así, existe $i_0 \in \{1, ..., n\}$ tal que $Z = X_{i_0}$ y $u = \iota_{i_0}$. Para concluir la prueba se observa que $u \in \mathcal{C}(Y, X_{i_0})$ y que $\phi(e) = (\iota_{i_0})_*(e) = \iota_{i_0} \circ e = f$. □

La importancia del resultado anterior radica en el hecho de que como es usual, para muchas pruebas podemos restringirnos a caso conexo en lugar de tratar morfismos generales.

Para $(\mathcal{C}, F)$ una categoría de Galois y $X \in \mathcal{C}$ de Galois, se define $\mathcal{C}^X$ la subcategoría plena de $\mathcal{C}$ cuyos objetos son aquellos cuyas componentes conexas son todas dominadas por $X$. Además, cuando se escribe $\mathcal{C}^X$ siempre se supone que $X \neq 0$ pues $\mathcal{C}^0 = \emptyset$. Así, sea $F^X : \mathcal{C}^X \to \mathbf{FSet}$ la restricción del funtor de fibra a dicha subcategoría. Con esta notación se tiene el siguiente resultado.

Proposición 4.38. *(Correspondencia de Galois) Sea $(\mathcal{C}, F)$ una categoría de Galois. Entonces,*

1. *Todo $(X, c) \in \mathcal{C}_*$ induce un isomorfismo de funtores $ev_c : \mathcal{C}(X, \_)|_{\mathcal{C}^X} \to F^X$. En particular este induce un isomorfismo de grupos $\mathrm{Aut}(F^X) \cong \mathrm{Aut}(\mathcal{C}(X, \_)|_{\mathcal{C}^X})$. Además, por el lema de Yoneda estos grupos son isomorfos a $\mathrm{Aut}_{\mathcal{C}}(X)^{op}$.*
2. *El funtor $F^X : \mathcal{C}^X \to \boldsymbol{FSet}$ se factoriza a través de una equivalencia de categorías de acuerdo al siguiente diagrama, donde $U$ es el funtor que olvida.*

$$\begin{tikzcd}
\mathcal{C}^X \arrow[rr, "F^X"] \arrow[dr, "\simeq", "\hat{F^X}"'] & & \boldsymbol{FSet} \\
& \mathrm{Aut}_{\mathcal{C}}(X)^{op}\text{-}\boldsymbol{FSet} \arrow[ur, "U"'] &
\end{tikzcd}$$

Demostración. Para 1 nótese que $ev_c$ es natural pues dado $f : Y \to Z$ morfismo en $\mathcal{C}^X$, se tiene que al considerar el siguiente diagrama

$$\begin{array}{ccc} \mathcal{C}(X,Y) & \xrightarrow{f_*} & \mathcal{C}(X,Z) \\ {\scriptstyle ev_c(Y)}\downarrow & & \downarrow{\scriptstyle ev_c(Z)} \\ F^X(Y) & \xrightarrow[F^X(f)]{} & F^X(Z), \end{array}$$

este conmuta pues para $g \in \mathcal{C}(X,Y)$, se tiene que $(F^X(f) \circ ev_c(Y))(g) = F(f)F(g)(c) = F(f \circ g)(c) = ev_c(Z)(f \circ g) = (ev_c(Z) \circ f_*)(g)$.

Para probar que dicha transformación natural es un isomorfismo, es equivalente probar que objeto por objeto se tiene una isomorfismo, es decir, que para cada $Y \in \mathcal{C}^X$, la función $ev_c(Y) : \mathcal{C}(X,Y) \to F(Y)$, es una biyección. Pero, dado que esta función siempre es inyectiva pues $X$ es conexo, lo único que se va a probar es la suprayectividad. En efecto, sea $Y \in \mathcal{C}^X$. Se van a analizar dos casos:

1. $Y$ es conexo. Por definición de $\mathcal{C}^X$ existe un morfismo $X \to Y$, el cual es un epimorfismo estricto pues $Y$ es conexo. Ahora, si $d \in F(Y)$, entonces existe $e \in F(X)$ tal que $F(f)(e) = d$. Pero como $X$ es de Galois, existe $\sigma \in \mathrm{Aut}_{\mathcal{C}}(X)$ tal que $F(\sigma)(c) = e$. Así, nótese que $f \circ \sigma \in \mathcal{C}(X,Y)$, más aún, $F(f \circ \sigma)(c) = F(f)(e) = d$, lo que concluye la prueba en este caso.
2. $Y$ no conexo. Si $Y = \coprod_{i=1}^n Y_i$ es la descomposición en componentes conexas de $Y$, entonces por el lema anterior $\mathcal{C}(X,Y) \cong \sqcup_{i=1}^n \mathcal{C}(X,Y_i)$. Además, $F(Y) \cong \coprod_{i=1}^n F(Y_i)$. Así, el resultado se deduce del caso conexo pues cada $Y_i$ es conexo.

En lo que respecta a 2, nótese que por 1 hay una acción de $\mathrm{Aut}_{\mathcal{C}}(X)^{op}$ en $\mathcal{C}(X,Y)$ para $Y \in \mathcal{C}^X$, dada por precomponer. Así, $F^X(Y)$ tiene estructura de $\mathrm{Aut}_{\mathcal{C}}(X)^{op}$-conjunto. Luego, es claro que se da la factoización que se busca, donde $\hat{F^X}$ es a nivel de objetos $F^X$ con su estructura de $\mathrm{Aut}_{\mathcal{C}}(X)^{op}$-conjunto. Por lo tanto, lo que resta probar es que $\hat{F^X}$ es una equivalencia, para lo que se va a ver que este funtor es fiel, pleno y esencialmente suprayectivo.

Respecto a la propiedad de ser esencialmente suprayectivo, sea $E \in \mathrm{Aut}_{\mathcal{C}}(X)^{op}$-**FSet** y supóngase que este tiene acción transitiva. Luego, al considear $e \in E$, la función $p_e : \mathrm{Aut}_{\mathcal{C}}(X)^{op} \to E$ cuya regla de correspondencia es $p_e(\sigma) = \sigma \cdot e$, es un morfismo de $\mathrm{Aut}_{\mathcal{C}}(X)^{op}$-conjuntos suprayectivo. Así, sea $f_e := p_e \circ ev_{c_0}^{-1} : F(X) \to E$. Nótese que esta función es suprayectiva y además que si $\sigma \in \mathrm{Aut}_{\mathcal{C}}(X)_e^{op}$ y $\tau \in \mathrm{Aut}_{\mathcal{C}}(X)$, entonces $f_e(F(\sigma)(ev_{c_0}(\tau))) = f_e(ev_{c_0}(\sigma_*(\tau))) = p_e(\sigma \circ \tau) = (\sigma \circ \tau) \cdot e = \tau \cdot (\sigma \cdot e) = \tau \cdot e = f_e(ev_{c_0}(\tau))$. Por lo tanto, $f_e$ se factoriza a través de espacio cociente $F(X)/\,\mathrm{Aut}_{\mathbf{FSet}}\, F(X)_e^{op}$ mediante un morfismo $\overline{f_e}$. Pero nótese que existe en $\mathcal{C}$ el cociente $p : X \to X/\,\mathrm{Aut}_{\mathcal{C}}(X)_e$, el cual induce el cociente $F(X) \to$

$F(X)/\operatorname{Aut}_{\mathbf{FSet}} F(X)_e^{op}$. Dado que $X$ es conexo, se tiene que $G$ actúa sin puntos fijos en $F(X)$. Entonces, $|F(X)/\operatorname{Aut}_{\mathcal{C}}(X)_e| = \frac{|F(X)|}{|\operatorname{Aut}_{\mathcal{C}}(X)_e|} = [\operatorname{Aut}_{\mathcal{C}}(X) : \operatorname{Aut}_{\mathcal{C}}(X)_e] = |E|$, de donde se obtiene que $p_e$ es una biyección y por lo tanto es un isomorfismo de $\operatorname{Aut}_{\mathcal{C}}(X)^{op}$-conjuntos.

Lo que resta ver es que este funtor es fiel y pleno, es decir, que dados $Y, Z \in \mathcal{C}^X$, la función inducida $\hat{F^X} : \mathcal{C}(Y,Z) \to \operatorname{Aut}_{\mathcal{C}}(X)^{op}$-$\mathbf{FSet}(F(Y), F(Z))$ es una biyección. Más aún, por el lema anterior es suficiente con probar esto suponiendo que $Y$ y $Z$ son conexos. En efecto, nótese que la inyectividad es clara del teorema de rigidez. Respecto a la suprayectividad sea $f \in \operatorname{Aut}_{\mathcal{C}}(X)^{op}$-$\mathbf{FSet}(F(Y), F(Z))$. Así, dado $c \in F(Y)$, se tiene que $\operatorname{Aut}_{\mathcal{C}}(X)_c^{op} \subseteq \operatorname{Aut}_{\mathcal{C}}(X)_{f(c)}^{op}$. Si $p_c : X \to X/\operatorname{Aut}_{\mathcal{C}}(X)_c^{op}$ y $p_{f(c)} : X \to X/\operatorname{Aut}_{\mathcal{C}}(X)_{f(c)}^{op}$ son los morfismos caónicos del cociente, entonces la propiedad universal de $p_c$ implica que existe un único $g : X/\operatorname{Aut}_{\mathcal{C}}(X)_c^{op} \to X/\operatorname{Aut}_{\mathcal{C}}(X)_{f(c)}^{op}$ tal que $g \circ p_c = p_{f(c)}$. Así, el resultado se deduce de que como se vio en la suprayectividad esencial $F(X/\operatorname{Aut}_{\mathcal{C}}(X)_c^{op}) \cong F(Y)$ y $F(X/\operatorname{Aut}_{\mathcal{C}}(X)_{f(c)}^{op}) \cong F(Z)$ y así, $F(g) = f$. $\square$

## 3. El teorema principal

Sea $\mathcal{C}$ una categoría. Asociada a $\mathcal{C}$ existe una categoría que se conoce como la **categoría de sistemas proyectivos de** $\mathcal{C}$, que se denota por $\mathbf{Pro}(\mathcal{C})$, cuyos objetos son los sistemas proyectivos de $\mathcal{C}$, y cuyos morfismos son

$$\mathbf{Pro}(\mathcal{C})(X,Y) \cong \varprojlim_{j \in J} \varinjlim_{i \in I} \mathcal{C}(X_i, Y_j),$$

si $X = (\{X_i\}_{i \in I}, \{\phi_{ij} : X_i \to X_j\}_{j \leq i})$ y $Y = (\{Y_j\}_{j \in J}, \{\varphi_{ij} : Y_i \to Y_j\}_{j \leq i})$.

De la definición es claro que $\mathcal{C}$ tiene un encaje pleno en $\mathbf{Pro}(\mathcal{C})$. Además, si $F : \mathcal{C} \to \mathbf{FSet}$ es un funtor, este induce un funtor $\mathbf{Pro}(F) : \mathbf{Pro}(\mathcal{C}) \to \mathbf{Pro}(\mathbf{FSet})$.

El primer resultado de esta sección es en torno a una propiedad que cumple el funtor de fibra de una categoría de Galois, pues este resulta ser pro-representable.

Lema 4.39. *Sea $(\mathcal{C}, F)$ una categoría de Galois. La familia de clases de isomorfismo de objetos de Galois en $\mathcal{C}$,* $\operatorname{Gal}(\mathcal{C})$*, es un conjunto dirigido. Además, este permite definir un sistema proyectivo en $\mathcal{C}$.*

Demostración. $\mathrm{Gal}(\mathcal{C})$ tiene estructura de orden parcial por dominación. Para ver que este conjunto es dirigido, sean $X, Y \in \mathrm{Gal}(\mathcal{C})$. Como $X \times Y \in \mathcal{C}$, $X \times Y \geq X$ y $X \times Y \geq Y$, al tomar la clausura de Galois de $X \times Y$ se deduce que $\mathrm{Gal}(\mathcal{C})$ es dirigido.

Respecto a la segunda afirmación tómese $c \in \prod_{X \in \mathrm{Gal}(\mathcal{C})} F(X)$. Luego, si $X \leq Y$, por el teorema de rigidez existe un único $\phi^c_{XY} \in \mathcal{C}_*((Y, c_Y), (X, c_X))$. Así, nuevamente por el teorema de rigidez es claro que $(\mathrm{Gal}(\mathcal{C}), \{\phi^c_{XY} : Y \to X\}_{X \leq Y})$ es un sistema proyectivo. $\square$

Definición 4.40. *Un funtor pro-representable es* ***estrictamente pro-representable*** *si los morfismos de transición del sistema que lo pro-representa son epimorfismos.*

Proposición 4.41. *Para $(\mathcal{C}, F)$ una categoría de Galois, el funtor de fibra $F : \mathcal{C} \to$* ***FSet*** *es estrictamente pro-representable en $\mathcal{C}$.*

Demostración. Por el teorema de correspondencia de Galois (Proposición 4.38) se tiene que para cada $X \in \mathrm{Gal}(\mathcal{C})$, $\mathcal{C}(X, \_) \cong F^X$ con el isomorfismo dado por $ev_{c_X}$. Así, se tiene que $\varprojlim_{X \in \mathrm{Gal}(\mathcal{C})} ev_{c_X} : \varprojlim_{X \in \mathrm{Gal}(\mathcal{C})} \mathcal{C}(X, \_) \to \varprojlim_{X \in \mathrm{Gal}(\mathcal{C})} F^X$ es un isomorfismo natural. Más aún, $\varprojlim_{X \in \mathrm{Gal}(\mathcal{C})} F^X \cong F$, de lo que se deduce la pro-representabilidad del funtor $F$. Además, como por el lema anterior para $X \leq Y$ con $X, Y \in \mathrm{Gal}(\mathcal{C})$ se tiene que $\phi^c_{XY}$ tiene dominio $Y \neq 0$ y codominio $X$ que es conexo, entonces $\phi^c_{XY}$ es un epimorfismo estricto, lo que concluye la prueba. $\square$

Definición 4.42.

1. *Sea $\mathcal{C}$ una categoría de Galois y $F_1, F_2 : \mathcal{C} \to$* ***FSet*** *funtores de fibra. Al conjunto de isomorfismos de $F_1$ en $F_2$ se le llama el* ***conjunto de trayectorias*** *de $F_1$ en $F_2$ y se denota por $\pi_1(\mathcal{C}; F_1, F_2)$.*
2. *Si $(\mathcal{C}, F)$ es una categoría de Galois, a $\pi_1(\mathcal{C}; F, F)$ se le denota por $\pi_1(\mathcal{C}; F)$ y a este conjunto se le conoce como el* ***grupo fundamental de $\mathcal{C}$ con punto base*** *$F$.*

Ejemplo 4.43. *Sea $X$ un espacio conexo, localmente conectable por trayectorias y localmente simplemente conexo. Para cada $x \in X$, $\pi_1(\boldsymbol{FCov(X)}; F_x) \cong \pi_1(\hat{X}, x)$.*

Ejemplo 4.44. *Sea $X$ un esquema de la forma $X = \mathrm{Spec}\, k$. Para cada $x \in X$, $\pi_1(\boldsymbol{F\acute{E}t/X}; F_{\overline{x}}) \cong \pi_1(X, \overline{x})$. En particular para $k$ campo, $\pi_1(\boldsymbol{F\acute{E}t/X}; F_{\overline{x}}) \cong \mathrm{Gal}(k)$.*

Ejemplo 4.45. *Para $G$ un grupo profinito se tiene que* $\pi_1(G\text{-}\boldsymbol{FSet}; U) \cong G$.

Nótese que el último ejemplo dice que todo grupo profinito puede realizarse como el grupo fundamental de una categoría de Galois. Además, se observa que en cada uno de los ejemplos anteriores el grupo fundamental de una categoría de Galois resultó ser un grupo profinito. Este es un hecho general.

Proposición 4.46. *Si* $(\mathcal{C}, F)$ *es una categoría de Galois, entonces* $\pi_1(\mathcal{C}; F)$ *es un grupo profinito.*

Demostración. Considérese $G := \prod_{X \in \mathcal{C}} \mathrm{Aut}_{\mathbf{FSet}}(F(X))$. Si a cada elemento del producto se le da la topología discreta y a $G$ la topología producto, entonces $G$ tiene estructura de grupo topológico. Luego, sea $f : \pi_1(\mathcal{C}; F) \to G$ la función tal que $f(\eta) = (\eta_X)_{X \in \mathcal{C}}$. Esta función es claramente un monomorfismo de grupos. Así, nótese que se tiene un isomorfismo de grupos $\pi_1(\mathcal{C}; F) \cong \bigcap_{\phi \in \mathcal{C}(Y,X)} \{\eta \in G \mid \eta_X \circ F(\phi) = F(\phi) \circ \eta_Y\}$. El resultado se deduce de que cada uno de los intersectandos es un subgrupo cerrado de $G$, por lo que dicha intersección es un subgrupo cerrado. Además, un subgrupo cerrado de un grupo profinito es profinito. $\square$

El siguiente resultado que se busca es escribir a $\pi_1(\mathcal{C}; F)$, para $(\mathcal{C}, F)$ una categoría de Galois, como límite inverso. En esta dirección se requieren de algunos resultados previos.

Lema 4.47. *Para cualesquiera* $X, Y \in \mathrm{Gal}(\mathcal{C})$, $f, g : Y \to X$ *morfismos en* $\mathcal{C}$ *y* $\sigma_Y \in \mathrm{Aut}_{\mathcal{C}}(Y)$, *existe un único* $\sigma_X \in \mathrm{Aut}_{\mathcal{C}}(X)$ *tal que* $f \circ \sigma_Y = \sigma_X \circ g$.

Demostración. Para los objetos y morfismos de las hipótesis nótese que $g : Y \to X$ es un epimorfismo estricto por ser $X$ conexo y $Y \neq 0$. Así, la función $g^* : \mathrm{Aut}_{\mathcal{C}}(X) \to \mathcal{C}(Y, X)$ que se obtiene al restringir la función dada por precomponer con $g$ es inyectiva. Además, al ser $Y$ de Galois, el teorema de correspondencia implica que $|\mathcal{C}(Y, X)| = |F(X)|$. Pero como $X$ es de Galois, la definición implica que $|\mathrm{Aut}_{\mathcal{C}}(X)| = |F(X)|$. Por lo tanto se concluye que $g^*$ es una biyección. Luego, como $f \circ \sigma_Y \in \mathcal{C}(Y, X)$, entonces existe un único $\sigma_X \in \mathrm{Aut}_{\mathcal{C}}(X)$ tal que $g^*(\sigma_X) = f \circ \sigma_Y$, lo que concluye la prueba. $\square$

Corolario 4.48. *Para* $(\mathcal{C}, F)$ *una categoría de Galois, el conjunto* $\{\mathrm{Aut}_{\mathcal{C}}(X)\}_{X \in \mathrm{Gal}(\mathcal{C})}$ *es dirigido y define un sistema proyectivo.*

Demostración. El orden a considerar en el conjunto dado es nuevamente la dominación. Así, se observa que para $X, Y \in \mathrm{Gal}(\mathcal{C})$ se tiene que existe $Z \in \mathrm{Gal}(\mathcal{C})$ tal que $Z \geq X$ y $Z \geq Y$, con morfismos $f$ y $g$ testigos de cada una de las dominaciones respectivamente. Luego, el lema anterior implica que existen morfismos de grupos $\mathrm{Aut}_{\mathcal{C}}(Z) \to \mathrm{Aut}_{\mathcal{C}}(X)$ y $\mathrm{Aut}_{\mathcal{C}}(Z) \to \mathrm{Aut}_{\mathcal{C}}(Y)$, lo que muestra que el conjunto es dirigido.

Por otro lado, si $Y \geq X$ y $f$ es testigo de esta dominación, entonces por el lema anterior existe un morfismo de grupos $\phi_{XY} : \mathrm{Aut}_{\mathcal{C}}(Y) \to \mathrm{Aut}_{\mathcal{C}}(X)$, el cual es de hecho un epimorfismo. Todas estas funciones forman el sistema proyectivo para $\{\mathrm{Aut}_{\mathcal{C}}(X)\}$. $\square$

Para $(\mathcal{C}, F)$ una categoría de Galois, sea $G = \varprojlim_{X \in \mathrm{Gal}(\mathcal{C})} \mathrm{Aut}_{\mathcal{C}}(X)$. Por construcción es claro que $G$ es un grupo profinito. Además, nótese que para $X \in \mathrm{Gal}(\mathcal{C})$ se tiene una función $f_X : \pi_1(\mathcal{C}; F) \to \mathrm{Aut}_{\mathcal{C}}(X)$ definida mediante $f(\eta) = ev_{c_X}^{-1}(\eta_X(c_X))$. Nótese que estas funciones son compatibles con los morfismos de transición de $G$ pues para $X \leq Y$ se tiene que $(\phi_{XY} \circ f_Y)(\eta) = \phi_{XY}(ev_{c_Y}^{-1} \eta_Y(c_Y)) = ev_{c_X}^{-1} F(f) \eta_Y(c_Y) = ev_{c_X}^{-1} \eta_X F(f)(c_Y) = ev_{c_X}^{-1} \eta_X(c_X) = f_X(\eta)$.

Proposición 4.49. *El morfismo de grupos profinitos $f : \pi_1(\mathcal{C}; F) \to G^{op}$ es un isomorfismo de grupos profinitos.*

Demostración. Dado que $\pi_1(\mathcal{C}; F)$ es compacto y $G^{op}$ es Hausdorff, basta probar que $f$ es una función continua y biyectiva, para lo cual por la discusión previa lo único que falta probar es que $f$ es biyectiva. Sin embargo, de la definición de $\pi_1(\mathcal{C}; F)$ es claro que $f$ es inyectiva. Así, la suprayectividad de $f$ sea $(g_X)_{X \in \mathrm{Gal}(\mathcal{C})} \in G^{op}$. Luego, se observa que para $Z \in \mathcal{C}$ conexo se tiene que si $\hat{Z}$ denota su clausura de Galois, entonces se tiene la siguiente sucesión de funciones

$$F(Z) \xrightarrow[\cong]{ev_{c_Z}^{-1}} \mathcal{C}(\hat{Z}, Z) \xrightarrow[\cong]{g_Z^*} \mathcal{C}(\hat{Z}, Z) \xrightarrow[\cong]{ev_{c_Z}} F(Z)$$

Y denótese por $\eta_Z$ a dicha composición. Además, como el funtor $F$ preserva coproductos finitos, entonces al descomponer un elemento en sus componentes conexas se puede dar la definición de $\eta_X$ para cada $X \in \mathcal{C}$ y además, $\eta = (\eta_X)_{X \in \mathcal{C}} \in \pi_1(\mathcal{C}; F)$.

Para concluir se obseva que para $X \in \mathrm{Gal}(\mathcal{C})$ se tiene que $f_X(\eta) = ev_{c_X}^{-1}(\eta_X)(c_X) = g_X$, esto concluye la prueba. $\square$

El siguiente resultado tiene una interpretación muy interesante pues se recuerda que en el caso topológico, cuando existe una trayectoría que une dos puntos en un espacio, los grupos fundamentales en dichos puntos resultan ser isomorfos. De esto se concluye que para espacios conectables por trayectorias uno puede hablar de un grupo fundamental a secas, pues en todos los puntos de dicho espacio los grupos fundamentales son isomorfos. Así, el siguiente resultado se puede interpretar diciendo que en las categorías de Galois no hay problemas con los puntos bases pues siempre hay trayectorias entre ellos y por tal razón, no hay dependencia del funtor de fibra para el grupo fundamental de una categoría de Galois.

Teorema 4.50.

1. *Sea* $(\mathcal{C}, F)$ *una categoría de Galois. Entonces* $F$ *induce una equivalencia entre* $\mathcal{C}$ *y* $\pi_1(\mathcal{C}; F)$-***FSet***.
2. *Si* $F_1, F_2 : \mathcal{C} \to$ ***FSet*** *son funtores de fibra, entonces* $\pi_1(\mathcal{C}; F_1, F_2)$ *es no vacío. Además,* $\pi_1(\mathcal{C}; F_1)$ *es isomorfo a* $\pi_1(\mathcal{C}, F_2)$ *de manera no canónica salvo un automorfismo interior.*

Demostración. Para 1 nótese que por las proposiciones 4.41 y 4.49 basta con probar que $F^c : \mathbf{Pro}(\mathcal{C})(\mathcal{G}^c, \_)|_{\mathcal{C}} : \mathcal{C} \to \mathbf{FSet}$ se factoriza por una equivalencia de categorías $F^c : \mathcal{C} \to G^{op}$-**FSet**. En efecto, $F^c$ es esencialmente suprayectivo pues dado $X \in G^{op}$-**FSet**, al tener $X$ la topología discreta, la acción de $G^{op}$ en $X$ se factoriza por un cociente finito por $\mathrm{Aut}_{\mathcal{C}}(Y)$ para $Y \in \mathcal{C}$. Así, para concluir se puede aplicar el Teorema 4.38.

En lo que respecta a $F^c$ fiel y pleno, sean $X, Y \in \mathcal{C}$. Así, existe $Z \in \mathrm{Gal}(\mathcal{C})$ tal que $Z \geq X$ y $Z \geq Y$. Luego, el resultado se deduce de aplicar la Proposición 4.38 en $\mathcal{C}^X$, lo que concluye 1.

Respecto a 2, dado que $F_1$ y $F_2$ son pro-representables, basta con probar que sus sistemas inversos que los representan son isomorfos en la categoría $\mathbf{Pro}(\mathcal{C})$. Para esto sean $\mathcal{G}_1$ y $\mathcal{G}_2$ los respectivos sistemas de representación. Entonces,

$$\mathbf{Pro}(\mathcal{C})(\mathcal{G}_1^c, \mathcal{G}_2^d) \cong \varprojlim_{X \in \mathcal{G}_2^d} \varinjlim_{Y \in \mathcal{G}_1^c} \mathcal{C}(Y, X) \cong \varprojlim_{X \in \mathcal{G}_2^d} \varinjlim_{Y \in \mathcal{G}_1^c} \mathrm{Aut}_{\mathcal{C}}(X) \cong \varprojlim_{X \in \mathcal{G}_2^g} \mathrm{Aut}_{\mathcal{C}}(X).$$

Así, basta con probar que $\varprojlim_{X \in \mathcal{G}_2^d} \mathrm{Aut}_{\mathcal{C}}(X) \neq \emptyset$, afirmación que es clara pues cada $\mathrm{Aut}_{\mathcal{C}}(X)$ tiene la topología discreta y es finito, por lo que es un espacio compacto y Hausdorff no vacío, por lo que el límite inverso es no vacío. $\square$

## 4. Funtores fundamentales

DEFINICIÓN 4.51. *Sean $\mathcal{C}$ y $\mathcal{D}$ categorías de Galois. Un funtor $K : \mathcal{C} \to \mathcal{D}$ es **fundamental** si la asigación $K^* : Fun(\mathcal{D}, \boldsymbol{FSet}) \to Fun(\mathcal{C}, \boldsymbol{FSet})$ preserva funtores de fibra.*[1]

PROPOSICIÓN 4.52. *Sea $K : \mathcal{C} \to \mathcal{D}$ un funtor entre categorías de Galois. Entonces, $K$ es un funtor fundamental si y sólo si existe $F : \mathcal{D} \to \boldsymbol{FSet}$ un funtor de fibra tal que $F \circ K : \mathcal{C} \to \boldsymbol{FSet}$ es un funtor de fibra.*

DEMOSTRACIÓN. La ida es clara de la definición. El regreso es consecuencia directa del teorema principal. □

Sea **Gal** la 2-categoría cuyas:

1. 0-celdas son las categorías de Galois punteadas con los funtores de fibra.
2. 1-celdas son funtores fundamentales $K : (\mathcal{C}, F) \to (\mathcal{D}, F')$ tales que $F' \circ K = F$.
3. 2-celdas son isomorfismos entre funtores fundamentales.

Por otro lado, defina **Prof** la 2-categoría cuyas:

1. 0-celdas son los grupos profinitos.
2. 1-celdas son los morfismos de grupos profinitos.
3. 2-celdas son elementos $g' \in G'$ tales que $I_{g'} \circ f = g$ para $f, g : G \to G'$ 1-celdas, donde $I_{g'}$ es el automorfismo interno definido por $g'$.

Con lo anterior en mente la siguiente discusión es en torno a la funtorialidad del grupo fundamental sobre una categoría de Galois. La primera observación es que este asigna a una categoría de Galois un grupo profinito. Por otro lado, sea $K : \mathcal{C} \to \mathcal{D}$ un funtor fundamental. Si $F' \in Fun(\mathcal{D}, \mathbf{FSet})$ es un funtor de fibra, entoces $F := F' \circ K \in Fun(\mathcal{C}, \mathbf{FSet})$ es un funtor de fibra. Así, se tiene una asignación $f_K : \pi_1(\mathcal{D}; F') \to \pi_1(\mathcal{C}; F)$ cuya regla de correspondencia es $f_K(\eta) = \eta \circ K$. Esta función resulta ser un morfismo de grupos por la compatibilidad de las composiciones horizontal y vertical en la 2-categoría de categorías ("middle four interchance"). Más aún, $f_K$ es un morfismo de grupos profinitos. Además, del Teorema 4.50 se deduce que los isomorfismos entre grupos fundamentales están definidos de manera única salvo un automorfismo interno, es decir, estos dan lugar a un 2-morfismo en la 2-categoría de grupos profinitos. En resumen se tiene que $\pi_1 : \mathbf{Gal}^{op} \to \mathbf{Prof}$.

[1] En [**SGA1**] a estos funtores se le llama exactos.

Ahora, nótese que dado $G$ un grupo profinito, a este se le puede asociar una categoría de Galois $(G\text{-}\mathbf{FSet}, U)$, donde $U : G\text{-}\mathbf{FSet} \to \mathbf{FSet}$ es el funtor que olvida.

Sea $f : G \to H$ un morfismo de grupos profinitos. Así, dado $X \in H\text{-}\mathbf{FSet}$, puede definirse una acción continua de $G$ en $X$ dada por $g \cdot x := f(g)x$, donde $g \in G$ y $x \in X$. Si ${}_GX$ denota al conjunto $X$ con esta estructura de $G$-conjunto, esto da lugar a un funtor fundamental $K_f : H\text{-}\mathbf{FSet} \to G\text{-}\mathbf{FSet}$ definido por:

$$K_f(X) =_G X.$$

Además, para $\alpha : X \to Y$ morfismo en $H\text{-}\mathbf{FSet}$, $\alpha$ es $G$-equivariante al dotar a $X$ y $Y$ con estuctura de $G$-conjuntos. Así, se define:

$$\begin{gathered} K_f(\alpha) :_G X \to_G Y \\ K_f(\alpha) = \alpha \end{gathered}$$

Nótese que $K_f$ es un funtor de fundamental pues es claro que si $U : H\text{-}\mathbf{FSet} \to \mathbf{FSet}$ es el funtor que olvida, entonces $U \circ K_f : G\text{-}\mathbf{FSet} \to \mathbf{FSet}$ es el funtor que olvida.

Por construcción se tiene el siguiente resultado que puede interpretarse diciendo que las dos construcciones dadas anteriormente son inversas.

PROPOSICIÓN 4.53.

1. *Si $f : G \to H$ un morfismo de grupos profinitos, entonces $f_{K_f} = f$.*
2. *Si $K : (\mathcal{C}, F) \to (\mathcal{D}, F')$ es un funtor fundamental entre categorías de Galois, entonces el siguiente diagrama conmuta:*

$$\begin{tikzcd} \mathcal{C} \arrow[r, "K"] \arrow[d, "\hat{F}"', "\simeq"] & \mathcal{D} \arrow[d, "\simeq"', "\hat{F'}"] \\ G\text{-}\boldsymbol{FSet} \arrow[r, "K_{f_K}"'] & H\text{-}\boldsymbol{FSet} \end{tikzcd}$$

Más aún, nótese que dado $G \in \mathbf{Prof}_0$, a este se le asociar la categoría de Galois $(G\text{-}\mathbf{FSet}, U)$, donde $U : G\text{-}\mathbf{FSet} \to \mathbf{FSet}$ es el funtor que olvida. Además, $\pi_1(G\text{-}\mathbf{FSet}, U) \cong G$, y estos isomorfismos son naturales por construcción.

Por otro lado, a una categoría de Galois $(\mathcal{C}, F)$ se le asocia su grupo fundamental $\pi_1(\mathcal{C}, F)$, que es un grupo profinito. Además, este induce a su vez una categoría de Galois $(\pi_1(\mathcal{C}, F)\text{-}\mathbf{FSet}, U)$. Pero como se vio en el Teorema 4.50, se tiene que $\pi_1(\mathcal{C}, F)\text{-}\mathbf{FSet} \cong \mathcal{C}$.

Además, nótese que por el inciso 2 del Teorema 4.50 se deduce que el grupo fundamental de una categoría de Galois da lugar a un 2-funtor $\pi_1 : \mathbf{Gal}^{op} \to \mathbf{Prof}$. Por lo tanto, la discusión previa muestra que se tiene el siguiente resultado.

TEOREMA 4.54. *$\pi_1 : \boldsymbol{Gal}^{op} \to \boldsymbol{Prof}$ es una equivalencia de 2-categorías.*

Para concluir este capítulo se recuerda que en la teoría de categorías usual (1-categorías), las equivalencias son la noción más común de categorías que pueden considerarse como la misma y por tal razón el que estas existan permite traducir propiedades de una categoría en otra. El último resultado que se busca es en esta dirección. Para lo que resta de la sección $G$ y $H$ son dos grupos profinitos, $f : H \to G$ es un morfismo de grups profinitos, $K := K_f$, $\mathcal{C} = G\text{-}\mathbf{FSet}$ y $\mathcal{D} = H\text{-}\mathbf{FSet}$.

DEFINICIÓN 4.55.
1. *Para $(X, c) \in \mathcal{C}_*$, se escribirá $(X, c)_0 := (X_0, c)$ con $X_0$ componente conexa de $c$ en $X$.*
2. *$X \in \mathcal{C}$ **tiene una sección** si $1 \geq X$.*
3. *$X \in \mathcal{C}$ se **escinde totalmente** si es isomorfo a un coproducto finito de objetos terminales.*

LEMA 4.56.
1. *Para cada subgrupo abierto $U \subseteq G$,*
   - $\mathrm{im}(f) \subseteq U$ *si y sólo si* $(1_{\mathcal{D}}, *) \geq (K(G/U), 1)$ *en* $\mathcal{D}_*$.
   - *Sea* $K_G(\mathrm{im}(f)) \subseteq G$ *es el mínimo subgrupo normal de* $G$ *que contiene a* $\mathrm{im}(f)$. *Entonces* $K_G(\mathrm{im}(f)) \subseteq U$ *si y sólo si* $K(G/U)$ *se escinde totalmente en* $\mathcal{D}$.
2. *Para cualquier subgrupo abierto $V \subseteq H$,*
   a) $\mathrm{nuc}(f) \subseteq V$ *si y sólo si existe un subgrupo* $U \subseteq G$ *tal que* $(K(G/U), 1)_0 \geq (H/V, 1)$ *en* $\mathcal{D}_*$.
   b) *Si $f$ es un epimorfismo, entonces* $\mathrm{nuc}(f) \subseteq V$ *si y sólo si existe* $U \subseteq G$ *un subgrupo abierto tal que* $(K(G/U), 1)_0 \cong (H/V, 1)$ *en* $\mathcal{D}_*$.

DEMOSTRACIÓN. Para la primera afirmación de 1 nótese que $(1_{\mathcal{D}}, *) \geq (K(G/U), 1)$ si y sólo si la única función $g : * \to K(G/U)$ que manda a $*$ en $U$ es un morfismo, es decir, si y sólo si para cada $h \in H$, $U = g(*) = g(h*) = h \cdot g(*) = f(h)U$, lo que es equivalente a que $\mathrm{im}(f) \subseteq U$. Respecto a la segunda afirmación de 1 se observa que

$K_G(\mathrm{im}(f)) \subseteq U$ si y sólo si para cada $g \in G/U$ la función $h_g : * \to K(G/U)$ que manda a $*$ en $gU$ es un morfismo en $\mathcal{D}$. Esto da lugar a un epimorfismo $\coprod_{g\in G/U} * \to K(G/U)$ en $\mathcal{D}$, el cual es también inyectivo por tener dominio y codominio con la misma cardinalidad finita. En el regreso, para un isomorfismo $\coprod_{g\in G/H} * \cong K(G/U)$, considérese $\iota_i : * \to K(G/U)$ el morfismo que se obtiene al hacer composición de este con el $i$-ésimo morfismo canónico del coproducto. Por construcción $\iota_i = h_{\iota_i(*)}$, lo que concluye la prueba.

Para 2, como $V$ es cerrado y de índice finito en $H$, y como $G$ y $H$ son en particular compactos, $f(V)$ es cerrado y de índice finito en $\mathrm{im}(f)$, lo que implica que es abierto. Así, existe un subgrupo abierto $U \subseteq G$ tal que $U \cap \mathrm{im}(f) \subseteq f(V)$. Por definición, la componente conexa de 1 en $K(G/U)$ en $\mathcal{D}$ es: $\mathrm{im}(f)U/U \cong \mathrm{im}(f)/(U \cap \mathrm{im}(f)) \cong H/f^{-1}(U)$. Pero $f^{-1}(U) = f^{-1}(U \cap \mathrm{im}(f)) \subseteq V$, de donde hay un epimorfismo canónico $(\mathrm{im}(f)U/U, 1) \to (H/V, 1)$ en $\mathcal{D}_*$. Más aún, si $\mathrm{im}(f) = G$, entonces al tomar $U = f(V)$, $\phi$ es la inversa del isomorfismo canónico $H/V \to G/U$.

En la otra dirección, supóngase que existe $V \subseteq G$ abierto y un morfismo $\phi : (\mathrm{im}(f)U/U, 1) \to (H/V, 1)$ en $\mathcal{D}_*$. Entonces, para cada $h \in H$ se tiene que $\phi(f(h)U) = h \cdot \phi(1) = hV$. En particular, si $f(h) \in U$, entonces $hU = \phi(f(h)U) = \phi(U) = V$, de donde $\mathrm{nuc}(f) \subseteq f^{-1}(U) \subseteq V$. Nótese que como $\mathrm{nuc}(f)$ es normal en $H$, la condición $\mathrm{nuc}(f) \subseteq V$ no depende eventualmente de la elección de $c \in F(X)$, definiendo el isomorfismo $X \cong H/V$. □

Corolario 4.57.

1. *$f$ es trivial si y sólo si para cada $X \in \mathcal{C}$, $K(X)$ se escinde totalmente en $\mathcal{D}$.*
2. *$f$ es un monomorfismo si y sólo si para cualquier objeto conexo $X \in \mathcal{D}$ existe $Y \in \mathcal{C}$ conexo y una componente conexa $K(Y)_0$ de $K(Y)$ en $\mathcal{C}$ tal que $K(Y)_0 \geq X$ en $\mathcal{D}$.*
3. *Si $f$ es un epimorfismo, entonces $f$ es un isomorfismo si y sólo si $K$ es esencialmente suprayectivo.*

Demostración. Para la primera afirmación, respecto a la ida considérese $X \in \mathcal{C}$. Dado que $K(X)$ se descompone como unión ajena de sus órbitas, que son una cantidad finita, basta ver que cada órbita de escinde totalmente. Más aún, dado que para $x \in K(X)$, $Hx \cong H/H_x$ y $H_x$ es un subgrupo cerrado y con índice finito respecto a $H$ pues $[H : H_x] = |Hx|$, entonces basta ver que los elementos $K(H/U)$ se escinden para $U \subseteq H$ abierto. Sin embargo, como $\mathrm{im}(f) = \{e\}$, las hipótesis de 1 en el lema anterior se cumplen pues $K_G(\mathrm{im}(f)) = \{e\}$, por lo que el resultado se sigue.

Para el regreso, sea $U \subseteq H$ un abierto. Como $K(H/U)$ se escinde por hipótesis, entonces del lema anterior se sigue que $K_G(\mathrm{im}(f)) \subseteq U$, en particular $\mathrm{im}(f) \subseteq U$. Dado que $U \subseteq H$ fue arbitrario, esto implica que $\mathrm{im}(f) \subseteq \bigcap\{U \subseteq H \mid U \text{ es subgrupo abierto}\}$. Pero, como se vio en el Teorema 1.3, dicha intesección es $\{e\}$, de donde $\mathrm{im}(f) = \{e\}$.

Respecto a la ida de 2, la hipótesis implica que $\mathrm{nuc}(f) = \{e\}$. Ahora, sea $X \in \mathcal{D}$ conexo. Luego, $X$ debe ser una órbita en un punto y así, $X \cong H/V$ en $\mathcal{D}$, para $V \subseteq H$ un subgrupo abierto. Como trivialmente $\mathrm{nuc}(f) = \{e\} \subseteq V$, el inciso 2 del lema anterior implica que existe $U \subseteq G$ subgrupo abierto tal que $(K(G/U), 1)_0 \geq (H/V, 1)$ en $\mathcal{D}_*$, de donde se deduce que $K(G/U)_0 \geq H/V$. En la otra dirección sea $U \subseteq H$ un subgrupo abierto. Como $H/U \in \mathcal{D}$ es conexo, la hipótesis implica que existe $Y \in \mathcal{C}$ conexo tal que $K(Y)_0 \geq H/U$, donde $K(Y)_0$ es una componente conexa de $K(Y)$. Pero por 2 del lema anterior, esto implica que $\mathrm{nuc}(f) \subseteq U$. Además, como $U$ fue un subgrupo arbitario, el Teorema 1.3 implica que $\mathrm{nuc}(f) = \{e\}$, por lo que $f$ es un monomorfismo.

En la última afirmación, para la ida basta con probar que tiene suprayectividad esencial respecto a objetos conexos y, como se ha visto antes, estos tienen la forma $H/V$ con $V \subseteq H$ un subgrupo abierto. Así, como $f$ es un isomorfismo, en particular $\mathrm{nuc}(f) = \{e\}$. Así, $\mathrm{nuc}(f) \subseteq V$, por lo que del inciso 2 del lema anterior se deduce que existe $U \subseteq G$ subgrupo abierto tal que $(K(G/U), 1)_0 \cong (H/V, 1)$. De esto se deduce la suprayectividad esencial. Además, respecto al regreso, nótese que la suprayectividad esencial implica que $f$ es un monomorfismo pues para cada abierto $V \subseteq H$, existe $U \subseteq G$ subgrupo abierto tal que $(K(H/V), 1)_0 \cong (G/U, 1)$. En particular $(K(H/V), 1)_0 \geq (G/U, 1)$ y por 2 del lema anterior, $\mathrm{nuc}(f) \subseteq V$, de donde $\mathrm{nuc}(f) = \{e\}$. Así, se tiene que $f : G \to H$ es una función continua y biyectiva, pero al ser $G$ y $H$ profinitos, en particular $G$ es compacto y $H$ Hausdorff, por lo que $f$ es un homeomorfismo también y así, un isomorfismo. $\square$

En el siguiente resultado se muestran algunas propiedades demostradas anteriormente, así como otras nuevas. Este resultado muestra que la equivalencia de 2-categorías dada por $\pi_1 : \mathbf{Gal}^{op} \to \mathbf{Prof}$, permite traducir propiedades entre las 2-categorías en cuestión como en el caso 1-categórico. Aunque el resultado completo es muy interesante, vale la pena prestar atención en el inciso 4 pues al ser la 2-categoría de grupos profinitos una categoría con imagénes y núcleos, tiene sentido hablar de exactitud, concepto que para nada fue tocado en esta tesis. Lo interesante es que en este momento puede caracterizarse la exactitud usando los conceptos de la Definición 4.55, que aunque se ven difíciles de estudiar en la práctica, pueden llevarse a una condición de exactitud que es por lo general muy cómoda de verificar si es cierta o falsa. Estos son el tipo de resultados que en la teoría de 1-categorías hacen sumamente útil el tener una equivalencia de categorías.

Proposición 4.58.

1. *Las siguientes afirmaciones son equivalentes:*
   i) $f$ *es un epimorfismo.*
   ii) $K$ *manda objetos conexos en objetos conexos.*
   iii) $K$ *es fiel y pleno.*
2. $f$ *es un monomorfismo si y sólo si para cada* $X \in \mathcal{D}$ *existe* $Y \in \mathcal{C}$ *y una componente conexa de* $K(Y)$*,* $K(Y)_0$*, tal que* $K(Y)_0 \geq X$ *en* $\mathcal{D}$*.*
3. $f$ *es un isomorfismo si y sólo si* $K$ *es una equivalencia de categorías.*
4. *Sean* $K : \mathcal{C} \to \mathcal{D}$ *y* $K' : \mathcal{D} \to \mathcal{E}$ *funtores fundamentales entre categorías de Galois con morfismos de grupos profinitos inducidos* $f : H \to G$ *y* $g : L \to H$ *respectivamente. Entonces,*
   - $\mathrm{im}(g) \subseteq \mathrm{nuc}(f)$ *si y sólo si* $K'(K(X))$ *se escinde totalmente en* $\mathcal{E}$ *para* $X \in \mathcal{C}$*.*
   - $\mathrm{nuc}(f) \subseteq \mathrm{im}(g)$ *si y sólo si para cualquier objeto conexo* $X \in \mathcal{D}$ *tal que* $K'(X)$ *tiene una sección en* $\mathcal{E}$*, existe* $Y \in \mathcal{C}$ *y una componente conexa de* $K(Y)$*,* $K(Y)_0$*, tal que* $K(Y)_0 \geq X$ *en* $\mathcal{D}$*.*

Demostración. Para 1, en lo que respecta a *i)* $\Rightarrow$ *ii)* supóngase que $f$ es un epimorfismo y sea $X \in \mathcal{C}$ conexo. Así, $H$ actúa transitivamente en $X$. Entonces, dados $x, y \in K(X)$, existe $h \in H$ tal que $hx = y$. Al ser $f$ suprayectiva, existe $g \in G$ tal que $f(g) = h$. Por lo tanto, $g \cdot x = y$ y $G$ actúa transitivamente en $K(X)$, de lo que se deduce que $K(X)$ es conexo.

*ii)* $\Rightarrow$ *i)* Considérese un cociente de la forma $G/N$ con $N \trianglelefteq G$ abierto y normal. Este cociente es finito y además conexo. Luego, al usar la hipótesis $K(G/N)$ es conexo y así, el morfismo canónico $H \xrightarrow{f} G \xrightarrow{\pi_N} G/N$ es continuo y un epimorfismo por la hipótesis. Al denotar por $f_N$ a dicha composición y si $\mathcal{N} = \{N \trianglelefteq G \mid N \text{ es abierto}\}$, entonces es claro que $f = \varprojlim_{N \in \mathcal{N}} f_N$. Luego, $f$ es un epimorfismo en la categoría de grupos profinitos.

*i)* $\Rightarrow$ *iii)* Para $X, Y \in \mathcal{C}$, considérese la función inducida $K : \mathcal{C}(X, Y) \to \mathcal{D}(K(X), K(Y))$. Por definición es claro que $K$ es fiel. Para ver que es pleno, sea $g : K(X) \to K(Y)$. Nótese que $g \in \mathcal{C}(X, Y)$ pues dado $y \in G$, como $f$ es en particular suprayectiva existe $h \in H$ tal que $f(h) = y$. Así, para $x \in X$, $g(yx) = g(h \cdot x) = h \cdot g(x) = yg(x)$. Esto prueba que $g$ es $G$-equivariante y además, es claro que $K(g) = g$.

Para $iii) \Rightarrow i)$ Dado $U \subseteq G$ un subgrupo abierto propio, no existe morfismo $1 \to G/U$ en $\mathcal{C}$. Al ser $K$ fiel y pleno, no existe morfismo de 1 en $K(G/U)$ en $\mathcal{D}$. Pero, por el Lema 4.56 esto es equivalente a que $\mathrm{im}(f) \nsubseteq U$.

En lo que respecta a 2, este es el mismo enunciado que la afirmación 2 del corolario anterior. Para la ida de 3, al ser $f$ en particular un epimorfismo se tiene que $K$ es fiel y pleno, Además, por la afirmación 3 del corolario anterior $K$ es esencialmente suprayectivo y así, es una equivalencia de categorías. Para el regreso de 3, al ser $K$ es particular fiel y pleno, $f$ es un epimorfismo. Luego, por la afirmación 3 del corolario anterior, al ser $K$ esencialmente suprayectivo, $f$ es un isomorfismo.

Para 4, la primera afirmación se deduce del hecho de que $K' \circ K : \mathcal{C} \to \mathcal{E}$ es un funtor fundamental. Así, al aplicar la afirmación 1 del Corolario 4.57, $f \circ g : L \to G$ es trivial, es decir, para cada $x \in L$, $(f \circ g)(x) = e$. Pero esta condición es equivalente a decir que $\mathrm{im}(g) \subseteq \mathrm{nuc}(f)$.

En lo que respecta a la segunda afirmación de 4, para la ida sea $X \in \mathcal{D}$ conexo tal que $1 \geq K'(X)$ en $\mathcal{E}$. Como $X \cong H/U$ en $\mathcal{D}$, para $U \subseteq H$ un subgrupo abierto, entonces por la afirmación 1 del Lema 4.56 se tiene que $\mathrm{nuc}(f) \subseteq U$, por lo que de la hipótesis se deduce que $\mathrm{im}(g) \subseteq U$. Así, al aplicar la afirmación 2 del Lema 4.56, se deduce que existe $V \subseteq G$ un subgrupo abierto tal que $(K(G/V), 1)_0 \geq (H/U, 1)$, lo que prueba la afirmación.

Para el regreso, nótese que

$$\mathrm{im}(g) = \bigcap \{U \subseteq H \mid \mathrm{im}(g) \subseteq U \text{ y } U \text{ es un subgrupo abierto de } H\}.$$

Así, sea $U$ uno de tales intersectandos. Así, como $\mathrm{im}(g) \subseteq U$, por la primera afirmación del Lema 4.56 se tiene que $(1, *) \geq (K'(H/U), *)$ en $\mathcal{E}$. Como $H/U$ es conexo, la hipótesis implica que existe $Y \in \mathcal{C}$ tal que $K(Y)_0 \geq H/U$, donde $K(Y)_0$ es una componente conexa de $K(Y)$. Pero por la segunda afirmación del Lema 4.56 esto implica que $\mathrm{nuc}(f) \subseteq U$. Luego, el resultado se sigue de que este argumento no dependió del intersectando que se tomó y así, $\mathrm{nuc}(f) \subseteq \mathrm{im}(g)$. $\square$

# Bibliografía


[AT] Arhangel'skii A., Tkachenko M., *Topological Groups and Related Structures*, Atlantis Press/World Scientific, Amsterdam-Paris, 2008.

[A] Artin E., *Galois Theory*, University of Notre Dame Press, 1971.

[AM] Atiyah, M. F., Macdonald, I. G., *Introduction to Commutative Algebra*, Adisson-Wesley Publishing Company, 1906.

[BG] Berenstein C. A., Gay R., *Complex Variables An Introduction*, Springer Verlag New York Inc, 2001.

[B] Borceux F., *Handbook of Categorical Algebra 1: Basic Category Theory*, Cambridge University Press, Cambridge, 1994.

[BJ] Borceux F., Janelidze G., *Galois Theories*, Cambridge University Press, Cambridge, 2001.

[E] Eisenbud D., *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 2011.

[EGA1] Grothendieck A., *Élements de géométrie algébraique I: Le langage des schémas*, Publications mathématiques de l'I.H.E.S., tome 4, 1960.

[G71] Grothendieck A., *Revêtements étales et groupe fundamental*, Springer-Verlag Berlin-New York, 1971.

[G95] Grothendieck A., *La Longe Marche a travers la theorie de Galois (1980-1981)*, editado por Jean Malgoire, Universidad de Montpellier II, 1995.

[GAGA] Serre J-P. *Géométrie Algébrique et Géométrie Analytique*, Annales de l'Institut Fourier, 1955-1956.

[Ha] Hartshorne R., *Algebraic Geometry*, Springer-Verlag New York and Heildenberg, 1977.

[H] Hatcher A., *Algebraic Topology*, Cambridge University Press, 2002.

[K] Krull W., *Galoissche Theorie der unendlichen algebraischen Erweiterungen*, Math. Ann. 1928, pp 687-698.

[L] Lenstra H. W., *Galois theory for schemes*, Notas de clases disponibles en https://websites.math.leidenuniv.nl/algebra/GSchemes.pdf

[MM] Mac Lane S., Moerdijk I., *Sheaves in Geometry and Logic: A first introduction to topos theory*, Springer Universitext, 1992.

[Ma] Magid A. R., *The Separable Galois Theory of Commutative Rings*, CCR Press, 2014.

[Mat] Matsumura H., *Commutative Ring Theory*, Cambridge University Press, 1986.

[Mi] Milne J. S., *Étale cohomology*, Princenton University Press, Princenton, 1980.

[M] Mumford D., *The Red Book of Varieties and Schemes*, Springer-Verlag Berlin Heidelberg, 1999.

[N] Neeman A. *Algebraic and analytic geometry*, Cambridge University Press, 2007.

[Neu] Neukirch J., *Algebraic Number Theory*, Springer-Verlag Berlin, 1999.

[P] Pontrjagin L., *Topological Groups*, Princeton University Press, Princeton, 1946.

[RZ] Ribes L., Zalesskii P., *Profinite Groups*, Springer-Verlag Berlin Heidelberg, 2000.

[Ri] Riehl E., *Category Theory in Context*, Dover Publications Inc, Mineola, New York, 2016.
[R] Rotmann J., *An Introduction to Algebraic Topology*, Springer-Verlag New York, 1988.
[Se58] Serre J-P., *Espaces Fibrés algébiques*, Exposé 1, Séminaire Chevalley, 1958.
[Se73] Serre J-P., *A course in Arithmetic*, Springer-Verlag Berlin Heidelberg, 1973.
[Se97] Serre J-P., *Galois Cohomology*, Springer-Verlag Berlin Heidelberg, 1997.
[SGA1] Grothendieck A., *SGA1 (1960-1961)*, Springer Lecture Notes 224, 1971.
[Sh] Shatz S.S., *Profinite Groups, Arithmetic and Geometry*, Annals of Mathematics Studies, No. 67, Princeton University Press, 1972.
[Sw] Switzer R. M., *Algebraic Topology: Homology and Homotopy*, Springer-Verlag (Classics in mathematics), 2002.
[S] Szamuely T., *Galois Groups and Fundamental Groups*, Cambridge University Press, 2009.
[tD] tom Dieck, Tammo, *Algebraic Topology*, European Mathematical Society, 2008.
[W] Weibel C. A., *An introduction to homological algebra*, Cambridge University Press, 1997.

Apéndice A

# Teoría de Galois

Proposición A.1. *Sea $K|\,k$ una extensión de Galois y $L \in \mathcal{E}_{K|\,k}$ con $[L:k] < \aleph_0$. Entonces, todo automorfismo de campos de $L$ que fija a $k$ se extiende a un automorfismo de $K$ que fija a $k$.*

Demostración. Ver Proposición 3.1.2 del Capítulo 4 en [**BJ**, pp 37]. □

Proposición A.2. *Sea $L|\,k$ una extensión finita. Entonces*

$$|\operatorname{Hom}_k(L, \overline{k})| \leq [L:k]$$

*Además, la desigualdad anterior es igualdad si y sólo si la extensión $L|\,k$ es separable.*

Demostración. Ver el Lema 1.1.6 del Capítulo 1 en [**S**, pp 2–3]. □

Proposición A.3. *(Teorema del elemento primitivo) Sea $K|\,k$ una extensión de campos finita y separable. Entonces, existe $a \in K$ tal que $K = k(a)$*

Teorema A.4. *(TFTG para extensiones finitas) Sea $K|\,k$ una extensión de Galois finita. Denótese por $\mathcal{E}_{K|\,k}$ al conjunto de extensiones intermedias entre $k$ y $K$, así como $\mathcal{S}(\operatorname{Gal}(K|\,k))$ al conjunto de subgrupos del grupo de Galois $\operatorname{Gal}(K|\,k)$. Así, las funciones*

$$\begin{gathered}\operatorname{Aut}(K|_{-}\,) : \mathcal{E}_{K|\,k} \to \mathcal{S}(\operatorname{Gal}(K|\,k)) \\ L \mapsto \operatorname{Aut}(K|L)\end{gathered}$$

$$\begin{gathered}K^{-} : \mathcal{S}(\operatorname{Gal}(K|\,k)) \to \mathcal{E}_{K|\,k} \\ H \mapsto K^H := \{a \in K \mid \forall \sigma \in H(\sigma(a) = a)\}\end{gathered}$$

*Son inversas una de la otra y establecen una correspondencia biyectiva que invierte el orden entre* $\mathcal{E}_{K|\,k}$ *y* $\mathcal{S}(\mathrm{Gal}(K|\,k))$. *Además, dado* $L \in \mathcal{E}_{K|\,k}$, *la extensión* $K|L$ *es de Galois si y sólo si* $\mathrm{Aut}(K|L) \trianglelefteq \mathrm{Gal}(K|\,k)$. *En tal caso* $\mathrm{Gal}(L|\,k) \cong \mathrm{Gal}(K|\,k)/\,\mathrm{Gal}(K|L)$.

Apéndice B

# Álgebra Conmutativa

LEMA B.1. *(Rabinowitsch) Si $f \in A$ y $A_f$ es el anillo de fracciones de $A$ respecto al conjunto multiplicativo $S = \{f^n \mid n \in \mathbb{N}\}$, entonces existe un isomorfismo entre $A[t]/\langle ft - 1\rangle \cong A_f$*

PROPOSICIÓN B.2. *(Lema de Nakayama) Sea $M$ un $A$-módulo finitamente generado e $I \subseteq A$ un ideal tal que $I \subseteq J(A)$, con $J(A)$ el radical de Jacobson de $A$. Si $IM = M$, entonces $M = 0$.*

DEMOSTRACIÓN. Ver [**A**, pp 21–22]. $\square$

PROPOSICIÓN B.3. *(Teorema chino del residuo) Sean $k$ un campo y $\{f_i : A \to B_i\}_{i\in\{1,\ldots,n\}}$ una familia de morfismos de $k$-álgebras conmutativas suprayectivos tales que sus núcleos son primos relativos dos a dos. Entonces, el morfismo inducido $f = (f_1, \ldots, f_n) : A \to \prod_{i=1}^n B_i$ es suprayectivo. Más aún, este establece un isomorfismo de $k$-álgebras entre $A/\bigcap_{i=1}^n \mathrm{nuc}(f_i) = A/\prod_{i=1}^n \mathrm{nuc}(f_i) \cong \prod_{i=1}^n B_i$.*

DEMOSTRACIÓN. Ver la Proposición 2.1.12 de [**BJ**, pp 19]. $\square$

Apéndice C

# Geometría Algebraica

Definición C.1. *Un **esquema** es una pareja $(X, \mathcal{O}_X)$ que consta de un espacio topológico $X$ y una gavilla de anillos conmutativos unitarios sobre $X$, $\mathcal{O}_X$, tales que:*

- *Para cada $x \in X$, el tallo de $\mathcal{O}_X$ en $x$, $\mathcal{O}_{X,x}$, es un anillo local.*
- *Existe una cubierta abierta afín de $X$, $\{U_i\}_{i \in I}$, tal que $(U_i, \mathcal{O}_X|_{U_i})$ es un esquema afín.*

Definición C.2. *Un **morfismo de esquemas** $f : X \to Y$ consta de una función continua $f : X \to Y$ y una transformación natural $f^\sharp : \mathcal{O}_Y \to f_*\mathcal{O}_X$, tales que para cada $x \in X$, la función inducida en los tallos $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$, es un morfismo de anillos locales.*

Teorema C.3. *Existe un isomorfismo entre las categorías de anillos conmutativos unitarios **CR1ng** y la categoría opuesta de esquemas afines $\boldsymbol{AfSm}^{op}$. Este isomorfismo está dado por los funtores espectro de Zariski,* Spec : $\boldsymbol{CR1ng} \to \boldsymbol{AfSm}^{op}$, *y secciones globales* $\Gamma : \boldsymbol{AfSm}^{op} \to \boldsymbol{CR1ng}$.

Demostración. Ver Corolario 1 en [**M**, pp 113]. $\square$

Definición C.4. *Un morfismo de esquemas $\phi : Y \to X$ es **separado** si el morfismo diagonal inducido por $\phi$, $\Delta_\phi : Y \to Y \times_X Y$, es un encaje cerrado.*

Proposición C.5. *Sean $\phi : Y \to X$ y $\psi : Z \to Y$ morfismos de esquemas tales que $\phi \circ \psi : Z \to X$ es finito y $\phi$ es separado, entonces $\psi$ es finito.*

Demostración. Ver el Lema 5.3.2 de [**S**, pp 159]. $\square$

Definición C.6. *Un esquema $X$ es **entero** si para todo abierto $U \subseteq X$, el anillo $\mathcal{O}_X(U)$ es un dominio entero.*

Proposición C.7. *Sea $\phi : Y \to X$ un morfismo entre esquemas enteros suprayectivo con $Y$ noetheriano, normal y con dimensión 1. Entonces $\phi$ es localmente libre.*

Demostración. Ver Lema 5.2.4 en [**S**, pp 153]. $\square$

Proposición C.8. *(Lema de Nakayama) Sea $X$ un esquema neteriano y $\mathcal{F}$ una gavilla de $\mathcal{O}_X$-módulos coherente tal que $\mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} k(x) = 0$ para algún $x \in X$. Entonces, existe $U \subseteq X$ una vecindad abierta de $x$ tal que $\mathcal{F}|_U = 0$.*

Demostración. Ver [**M**, pp 212–213]. $\square$