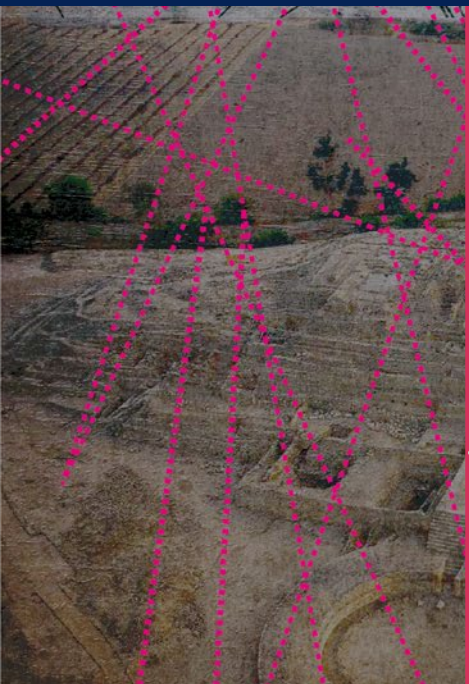
Capítulo 1



Editores

VIII Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2015

CIMPA RESEARCH SCHOOL

BIBLIOTECA NACIONAL DEL PERÚ
Centro Bibliográfico Nacional

512.0072 E

VIII Escuela doctoral intercontinental de matemáticas PUCP-UVA 2015: CIMPA research school / Francisco Ugarte Guerra, Nuria Corral Pérez, editores.-- 1a ed.-- Lima: Pontificia Universidad Católica del Perú, Fondo Editorial, 2016 (Lima: Tarea Asociación Gráfica Educativa).

244 p.; il., retrs.; 21 cm.

Incluye bibliografías.

D.L. 2016-12927
ISBN 978-612-317-203-9

1. Algebra - Estudio y enseñanza 2. Teoría de los números 3. Teoría de Galois 4. Teoría de los grupos 5. Ecuaciones diferenciales I. Ugarte Guerra, Francisco, 1972-, editor II. Corral Pérez, Nuria, editora III. Pontificia Universidad Católica del Perú

BNP: 2016-1193

VIII Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2015
Francisco Ugarte Guerra y Nuria Corral Pérez, editores

Av. Universitaria 1801, Lima 32, Perú
feditor@pucp.edu.pe
www.fondoeditorial.pucp.edu.pe

Corrección de estilo y cuidado de la edición: Fondo Editorial PUCP
Diseño de cubierta: Francisco Ugarte

Primera edición: octubre de 2016
Tiraje: 500 ejemplares

Hecho el Depósito Legal en la Biblioteca Nacional del Perú Nº 2016-12927
ISBN: 978-612-317-203-9
Registro del Proyecto Editorial: 31501361601055

Impreso en Tarea Asociación Gráfica Educativa
Pasaje María Auxiliadora 156, Lima 5, Perú

Il s'agit de symétries, mais en un sens assez subtil,
qu'il faut radicalement distinguer du sens naïf.
J. P. Ramis

1. Introducción. La Teoría de la Ambigüedad

En una Conferencia en Valladolid en mayo de 2011, J.P. Ramis [31] citaba una frase de A. Connes:

> *La théorie de Galois est devenue tellement classique en mathématiques que les textes qui la présentent sont pour la plupart d'une facilité apparente qui est déconcertante et terriblement trompeuse car en trivialisant les énoncés, elle enmasque souvent la portée métamathématique. Il n'est donc sans doute pas inutile même pour le mathématicien professionnel de relire ces textes avec la fraîcheur nécessaire, i.e. en essayant de réfléchir directement aux énoncés sans utiliser l'artillerie lourde.*

Ese es precisamente nuestro objetivo en este curso, intentaremos presentar una parte de las numerosas aproximaciones a la Teoría de Galois limitando el uso de la *artillería pesada* y tratando de ir a las ideas más que al formalismo subyacente.

Como se ha repetido muchas veces, el nombre usado por Galois al final de su vida para referirse a lo que hoy se conoce por *Teoría de Galois* es el de *Teoría de la Ambigüedad*. En apoyo de esta afirmación se citan siempre los párrafos finales de su carta-testamento del 29 de mayo de 1832.

En ella Galois escribe:

> *Tu sais, mon cher Auguste, que ces sujets ne sont pas les seuls que j'aie explorés. Mes principales méditations depuis quelque temps étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté. Il s'agissait de voir a priori dans une relation entre des quantités ou fonctions transcendantes quels échanges on pouvait faire, quelles quantités on pouvait substituer aux quantités données sans que la relation pût cesser d'avoir lieu. Cela fait reconnaître tout de suite l'impossibilité de beaucoup d'expressions que l'on pourrait chercher.*

En su discurso de ingreso en la Academia de Ciencias de Francia J.P. Ramis (ver [30]) cita a Birkhoff (ver [2]) que remonta la idea galoisiana de ambigüedad al *Principio de la razón suficiente* de Leibniz; Birkhoff enuncia su principio identificando la ambigüedad con la acción de un grupo:

> **Principle of sufficient reason** *If there appears in any theory T a set of ambiguously determined (i e. symmetrically entering) variables, then these variables can themselves be determined only to the extent allowed by the corresponding group G. Consequently any problem concerning these variables which has a uniquely determined solution, must itself be formulated so as to be unchanged by the operations of the group G (i e . must involve the variables symmetrically).*
>
> **Heuristic Conjecture** *The final form of any scientific theory T is:*
>
> 1. *Based on a few simple postulates*
> 2. *Contains an extensive ambiguity, associated symmetry, and an underlying group G*
>
> *In such wise that, if the language and laws of the theory of groups be taken for granted, the whole theory T appears as nearly self-evident in virtue of the above Principle.*

Birkhoff presenta un ejemplo de su teoría: tomamos un cuadrado de papel y rotulamos sus esquinas con las letras A, B, C, D, desde la parte superior y de izquierda a derecha, con el cuadrado frente a nosotros hay cuatro posiciones posibles que corresponden a los cuatro giros de múltiplos enteros de 90 grados. Si quitamos los rótulos aparece la ambigüedad. Para Birkhoff ambigüedad y simetría son la misma cosa, entiende la ambigüedad de forma absoluta, hay ambigüedad o no la hay, y si la hay está reflejada en un grupo de simetría.

Para Ramis (ver [31]) la ambigüedad tiene unas diferencias sutiles con la simetría, tanto en su naturaleza, ya que es relativa, como en su formulación, pues no se refleja en un grupo sino en un torsor. Veamos con más detalles ambos tipos de diferencias.

Ramis retoma el ejemplo de Birkhoff: consideramos un cuadrado blanco de papel con las cuatro esquinas coloreadas alternativamente de rojo y de verde, colocamos el papel delante de nosotros y cerramos los ojos, al volver a abrirlos y ver el papel exactamente igual no podemos saber si no lo ha tocado nadie o si alguien lo ha girado 180 grados. Si fuésemos daltónicos la ambigüedad sería mayor pues tampoco detectaríamos los giros de 90 y 270 grados. Es decir, la ambigüedad es en parte inherente a la teoría y en parte a la información o a la capacidad de observar del observador.

De modo más general supongamos que dos jugadores A y B se enfrentan ante un tablero, el jugador A manipula el tablero y el B debe adivinar lo que ha hecho A. Si el conocimiento de B es imperfecto, puede haber jugadas indetectables o varias jugadas que, en lo que B puede observar, dan el mismo resultado. Si por alguna razón la capacidad de observación de B cambia, la ambigüedad lo hace también.

En la Teoría de Galois de ecuaciones algebraicas si el tablero está formado por las raíces de un polinomio irreducible con coeficientes racionales y las únicas operaciones que puede hacer B con ellas son las de adición, multiplicación, resta y división, B no puede detectar la elección de una de las raíces hecha por A, ya que lo único que sabe de ella es su polinomio mínimo. En cambio sí puede detectar una permutación si las raíces de la ecuación verifican relaciones algebraicas con coeficientes racionales. El grupo formado por las permutaciones indetectables por B, es exactamente el grupo de Galois de la ecuación. Si el conocimiento de B mejora porque puede usar algunos numeros algebraicos adecuados, es decir, ampliar el cuerpo base, el grupo de ambigüedad disminuye y esta es la correspondencia de Galois.

Planteando la situación de modo ligeramente diferente, si tenemos una extensión algebraica L de un cuerpo K y dos jugadores A que vive en L y B que vive en K, si B no puede operar sino con los elementos de K, cuando A le muestra un elemento de L lo único que puede averiguar de él es su polinomio característico y dos elementos con el mismo polinomio característico son indistinguibles. Si ampliamos el conocimiento de B, es decir, lo situamos en un cuerpo entre K y L, mejora su capacidad de distinguir los elementos que le muestra A al poder encontrar nuevas relaciones algebraicas entre ellos.

Ejemplo 1.1.– Consideramos la ecuación $x^4 - 10x^2 + 1 = 0$ con coeficientes en $\mathbb{Q}$, sus raíces son:

$$\xi_1 = \sqrt{2} + \sqrt{3},\ \xi_2 = \sqrt{2} - \sqrt{3},\ \xi_3 = -\sqrt{2} + \sqrt{3},\ \xi_4 = -\sqrt{2} - \sqrt{3}$$

y están ligadas por las relaciones:

$$\begin{aligned} \xi_1 + \xi_4 &= 0 \\ \xi_2 + \xi_3 &= 0 \\ (\xi_1 + \xi_2)^2 &= 8 \\ (\xi_1 + \xi_3)^2 &= 12 \end{aligned}$$

El grupo de Galois está formado por las permutaciones:

$$G = \{(1), (1,4)(2,3), (1,2)(3,4), (1,3)(2,4)\}.$$

En unas notas no publicadas citadas por Viaud [37] P. Cartier propone el siguiente esquema para la Teoría de Galois. Dado un polinomio irreducible separable:

$$P(x) = x^n + a_1 x^{n-1} + ... + a_n \in K[x],$$

si L es su cuerpo de descomposición y $\{r_1, ..., r_n\}$ son sus raíces, podemos considerar el conjunto de $n!$ puntos de L^n:

$$R(P(x)) = \{(r_{\sigma(1)}, ..., r_{\sigma(n)}) \mid \sigma \in S_n\}.$$

Si dotamos a L de la K- topología de Zariski este conjunto es cerrado, porque es el conjunto de ceros de la familia de polinomios con coeficientes en K (Relaciones de Cardano):

$$\{s_j(x_1, ..., x_n) = (-1)^j a_j\}_{i \leq j \leq n}$$

donde las s_j son las funciones simétricas elementales.

En la ecuación general este cerrado es irreducible, pero para ecuaciones particulares puede haber entre los grupos de raíces relaciones algebraicas con coeficientes en K eso se traduce en que el cerrado $R(P)$ es reducible y se descompone en unión de componentes irreducibles:

$$R(P) = R_1 \cup .... \cup R_t.$$

Estas componentes tienen el mismo estabilizador que es exactamente el grupo de Galois de la ecuación.

Ejemplo 1.2.– Consideramos la ecuación $x^3 - 2 = 0$ con coeficientes en $\mathbb{Q}$. Si w es una raíz primitiva cúbica de 1, $w^2 + w + 1 = 0$. Las soluciones de la ecuación son

$$\{\sqrt[3]{2},\ w\sqrt[3]{2},\ w^2\sqrt[3]{2}\}$$

y el cuerpo de descomposición de la ecuación es $L = \mathbb{Q}(w, \sqrt[3]{2})$. El conjunto $R(x^3 - 2)$ está definido en L^3 por las ecuaciones:

$$(E) : \left\{ \begin{array}{rcl} X+Y+Z & = & 0 \\ XY+XZ+YZ & = & 0 \\ XYZ & = & 2 \end{array} \right.$$

y este cerrado es irreducible, entonces el grupo de Galois sobre $\mathbb{Q}$ de la ecuación es S_3, pero si ahora ampliamos el cuerpo base a $K = \mathbb{Q}(w)$, $R(x^3-2)$ se descompone en unión de dos cerrados irreducibles:

$$R(x^3 - 2) = C_1 \cup C_2$$

$$C_1 = \{(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}), (w\sqrt[3]{2}, w^2\sqrt[3]{2}, \sqrt[3]{2}), (w^2\sqrt[3]{2}, \sqrt[3]{2}, w\sqrt[3]{2})\}$$

$$C_2 = \{(\sqrt[3]{2}, w^2\sqrt[3]{2}, w\sqrt[3]{2}), (w\sqrt[3]{2}, \sqrt[3]{2}, w^2\sqrt[3]{2}), (w^2\sqrt[3]{2}, w\sqrt[3]{2}, \sqrt[3]{2})\}$$

obtenidos añadiendo a las ecuaciones del sistema (E), la ecuación $Y = wX$ para el primer cerrado y la $Y = w^2X$ para el segundo.

El estabilizador de ambas componentes irreducibles es A_3 que es ahora el grupo de Galois de la ecuación sobre K.

En la segunda situación del ejemplo se precisa el significado de la ambigüedad, las raíces de la ecuación son igualmente indistinguibles sobre $\mathbb{Q}$ y sobre K, pero en el segundo caso hay relaciones internas entre ellas que no aparecen en el primero y el grupo de Galois detecta la aparición de estas relaciones.

Este es exactamente el planteamiento de Galois:

> *Soit une équation donnée, dont a, b, c, ..., sont les m racines. Il y aura toujours un groupe de permutations des lettres a, b, c, ..., qui jouira de la propriété suivante:*
>
> 1. *que toute fonction des racines invariante par les substitutions de ce groupe, soit rationnellement connue.*
> 2. *réciproquement, que toute function des racines, determinée ratinnellement, soit invariante par ces substitutions.*

Aquí aparece la segunda diferencia, aunque Galois usa la palabra grupo, no se refiere a este objeto algebraico definido por Cayley más de cincuenta años después; considera las substituciones, es decir, el conjunto de todas las permutaciones de las raíces con la acción simple y transitiva del grupo de permutaciones, como hemos visto más arriba, y esto es lo que se conoce hoy por un *espacio*

principal homogéneo o *torsor*. En este punto radica la diferencia entre el tratamiento tradicional de la teoría formalizado después de la muerte de Galois y el planteamiento de Grothendieck, inspirado también en la obra de Riemann, Poincaré y Schwarz.

Veremos que en el punto de vista de Grothendieck no solo se vuelve a la obra de Galois con una interpretación más fiel, sino que se trata de explicar las razones de la ambigüedad. En la versión topológica de la Teoría de Galois, las relaciones invisibles entre las raíces de las ecuaciones algebraicas, son perfectamente visibles, se puede llevar un punto de la fibra a otro punto de la fibra si están conectados por un camino, y este tipo de conexión es el que es capaz de poner de manifiesto Grothendieck con el funtor de puntos del que hablaremos posteriormente.

La ambigüedad galoisiana se presenta en muy distintos contextos y el artículo de Y. Andre [1] contiene gran número de ellos.

2. Introducción a la teoría axiomática de conjuntos. Universos

En diversos puntos de esta exposición, la construcción del cierre algebraico o el pequeño viaje por la Teoría de Categorías por ejemplo, no hacemos referencia a las Clases (en sentido conjuntista) y usamos sistemáticamente el axioma de elección y el lema de Zorn. Ello se debe a que nos situamos en el contexto de los Universos de Grothendieck. Para entender este contexto haremos una breve exposición de la teoría axiomática de conjuntos.

En el comienzo de casi cualquier texto de cualquier rama de las matemáticas se cita la palabra *conjunto* o uno de sus sinónimos (el diccionario ideológico de Casares cita 76), pero el contenido de esa palabra está muy lejos de ser trivial, y su uso motivó, el siglo pasado, una crisis de fundamentos con enormes consecuencias tanto en la investigación como en la enseñanza de las matemáticas.

Se puede argüir que la palabra y por tanto su contenido están descritos en el lenguaje común y no hace falta formalizarlos. Siguiendo esta idea y teniendo en cuenta que hablamos un idioma, el español, y la palabra *conjunto* es una palabra de nuestro idioma, podemos ir al diccionario de la R.A.E. y buscar su significado; encontramos que tiene cuatro acepciones y la cuarta es la que más

se adapta a lo que nos interesa: *un conjunto es un agregado de varias cosas*. La palabra *conjunto* se reduce entonces a la palabra *agregado*. El diccionario nos dice de nuevo que, en su segunda acepción, un *agregado es un conjunto de cosas homogéneas*. Parece pues que el diccionario no resuelve nuestro problema, y que, aunque todos tengamos muy claro por nuestra experiencia previa lo que es un conjunto, el diccionario no es capaz de definirlo.

Si vamos al terreno profesional, los conjuntos comienzan a considerarse un objeto de estudio, por sí mismos, de las matemáticas a finales del siglo XIX, aunque ya desde hace más de 2500 años se definía una recta o una circunferencia como un conjunto de puntos que cumplen una cierta propiedad, y desde entonces la finalidad de la matemática ha sido el estudio de conjuntos, definidos de una u otra forma y con más o menos estructura suplementaria.

Los primeros trabajos sobre Teoría de conjuntos se deben a Georg Cantor (1845 - 1918), se publicaron entre los años 1879 y 1884 y están centrados en explicar la diversidad de infinitos. Como es habitual el trabajo absolutamente innovador de Cantor recibió numerosas críticas, no precisamente agradables:

- *Las ideas de Cantor son una enfermedad grave que infecta las matemáticas* (Poincaré).
- *Charlatán. Corruptor de la juventud* (Kronecker).

Cantor no pudo sobreponerse a la mala acogida de sus ideas y murió en un sanatorio mental. Y aún después de su muerte continuaron algunas críticas:

- *Sus ideas son un sinsentido. Es una teoría risible* (Wittgestein).

Al final sus ideas se impusieron, como bien sabemos, y Hilbert llegó a afirmar:

- *Nadie nos expulsará del paraíso creado por Cantor*.

La definición de conjunto de Cantor no se aleja mucho de la del diccionario:

Entendemos por conjunto la agrupación en un todo de objetos de nuestra intuición o nuestro pensamiento.

Analizando con cuidado la definición encontramos que para Cantor:

- Todo conjunto tiene *elementos*, los objetos que lo forman.
- Un conjunto queda determinado por sus elementos.
- Los elementos de un conjunto son objetos que están en algún sitio real o concebible (Universo).

Para describir un conjunto basta enumerar sus elementos, pero esto a veces no es posible, y alternativamente podemos establecer una condición verificada por los elementos del conjunto y solo por ellos. El problema es definir qué entendemos por condición y para Cantor una *condición bien definida* es una afirmación referida a objetos del Universo tal que para cada objeto podamos afirmar sin ambigüedad si la afirmación es cierta o falsa. Entonces el Principio general de Comprensión establece que:

Principio.- *Para toda condición bien definida P, existe un conjunto cuyos miembros son exactamente los objetos que verifican la condición*.

Este principio es la base de la teoría de conjuntos ya que todas las operaciones con conjuntos se basan en él. Y precisamente en este principio está el problema que causó la crisis de fundamentos de principios del siglo XX en las matemáticas.

Paradoja de Bertrand Russel.- *El Principio general de Comprensión no es válido.*

Si admitimos la validez del principio, y admitimos que nuestra definición de conjuntos es adecuada, la propiedad:

- $P(X) \equiv X$ es un conjunto

es una condición bien definida, por tanto el *conjunto de todos los conjuntos*:

$$\mathcal{C} = \{X \ \mid \ X \text{ es un conjunto}\}$$

es efectivamente un conjunto y por tanto verifica que:

$$\mathcal{C} \in \mathcal{C}.$$

Se pueden poner fácilmente ejemplos de conjuntos que no verifican esta propiedad, y de nuevo el Principio general de Comprensión establece que:

$$\mathcal{B} = \{X \ \mid \ X \in \mathcal{C},\ X \notin X\}$$

es un conjunto, pero este hecho nos lleva a un absurdo, ya que:

$$\mathcal{B} \in \mathcal{B} \ \Leftrightarrow \ \mathcal{B} \notin \mathcal{B}$$

La razón del problema está en que definir algo es referir una palabra a otras, la aplicación repetida de este proceso nos lleva más o menos pronto a un círculo vicioso. La forma de romper este círculo consiste en referir todas las palabras a palabras primitivas cuyo significado es indudable; esto se hace en el lenguaje de modo implícito, pero, como hemos visto, puede dar lugar a contradicciones.

Al tratar de definir *conjunto* hemos caído en una trampa del lenguaje. Podemos salir de ella diciendo que los conjuntos que no son miembros de sí mismos no forman un conjunto, pero eso choca con el significado aceptado de la palabra conjunto. Entonces debemos vaciar de contenido previo esta palabra y describir de modo inequívoco el contenido matemático que le asignaremos de aquí en adelante. Eso podemos hacerlo mediante lo que se llama una *axiomática*. Lo que hace una axiomática es fijar claramente las propiedades de objetos, que no se definen sino por cumplir estas propiedades, es decir, es una selección de palabras primitivas, a las que se asocia inequívocamente un contenido.

La primera axiomática de la teoría de conjuntos se debe a Ernest Zermelo (1871 - 1953) y está publicada en 1908. La axiomática de Zermelo fue completada en 1922 por Abraham (Adolf) Fraenkel (1891- 1965), se conoce como la teoría Z-F, en ella las nociones de Conjunto y Pertenencia, son nociones primitivas y toda la teoría se refiere a estas nociones. Esta es la axiomática que expondremos a continuación.

Nos situamos en la base de las matemáticas y debemos comenzar de cero explicando que es lo que se llama un *sistema formal*. Un sistema formal está compuesto por:

1. Una colección de símbolos, llamada *alfabeto*.
2. Una colección de familias de símbolos, cada una de las cuales se llama una *fórmula*.
3. Una colección de fórmulas llamadas *axiomas*.
4. Un conjunto de *reglas de deducción*, que son fórmulas que constan de una entrada, que es una sucesión finita de fórmulas, y una salida, que es una fórmula única.

En un sistema formal debe haber un modo mecánico de decidir si un conjunto de símbolos dado es o no una fórmula, y si una fórmula dada es o no un axioma; ese modo puede ser simplemente la enumeración, si las fórmulas o los axiomas son un conjunto finito. Del mismo modo también debe haber un método que permita constatar si la aplicación de las reglas se hace correctamente.

Una *demostración* no es entonces más que una sucesión de fórmulas que comienza por un axioma y es tal que todas las fórmulas de la sucesión son axiomas, o se obtienen de fórmulas anteriores de la sucesión por la aplicación de las reglas de deducción. Un *teorema* es la última fórmula de una demostración.

Hay un ejemplo interesante de sistema formal descrito por D. Hofstadter ([20]) en su libro *Gödel, Escher, Bach:Un eterno y grácil bucle*, el sistema formal llamado MU:

El alfabeto de MU está compuesto por las letras $\{$ M, U, I$\}$, las fórmulas son todas las sucesiones no vacías compuestas por los tres símbolos repetidos cuantas veces se desee. Hay un único axioma MI, y las reglas de deducción son:

1. A cualquier sucesión de símbolos que termine en I se le puede añadir una U al final.

2. En toda fórmula que empiece con M, se puede duplicar la sucesión de símbolos situados después de la M.

3. Si en una fórmula aparecen tres I seguidas, se pueden reemplazar por una U.

4. Dos U consecutivas se pueden borrar.

Veamos ejemplos de demostraciones:

1. MI, MIU, MIUIU

2. MI, MII, MIIII, MIU

3. MI, MII, MIIII, MUI, MUIU, MUIUUIU, MUIIU

Se aprecia que todas ellas comienzan por el único axioma, en la primera se aplica la regla 1 y luego se aplica la 2, en la segunda y tercera se aplica dos veces la regla 2 y hay dos posibilidades de aplicar la 3, con las tres primeras I o con las tres ultimas, una vez aplicada esta regla, en la segunda nos paramos y en la tercera aplicamos de nuevo las reglas 1, 2 y 4.

Como se aprecia claramente si implementamos el sistema en un ordenador éste puede demostrar cada teorema en un tiempo finito, y puede proceder de modo sistemático aplicando sucesivamente en cada etapa todas las reglas posibles. Pero en vez de probar sistemáticamente teoremas, podemos plantearnos la pregunta de si MU puede ser un teorema en este sistema; la respuesta es negativa, pero este resultado no es un teorema del sistema, es decir, no se puede encontrar una demostración del mismo utilizando el proceso descrito más arriba.

Se puede probar que MU no es un teorema al demostrar que en todo teorema de este sistema el número de veces que aparece el símbolo I no es divisible por tres. Este resultado que no es un teorema del sistema, sino sobre el sistema y se prueba fuera de este, es decir, no sería demostrable automáticamente por un computador, recibe, con todos los resultados de este tipo, el nombre de metateorema.

Hay un tipo de sistemas formales especialmente adaptados para las matemáticas, los llamados *lógicas de primer orden*. No entraremos aquí en la definición general de una lógica de primer orden, nos limitaremos a describir, con alguna ligera imprecisión justificable por el ahorro de espacio, la lógica de primer orden correspondiente a la teoría de conjuntos.

Los símbolos de esta lógica son:

$\mathbf{x}, \mathbf{y}, \mathbf{z}, ...$: variables
$\mathbf{a}, \mathbf{b}, \mathbf{c}, ...$: constantes
$=$: igual
$\in$: pertenece a
$\neg$: no
$\Rightarrow$: implica
$\forall$: para todo
$(), :$ simbolos de separación

Para más comodidad se añaden cuatro símbolos más, con una regla de sustitución:

$\wedge$: y : $(\phi \wedge \psi)$ substituye a : $(\neg(\phi) \Rightarrow \psi)$
$\vee$: ó : $(\phi \vee \psi)$ substituye a : $(\neg(\phi \Rightarrow (\neg\psi)))$
$\Leftrightarrow$: equivale : $(\phi \Leftrightarrow \psi)$ substituye a : $(\neg((\phi \Rightarrow \psi) \Rightarrow (\psi \Rightarrow \phi))$
$\exists$: existe : $(\exists x(\phi))$ substituye a : $(\neg(\forall x)(\neg\phi))$

Las fórmulas de la lógica se describen en tres etapas. Se llama *términos* a los símbolos correspondientes a variables y constantes. Se llama *fórmulas básicas* a las fórmulas:

$$x = y, \quad x \in y, \text{ donde } x \text{ e } y \text{ son términos.}$$

Entonces las fórmulas de la lógica son:

1. Las fórmulas básicas.
2. $\neg\varphi$: si φ es una fórmula.
3. $\varphi \vee \psi$: si φ, ψ son fórmulas.
4. $\varphi \wedge \psi$: si φ, ψ son fórmulas.
5. $\varphi \Rightarrow \psi$: si φ, ψ son fórmulas.
6. $\varphi \Leftrightarrow \psi$: si φ, ψ son fórmulas.
7. $\forall x(\varphi(x))$: si φ es una fórmula en la que interviene x.
8. $\exists x(\varphi(x))$: si φ es una fórmula en la que interviene x.

Los axiomas se pueden separar en tres grupos, los de la lógica de proposiciones, los relativos a los

cuantificadores $\forall,\ \exists$ y los relativos a $=$:

A_1. $\varphi \Rightarrow (\psi \Rightarrow \varphi)$.
A_2. $(\varphi \Rightarrow (\psi \Rightarrow \theta)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \theta))$.
A_3. $((\neg\varphi) \Rightarrow (\neg\psi)) \Rightarrow (\psi \Rightarrow \varphi)$.
B_1. $(\forall x(\varphi)) \Rightarrow \varphi[t/x]$.
B_2. $(\forall x(\varphi \Rightarrow \psi)) \Rightarrow (\varphi \Rightarrow \forall x(\psi))$ si x no aparece en φ.
C_1. $t = t$ para todo término t.
C_2. $(t = u) \Rightarrow (u = t)$ para todo par de términos t, u.
C_3. $(t = u) \Rightarrow ((t = v) \Rightarrow (u = v))$ para t, u, v términos.
C_4. $(t = u) \Rightarrow (\psi[t/x, t/y] \Rightarrow \psi[t/x, u/y])$ x, y variables, ψ fórmula.

La notación $\varphi[t/x],\ \psi[t/x, t/y]$ significa el resultado de substituir la variable x por el término t en la fórmula correspondiente, siempre que x sea una *variable libre*; es decir, no vaya precedida inmediatamente por un *cuantificador* $(\exists,\ \forall)$.

Por último las reglas de deducción de la lógica de primer orden son solo dos:

1. Las entradas $\varphi, (\varphi \Rightarrow \psi)$ producen ψ.

2. La entrada φ produce $\forall x, \varphi(x)$, donde x es cualquier variable.

A la lógica de primer orden se le puede asignar una semántica, de la misma forma que a la lógica proposicional habitual, con una tabla de valores obtenida asignando a cada fórmula un valor: verdadero o falso, en función de los asignados arbitrariamente a las fórmulas básicas, y siguiendo luego las reglas usuales: ϕ solo puede ser verdadero o falso (principio del tercio excluso) , ϕ no puede ser verdadero y falso a la vez (principio de contradicción), $\neg\phi$ verdadero si y solo si ϕ falso, etcétera.

Se demuestra que una fórmula es verdadera en toda valoración si y solo si es un axioma o un teorema en el sistema formal descrito, es decir, la semántica proporciona una forma alternativa de construir demostraciones.

A esta lógica de primer orden le podemos añadir, para construir la teoría de conjuntos, los siguientes axiomas (Zermelo - Fraenkel) en los que la palabra conjunto corresponde a la de símbolo constante y se utiliza la expresión: a es un elemento de un conjunto b, para expresar la fórmula $a \in b$:

1. *Axioma de extensión* : si dos conjuntos tienen los mismos elementos, son iguales.

2. *Axioma del vacío* : existe un conjunto que no tiene elementos (al que representaremos por $\emptyset$ y llamaremos conjunto vacío).

3. *Axioma del conjunto de dos elementos* : si a e b son conjuntos, existe un conjunto cuyos elementos son exactamente a y b.

4. *Axioma de unión*: si x es un conjunto, existe un conjunto, al que llamaremos $\bigcup x$, cuyos elementos son los elementos de todos los elementos de x.

5. *Axioma del conjunto de partes*: si x es un conjunto, existe un conjunto $\mathcal{P}(x)$ cuyos elementos son todos los subconjuntos de x.

6. *Axioma de infinitud*: existe un conjunto a tal que:

$$\emptyset \in a \text{ y } (x \in a) \Rightarrow (\{x\} \in a)$$

7. *Axioma de selección*: si ϕ es una fórmula en el lenguaje de la teoría de conjuntos, x una variable libre en ϕ y a es un conjunto, existe un conjunto compuesto por los elementos de a que verifican $\phi(x)$.

8. *Axioma de reemplazamiento*: sea ϕ una fórmula en la que intervienen libremente dos variables x e y y es tal que para cada cada x existe como máximo un y que verifica la fórmula. Entonces si a es un conjunto, existe un conjunto cuyos elementos son los y tales que $\phi(x, y)$ se verifica para algún elemento x de a.

9. *Axioma de fundamento*: para todo conjunto no vacío x existe $y \in x$ tal que $x \cap y = \emptyset$.

10. *Axioma de elección*: si $f : x \longrightarrow y$ es una aplicación, con $f(z) \neq \emptyset$, $\forall z \in x$, existe una aplicación $g : x \longrightarrow \bigcup_{z \in x} f(z)$, tal que $g(z) \in f(z), \forall z \in x$.

Tal como hemos enunciado los axiomas, intervienen en algunos de ellos palabras que no hemos definido, pero que se puede probar que corresponden a objetos cuya existencia está garantizada por los axioma anteriores. También hemos dado los enunciados de forma literaria, porque, aunque todos ellos se escriben en el lenguaje que hemos desarrollado, se comprenden más fácilmente en esta formulación. Así por ejemplo, el enunciado del axioma de extensión sería:

$$(\forall x)(\forall y)(x = y) \Leftrightarrow (\forall z)((z \in x) \Leftrightarrow (z \in y))$$

y el de unión:

$$(\forall x)(\exists y)(\forall z)((z \in y) \Leftrightarrow (\exists w)((w \in x) \wedge (z \in w)))$$

El axioma de extensión significa que un conjunto está unívocamente determinado por sus elementos; esto justifica que si los elementos de un conjunto a son $a_1, a_2, ..., a_n$ escribamos

$a = \{a_1, a_1, ..., a_n\}$. También justifica que hablemos de *el* conjunto vacío. Podemos decir que el conjunto x es un *subconjunto* del conjunto y y escribir $x \subset y$, si $(\forall z)((z \in x) \Rightarrow (z \in y))$, con esta notación el axioma del conjunto de partes puede enunciarse ya sin problemas. El axioma de selección junto con el del conjunto de dos elementos, garantiza que si x es un conjunto también lo es $\{x\}$. Observemos que en ningún caso debe confundirse x con $\{x\}$, como tampoco deben confundirse $\in$ y $\subset$.

El axioma de infinitud lleva consigo por ejemplo la existencia del conjunto:

$$\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, ...$$

es decir, en términos un poco informales, establece la existencia de conjuntos infinitos. Obsérvese que en cambio, por el axioma de fundamento, no se pueden encontrar cadenas infinitas:

$$..... \in x_2 \in x_1 \in x_0$$

ya que si una tal cadena existiera, tomando el conjunto $x = \{x_n \mid n \in \mathbb{N}\}$, si $y \in x$ existe un $n \in \mathbb{N}$ con $x_n = y$, entonces $x_{n+1} \in y \cap x$ y en consecuencia $y \cap x \neq \emptyset$.

Señalemos por último que con esta axiomática se evita la paradoja de Russel. Para comprobarlo veamos en primer lugar que ningún conjunto puede ser elemento de si mismo. En efecto si x es un conjunto y $x \in x$, podemos formar el conjunto $z = \{x\}$, entonces por el axioma de fundamento, al ser x el único elemento de z debe ser $x \cap z = \emptyset$, pero $x \in x \cap z$, luego se llega a contradicción. Entonces el *conjunto* de todos los conjuntos que no son elementos de si mismos sería el *conjunto* de todos los conjuntos, pero si hubiese un conjunto S de todos los conjuntos, sería $S \in S$ y hemos visto que eso no es posible.

La axiomática de Zermelo incluye, de modo implícito y confuso, el concepto de propiedad bien definida. Dentro de nuestra estructura se puede dar una definición formal como hace por ejemplo el texto de Moschovakis, [28], pero no la incluiremos aquí, porque esencialmente duplica algunas de las construcciones anteriores. Únicamente señalaremos que la paradoja de Russel establece que no todos los objetos que podemos manejar son conjuntos, entonces falta describir esos *no conjuntos*, en otras palabras falta decir qué sucede con las condiciones bien definidas que no definen conjuntos. Esa cuestión nos hace ver que aunque en las líneas anteriores hemos trabajado mucho para escapar de la indefinición sin usar definiciones, realmente no hemos resuelto el problema, lo hemos alejado un poco, porque no hemos salido del *todo* o *universo* de la definición ingenua de Cantor. Veamos ahora como se puede dar solución al problema.

Una respuesta es introducir unos nuevos *objetos de nuestro pensamiento*, a los que llamaremos clases. Y con la tendencia de los matemáticos a resolver los problemas de un modo obvio definimos de modo intuitivo una clase diciendo que para toda condición definida P, existe una clase C

tal que:

$$x \in C \Leftrightarrow x \text{ verifica } P$$

de modo formal escribimos para la propiedad P y el objeto x $P(x) \Leftrightarrow x$ verifica P, y decimos que P es *coextensiva* con un conjunto C y escribimos $P \sim C$, si:

$$P \sim C \Leftrightarrow (\forall x)[P(x) \Leftrightarrow x \in C]$$

No vamos a entrar en más detalles de teoría axiomática de conjuntos que alargarían demasiado este capítulo. El lector interesado puede consultar cualquiera de los buenos manuales que existen sobre el tema como el de Cameron [7] o el de Moschovakis [28] por ejemplo.

Alexander Grothendieck (1928 - 2014) (ver Gabriel [14]) introduce en 1963 la noción de *Universo*, como un conjunto con una relación de pertenencia entre sus elementos $\in$ que es un modelo de la teoría de conjuntos de Z-F. Un Universo U tiene que tener las propiedades siguientes:

- $(x \in y, y \in U) \Rightarrow x \in U$.
- U contiene al conjunto de los naturales.
- Si $x \in U,\ y \in U$ entonces $\{x, y\} \in U$.
- El conjunto de partes de un elemento de U está en U.
- U es cerrado para uniones.
- La imagen de un elemento de U por una función definida por una fórmula de la lógica de primer orden está en U.

Grothendieck añade un nuevo axioma a Z-F: *para todo conjunto existe al menos un Universo que lo contiene.*

Así al trabajar con la totalidad de conjuntos, grupos, etcétera, de un universo no salimos de la teoría de conjuntos y evitamos las paradojas. Pero, como es habitual, encontramos de nuevo un problema:

- *¿Los resultados obtenidos en un problema dependen del universo en que consideremos el problema?*

La respuesta es negativa en general, pero existen ejemplos en que la respuesta es afirmativa (ver Low [23]), pero son construcciones tan sofisticadas que no las tendremos en cuenta.

3. Teoría clásica de Galois

Esta sección está dedicada a introducir las definiciones y enunciados de la Teoría de Galois Clásica que, en principio, se supone conocida por los alumnos, por lo cual omitiremos casi todas las demostraciones.

Sea k un cuerpo, una *extensión* de k es un cuerpo K del cual k es un subcuerpo, para representar el hecho de que K es una extensión de k escribiremos $K|k$. Si $K_1|k$ y $K_2|k$ llamaremos k-homomorfismo (resp. k isomorfismo) de K_1 en K_2 a todo homomorfismo (resp. isomorfismo) $f : K_1 \to K_2$ tal que $f(a) = a, \forall a \in k$.

Si $K|k$, entonces K es un k-espacio vectorial y a $[K : k] = dim_k(K)$ se le llama *grado* de la extensión. Si K es una extensión de k y $\alpha \in K$, podemos construir el subanillo $k[\alpha] \subset K$ y el núcleo del homomorfismo de evaluación:

$$v_\alpha : k[x] \to k[\alpha],\ v_\alpha(p(x)) = p(\alpha)$$

es un ideal primo de $k[x]$. Si $Ker(v_\alpha) = 0$ se dice que α es *trascendente* sobre k y si $Ker(v_\alpha) \neq 0$ entonces $Ker(v_\alpha)$ es un ideal maximal principal con un único generador mónico irreducible $f_\alpha(x) \in k[x]$. En este caso se dice que α es *algebraico* sobre k y que $f_\alpha(x)$ es su *polinomio mínimo*. Obviamente en estas condiciones:

- $k[x]/(f_\alpha(x)) \simeq k[\alpha]$.

- $k[\alpha]$ es el mínimo subcuerpo de K que contiene a k y a α (por ello en lo sucesivo lo representaremos por $k(\alpha)$).

- $[k(\alpha) : k] = grado(f_\alpha(x))$.

Una extensión $K|k$ se dice *algebraica* si todos los elementos de K son algebraicos sobre k. Toda extensión finita (es decir, de grado finito) es algebraica pero el recíproco no es cierto. Un cuerpo se llama *algebraicamente cerrado* si no admite extensiones algebraicas propias, o lo que es lo mismo:

- *Un cuerpo K es algebraicamente cerrado si y solo si todo polinomio de $K[x]$ factoriza en $K[x]$ en producto de factores lineales.*

Un *cierre algebraico* de un cuerpo k es un cuerpo $\overline{k}$ extensión algebraica de k y algebraicamente cerrado.

Proposición 3.1.– *Sea k un cuerpo:*

1. *Existe un cierre algebraico de k.*
2. *Si K_1 y K_2 son dos cierres algebraicos de k, K_1 y K_2 son k- isomorfos.*
3. *Si $\overline{k}$ es un cierre algebraico de k, para toda extensión algebraica L de k existe un k- homomorfismo de L en $\overline{k}$.*
4. *El homomorfismo anterior se extiende a un k -isomorfismo del cierre algebraico $\overline{L}$ de L en $\overline{k}$.*

La prueba de esta proposición depende esencialmente del lema de Zorn y pese a la falta de unicidad en todos los objetos que aparecen en la proposición, hablaremos de "el cierre algebraico" $\overline{k}$ de k y consideraremos todas las extensiones algebraicas de k sumergidas en él.

Un polinomio $f(x) \in k[x]$ se dice *separable* si no tiene raíces multiples en $\overline{k}$, un elemento algebraico sobre k se dice *separable* si lo es su polinomio mínimo y una extensión algebraica $K|k$ se llama *extensión separable* si todos los elementos de K son separables sobre k.

- En característica cero todas las extensiones algebraicas son separables.
- En característica $p > 0$ si $a \in k,\ a \notin k^p$, $x^p - a$ no es un polinomio separable.
- Una extensión finita $L|k$ es separable si y solo si $L = k(\alpha_1, ..., \alpha_r)$ y todos los α_i son separables sobre k (más aún, el *Teorema del elemento primitivo* establece que $r = 1$).

- Si $\overline{k}$ es un cierre algebraico de k:

$$k_s = \{\alpha \in \overline{k} \mid \alpha\text{es separable sobre } k\}$$

es un cuerpo que recibe el nombre de *cierre separable* de k

- k_s es único salvo k-isomorfismos, y toda extensión separable de k es isomorfa a un subcuerpo de k_s.

Destacamos el resultado más importante que se prueba fácilmente por inducción:

Proposición 3.2.– *Si L es una extensión separable de k y $[L : k] = n$ existe exactamente n k-homomorfismos de L en k_s*

En lo que sigue dada una extensión $L|k$, designaremos por $Aut_k(L)$ al grupo de k-automorfismos de L, y si H es un subgrupo de $Aut_k(L)$, designamos con:

$$L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha,\ \forall \sigma \in H\}$$

Obviamente L^H es un subcuerpo de L que contiene a k.

Definición 3.3.– *Una extensión algebraica $L|k$ se dice* galoisiana *si y solo si $L^G = k$, con $G = Aut_k(L)$. Si $L|k$ es galoisiana escribiremos $Aut_k(L) = Gal(L|k) = Gal_k(L)$*

El cierre separable k_s de k es una extensión galoisiana ya que si $\alpha \in k_s \setminus k$ su polinomio mínimo tiene al menos una raíz $\beta \neq \alpha$, entonces podemos construir un k-homomorfismo:

$$\tau : k(\alpha) \to \overline{k},\ \tau(\alpha) = \beta$$

Este homomorfismo se extiende a un automorfismo de $\overline{k}$ y como todo k-automorfismo de $\overline{k}$ deja invariante k_s (ya que todo elemento de $\overline{k}$ y su imagen tienen el mismo polinomio mínimo), tenemos un automorfismo de k_s que mueve α, y en consecuencia si $G = Aut_k(k_s)$, $k_s^G = k$.

Las extensiones galoisianas se caracterizan por las dos propiedades del teorema siguiente:

Teorema 3.4.– *Si $L|k$ es una extensión algebraica las propiedades siguientes son equivalentes:*

1. *$L|k$ es una extensión galoisiana.*
2. *$L|k$ es separable y el polinomio mínimo sobre k de todo elemento $\alpha \in L$ factoriza en $L[x]$ en producto de factores lineales (extensión normal).*
3. *Existe un cierre separable k_s de k que contiene a L y todo automorfismo $\tau \in Gal(k_s|k)$ verifica que $\tau(L) \subset L$*

Demostración:

Para probar que $1 \Rightarrow 2$, dado $\alpha \in L$ construimos su estabilizador $H \subset Gal_k(L)$, y formamos el conjunto de clases por la izquierda $Gal_k(L)/H$, este conjunto es finito porque si tomamos un representante σ_i de cada clase las $\sigma_i(\alpha)$ son raíces distintas del polinomio mínimo $f_\alpha(x)$ de α. El polinomio:

$$p(x) = \prod_i (x - \sigma_i(\alpha)),$$

está en $k[x]$ porque es invariante por $Gal_k(L)$. Como $f_\alpha(x)$ es irreducible y $p(x)|f_\alpha(x)$ es $p(x) = f_\alpha(x)$ y $f_\alpha(x)$ es separable y tiene todas sus raíces en L.

La implicación $2 \Rightarrow 3$, se sigue de que los k-automorfismos envían cada elemento de L en otra raíz de su polinomio mínimo. Por último $3 \Rightarrow 1$, se sigue de la prueba de la separabilidad de k_s.

□

Una consecuencia inmediata de este teorema es que:

Consecuencia 3.5.– *Si $L|k$ es una extensión finita las condiciones siguientes son equivalentes:*

1. *$L|k$ es galoisiana.*
2. *L es el cuerpo de descomposición de un polinomio separable irreducible de $k[x]$.*
3. *$\sharp(Aut_k(L)) = [L : k]$.*

Demostración:

$1 \Rightarrow 2$, por el teorema del elemento primitivo y la segunda afirmación del teorema. $2 \Rightarrow 3$. es trivial y $3 \Rightarrow 1$, porque si $G = Aut_k(L)$, $L|L^G$ es galoisiana y $Aut_k(L) = Aut_{L^G}(L)$ entonces por $1 \Rightarrow 3$ aplicado a $L|L^G$:

$$[L : L^G] = \sharp(Aut_{L^G}(L)) = \sharp(Aut_k(L)) = [L : k]$$

Luego $k = L^G$ y $L|k$ es galoisiana. □

Otra consecuencia de este teorema es el llamado *Teorema fundamental de la Teoría de Galois*

Teorema 3.6.– *Si $L|k$ es una extensión de Galois finita y llamamos $Gal_k(L) = G$, las aplicaciones entre los conjuntos ordenados por inclusión de subcuerpos de L que contienen a k, $\mathcal{S}(L|k)$, y de subgrupos de G, $\mathcal{S}(G)$: dadas por:*

$$\mathcal{I} : \mathcal{S}(L|k) \to \mathcal{S}(G),\ \mathcal{I}(M) = Aut_M(L)$$

$$\mathcal{V} : \mathcal{S}(G) \to \mathcal{S}(L|k),\ \mathcal{V}(H) = L^H$$

son inversas una de la otra y invierten el orden.
Además la extensión $M|k$ es Galois si y solo si $H = \mathcal{I}(M)$ es normal en G y en este caso:

$$Gal_k(M) \simeq G/H$$

Demostración:

Si $M \in \mathcal{S}(L|k)$ por 3 de 3.4 $L|M$ es galoisiana y:

$$H = Gal_M(L) \Rightarrow \mathcal{V}\mathcal{I}(M) = L^H = M$$

Recíprocamente si H es un subgrupo de G, $L|L^H$ es galoisiana por definición y:

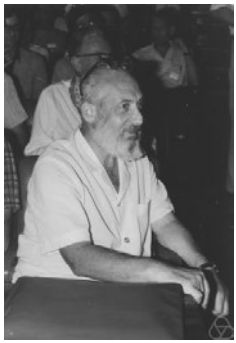
$$H = Gal_{L^H}(L) = \mathcal{I}\mathcal{V}(H)$$

Ahora si H es un subgrupo normal de G y $M = L^H$, como los elementos de H fijan M, hay una acción de G/H sobre M que permite identificar G/H con $Aut_k(M)$ porque todo k automorfismo de M se extiende a L. Entonces:

$$M^{G/H} = L^G = k$$

y en consecuencia $M|k$ es galoisiana.

Recíprocamente por 3 de 3.4 si $M|k$ es galoisiana existe el homomorfismo de restricción $G \to Gal_k(M)$ y es sobre. El núcleo de este homomorfismo es H luego que da completo el teorema. □



In order to deal in a general way with such situations, we introduce the concept of a category. Thus a category 21 will consist of abstract elements of two types: the objects A (for example, vector spaces, groups) and the mappings a (for example, linear transformations, homomorphisms).

This may be regarded as a continuation of the Klein Erlanger Programm, in the sense that a geometrical space with its group of transformations is generalized to a category with its algebra of mappings.

S. Eilenberg

4. Lenguaje básico de categorías

En esta sección introduciremos las definiciones básicas de Teoría de categorías: categoría, funtor, traslación natural, etcétera, que necesitaremos en nuestro trabajo. En una sección posterior hablaremos de funtores representables y nos limitaremos a lo estrictamente necesario.

La Teoría de categorías se origina en la obra de Eilemberg-McLane [26] y tiene una doble conexión con los objetos que vamos a estudiar, ya que las categorías son un lenguaje necesario para las extensiones infinitas y para las versiones de Grothendieck de la Teoría de Galois y, además, los grupoides que aparecen al final de nuestro trabajo se pueden presentar, de un modo sofisticado, como un tipo especial de categoría, que a su vez Ehresman [11] utiliza para dar una versión alternativa de la Teoría.

En principio, y puesto que hablaremos de las categorías de conjuntos, grupos etcétera, tendríamos que hablar de la *clase* de objetos de una categoría, y llamar categoría pequeña a aquella cuyos objetos forman un conjunto, pero estimamos, como hemos señalado en la primera sección que es preferible acogernos a los Universos de Grothendieck [26] [14], y limitarnos a categorías con un conjunto de objetos. De modo que expresiones como “los conjuntos”, “los grupos” y otras similares, se refieren al conjunto de conjuntos, al conjunto de grupos etcétera de un universo.

Definición 4.1.– *Una* categoría $\mathfrak{C}$ *es:*

- *Un conjunto* $Ob(\mathfrak{C})$ *a cuyos elementos llamaremos objetos*
- *Un conjunto* $Hom_{\mathfrak{C}}(A,B)$*, para cada par de objetos* (A,B)*, a cuyos elementos llamaremos morfismos de A en B. Escribiremos indistintamente* $f \in Hom_{\mathfrak{C}}(A,B)$ *y* $f : A \to B$ *y llamaremos a* A *y* B *dominio y rango de* f *respectivamente.*
- *Una composición de morfismos:*

$$Hom_{\mathfrak{C}}(A,B) \times Hom_{\mathfrak{C}}(B,C) \to Hom_{\mathfrak{C}}(A,C),\ (f,g) \mapsto gf$$

Si existe la composición de f *y* g*, es decir, si el rango de* f *coincide con el dominio de* g *se dice que son componibles. La composición debe verificar las propiedades usuales:*

- *Asociativa:* $\exists\, gf, \exists\, hg \Rightarrow (hg)f = h(gf)$.
- *Para cada objeto* A, $\exists 1_A : A \to A$ *de modo que* $f : A \to B \Rightarrow f1_A = 1_B f = f$.

Una categoría $\mathfrak{D}$ se dice una *subcategoría* de otra $\mathfrak{C}$ si y solo si:

- $Ob(\mathfrak{D}) \subset Ob(\mathfrak{C})$.
- $\forall A, B \in Ob(\mathfrak{D}),\ Hom_{\mathfrak{D}}(A,B) \subset Hom_{\mathfrak{C}}(A,B)$.
- Las composiciones de morfismos coinciden.

La subcategoría $\mathfrak{D}$ de $\mathfrak{C}$ se dice *subcategoría completa* si y solo si:

$$\forall A, B \in Ob(\mathfrak{D}),\ Hom_{\mathfrak{D}}(A,B) = Hom_{\mathfrak{C}}(A,B)$$

Ejemplos 4.2.–

Ejemplo. 4.2.1.- Los conjuntos y las aplicaciones, los grupos y los homomorfismos de grupos, los espacios topológicos y las aplicaciones continuas, etcétera. son ejemplos de categorías, a las que representaremos como ((Sets)), ((Gr)), ((Top)), etcétera.
La categoría de conjuntos finitos es una subcategoría de la de conjuntos, y la categoría de grupos abelianos es una subcategoría de la de grupos, pero la categoría de grupos no es una subcategoría de la de conjuntos porque sobre un mismo conjunto caben varias estructuras de grupo.

Ejemplo. 4.2.2.- Si $\mathfrak{C}$ es una categoría podemos construir su *categoría dual* $\mathfrak{C}^*$ en la forma siguiente:

- $Ob(\mathfrak{C}^*) = Ob(\mathfrak{C})$.
- Para cada par de objetos $A, B,\ Hom_{\mathfrak{C}^*}(A, B) = Hom_{\mathfrak{C}}(B, A)$.
- La composición de morfismos en $\mathfrak{C}^*$ es:

$$Hom_{\mathfrak{C}^*}(A, B) \times Hom_{\mathfrak{C}^*}(B, C) \to Hom_{\mathfrak{C}^*}(A, C),\ (f, g) \mapsto fg.$$

$\mathfrak{C}^*$ es una categoría y su existencia nos permite establecer un *Principio de dualidad* en Teoría de categorías:

> *Un resultado cierto en una categoría general sigue siendo cierto si cambiamos el sentido de las flechas y el orden en la composición de morfismos.*

Ejemplo. 4.2.3.- Si $\mathfrak{C}$ es una categoría podemos construir la categoría $Morf(\mathfrak{C})$ como sigue:

- Si $\bigsqcup$ representa la unión disjunta de conjuntos.

$$Ob(Morf(\mathfrak{C})) = \bigsqcup_{X,Y \in Ob(\mathfrak{C})} Hom_{\mathfrak{C}}(X, Y)$$

- $\forall\ f \in Hom_{\mathfrak{C}}(X, X'),\ \forall\ g \in Hom_{\mathfrak{C}}(Y, Y')$

$$Hom_{Morf(\mathfrak{C})}(f, g) = \{(h, k) \in Hom_{\mathfrak{C}}(X, Y) \times Hom_{\mathfrak{C}}(X', Y') \mid kf = gh\}$$

$$\begin{array}{ccc} X & \xrightarrow{\quad h \quad} & Y \\ \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle g} \\ X' & \xrightarrow{\quad k \quad} & Y' \end{array}$$

- La composición de morfismos es: $\exists\ gf,\ \exists kh \Rightarrow (g, k)(f, h) = (gf, kh)$

Se usan varias subcategorías de $Morf(\mathfrak{C})$ por ejemplo:

- Si S es un objeto de la categoría $\mathfrak{C}$ podemos construir una nueva categoría, la categoría relativa a S, $\mathfrak{C}/S$, como la subcategoría de $Morf(\mathfrak{C})$, cuyos objetos son:

$$Ob(\mathfrak{C}/S) = \bigcup_{X \in Ob(\mathfrak{C})} Hom_{\mathfrak{C}}(X, S)$$

  y cuyos morfismos son los de $Morf(\mathfrak{C})$ con segunda componente la identidad. A cada objeto de $\mathfrak{C}/S$, $p : X \to S$, lo representaremos por (X, p)

- Se puede hace la construcción dual de la categoría relativa, que, aplicada a la categoría de anillos conmutativos con uno y homomorfismos que preservan el uno da lugar a la categoría de S - álgebras.

- Si $\mathfrak{C}$ es la categoría de conjuntos o la de espacios topológicos podemos tomar la subcategoría completa de $\mathfrak{C}$ cuyos objetos son las inclusiones, si $j : Y \hookrightarrow X$ es una inclusión la representamos por (X, Y) y a esta categoría la llamamos categoría de pares de $\mathfrak{C}$

- La subcategoría completa de la categoría de pares en la que nos quedamos solamente con los pares (X, x) donde x es un punto de X se llama categoría de espacios punteados o de conjuntos punteados.

Ejemplo. 4.2.4.- Hay categorías más extrañas adscritas a estructuras algebraicas o topológicas. Por ejemplo:

- Si X es un espacio topológico se puede construir una categoría $\mathcal{T}_X$ cuyos objetos son los abiertos de X y $Hom_{\mathcal{T}_X}(U, V)$ está formado solo por la inclusión si $U \subset V$ y es el vacío en caso contrario.

- Si G es un grupo se puede construir una categoría $\mathcal{G}$ con un único objeto, al que podemos llamar O, con $Hom_{\mathcal{G}}(O, O) = G$ y tomando como composición de morfismos el producto de elementos de G.

- Si X es un conjunto con una relación $\sim$ simétrica y transitiva, una relación de orden parcial o de equivalencia por ejemplo, podemos construir una categoría $X^{\sim}$, tomando a X como conjunto de objetos, y:

$$\forall x, y \in X,\ Hom_{X^{\sim}}(x, y) = \begin{cases} \emptyset & \text{si} \quad x \nsim y \\ \{(x, y)\} & \text{si} \quad x \sim y \end{cases}$$

  con la composición:

$$(x, y)(y, z) = (x, z.)$$

- Dado un anillo A podemos construir la *categoría de matrices sobre* A tomando como objetos los enteros positivos, como morfismos entre m y n las matrices $n \times m$ y como composición el producto de matrices.

- Como tendremos ocasión de ver más adelante, se puede definir una estructura algebraica, el *grupoide*, como una categoría en la que todos los morfismos son isomorfismos.

Podemos plantearnos ahora la descripción de los morfismos especiales que correspondan a las nociones de homomorfismo inyectivo, sobreyectivo e isomorfismo. Hay varias definiciones posibles que son equivalentes en algunas categorías y no lo son en otras. Las más usuales son:

Definición 4.3.– *Sea $f \in Hom_{\mathfrak{C}}(A, B)$:*

1. *Se dice que f es un monomorfismo si y solo si:*

$$\forall X \in Ob(\mathfrak{C}),\ \forall g, h \in Hom_{\mathfrak{C}}(X, A),\ (fg = fh \Rightarrow g = h)$$

2. *Se dice que f es un epimorfismo si y solo si:*

$$\forall X \in Ob(\mathfrak{C}),\ \forall g, h \in Hom_{\mathfrak{C}}(B, X),\ (gf = hf \Rightarrow g = h)$$

3. *Se dice que f es un bimorfismo si y solo si es monomorfismo y epimorfismo simultáneamente.*

4. *Se dice que f es una retracción si y solo si:*

$$\exists g \in Hom_{\mathfrak{C}}(B, A),\ fg = 1_B.$$

5. *Se dice que f es una sección si y solo si:*

$$\exists g \in Hom_{\mathfrak{C}}(B, A),\ gf = 1_A.$$

6. *Se dice que f es un isomorfismo si y solo si:*

$$\exists g \in Hom_{\mathfrak{C}}(B, A),\ gf = 1_A,\ fg = 1_B.$$

Es un ejercicio sencillo comprobar que:

1. Monomorfismo y epimorfismo son duales, lo mismo que retracción y sección.
2. Si f es retracción es epimorfismo y si f es sección es monomorfismo, en consecuencia si f es isomorfismo es bimorfismo.
3. f es isomorfismo si y solo si tiene inverso.
4. En la categoría de conjuntos epimorfismo, retracción y aplicación sobre son equivalentes y monomorfismo, sección y aplicación inyectiva también, y lo mismo sucede en la de espacios vectoriales

5. En una categoría de conjuntos con una estructura:

$$f \text{ sección} \Rightarrow \ f \text{ inyectiva} \Rightarrow \ f \text{ monomorfismo}$$

$$f \text{ retracción} \Rightarrow \ f \text{ sobre} \Rightarrow \ f \text{ epimorfismo}$$

$$f \text{ isomorfismo} \Rightarrow \ f \text{ biyectiva} \Rightarrow \ f \text{ bimorfismo}$$

6. La inmersión $\mathbb{Z} \to \mathbb{Q}$ es bimorfismo de anillos pero no es sobre

7. Una aplicación biyectiva continua no abierta no es retracción en la categoría de espacios topológicos.

8. La inmersión $2\mathbb{Z} \to \mathbb{Z}$ es inyectiva pero no es sección.

9. En la categoría de grupos abelianos divisibles la aplicación natural $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ es un monomorfismo pero no es inyectiva.

Definidos estos tipos de morfismos, podemos introducir conceptos comunes en álgebra y topología:

Definición 4.4.–

1. *Llamaremos* subobjeto *de un objeto A a un par (S, f) donde $f : S \to A$ es un monomorfismo.*

2. *Llamaremos* objeto cociente *de un objeto A a un par (E, f) donde $f : A \to E$ es un epimorfismo.*

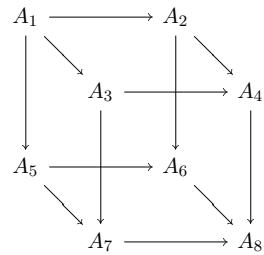
3. *Diremos que $I \in Ob(\mathfrak{C})$ es un* objeto inicial *si $Hom_{\mathfrak{C}}(I, A)$ tiene un solo elemento cualquiera que sea A.*

4. *Diremos que $F \in Ob(\mathfrak{C})$ es un* objeto final *si $Hom_{\mathfrak{C}}(A, F)$ tiene un solo elemento cualquiera que sea A.*

5. *Diremos que $O \in Ob(\mathfrak{C})$ es un* objeto cero *si es simultáneamente objeto inicial y objeto final.*

Claramente dos objetos iniciales, finales o cero son siempre isomorfos.

Ejercicio 4.5.– Dado el diagrama:



En el que todas las caras, excepto la superior son conmutativas y el morfismo $A_4 \to A_8$ es un monomorfismo. Probar que la cara superior es también conmutativa.

Definición 4.6.– *Dadas dos categorías $\mathfrak{C}$ y $\mathfrak{D}$ se llama* funtor *de la primera en la segunda, a:*

- *Una aplicación $F : Ob(\mathfrak{C}) \to Ob(\mathfrak{D})$*
- *Para todo par de objetos de $\mathfrak{C}$, A, B, una de las dos opciones siguientes:*
  - *Una aplicación $F : Hom_{\mathfrak{C}}(A, B) \to Hom_{\mathfrak{D}}(F(A), F(B))$ tal que: $F(1_A) = 1_{F(A)}$, $F(gf) = F(g)F(f)$*
  - *Una aplicación $F : Hom_{\mathfrak{C}}(A, B) \to Hom_{\mathfrak{D}}(F(B), F(A))$ tal que: $F(1_A) = 1_{F(A)}$, $F(gf) = F(f)F(g)$*

En el primer caso el funtor se llama covariante *y en el segundo* contravariante. *Un functor contravariante $F : \mathfrak{C} \to \mathfrak{D}$ se puede interpretar siempre como un funtor covariante $F^* : \mathfrak{C}^* \to \mathfrak{D}$.*

Obviamente la composición de funtores es un funtor y la identidad también, de modo que tiene sentido hablar de la categoría $((Cat))$ cuyos objetos son las categorías y cuyos morfismos son los funtores.

Ejemplos 4.7.–

Ejemplo. 4.7.1.- Si $\mathfrak{C}$ es una categoría y T es un objeto, podemos asociar a T dos funtores de $\mathfrak{C}$ en la categoria de conjuntos $((Sets))$:

- $h_T(-)$ definido por: $h_T(S) = Hom_{\mathfrak{C}}(T, S), \forall f : S \to U,\ \forall \varphi \in h_T(S)$, $h_T(f)(\varphi) = f\varphi \in h_T(U)$.
- $T(-)$ definido por: $T(S) = Hom_{\mathfrak{C}}(S, T), \forall f : S \to U,\ \forall \varphi \in T(U)$, $T(f)(\varphi) = \varphi f \in T(S)$.

El primero es covariante y el segundo contravariante.

Ejemplo. 4.7.2.- Si X e Y son espacios topológicos y $f : X \to Y$ es una aplicación continua tenemos un funtor:

$$\overline{f} : \mathcal{T}_Y \to \mathcal{T}_X,\ \overline{f}(V) = f^{-1}(V).$$

Ejemplo. 4.7.3.- Podemos asociar a cada espacio topológico X la $\mathbb{R}$- álgebra, $\mathcal{C}(X, \mathbb{R})$ de las funciones continuas reales sobre X, y a cada aplicación continua $f : X \to Y$ el homomorfismo:

$$\overline{f} : \mathcal{C}(Y, \mathbb{R}) \to \mathcal{C}(X, \mathbb{R}),\ \overline{f}(h) = hf$$

y tenemos un funtor de la categoría de espacios topológicos en la de $\mathbb{R}$- álgebras.

Ejemplo. 4.7.4.- Si X es un espacio topológico, todo funtor contravariante $\mathcal{P}$ de $\mathcal{T}_X$ en una categoría $\mathfrak{C}$, se llama un *prehaz* sobre X con valores en $\mathfrak{C}$. Si $U \subset V$ son abiertos de X, el morfismo $\rho_{V,U} : \mathcal{P}(V) \to \mathcal{P}(U)$ se llama *restricción* de V a U.
Si X e Y son espacios topológicos podemos asociar a cada abierto U de X el conjunto de aplicaciones continuas de U en Y. Tomando como restricción la restricción usual de funciones tenemos un prehaz sobre X, $\mathcal{C}_Y$.
Este prehaz verifica la propiedad siguiente:

> Dado un recubrimiento abierto $\{U_i\}_{i \in I}$ de un abierto U, y dadas funciones continuas $\{f_i : U_i \to Y\}_{i \in I}$ tales que:
>
> $$f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j},\ \forall i, j \in I$$
>
> entonces:
>
> $$\exists f : U \to Y, \text{ continua única tal que : } f|_{U_i} = f_i,\ \forall i \in I$$
>
> por verificarse esta propiedad se dice que este prehaz es un *haz*.

La propiedad anterior se enuncia trivialmente para todos los prehaces de conjuntos con una estructura.

También es un prehaz sobre X la correspondencia $\overline{\mathcal{C}_{\mathbb{R}}}$ que asocia a cada abierto U el conjunto de funciones reales continuas y acotadas sobre U.
El prehaz de conjuntos $\overline{\mathcal{C}_{\mathbb{R}}}$, no es un haz en general. Si $X = (0,1) \subset \mathbb{R}$, los $U_n = (1/n, 1), n \in \mathbb{N}$ forman un recubrimiento abierto de $(0,1)$, y las funciones reales $f_n : U_n \to \mathbb{R},\ f_n(x) = 1/x$ cumplen la condición de haz y no definen una función acotada sobre $(0,1)$.

Ejemplo. 4.7.5.- Si P es un prehaz sobre un espacio X y $f : X \to Y$ es una aplicación continua, podemos definir un prehaz sobre Y, llamado *prehaz imagen directa* de $\mathcal{P}$ por f, por:

$$\forall V \in T_Y,\ f_*(\mathcal{P})(V) = \mathcal{P}(f^{-1}(V)).$$

Claramente $f_*(\mathcal{P}) = \mathcal{P}\overline{f}$.

Ejemplo. 4.7.6.- Si $f : S \to T$ es un morfismo de una categoría $\mathfrak{C}$ se puede construir un funtor (*Imagen directa*) $f_* : \mathfrak{C}/S \to \mathfrak{C}/T$ por:

- $f_*(g : X \to S) = (fg) : X \to T$.
- f_* es la identidad sobre los morfismos.

Como consecuencia obtenemos un funtor $R : \mathfrak{C} \to ((Cat))$ asociando a cada objeto S la categoría $\mathfrak{C}/S$ y a cada morfismo f el funtor f_*

Ejemplo. 4.7.7.- La correspondencia que asocia a cada grupo, anillo, espacio topológico etcétera el conjunto subyacente a su estructura y a cada homomorfismo, aplicación continua, etcétera. la aplicación subyacente es un funtor covariante que se llama *funtor de olvido*.

Dados dos funtores $F, G : \mathfrak{C} \to \mathfrak{D}$ (ambos covariantes o ambos contravariantes) se llama una transformación natural de F en G a una familia de morfismos

$$N_X : F(X) \to G(X),\ \forall X \in Ob(\mathfrak{C})$$

Tales que:

- Caso covariante. $\forall f : X \to Y, N_Y F(f) = G(f) N_X$

$$\begin{array}{ccc} F(X) & \xrightarrow{N_X} & G(X) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{N_Y} & G(Y) \end{array}$$

- Caso contravariante. $\forall f : X \to Y, N_X F(f) = G(f) N_Y$

$$\begin{array}{ccc} F(Y) & \xrightarrow{N_Y} & G(Y) \\ \Big\downarrow{\scriptstyle F(f)} & & \Big\downarrow{\scriptstyle G(f)} \\ F(X) & \xrightarrow{N_X} & G(X) \end{array}$$

La composición de transformaciones naturales es una transformación natural y la identidad también, por tanto dadas dos categorías, tomando como objetos los funtores entre ellas y como morfismos las transformaciones naturales tenemos una categoría, los isomorfismos en esa categoría, es decir, las transformaciones naturales con inversa se llaman *isomorfismos naturales*.

Ejemplos 4.8.–

Ejemplo. 4.8.1.- Todo morfismo $g : X \to Y$ induce transformaciones naturales:

- $\forall S \in Ob(\mathfrak{C}),\ h_S(g) : X(S) \to Y(S),\ h_S(g)(f) = gf.$
- $\forall S \in Ob(\mathfrak{C}),\ S(g) : h_Y(S) \to h_X(S),\ S(g)(f) = fg.$

Ejemplo. 4.8.2.- Toda aplicación continua $f : X \to Z$ induce una transformación natural (*morfismo de haces*):

$$F : \mathcal{C}_Z \to f_*(\mathcal{C}_X),\ F_U : \mathcal{C}_Z(U) \to f_*(\mathcal{C}_X)(U) = \mathcal{C}_X(f^{-1}(U)),\ F_U(g) = gf,\ \forall g \in \mathcal{C}_Z(U)$$

Dos categorías $\mathfrak{C},\ \mathfrak{D}$ se dice que son *isomorfas* si existen funtores:

$$F : \mathfrak{C} \to \mathfrak{D},\ G : \mathfrak{D} \to \mathfrak{C}$$

tales que:

$$F.G = 1_{\mathfrak{D}},\ G.F = 1_{\mathfrak{C}}.$$

Dos categorías $\mathfrak{C},\ \mathfrak{D}$ se dicen *equivalentes* si existen funtores: $F : \mathfrak{C} \to \mathfrak{D},\ G : \mathfrak{D} \to \mathfrak{C}$ e isomorfismos naturales

$$\alpha : F.G \to 1_{\mathfrak{D}},\ \beta : G.F \to 1_{\mathfrak{C}}.$$

Cualquiera de los dos funtores $F,\ G$ se llama en este caso una *equivalencia de categorías*.

Es un ejercicio fácil probar que:

Un funtor $F : \mathfrak{C} \to \mathfrak{D}$ es una equivalencia de categorías si y solo si es fiel, completo y esencialmente suprayectivo, es decir, si y solo si para todo par de objetos X, Y de $\mathfrak{C}$, se tiene que $F : Hom_{\mathfrak{C}}(X, Y) \to Hom_{\mathfrak{D}}(F(X), F(Y))$ es biunívoca y para todo objeto Z de $\mathfrak{D}$ existe un objeto X de $\mathfrak{C}$ tal que $F(X)$ es isomorfo a Z.

Ejemplo 4.9.– La categoría de K- espacios vectoriales de dimensión finita es equivalente a la categoría de matrices sobre K descrita en el ejemplo 4.2.2

5. Funtores representables

Como hemos señalado, a cada objeto X de una categoría $\mathfrak{C}$ se le pueden asociar dos funtores: el funtor contravariante (funtor de puntos):

$$X(-) : \mathfrak{C} \to ((Sets)),\ X(S) = Hom_{\mathfrak{C}}(S, X).$$

Y un funtor covariante dado por:

$$h_X(-) : \mathfrak{C} \to ((Sets)),\ h_X(S) = Hom_{\mathfrak{C}}(X, S).$$

- El objeto X queda unívocamente determinado salvo isomorfismos por cada uno de estos funtores.

- $Hom_{\mathfrak{C}}(X, Y)$ se corresponde biunívocamente con las transformaciones naturales de $X(-)$ en $Y(-)$ y con las transformaciones naturales de $h_Y(-)$ en $h_X(-)$.

Un functor contravariante $F : \mathfrak{C} \to ((Sets))$ se dice *representable* si existe $X \in \mathfrak{C}$ tal que $F \simeq X(-)$, y si F es covariante, se dice *representable* si existe $X \in \mathfrak{C}$ tal que $F \simeq h_X(-)$

- Si un functor es representable su representante es único salvo isomorfismos.

- Si no es representable cabe la posibilidad de construir una categoría más amplia que $\mathfrak{C}$ en la que lo sea.

Si X representa F, el a de $F(X)$ correspondiente a la identidad $1_X \in Hom_{\mathfrak{C}}(X,X) \simeq F(X)$ se llama aplicación universal. De la definición se sigue que el par $(X,a),\ a \in F(X)$ queda unívocamente caracterizado, salvo isomorfismos, en el caso contravariante por la propiedad:

$$\forall S \in Ob(\mathfrak{C}),\ \forall b \in F(S),\ \exists \beta : S \to X \text{ único} \mid F(\beta)(a) = b$$

y en el caso covariante por:

$$\forall S \in Ob(\mathfrak{C}),\ \forall b \in F(S),\ \exists \beta : X \to S \text{ único} \mid F(\beta)(a) = b.$$

Ejemplos 5.1.–

Ejemplo. 5.1.1.- Si $\mathfrak{C}$ es una categoría de conjuntos con una estructura, grupos, K-espacios vectoriales, K-álgebras, etcétera, para cada conjunto C podemos considerar el funtor:

$$H_C : \mathfrak{C} \to ((Sets)),\ H_C(S) = Aplic(C,S).$$

El funtor es representable si y solo si existen un par (L_C, a), con $a : C \to L_C$ una aplicación tal que para todo objeto S y toda aplicación $b : C \to S$ existe un único morfismo $\beta : L_C \to S$ tal que $\beta a = b$.
Obsérvese que:

- Si $\mathfrak{C}$ es la categoría de grupos, L_C es el grupo libre generado por C.
- Si $\mathfrak{C}$ es la categoría de K -espacios vectoriales, L_C es el espacio vectorial de las combinaciones lineales formales de elementos de C con coeficientes en K.
- Si $\mathfrak{C}$ es la categoría de K- álgebras, L_C es el anillo de polinomios en los elementos de C con coeficientes en K.
- Si $\mathfrak{C}$ es la categoría de espacios topológicos, L_C es C con la topología discreta.

Ejemplo. 5.1.2.- En la categoría de espacios vectoriales sobre un cuerpo: dados dos espacios V y W el funtor $Bihom(V \times W, -)$ que asocia a cada espacio T las aplicaciones bilineales de $V \times W$ en T es covariante y representable, su representante es $V \bigotimes W$ y la aplicación universal

$$a : V \times W \to V \bigotimes W,\ a(v,w) = v \otimes w$$

es decir, el producto tensorial queda caracterizado porque para toda aplicación bilineal $F : V \times W \to T$ existe un único homomorfismo $f : V \bigotimes W \to T$ tal que $F = fa$.

Ejemplos 5.2.– [Límites y colímites] Un *esquema de diagrama* es un par de conjuntos:

$$\mathcal{E} = (I, \Delta),\ \delta \subset I \times I.$$

diagrama en una categoría $\mathfrak{C}$ sobre el esquema de diagrama $\mathcal{E}$ es un par:

$$\mathcal{D}_{\mathcal{E}} = (\{D_i\}_{i\in I}, \{d_{i,j}\}_{(i,j)\in\Delta}),\ D_i \in Ob(\mathfrak{C}),\ d_{i,j} \in Hom_{\mathfrak{C}}(D_i, D_j).$$

Un *morfismo de diagramas*, $F : \mathcal{A}_{\mathcal{E}} \to \mathcal{B}_{\mathcal{E}}$ sobre el mismo esquema $\mathcal{E} = (I, \Delta)$ es una familia de morfismos, $f_i : A_i \to B_i,\ \forall i \in I$ tales que $\forall\ (i, j) \in \Delta$ los diagramas:

$$\begin{array}{ccc} A_i) & \xrightarrow{f_i} & A_j \\ \downarrow{\scriptstyle a_{i,j}} & & \downarrow{\scriptstyle f_j} \\ B_i & \xrightarrow{b_{i,j}} & B_j \end{array}$$

sean conmutativos. Obviamente los diagramas sobre un esquema $\mathcal{E}$ y sus morfismos forman una categoría. Dado un diagrama $\mathcal{D}_{\mathcal{E}}$, podemos considerar los funtores $\mathcal{L}_{\mathcal{D}},\ \mathcal{C}_{\mathcal{D}}$ de $\mathfrak{C}$ en la categoría de conjuntos, dados por:

- $\mathcal{L}_{\mathcal{D}}(X) = \{(f_i)_{i\in I} \in \prod Hom\mathfrak{C}(D_i, X) \mid f_j d_{i,j} = f_i\ \forall (i, j) \in \delta\}$,
- $\forall g : X \to Y,\ \mathcal{L}_{\mathcal{D}}(g)((f_i)_{i\in I}) = (gf_i)_{i\in I}$,

y por:

- $\mathcal{C}_{\mathcal{D}}(X) = \{(f_i)_{i\in I} \in \prod Hom\mathfrak{C}(X, D_i) \mid d_{i,j} f_i = f_j\ \forall (i, j) \in \delta\}$,
- $\forall g : Y \to X,\ \mathcal{L}_{\mathcal{D}}(g)((f_i)_{i\in I}) = (f_i g)_{i\in I}$.

Si el funtor $\mathcal{L}_{\mathcal{D}}$ es representable, su representante se llama, *límite, límite directo o límite inductivo* del diagrama $\mathcal{D}$. El representante, si existe, del funtor $\mathcal{C}_{\mathcal{D}}$ se llama *colímite, límite inverso o límite proyectivo* del diagrama $\mathcal{D}$.

El límite de un diagrama $\mathcal{D}_{\mathcal{E}} = (\{D_i\}_{i\in I}, \{d_{i,j}\}_{(i,j)\in\Delta})$ es por tanto un par:

$$\varinjlim \mathcal{D} = (L, (f_i)_{i\in I}),\ L \in Ob(\mathfrak{C}),\ f_i : D_i \to L,\ \forall i \in I$$

tal que :

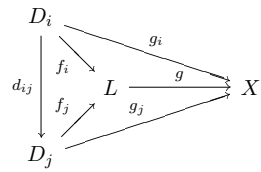
1. $\forall (i,j) \in \Delta, \quad f_j d_{i,j} = f_i$.

2. $$\forall (X, (g_i)_{i\in I}),\ X \in Ob(\mathfrak{C}),\ g_i : D_i \to L,\ \forall i \in I$$

   tales que

   $$\forall (i,j) \in \Delta, \quad g_j d_{i,j} = g_i$$

   existe un único morfismo $g : L \to X$ tal que $\forall i \in I,\ g f_i = g_i$.



Invirtiendo las flechas tenemos el límite inverso, que es un par:

$$\varprojlim \mathcal{C} = (C, (f_i)_{i\in I}),\ C \in Ob(\mathfrak{C}),\ f_i : C \to D_i,\ \forall i \in I$$

tal que :

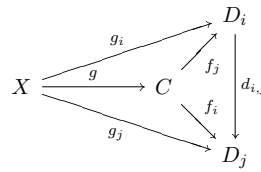
1. $\forall (i,j) \in \Delta, \quad d_{i,j} f_i = f_j$

2. $$\forall (X, (g_i)_{i\in I}),\ X \in Ob(\mathfrak{C}),\ g_i : X \to D_i,\ \forall i \in I$$

   tales que

   $$\forall (i,j) \in \Delta, \quad d_{i,j} g_i = g_j$$

   existe un único morfismo $g : X \to C$ tal que $\forall i \in I,\ f_i g = g_i$



Para una categoría de objetos con una estructura y unas condiciones adicionales razonables, los límites directo e inverso existen y se construyen como sigue:

Límite inverso Puesto que los D_i son conjuntos, se puede construir su producto cartesiano y tomar:

$$L = \{(x_i)_{i\in I} \in \prod_{i\in I} D_i \mid d_{i,j}(x_i) = x_j,\ \forall (i,j) \in \Delta\}$$

y las aplicaciones inducidas por las proyecciones.

Límite directo . Si δ define una relación de orden filtrante por la derecha en I, y si $\mathcal{D}$ es conmutativo es decir:

$$\forall\ i,j,k \in I, (i,j) \in \Delta, (j,k) \in \Delta \Rightarrow d_{i,k} = d_{j,k}d_{i,j},\ \forall i \in I,\ d_{i,i} = 1_{D_i}$$

Podemos construir en la unión disjunta de los D_i, $\bigsqcup_{i\in I} D_i$ la relación de igualdad:

$$\forall\ x_i \in D_i, x_j \in D_j, x_i \sim x_j \Leftrightarrow \exists k \in I,\ (i,k) \in \Delta,\ (j,k) \in \Delta\ d_{i,k}(x_i) = d_{j,k}(x_j)$$

Entonces

$$C = \bigsqcup_{i\in I} D_i/\sim$$

con las aplicaciones composición de las inclusiones y la aplicación natural de paso al cociente. Esta construcción se puede hacer omitiendo la condición de ser Δ una relación de orden y modificando la definición de la relación.

Ejemplo. 5.2.1.- El *producto directo* es el límite de un diagrama sin morfismos. Dada una familia de objetos de $\mathfrak{C}$, $\{C_i\}_{i\in I}$ si el funtor $F : \mathfrak{C} \to ((Sets))$

$$F(T) = \prod_{i\in I} Hom_{\mathfrak{C}}(T, C_i)$$

es representable, su representante se llama producto de la familia y se escribe como $\prod_{i\in I} C_i$. La aplicación universal es la familia de proyecciones:

$$a = (\pi_j)_{j\in I}, \pi_j : \prod_{i\in I} C_i \to C_j$$

de modo que para cada objeto de $\mathfrak{C}$ y cada familia de morfismos $b = (b_i : T \to C_i)_{i\in I}$ existe un único morfismo $\beta : T \to \prod_{i\in I} C_i$ tal que:

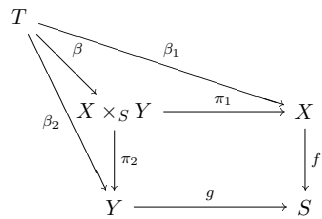
$$b = F(a) \Leftrightarrow b_j = \pi_j\beta\ \forall j \in I$$

Es interesante observar que $\prod_{i\in I} C_i$ no está bien definido, ya que el objeto descrito en la definición está determinado salvo isomorfismo, lo que sabemos es que entre cada dos determinaciones del objeto hay un isomorfismo único con la propiedad de conmutar con las proyecciones.

Aquí tenemos también un ejemplo de como un funtor no representable puede hacerse representable ampliando su categoría inicial, el funtor producto de una familia infinita no es representable en una categoría de K-espacios vectoriales de dimensión finita pero sí lo es en la categoría de K-espacios vectoriales.

Ejemplo. 5.2.2.- Si en la categoría $\mathfrak{C}/S$ existe el producto de un par de objetos $f : X \to S$, $g : Y \to S$ este producto se llama *producto fibrado* de X e Y sobre S y se representa por $X \times_S Y$. $X \times_S Y$ queda unívocamente caracterizado, salvo isomorfismos, por las propiedades siguientes:

- Existen morfismos $\pi_1 : X \times_S Y \to X,\ \pi_2 : X \times_S Y \to Y$, tales que $f\pi_1 = g\pi_2$.
- Para cada par de morfismos $\beta_1 : T \to X,\ \beta_2 : T \to Y$, tales que $f\beta_1 = g\beta_2$ existe un único morfismo $\beta = \beta_1 \times_S \beta_2 : T \to X \times_S Y$ tal que $\pi_1\beta = \beta_1,\ \pi_2\beta = \beta_2$.



Como hemos dicho en el ejemplo anterior, el producto fibrado, si existe, no está unívocamente determinado. De la caracterización anterior está claro también que es funtorial en las dos variables módulo isomorfismos. A veces se puede dar un criterio que permite elegir un producto fibrado para cada par de objetos, por ejemplo:
Si $\mathfrak{C}$ es una categoría de conjuntos con una estructura, se puede elegir un producto fibrado de $f : X \to S, g : Y \to S$ dado por:

$$X \times_S Y = \{(x, y) \in X \times Y \quad f(x) = g(y)\}$$

En particular si X e Y son subconjuntos de S su producto fibrado es $X \cap Y$.
Observemos que el producto fibrado se puede considerar también como el límite del diagrama.

$$\mathcal{D} = X \longrightarrow S \longleftarrow Y$$

Ejemplo. 5.2.3.- Dado un morfismo $f : S \to T$ podemos construir para cada objeto de $\mathfrak{C}/T$, $(X \to T)$ su (*imagen recíproca*) $f^*(X \to T)$ por:

- $f^*(X \to T) = (\pi_2 : X \times_T S \to S)$

- Dado un morfismo g en $\mathfrak{C}/T$ de $\alpha : X \to T$ a $\beta : Y \to T$, se tiene que $f^*(g) = \pi_2 \times_T g\pi_1 : X \times_T S \to Y \times_T S$.

y la imagen recíproca está determinada salvo isomorfismos, por tanto, al contrario que la imagen directa, no es un funtor a menos que, como sucede en la mayoría de las categorías, podamos elegir de modo canónico un representante del producto fibrado.

Ejemplo. 5.2.4.- Al igual que el producto directo, el *coproducto o suma directa* es el colímite de un diagrama sin morfismos. Dada una familia de objetos de $\mathfrak{C}$, $\{C_i\}_{i\in I}$ si el funtor $F : \mathfrak{C} \to ((Sets))$

$$F(T) = \prod_{i\in I} Hom_{\mathfrak{C}}(C_i, T)$$

es representable, su representante se llama *coproducto* de la familia y se escribe como $\coprod_{i\in I} C_i$. La aplicación universal es la familia de secciones:

$$q = (q_j)_{j\in I}, q_j : C_j \to \coprod_{i\in I} C_i$$

de modo que para cada objeto de $\mathfrak{C}$ y cada familia de morfismos $b = (b_i : C_i \to T)_{i\in I}$ existe un único morfismo $\beta : \coprod_{i\in I} C_i \to T$ tal que:

$$b = F(q) \Leftrightarrow b_j = \beta q_j,\ \forall j \in I.$$

Del mismo modo que en el ejemplo anterior se define el coproducto fibrado como el coproducto en la categoría relativa $\mathfrak{C}/S$. El coproducto de una familia de conjuntos es su unión disjunta, el de una familia de espacios topológicos es su suma topológica. El coproducto fibrado de subconjuntos de un conjunto es su unión, y el coproducto de dos K-álgebras respecto sus morfismos estructurales es su producto tensorial.

Ejemplo. 5.2.5.- Si $\mathcal{P}$ es un prehaz de conjuntos sobre un espacio topológico X y $x \in X$ podemos considerar el diagrama:

$$\mathcal{D}_x = (\{\mathcal{P}(U)\}_{x\in U}, \{\rho_{V,U}\}_{x\in U\subset V}).$$

Entonces $\mathcal{P}_x = \varinjlim(\mathcal{D}_x)$ recibe el nombre de *fibra del prehaz* $\mathcal{P}$ en x. Como hemos visto antes, la construcción se hace partiendo de la unión disjunta:

$$\mathcal{U}_x = \bigsqcup_{x\in U} \mathcal{P}(U) = \{(U, s) \mid x \in U,\ s \in \mathcal{P}(U)\}$$

y pasando al conjunto cociente por la relación:

$$(U, s) \sim (V, t) \Leftrightarrow \exists W,\ x \in W \subset U \cap V,\ \rho_{U,W}(s) = \rho_{V,W}(t).$$

Cada clase se llama un *germen* en x. El germen de (U, s) se representa por $[s]_x$ y cada elemento del germen se llama *representante* del mismo.
Si $\mathcal{P}$ es un haz de grupos, anillos, etcétera., sus fibras tienen esa estructura, pues para operar dos gérmenes basta elegir representantes con el mismo abierto y operar con ellos. Obviamente la fibra define un funtor ya que a todo morfismo de prehaces se le puede asociar un morfismo en las fibras por la definición de límite.
Usando las fibras se pueden regularizar los prehaces transformándolos en haces. Para cada prehaz de conjuntos, o conjuntos con una estructura, $\mathcal{P}$ se puede construir el *espacio étale* asociado, formando la unión disjunta de sus fibras y la proyección natural:

$$|\mathcal{P}| = \bigsqcup_{x \in X} \mathcal{P}_x,\ \pi : |\mathcal{P}| \to X,\ \pi([s]_x) = x$$

tomando para cada $s \in \mathcal{P}(U)$ la sección de la proyección:

$$\widetilde{s} : U \to |\mathcal{P}|,\ \widetilde{s}(x) = [s]_x$$

y considerando en $|\mathcal{P}|$ la topología final de estas aplicaciones. Así, una base de abiertos de la topología de $|\mathcal{P}|$ está formada por los conjuntos:

$$C_{V,s} = \{[s]_y\}_{y \in V},\ s \in \mathcal{P}(V),$$

y con ella la proyección π es un homeomorfismo local.
Una vez construido el espacio étale, podemos construir un nuevo prehaz, que de hecho es un haz y se denomina *haz asociado al prehaz*, asociando a cada abierto U de X las secciones continuas de π sobre U, es decir:

$$\widetilde{\mathcal{P}}(U) = \{\sigma : U \to |\mathcal{P}| \mid \sigma \text{ continua},\ \pi\sigma = 1_U\}$$

De este modo si $\sigma : U \to |\mathcal{P}|$ es una aplicación:

$$\sigma \in \widetilde{\mathcal{P}}(U) \Leftrightarrow \forall x \in U,\ \exists V, x \in V \subset U,\ \exists s \in \mathcal{P}(V),\ \sigma|_V = \widetilde{s}$$

Se comprueba fácilmente que:

- Si $\mathcal{P}$ es un prehaz de conjuntos con una estructura, $\widetilde{\mathcal{P}}$ es, de modo natural, un haz de conjuntos con la misma estructura.
- Que hay un morfismo canónico $F : \mathcal{P} \to \widetilde{\mathcal{P}}$ dado por $F_U(s) = \widetilde{s}$ pero los F_U no son en general ni inyectivos ni sobre.

- $\mathcal{P}$ es un haz si y solo si $\mathcal{P} = \widetilde{\mathcal{P}}$

Observemos que si llamamos *espacio étale* sobre un espacio topológico X a un par (Y, π) donde Y es un espacio topológico y π es un homeomorfismo local, la categoría de haces sobre X es naturalmente equivalente a la subcategoría completa de $\mathfrak{T}/X$ cuyos objetos son espacios étale. Este es el punto de vista de la teoría de haces de Godement [16], rechazado totalmente por Grothendieck [18], pero que a veces es cómodo usar.

En general se pueden leer más fácilmente las propiedades de un objeto en el funtor de puntos al que representa que en el objeto mismo.

Ejemplos 5.3.–

Ejemplo. 5.3.1.- En geometría algebraica se asocia a cada anillo A un espacio topológico, su *espectro* dado por:

$$Spec(A) = \{\mathfrak{p} \mid \mathfrak{p} \text{ ideal primo de A}\}$$

dotado de la topología (*topología de Zariski*) con base de abiertos:

$$\mathfrak{Z}_A = \{D(f)\}_{f \in A},\ D(f) = \{\mathfrak{p} \in Spec(A) \mid f \notin \mathfrak{p}\}$$

Las correspondencias:

- $A \mapsto Spec(A)$
- $(f : A \to B) \mapsto f^{-1} : Spec(B) \to Spec(A)$

definen un funtor contravariante de la categoría de anillos (conmutativos y homomorfismos unitarios) en la de espacios topológicos.
Podemos definir un prehaz sobre $Spec(A)$ asignando a cada abierto de la base $D(f)$ el anillo de fracciones:

$$A_f = \{\frac{a}{f^n} \mid a \in A,\ n \in \mathbb{N}\}$$

a este prehaz se le asocia su haz asociado, $\widetilde{A}$, y el par $(Spec(A), \widetilde{A})$ se llama un *esquema afín*. La categoría de esquemas afines es isomorfa a la categoría de anillos.
El *grupo lineal* es el esquema afín:

$$GL_n = Spec(\mathbb{Z}[(x_{i,j}), t]/(det(x_{i,j})t - 1)$$

en el que no se aprecia la estructura de grupo. En cambio para un anillo A:

$$GL_n(Spec(A)) = Hom_{Spec(\mathbb{Z})}(Spec(A), GL_n) =$$

$$= Hom(\mathbb{Z}[(x_{i,j}), t]/(det(x_{i,j})t - 1), A) = GL_n(A).$$

Ya que los homomorfismos de anillos de $\mathbb{Z}[(x_{i,j}), t]/(det(x_{i,j})t - 1)$ en A se obtienen dando valores a las $(x_{i,j})$ y a t que anulen a $det(x_{i,j})t - 1$, es decir, se corresponden con las matrices $n \times n$ de elementos de A con determinante inversible.

Ejemplo. 5.3.2.- La definición formal de esquema en grupos, grupo algebraico, grupo analítico, grupo de Lie etcétera sigue siempre el siguiente proceso:
Se parte de una categoría $\mathfrak{G}$ con productos finitos y un objeto cero U, es decir, un objeto tal que

$$\forall S \in Ob(\mathfrak{G}),\ Hom_{\mathfrak{G}}(U, S) = \{0\},\ Hom_{\mathfrak{G}}(S, U) = \{e\}$$

. Entonces una estructura de grupo en un objeto G de esa categoría es una terna de morfismos:

- $\mu : G \times G \to G$
- $e : U \to G$
- $p : G \to G$

correspondientes a producto, unidad e inverso, que verifican las propiedades usuales:

- Asociativa: el diagrama:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mu \times 1_G} & G \times G \\ \downarrow{\scriptstyle 1_G \times \mu} & & \downarrow{\scriptstyle \mu} \\ G \times G & \xrightarrow{\mu} & G \end{array}$$

  es conmutativo

- Elemento neutro: los diagramas:

$$\begin{array}{ccc} G & \xrightarrow{0 \times 1_G} & U \times G \\ \downarrow{\scriptstyle 1_G} & & \downarrow{\scriptstyle e \times 1_G} \\ G & \xleftarrow{\mu} & G \times G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{1_G \times 0} & G \times U \\ \downarrow{\scriptstyle 1_G} & & \downarrow{\scriptstyle 1_G \times e} \\ G & \xleftarrow{\mu} & G \times G \end{array}$$

  son conmutativos

- Inverso: los diagramas:

$$\begin{array}{ccc} G & \xrightarrow{1_G\times 1_G} & G\times G \\ \downarrow{\scriptstyle e,0} & & \downarrow{\scriptstyle p\times 1_G} \\ G & \xleftarrow{\mu} & G\times G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{1_G\times 1_G} & G\times G \\ \downarrow{\scriptstyle e,0} & & \downarrow{\scriptstyle 1_G\times p} \\ G & \xleftarrow{\mu} & G\times G \end{array}$$

son conmutativos.

Esta definición significa que para cada objeto T el conjunto $Hom_{\mathfrak{G}}(T,G)$ con la operación:

$$(f.g)=\mu(f,g),\ (f,g):T\to G\times G,\ \pi_1.(f,g)=f,\ \pi_2.(f,g)=g$$

es un grupo. Si los objetos de la categoría son conjuntos, la definición lleva consigo que se define una estructura de grupo en todos ellos.

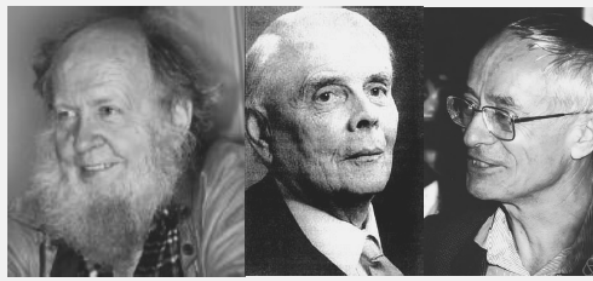
Ejemplo. 5.3.3.- La acción de un grupo de $\mathfrak{G}$ sobre un objeto X, se define como un morfismo:

$$\sigma : G\times X\longrightarrow X$$

con las propiedades usuales (presentadas en forma de diagrama como en el ejemplo anterior) y significa que para todo objeto T de $\mathfrak{G}$, el grupo $Hom_{\mathfrak{G}}(T,G)$ actúa sobre el conjunto $Hom_{\mathfrak{G}}(T,X)$. Podemos construir ahora un nuevo funtor:

$$F:\mathfrak{G}\longrightarrow((Sets)),\ F(T)=Hom_{\mathfrak{G}}(T,X)/Hom_{\mathfrak{G}}(T,G)$$

que en las categorías citadas como ejemplos no es representable, y de este problema surge el concepto de Stack como objeto de una categoría más amplia en la que se tiene la representabilidad de este funtor.



The first comprehensive exposition of the theory of profinite groups appeared in the book 'Cohomologie Galoisienne' by J-P. Serre in 1964.

L. Ribes

6. Extensiones infinitas

Definición 6.1.– *Un* grupo topológico *es un grupo G dotado de una topología de modo que:*

1. *La aplicación $G \times G \to G,\ (g,h) \mapsto gh$ es continua.*
2. *La aplicación $G \to G,\ g \mapsto g^{-1}$ es continua.*

Si G es un grupo topológico se verifica que para todo $g \in G$ la aplicación

$$\tau_a : G \to G,\ \tau_a(x) = ax$$

es un homeomorfismo. En consecuencia:

- Si H es un subgrupo abierto de G, todas las clases gH son abiertas, por tanto H es cerrado. Recíprocamente, si H es un subgrupo cerrado de índice finito, H es también abierto.
- Si un subgrupo de G contiene a un subgrupo abierto es también abierto.
- Si $\{N_i\}_{i\in I}$ es un sistema fundamental de entornos de 1, los $\{gN_i\}_{i\in I}$ son un sistema fundamental de entornos de g.
- Una familia de subconjuntos de G, $\{S_i\}_{i\in I}$ es un sistema fundamental de entornos de $1 \in G$ para una topología con la cual G es un grupo topológico si y solo si:

1. $1 \in S_i,\ \forall i \in I.$
2. $\forall i,j \in I,\ \exists\, k \in I,\ S_k \subset S_i \cap S_j.$
3. $\forall i \in I,\ \exists\, j \in I,\ S_j.S_j \subset S_i.$
4. $\forall i \in I,\ \exists\, j \in I,\ S_j \subset \S_i^{-1}.$
5. $\forall i \in I,\ \forall g \in G \exists\, j \in I,\ S_j \subset g\S_i g^{-1}.$

Proposición 6.2.– *En la categoría de grupos topológicos existe el límite proyectivo.*

Demostración: en la construcción que dimos en 5.2 si $\mathcal{G} = (\{G_i\}_{i\in I}, \{g_{i,j}\}_{(i,j)\in\Delta})$ es un diagrama de grupos, $\prod_{i\in I} G_i$ tiene una estructura natural de grupo topológico con la topología producto de las de los G_i. Las proyecciones son homomorfismos continuos y $\varprojlim \mathcal{G}$ es un subgrupo de $\prod_{i\in I} G_i$ que con la topología inducida es un grupo topológico.

□

Proposición 6.3.– *El límite proyectivo de un diagrama de grupos finitos con la topología discreta es un grupo topológico compacto y totalmente desconectado.*

Demostración: si $\mathcal{G} = (\{G_i\}_{i\in I}, \{g_{i,j}\}_{(i,j)\in\Delta})$ es un diagrama de grupos finitos con la topología discreta, $\prod_{i\in I} G_i$ es compacto (Teorema de Tychonoff). Veamos que $\varprojlim \mathcal{G} \subset \prod_{i\in I} G_i$ es cerrado y por tanto compacto.

Si $\mathbf{x} = (x_i)_{i\in I} \notin \varprojlim \mathcal{G}$ entonces $\exists (i,j) \in \delta, x_j \neq g_{i,j}(x_i)$ y como la topología de los G_i es la discreta, si llamamos π_i a las proyecciones, $E_{i,j} = \pi_i^{-1}(x_i) \cap \pi_j^{-1}(x_j)$ es un entorno abierto de $\mathbf{x}$, que no corta a $\varprojlim \mathcal{G}$.

La condición de totalmente desconectado equivale a que para cada por de elementos, hay un subconjunto abierto-cerrado que contiene a uno de ellos y no contiene al otro, en un grupo basta probar que si $g \neq 1$ existe un subgrupo abierto que no contiene a g, ya que todo subgrupo abierto es cerrado. En nuestro caso es trivial porque si $e_i \in G_i$ es el uno y $\mathbf{e}$ es el uno de $\varprojlim \mathcal{G}$,

$$\mathbf{x} = (x_i)_{i\in I} \neq \mathbf{e} \Leftrightarrow \exists i \in I,\ x_i \neq e_i \Leftrightarrow \mathbf{x} \notin \pi_i^{-i}(e_i) = Ker\pi_i$$

□

Proposición 6.4.– *Todo grupo topológico G compacto y totalmente desconectado, es límite proyectivo de un diagrama de grupos finitos con la topología discreta.*

Demostración: como G es un grupo topológico podemos construir el conjunto $\mathcal{U}(G) = \{H_i\}_{i\in I}$ de subgrupos abiertos invariantes de G, todo subgrupo abierto de G es cerrado y como G es compacto es de índice finito. Luego los G/H_i son todos grupos finitos. Sea

$\delta = \{(i,j) \in I \times I \mid H_i \subset H_j\}(i)$, podemos construir el diagrama de grupos finitos:

$$\mathcal{P} = (\{P_i\}_{i\in I}, \{p_{i,j}\}_{(i,j)\in\Delta}),\ P_i = G/H_i,\ p_{i,j} : G/H_i \to G/H_j . p_{i,j}(g.H_i) = g.H_j$$

dotando estos grupos de la topología discreta, los homomorfismos naturales:

$$n_i : G \to G/H_i,\ n_i(g) = g.H_i$$

son continuos porque los H_i son abiertos. Entonces por la definición de límite proyectivo existe un único homomorfismo continuo que también es abierto: $n : G \to \varprojlim \mathcal{P}$ tal que:

$$\forall i \in I, \pi_i n = n_i \Leftrightarrow n(g) = (g.H_i)_{i\in I}$$

Tenemos que probar que n es un isomorfismo de grupos topológicos. La suprayectividad de n es un ejercicio simple, es más difícil probar la inyectividad.

Para ver que n es inyectiva basta hay que probar que $\bigcap_{i\in I} H_i = u$ donde u es el uno de G, o lo que es lo mismo que:

$$g \in G,\ g \neq u \Rightarrow \exists i \in I,\ g \notin H_i.$$

Como G es totalmente desconectado, existe un abierto-cerrado V, tal que $u \in V,\ g \notin V$. Sea $W = V \cap V^2$. Como V es cerrado, es compacto y V^2 también, luego W es compacto. Si $x \in W$, como también $u \in W$, el producto en G es continuo, V es abierto y $xu = x$, existen entornos de x y u en V, N_x, M_x tales que $N_x.M_x \subset V$ y obviamente $N_x.M_x \subset V^2$, luego $N_x \cap M_x \subset W$. Los $\{N_x\}_{x\in U}$ forman un recubrimiento abierto, que tiene un subrecubrimiento finito $\{N_{x_1}...N_{x_n}\}$. Si $M = \bigcap_1^n M_{x_i}$, M y $P = M \cap M^{-1}$ son entornos abiertos de u en V. Además:

$$V.P \subset V.M = \bigcup_1^n N_{x_i}.M \subset \bigcup_1^n N_{x_i}.M_{x_i} \subset V.$$

Luego por inducción $V.P^n \subset V, \forall n \in \mathbb{N}$. Sea $H = \bigcup_1^\infty P^r$ el subgrupo de G generado por M, $H \subset V$ porque:

$$P \subset V \Rightarrow P^2 = P.P \subset P.V \subset V \text{etcétera.}$$

y como $M \subset P$ es un entorno abierto de u M es un subgrupo abierto y como G es compacto, H es de índice finito, luego tiene un número finito de conjugados. La intersección de los conjugados de H es un subgrupo invariante abierto, y por tanto de índice finito contenido en V y que por tanto no contiene a g □

Los resultados anteriores van encaminados a caracterizar los grupos de Galos de extensiones infinitas. Observemos que si K es una extensión galoisiana de k y M es una extensión intermedia se verifica que:

- K es una extensión galoisiana de M, ya que es separable y $\forall a \in K$ el polinomio mínimo de a sobre M es un divisor del polinomio mínimo de a sobre k y por tanto tiene todas sus raíces en K.

- Todo k-homomorfismo $f : M \to K$ se extiende a un k automorfismo de K, usando Zorn es trivial que f se extiende a un homomorfismo inyectivo $\overline{f} : K \to K$. $\overline{f}$ es sobre porque $\forall a \in K$ si su polinomio mínimo es de grado n tiene n raíces en K, luego tiene n raíces en $Im\overline{f}$ y una de ellas es necesariamente $\overline{f}(\alpha)$.

- El homomorfismo de restricción $Gal_k(K) \to Gal_k(M)$ es sobre. Trivial del punto anterior.

- Si $M|k$ es finita de k existe una extensión galoisiana finita de k, $M^*,\ M \subset M^* \subset K$. En efecto por el teorema del elemento primitivo, $M = k(\alpha),\ \alpha \in K$, entonces si M^* es el cuerpo de descomposición del polinomio mínimo de α, $M \subset M^* \subset K$ y $M^*|k$ es galoisiana.

Si consideramos ahora el conjunto $\mathcal{L} = \{L_i\}_{i \in I}$ de todas las extensiones galoisianas finitas de k contenidas en K, por el teorema fundamental de la Teoría de Galois si $L_i \subset L_j$ tenemos un homomorfismo suprayectivo:

$$\tau_{j,i} : Gal_k(L_j) \to Gal_k(L_i) \simeq Gal_k(L_j)/Gal_{L_i}(L_j)$$

Si $\mathcal{G}$ es el diagrama de grupos finitos sobre el esquema $\mathcal{E} = (I, \Delta), \Delta = \{(j,i) \in I \times I,\ L_i \subset L_j\}$ dado por:

$$\mathcal{G} = (\{G_i\}_{i \in I}, \{\tau_{j,i}\}_{(j,i) \in \delta}),\ G_i = Gal_k(L_i) \forall i$$

se verifica que:

Teorema 6.5.– *$Gal_k(K) = \varprojlim \mathcal{G}$ y en consecuencia $Gal_k(K)$ es un grupo profinito y admite una topología con la cual es compacto y totalmente desconectado.*

Demostración: Por la definición de límite proyectivo, y dado que existen homomorfismos continuos

$$\sigma_i : Gal_k(K) \to Gal_k(L_i),\ \sigma_i(f) = f|_{L_i}$$

con $\tau_{j,i}\sigma_j = \sigma_i,\ \ \forall (j,i) \in \Delta$, existe un homomorfismo $\sigma Gal_k(K) \to \varprojlim \mathcal{G}$ tal que $\forall i \in I, \pi_i \sigma = \sigma_i$, este homomorfismo está dado por:

$$\forall f \in Gal_k(K),\ \sigma(f) = (f|_{L_i})_{i \in I}$$

hay que probar que σ es un isomorfismo.

Como $K^{Gal_k(K)} = k$:

$$\forall f \in Gal_k(K),\ \exists \alpha \in K \setminus k,\ f(\alpha) \neq \alpha.$$

Y como existe una extensión galoisiana finita de k, L_i, tal que $k(\alpha) \subset L_i$, es $f|L_i \neq Id$ luego $Ker\sigma = Id$. Trivialmente σ es sobre, porque si $(f_i)_{i\in I} \in \varprojlim \mathcal{G}$ para cada $\alpha \in K \setminus k$ existe un $i_\alpha \in I$ con $k(\alpha) \subset L_{i_\alpha}$, definimos entonces:

$$f(\alpha) = f_{i_\alpha}(\alpha)$$

y es inmediato que $f \in Gal_k(K)$ y $\sigma(f) = (f_i)_{i\in I}$ □

Como consecuencia de este resultado podemos dar una base de entornos del uno de $Gal_k(K)$. En efecto, al ser la topología de $Gal_k(K)$ la inducida por la del producto de los grupos de Galois de las subextensiones galoisianas finitas, si $\pi_i : Gal_k(K) \to Gal_k(L_i)$ es la restricción, teniendo en cuenta que la topología de los $Gal_k(L_i)$ es la discreta, los $\pi_i^{-1}1_{L_i} = Ker\pi_i$ son subgrupos abiertos normales que forman una base de entornos de uno de la topología de $Gal_k(K)$.

Si S es un sistema finito de generadores de $L_i|k$,

$$Ker\pi_i = \{\sigma \in Gal_k(K) \mid \sigma(s) = s \forall s \in S\}.$$

Si T es un subconjunto finito de K, $k(T)$ es una subextensión finita de K y está contenida en una subextensión galoisiana finita L_i, que se puede suponer generada por $S \supset T$, entonces:

$$Ker\pi_i \subset G(T) = \{\sigma \in Gal_k(K) \mid \sigma(s) = s \forall s \in T\}$$

Luego los $G(S)$, con S subconjunto finito de K, forman una base de entornos de uno en $Gal_k(K)$ y son subgrupos abiertos.

Definición 6.6.– *La topología de $Gal_k(K)$ como límite proyectivo, que acabamos de construir, se conoce por* topología de Krull *[22] de $Gal_k(K)$*

Podemos extender ahora el teorema fundamental a extensiones infinitas:

Teorema 6.7.– *[Galois- Krull] Para toda subextensión de Galois de una extensión galoisiana $K|k$ el grupo $Gal_L(K)$ es un subgrupo cerrado de $Gal_k(K)$. Las correspondencias que asocian a cada subextensión L el grupo $Gal_L(K)$ y a cada subgrupo cerrado H de $Gal_k(K)$ la subextensión K^H son inversas una de la otra y definen una biyección entre el conjunto de subgrupos cerrados de $Gal_k(K)$ y el de subextensiones de $K|k$.*
Además, una subextensión L de $K|k$ es galoisiana si y solo si $Gal_L(K)$ es normal, y en este caso $Gal_k(L) \simeq Gal_k(K)/Gal_L(K)$.

Demostración: Para probar el teorema, recordemos que $Gal_k(K)$ es límite proyectivo de los grupos de Galois de sus subextensiones galoisianas finitas L_i con la topología discreta, y que cada $Gal_k(L_i)$ es un grupo cociente finito de $Gal_k(K)$. Tomemos ahora una subextensión finita de K, $F|k$, esta subextension finita está contenida en una de las L_i y el grupo $Gal_F(L_i)$ es un subgrupo de $Gal_k(L_i)$ que tiene una contraimagen $T_F \subset Gal_k(K)$. Como la proyección del límite es continua, T_F es un subgrupo abierto y por tanto cerrado. Obviamente todos los elementos de T_F fijan F y los elementos de $Gal_F(K)$ restringen a elementos de $Gal_F(L_i)$, luego $T_F = Gal_F(K)$ es un subgrupo cerrado de $Gal_k(K)$.

Si $M|k$ es una extensión arbitraria se puede escribir como unión de una familia de extensiones finitas M_j, $Gal_k(M)$ sería intersección de los $Gal_k(M_j)$ y por tanto sería un subgrupo cerrado.

Recíprocamente, si H es un subgrupo de $Gal_k(K)$ podemos construir $M = K^H$, $Gal_M(K)$ es cerrado y contiene a H, y por tanto a su cierre $\overline{H}$. Si probamos que $Gal_M(K) \subset \overline{H}$ sería $Gal_M(K) = \overline{H}$ y si H es cerrado hemos terminado. Si $\sigma \in Gal_M(K) \setminus \overline{H}$ existe un entorno de σ que no corta a H, es decir, existe un subgrupo abierto invariante $G(S)$ de $Gal_k(K)$ tal que

$$\sigma.G(S) \cap H = \emptyset \Leftrightarrow \sigma \notin G(S).H$$

Entonces poe el teorema fundamental de la Teoría de Galois para la extensión galoisiana $k(S)|k$ existe algún elemento $\alpha \in k(S)$ invariante por H pero no por σ, luego $\sigma \notin Gal_M(K)$

□

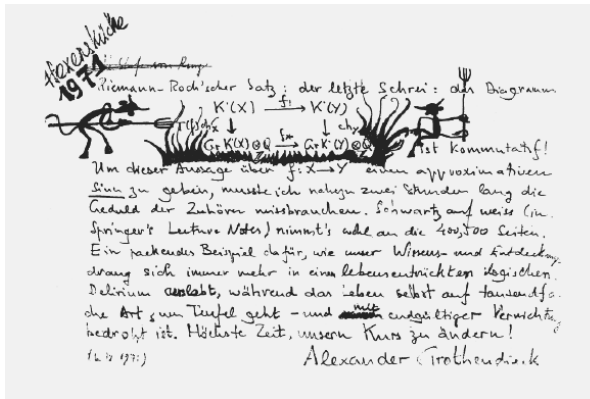
Veamos un ejemplo de grupo de Galois que admite subgrupos que no son cerrados, para probar que el teorema de Krull no es generalización trivial del de Galois. Si consideramos el cuerpo primo de característica p, $F_p = \mathbb{Z}/(p)$, su cierre separable $F_{p,s}$ contiene para cada n una subextensión única $F_{p,n}$ con:

$$[F_{p,s} : F_p] = n,\ Gal_{F_p}(F_{p,s}) \simeq \mathbb{Z}/(n),\ \text{generada por el automorfismo de Frobenius } \sigma(x) = x^p$$

Entonces los homomorfismos de restricción son los habituales:

$$\tau_{m,n} : \mathbb{Z}/(n) \to \mathbb{Z}/(m),\ \tau(r + (n)) = r + (m),\ m|n$$

y el grupo de Galois $Gal_{F_p}(F_{p,s})$ es el límite proyectivo $\widehat{\mathbb{Z}}$ de los $\mathbb{Z}/(n)$ que contiene al grupo $\mathbb{Z}$ que no es subgrupo cerrado.



7. Teoría de Galois-Grothendieck

En esta sección vamos a introducir una Teoría de Galois cuyos objetos no son las extensiones separables de un cuerpo sino las álgebras finitas separables. Ahora la contraparte no son los grupos de automorfismos sino los conjuntos finitos con la acción de un grupo. Comenzamos por tanto con la descripción de los conjuntos con acción de un grupo G o G-conjuntos.

Si G es un grupo llamaremos G-conjunto a todo conjunto con una acción de G, es decir, a un par (X, p) donde X es un conjunto y

$$p : X \times G \to X,\ p(x, g) = xg$$

una aplicación tal que:

- $(xg)h = x(gh)$
- $xe_G = x$ (e_G es la unidad de G).

La acción de un grupo G sobre un conjunto E se dice *simple* si:

$$\forall x \in E,\ \rho_x : G \to E,\ \rho_x(g) = xg \text{ es inyectiva}$$

y se dice *transitiva* si:

$$\forall x, y \in E,\ \exists g \in G,\ xg = y$$

y se dice *trivial* si

$$\forall x \in E,\ \forall g \in G,\ xg = x$$

Un G- morfismo o morfismo equivariante entre dos G-conjuntos es una aplicación que conmuta con la acción

$$\varphi : X \to Y,\ \varphi(xg) = \varphi(x)g$$

La órbita de un elemento $x \in X$ de un G-conjunto es el subconjunto:

$$O_x = \{xg \mid g \in G\}$$

Y el conjunto de órbitas se llama conjunto cociente por la acción de G y se representa por X/G.

Los G-conjuntos y G-morfismos forman una categoría $((G - Sets))$. Como cada conjunto se puede dotar de la acción trivial y toda aplicación es equivariante para la acción trivial, la categoría $((Sets))$ es una subcategoría de la $((G - Sets))$

Si $\rho : G \to H$ es un homomorfismo de grupos, todo H-conjunto X se puede dotar de estructura de G-conjunto por:

$$\forall x \in X,\ g \in G,\ xg = x\rho(g)$$

Todo H- morfismo es también un G- morfismo, tenemos así un funtor:

$$\rho^* : ((H - Sets)) \to ((G - Sets)).$$

También las correspondencias que asocian:

- A cada grupo G la categoría de los G-conjuntos $((G - Sets))$
- A cada homomorfismo $\rho : G \to H$, el funtor

$$\rho^* : ((H - Sets)) \to ((G - Sets))$$

definen un funtor de la categoría de grupos en la de categorías.

Las correspondencias:

$$X \mapsto X/G, f \mapsto f_O,\ f_O(O_x) = O_{f(x)}$$

definen un funtor: $((G - Sets)) \to ((Sets))$.

Consideremos ahora un cuerpo k con su cierre algebraico y su cierre separable $k \subset k_s \subset \overline{k}$, y llamemos $G = Gal_k(k_s)$ al grupo de Galois absoluto de k dotado de la topología de Krull. Si L

es una extensión separable finita de k, $Hom_k(L, k_s)$ es un conjunto finito de $[L : k]$ elementos y hay una acción natural de G sobre este conjunto dada por:

$$G \times Hom_k(L, k_s) \to Hom_k(L, k_s),\ (\sigma, f) \mapsto \sigma.f.$$

Proposición 7.1.– *La acción de G sobre $Hom_k(L, k_s)$ descrita arriba es continua y transitiva supuesto dotado $Hom_k(L, k_s)$ de la topología discreta.*

Demostración: Si f y g son homomorfismos de L en k_s, gf^{-1} es un homomorfismo de $f(L)$ en k_s que extiende a un automorfismo σ de k_s que verifica que $\sigma f = g$ luego la acción es transitiva. Para probar la continuidad basta probar que la contraimagen por la acción de cada elemento $f \in Hom_k(L, k_s)$ es abierta, es decir, que es abierto:

$$\{(\sigma, g) \in Hom_k(L, k_s) \mid \sigma g = f\} = \bigcup_{h \in Hom_k(L,k_s)} \{(\sigma, h) \mid \sigma h = f\}$$

Pero si fijamos (σ_h, h), con $\sigma_h h = f$ y G_f es el estabilizador de f en G:

$$\tau h = f \Leftrightarrow \tau \in \sigma_h G_f$$

Por tanto basta probar que G_f es abierto, pero $G_f = Gal_{f(L)}(k_s)$ que es un subgrupo abierto de G porque L está contenida en una subextension galoisiana. □

Observemos que de la prueba de la proposición se obtiene que:

- Como la acción de G sobre $Hom_k(L, k_s)$ es transitiva, fijo un elemento $f_0 \in Hom_k(L, k_s)$ todo elemento $g \in Hom_k(L, k_s)$ se escribe como $g = \sigma f_0$ pero no en forma única porque si G_0 es el estabilizador de f_0:

  $$\sigma f_0 = \tau f_0 \Leftrightarrow \tau^{-1}\sigma f_0 = f_0 \Leftrightarrow \tau^{-1}\sigma \in G_0 \Leftrightarrow \sigma G_0 = \tau G_0$$

  En consecuencia la aplicación:

  $$T : Hom_k(L, k_s) \to G_0/G,\ T(g) = \sigma G_0 \Leftrightarrow g = \sigma G_0$$

  es un isomorfismo de G-conjuntos.

- Si $L|k$ es galoisiana y finita, G_0 es un subgrupo invariante de índice finito de G y $Hom_k(L, k_s)$ es isomorfo al cociente G/G_0 con la G-acción natural.

Si L y M son extensiones separables finitas de k y $\varphi : L \to M$ es un k-homomorfismo, tenemos una aplicación:

$$\varphi^* : Hom_k(M, k_s) \to Hom_k(L, k_s),\ \varphi^*(f) = f\varphi$$

que es equivariante. Por tanto tenemos un funtor F de la categoría de extensiones separables de k y k- homomorfismos en la subcategoría completa de la categoría de G- conjuntos finitos, cuyos objetos son los G-conjuntos finitos con acción continua y transitiva de G.

Proposición 7.2.– *El funtor F es una equivalencia de categorías.*

Demostración: Para probar la proposición hemos de demostrar que F es fiel, completo y esencialmente suprayectivo, es decir, que para todo par de extensiones separables, $L,\ M$, de k:

$$F : Hom_k(L, M) \to Hom_G(Hom_k(M, k_s), Hom_k(L, k_s))$$

es biunívoca y para todo G-conjunto C con una acción de G continua y transitiva existe una extensión separable L de k, tal que $Hom_k(L, k_s)$ es G-isomorfo a C.

Probemos primero que F es esencialmente suprayectivo. Dado el G -conjunto C, sea $c \in C$ y sea $H \subset G$ el estabilizador de c que es un subgrupo abierto de G por la continuidad de la acción y por tanto cerrado, $k_s^H = L$ es una extensión separable finita de k y tenemos G isomorfismos de C y de $Hom_k(L, k_s)$ en H/G, luego ambos G-conjuntos son isomorfos.

Para probar la primera condición observemos que al ser transitiva la acción de G sobre $Hom_k(M, k_s)$, un G -homomorfismo

$$\theta : Hom_k(M, k_s) \to Hom_k(L, k_s)$$

queda determinado por la imagen de un único elemento. Elegimos $f_0 \in Hom_k(M, k_s)$ y θ queda determinado por $\theta(f_0)$. Como θ es equivariante, los elementos del estabilizador H de f_0, fijan también $\theta(f_0)$, si U es el estabilizador de este elemento tenemos una inclusión $H \subset U$ que lleva consigo otra $k_s^U \subset k_s^H$ pero $k_s^U = \theta(f_0)(L)$ y $k_s^H = f_0(M)$ tenemos entonces un k -homomorfismo de L en M, $f_0^{-1}\theta(f_0)$ que es el único que se aplica sobre θ.

□

Observaciones 7.3.– La proposición anterior es válida si cambiamos k_s por cualquier extensión galoisiana M de k y las extensiones separables por subextensiones de M.

Ahora substituiremos las extensiones separables de k por un cierto tipo de k- álgebras para extender la equivalencia a todos los G conjuntos finitos con acción continua de G.

Definición 7.4.– *Llamamos k- álgebra finita a toda k-álgebra que es de dimensión finita como k-espacio vectorial. Si A es una k-álgebra finita, a la dimensión de A como k-espacio vectorial $[A:k] = dim_k(K)$ se le llama grado de A. Una k álgebra finita étale es una k- álgebra producto de un número finito de extensiones separables finitas de k.*

Ejemplos 7.5.– Ejemplo. 7.5.1.- Si $f(x) \in k[x]$ y

$$f(x) = \prod_{i=1}^{n} f_i(x)^{r_i}$$

es la descomposición de $f(x)$ en producto de irreducibles, $A = k[x]/(f(x))$ es una k-álgebra finita que se descompone en producto de k-álgebras locales:

$$A \simeq \prod_{i=1}^{n} k[x]/(f_i(x)^{r_i})$$

A es un álgebra étale si y solo si $r_i = 1, \forall i$ y los f_i son todos separables, es decir, si $f(x)$ es separable en $k[x]$.

Ejemplo. 7.5.2.- No todas las k- álgebra finitas son como la del ejemplo anterior. Por ejemplo $k[x,y]/(x,y)^2$ no se puede escribir nunca como un álgebra cociente de un anillo de polinomios en una variable.

Ejemplo. 7.5.3.- Una k -álgebra A finita y sin divisores de cero es un cuerpo, ya que si $a \in A,\ a \neq 0$, a es algebraico sobre k y su polinomio mínimo es irreducible, en particular si el polinomio mínimo de a es:

$$f(x) = b_0 + b_1 x + ... + x^n$$

entonces $b_0 \neq 0$ y:

$$a.(\frac{-1}{b_0})(b_1 + b_2 a + ... + a^{n-1}) = 1$$

y a es inversible.
En consecuencia si A es una k-álgebra separable, $A \overset{\tau}{\simeq} L_1 \times ... \times L_r$, y F es una extensión de K, si llamamos:

$$q_i : L_i \to A,\ q_i(l_i) = \tau(0,..,l_i,..,0)$$

para cada k-Homomorfismo $f : A \to K$ existe un único $i,\ 1 \leq i \leq r$,tal que $fq_i \neq 0$, ya que si $fq_i \neq 0, fq_i \neq 0$, sería:

$$fq_i(1_{L_i}) \neq 0,\ fq_j(1_{L_j}) \neq 0,\ (fq_i(1_{L_i}))(fq_j(1_{L_j})) = f(q_i(1_{L_i}).q_j(1_{L_j})) = 0$$

Como cada homomorfismo $g : L_i \to K$ induce un homomorfismo $g.\pi_i : A \to K$ tenemos una correspondencia biunívoca entre $Hom_k(A, K)$ y la unión disjunta de los $Hom_k(L_i, K)$.

Teorema 7.6.– *[Teorema de Galois-Grothendieck] El funtor F de la categoría de k -álgebras étale en la categoría de G- conjuntos finitos con acción continua, dado por:*

$$F(A) = Hom_k(A, k_s),\ F(\varphi)(f) = \varphi.f$$

es una equivalencia de categorías.

El teorema es consecuencia inmediata de la proposición 7.2 y del ejemplo anterior.

Observemos también que el teorema sigue siendo cierto si cambiamos el cierre separable por cualquier extensión galoisiana M de k y reducimos la categoría inicial a la de k- álgebras étale producto de subcuerpos de M.

I asked Weyl why he had published his 1923/24 papers Analysis Situs Combinatorio, in the Revista Matematica Hispano- Americana, and in Spanish! Weyl replied that he did not want to draw attention to the publication, that his colleagues should not read them.

Beno Eckmann

H. Weyl, Analysis situs combinatorio, Rev. Mat. Hisp.-Amer. 5(1923), 43–69; (continuacion) 6 (1924), 1–9; 33–41

8. Revestimientos. Teoría de Galois topológica

En esta sección trabajaremos en la categoría de espacios topológicos sobre un espacio B, $\mathfrak{T}/B$. Y, sobre todos los grupos que manejamos consideraremos siempre la topología discreta. Observemos que si dotamos a un grupo G de la topología discreta y G actúa sobre un espacio topológico X, decir que la acción de G es continua equivale a que $\forall g \in G$ la aplicación biunívoca $x \mapsto gx$ es un homeomorfismo, por tanto siempre entenderemos que la acción de los grupos sobre los espacios topológicos es una acción como grupos de homeomorfismos.

Definición 8.1.– *Si E y B son espacios topológicos y $p : E \to B$ es una aplicación, un abierto U de B se dice* bien cubierto por *p si:*

$$p^{-1}(U) = \bigcup_{i \in I} X_i$$

de modo que:

- *X_i es abierto en E, $\forall i \in I$.*
- *$X_i \cap X_j = \emptyset,\ \forall i, j \in I,\ i \neq j$.*
- *$p|_{X_i} : X_i \to U$ es un homeomorfismo $\forall i \in I$.*

La aplicación $p : E \to B$ se llama una proyección recubridora *si todo punto $x \in B$ tiene un entorno bien cubierto por p. En este caso se dice que el objeto de $\mathfrak{T}/B$, (X, p) (p es continua por la definición) es un* revestimiento *o un* espacio recubridor *de B.*

Ejemplos 8.2.– Ejemplo. 8.2.1.- La primera proyección $\pi_1 : B \times I \to B$, tomando en I la topología discreta, es un revestimiento. Un revestimiento se dice *trivial* si es isomorfo en $\mathfrak{T}/B$ a uno de este tipo.
Los revestimientos son exactamente los objetos localmente triviales de $\mathfrak{T}/B$, es decir, los pares (X, p) tales que todo punto $x \in X$ posee un entorno abierto U_x, tal que $(p^{-1})(U_x), p|_{p^{-1})(U_x)}$ es trivial en $\mathfrak{T}/U_x$

Ejemplo. 8.2.2.- : La aplicación

$$p : \mathbb{R} \to S^1,\ \pi(x) = e^{2\pi i x}$$

es un revestimiento no trivial. Observemos que si definimos una acción de $\mathbb{Z}$ sobre $\mathbb{R}$, por:

$$\mathbb{Z} \times \mathbb{R} \to \mathbb{R},\ (n, x) \mapsto x + n$$

es $\mathbb{R}/\mathbb{Z} \simeq \S^1$ y π es la aplicación de paso al cociente.
Este ejemplo es general. Si un grupo G actúa de modo continuo sobre un espacio topológico X, se dice que la acción de G es *propiamente discontinua* si podemos elegir para cada punto $x \in X$ un entorno abierto U_x tal que $U_x \cap g.U_x = \emptyset,\ \forall g \in G \setminus \{e\}$, siendo e el elemento unidad de G. Entonces si G actúa sobre X de modo propiamente discontinuo, la aplicación natural sobre el espacio de órbitas $p : X \to G/X$ es una proyección recubridora.

Ejercicios 8.3.– Ejercicio. 8.3.1.- .- Si $p : X \to B$ es una proyección recubridora, probar que:

- La fibra de p en cada punto $x \in X,\ p^{-1}(x)$ es discreta, (con la topología de subespacio de X), y si B es conexo las fibras de p tienen todas el mismo cardinal.
- p es un homeomorfismo local.
- La topología de B es la topología final de p, es decir, $V \subset B$ es abierto si y solo si $p^{-1}(V) \subset X$ es abierto.

Ejercicio. 8.3.2.- .- ¿Es cierto que si B es conexo y $p : X \to B$ cumple las tres condiciones anteriores p es una proyección recubridora?

Ejercicio. 8.3.3.- .- Probar que si un grupo G actúa sobre un espacio X de modo propiamente discontinuo, la aplicación natural $p : X \to G/X$ es una proyección recubridora.

Definición 8.4.– *Si (E, p) es un revestimiento de B, llamamos* transformación recubridora *de (E, p) a todo automorfismo de (E, p) en $\mathfrak{T}/B$.*

Observemos que como consecuencia de la definición las transformaciones recubridoras de (E, p) forman un grupo $G = Aut_{\mathfrak{T}/B}(E, p)$ y este grupo actúa naturalmente sobre E, pero también actúa sobre cada fibra de p por:

$$\forall b \in B,\ G \times p^{-1}(b) \to p^{-1}(b),\ (\theta, z) \mapsto \theta(z)$$

Proposición 8.5.– *Si B es localmente conexo, (E, p) es un revestimiento de B o más generalmente si p es un homeomorfismo local y E es Hausdorff y si $f, g \in Hom_{\mathfrak{T}/B}((X, q), (E, p))$ y X es conexo, se verifica que:*

$$\exists x \in X,\ f(x) = g(x) \Rightarrow f = g$$

Demostración:

Como X es conexo, basta probar que $C = \{z \in X \mid f(z) = g(z)\} \neq \emptyset$ es abierto y cerrado. Si $z \in C$, tomamos un entorno U_z de $q(z) = p(f(z)) = p(g(z)) \in B$ conexo tal que existe un entorno de $f(z) = g(z)$ en E, W_z, tal que $p|_{W_z} : W_z \simeq U_z$, entonces f y g coinciden en $f^{-1}(W_z) \cap g^{-1}(W_z)$. Ahora:

- Si E es Hausdorff la diagonal Δ de $E \times E$ es cerrada y para la aplicación continua

  $$(f, g) : X \to E \times E,\ (f, g)(x) = (f(x), g(x))$$

  $C = (f, g)^{-1}(\Delta)$ es cerrado.

- Si p es una proyección recubridora y exigimos a U_z que esté bien cubierto, si $z \notin C$, $f(z)$ y $g(z)$ están en hojas distintas luego admiten entornos disjuntos y $U_z \cap C = \emptyset$.

En ambos casos C es cerrado.

□

Consecuencia 8.6.– *Si θ es una transformación recubridora de (E, p) y E es conexo:*

$$\exists z \in E,\ \theta(z) = z \Rightarrow \theta = 1_E$$

y si $b \in B$ y U_b es un entorno conexo de b bien cubierto por p y

$$p^{-1}(U_b) = \bigcup_{i \in I} U_i$$

es la descomposición en hojas de $p^{-1}(U_b)$*:*

$$\forall i \in I,\ \exists j \in I, \theta(U_i) = U_j$$

Una consecuencia no trivial de 8.6 es el teorema siguiente:

Teorema 8.7.– *Si* B *es localmente conexo, y* (E,p) *es un espacio recubridor conexo de* B*, el grupo* $G = Aut_{\mathfrak{T}/B}(E,p)$ *actúa sobre sobre* E *de modo propiamente discontinuo.*
Recíprocamente si H *es un grupo que actúa sobre un espacio conexo* X *de modo propiamente discontinuo, el grupo de automorfismos del revestimiento* $q : X \to H/X$ *es isomorfo a* H

Demostración: Si $x \in E$ y $p(x) = b$ existe un entorno conexo U_b de b en B bien cubierto por p, sea

$$p^{-1}(U_b) = \bigcup_{i \in I} U_i$$

la descomposición en hojas de $p^{-1}(U_b)$, y sea U_i la hoja que contiene a x. Entonces por 8.6:

$$\theta \in G,\ \theta \neq Id \Rightarrow \theta(x) \in p^{-1}(b),\ \theta(x) \neq x$$

Luego:

$$\theta(x) \in U_j,\ j \neq i \Rightarrow U_i \cap \theta.U_i = U_i \cap \theta(U_i) = U_i \cap U_j = \emptyset$$

Para probar el recíproco observemos que al actuar H como grupo de homeomorfismos y conmutar su acción con la proyección sobre el espacio de órbitas, H se identifica a un subgrupo de $Aut_{\mathfrak{T}/(H/X)}(X,p)$. Por otra parte si $\theta \in Aut_{\mathfrak{T}/(H/X)}(X,p)$ y $x \in X$:

$$p(\theta(x)) = p(x) = H.x \Rightarrow \exists h \in H,\ h.x = \theta(x) \Rightarrow h = \theta$$

por 8.5

□

Si consideramos ahora B localmente conexo y un revestimiento (E,p) de B, con E conexo y llamamos G al grupo de transformaciones recubridoras de (E,p), como las transformaciones recubridoras dejan invariantes las fibras, tenemos un diagrama:

$$\begin{array}{ccc} & E & \\ {\scriptstyle n}\swarrow & & \searrow{\scriptstyle p} \\ G/E & \xrightarrow{\ \overline{p}\ } & B \end{array}$$

$$n(x) = G.x, \qquad \overline{p}(G.x) = p(x)$$

Definición 8.8.– *Si B es localmente conexo, un revestimiento (E,p) de B se dice* revestimiento de Galois *si E es conexo y la aplicación $\overline{p}$ es un homeomorfismo.*

Los revestimientos de Galois se caracterizan por la acción de G en las fibras de la proyección.

Proposición 8.9.– *Si (E,p) es un revestimiento conexo de un espacio localmente conexo B y G es el grupo de transformaciones recubridoras de (E,p). Las condiciones siguientes son equivalentes:*

1. *(E,p) es un revestimiento de Galois.*
2. *G actúa transitivamente sobre todas las fibras de p.*

Si B es conexo las afirmaciones anteriores son equivalentes a:

- *G actúa transitivamente sobre una fibra de p.*

Demostración:

Las primera afirmación implica la segunda, porque decir que $\overline{p}$ es biunívoca equivale a decir que $G.x = p^{-1}(p(x)),\ \forall x \in E$, es decir, que la acción en las fibras es transitiva. Y la segunda implica la primera porque $(G/E,\overline{p})$ es un revestimiento de B con las fibras compuestas por un solo punto.

Si B es conexo todas las fibras de $\overline{p}$ tienen el mismo cardinal, luego basta conque una fibra esté compuesta por un solo punto para que lo estén todas. □

Para demostrar la versión topológica del teorema fundamental de la Teoría de Galois necesitamos un lema previo:

Lema 8.10.– *Si (Z,q) y (E,p) son revestimientos de un espacio localmente conexo B y Z es conexo, todo morfismo $f:(E,p)\to(Z,q)$ es una proyección recubridora.*

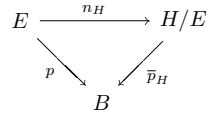
Demostración: Si $z \in Z$ podemos construir un entorno abierto conexo U de $q(z)$ en B bien cubierto por p y q, entonces tenemos un entorno abierto conexo W de z tal que $q|_W : W \to V$ es un homeomorfismo. Si las hojas de p sobre V son $\{T_i\}_{i\in I}$ y si

$$J = \{i \in I \mid T_j \cap f^{-1}(z) \neq \emptyset\}$$

es inmediato que $f|_{T_j} : T_j \to W$ es un homeomorfismo y que $f^{-1}(W) = \bigcup_{j\in J} T_j$. □

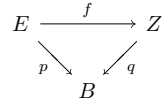
Teorema 8.11.– *[Teorema de Galois para revestimientos] Si (E,p) es un revestimiento de Galois de un espacio localmente conexo B y G es el grupo de transformaciones recubridoras de (E,p):*

1. *Para cada subgrupo H de G la proyección p induce una aplicación natural $\overline{p}_H : H/E \to B$ que hace conmutativo el diagrama:*



   y es una proyección recubridora.

2. *Para todo revestimiento conexo (Z,q) de B tal que exista un morfismo $f : (E,p) \to (Z,q)$, es decir, que sea conmutativo el diagrama:*



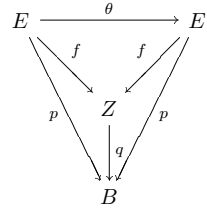
   entonces (E,f) es un revestimiento de Galois de X y si H_Z el grupo de transformaciones recubridoras (E,f), H_Z es un subgrupo de G y (Z,q) es isomorfo a $(H_Z/E, \overline{p}_{H_Z})$.

3. *Las correspondencias anteriores son inversas una de la otra.*

4. *(Z,q) es un revestimiento de Galois si y solo si H_Z es subgrupo invariante de G y en este caso $G/H_Z \simeq Aut_{\mathfrak{X}/B}(Z,q)$.*

Demostración: probemos la primera afirmación. $\overline{p}_H : H/E \to B$ es continua por serlo p y ser la topología de H/E la final de n_H, por otra parte sobre un abierto V bien cubierto por p, $p^{-1}(V) \simeq V \times I$ con I conjunto con la topología discreta, y hay un acción de H, como subgrupo de G, sobre I, entonces $\overline{p}_H^{-1}(V) \simeq V \times H/I$, y se sigue (1).

Para probar (2) observemos que por el lema (E,f) es un revestimiento de X y si H_Z es el grupo de transformaciones recubridoras de (E,f), $H_Z \subset G$ porque todo automorfismo de X que conmuta con f, conmuta con p



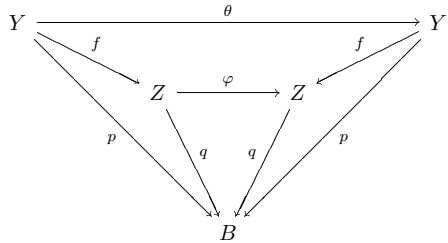
Solo queda probar que H_Z actúa transitivamente en las fibras de f y que en consecuencia (E, f) es galoisiano. Si $z \in Z$ y

$$e_1, e_2 \in f^{-1}(z) \subset p^{-1}(q(z)),$$

como (E, p) es galoisiano, existe $\theta \in G,\ \theta(e_1) = e_2$, para probar que $\theta \in H$ solo hay que probar que conmuta con f, pero f y $f\theta$ son morfismos de revestimientos de (E, p) en (Z, q) y $f\theta(e_1) = f(e_2) = z$ luego al coincidir en un punto ambas coinciden.

El enunciado (3) es trivial. Para probar el (4) observemos que si H_Z es invariante en G, el grupo cociente G/H actúa de modo natural en $Z = H/E$ y esta acción deja invariantes las fibras de q, luego G/H se identifica a un subgrupo del grupo de transformaciones recubridoras de (Z, q) y de nuevo es inmediato que este subgrupo es todo el grupo, luego (Z, q) es de Galois.

Recíprocamente, si (Z, q) es galoisiano, necesitamos un homomorfismo de G en $Aut(Z, q)$ es decir, para cada $\theta \in G$ construir un $\varphi \in Aut(Z, q)$ que haga conmutativo el diagrama:



Para ello tomamos un punto $e \in E$:

$$p(e) = p\theta(e) \Rightarrow q(f(e)) = q(f\theta(e)).$$

Luego $f(e)$ y $f\theta(e)$ están en la misma fibra de q y como (Z, q) es galoisiano $Aut(Z, q)$ actúa transitivamente y existe un (único) $\varphi \in Aut(Z, q)$ tal que $\varphi(f(e)) = f\theta(e)$ y en consecuencia $\varphi.f = f.\theta$. Obviamente la correspondencia $\theta \mapsto \varphi$ es un homomorfismo y su núcleo es H_Z, luego H_Z es un subgrupo invariante. □

Del mismo modo que hemos construido una Teoría de Galois de revestimientos paralela a la clásica, podemos construir otra paralela a la Teoría de Galois-Grothendieck, aquí el papel del cierre separable lo tiene el revestimiento universal y el del grupo de Galois absoluto lo juega el grupo fundamental.

Recordaremos los resultados básicos de la teoría de homotopía. Partimos de un espacio topológico arbitrario X y llamaremos I al segmento $[0, 1] \subset \mathbb{R}$ con la topología inducida. Un

camino en X es un aplicación continua $\sigma : I \to X$, $\sigma(0)$ y $\sigma(1)$ se llaman usualmente *extremos de* σ aunque cuando queremos distinguirlos llamamos a $\sigma(0)$ *origen* y a $\sigma(1)$ *extremo* de σ.

Dados dos caminos σ y τ con los mismos extremos, diremos que son *homótopos*, y escribiremos $\sigma \simeq \tau$ si existe una aplicación continua (*homotopía*) $F : \times I \to X$ tal que:

- $F(s,0) = \sigma(s),\ \forall s \in I$
- $F(s,1) = \tau(s),\ \forall s \in I$
- $F(0,t) = \sigma(0) = \tau(0),\ \forall t \in I$
- $F(1,t) = \sigma(1) = \tau(1),\ \forall t \in I$

Observemos que para cada $t \in I$ fijo

$$F_t : I \to X,\ F_t(s) = F(s,t)$$

es un camino en X con extremos $F_t(0)=F(0,t)=\sigma(0)=\tau(0)$ y $F_t(1)=F(1,t)=\sigma(1)=\tau(1)$ y que $F_0 = \sigma,\ F_1 = \tau$, es decir, tenemos una familia *continua* de caminos que enlaza σ con τ. Un camino σ con ambos extremos iguales, es decir, tal que $\sigma(0) = \sigma(1)$, se llama un *lazo* con base en $\sigma(0)$, el camino constante $c_x : I \to X,\ c_x(t) = x\, \forall t \in I$ es un ejemplo de lazo, y un lazo homótopo al constante se dice que es homotópicamente trivial.

Dados dos caminos en X, σ, τ, tales que $\sigma(1) = \tau(0)$ definimos su concatenación $\sigma * \tau$ como el camino:

$$\sigma * \tau : I \to X,\ \sigma * \tau(t) = \begin{cases} \sigma(2t) & 0 \leq t \leq 1/2 \\ \tau(2t-1) & 1/2 \leq t \leq 1 \end{cases}$$

Se puede comprobar fácilmente que:

- La relación de homotopía es una relación de igualdad en el conjunto de caminos en X, a la clase en esta relación de un camino σ, la representaremos por $[\sigma]$
- La concatenación de caminos es estable por homotopía, es decir:

$$\sigma \simeq \sigma',\ \tau \simeq \tau',\ \sigma(1) = \tau(0) \Rightarrow \sigma * \tau \simeq \sigma' * \tau'$$

- Si σ es un lazo con base en x, $c_x * \sigma$ y $\sigma * c_x$ son homótopos a σ.
- Si σ, τ y υ, son caminos en X tales que $\sigma(1) = \tau(0),\ \tau(1) = \upsilon(0)$, es:

$$\sigma * (\tau * \upsilon) = (\sigma * \tau) * \upsilon.$$

- Si σ es un camino y llamamos σ^{-1} al camino definido por:

$$\sigma^{-1} : I \to X,\ \sigma^{-1}(t) = \sigma(1-t)$$

verifica que:

$$\sigma * \sigma^{-1} \simeq c_{\sigma(0)},\ \sigma^{-1} * \sigma \simeq c_{\sigma(1)}.$$

Entonces el conjunto $\pi_i(X, x_0)$ de clases de homotopía de lazos con base en un punto $x_0 \in X$ con la operación de concatenación,

$$[\sigma][\tau] = [\sigma * \tau]$$

es un grupo, el elemento unidad es la clase de lazos homotópicamente triviales $[c_{x_0}]$ y el inverso de una clase $[\sigma]$, la clase $[\sigma^{-1}]$.

Definición 8.12.– *El grupo $\pi_i(X, x_0)$ se llama* grupo fundamental o grupo de Poincaré *de X en x_0. Un espacio X se llama* simplemente conexo *si es conexo por caminos y su grupo fundamental es trivial.*

El grupo fundamental verifica las propiedades siguientes:

- Si σ es un camino con $\sigma(0) = x,\ \sigma(1) = y$, la correspondencia:

$$\overline{\sigma} : \pi_1(X, y) \to \pi_1(X, x),\ \overline{\sigma}([\tau]) = [\sigma]^{-1}[\tau][\sigma]$$

es un isomorfismo de grupos.

- Si X es conexo por caminos, todos los grupos fundamentales de X son isomorfos, y los representaremos, omitiendo el punto base, por $\pi_1(X)$.

- Si $f : X \to Y$ es una aplicación continua, $x \in X$ y $f(x) = y$, la correspondencia:

$$f_* : \pi_1(X) \to \pi_1(Y),\ f_*([\sigma]) = [f\sigma]$$

es un homomorfismo de grupos.

- Las correspondencias:

$$(X, x) \mapsto \pi_1(X, x),\ f \mapsto f_*$$

definen un funtor covariante de la categoría de espacios con un punto fijo en la categoría de grupos.

- Si un espacio E es simplemente conexo, dos caminos en E con el mismo origen y el mismo extremo son homótopos.

Relacionaremos ahora el grupo fundamental con los revestimientos:

Teorema 8.13.– *[Teorema de elevación] Si (E,p) es un revestimiento de B, $x \in B$ y $z \in p^{-1}(x)$ para todo camino en B con origen en x, σ, existe un único camino τ en E con origen en z, que se proyecta sobre σ, es decir, tal que*

$$p\tau = \sigma,\ \tau(0) = z.$$

Además si $\sigma_1,\ \sigma_2$ son caminos homótopos con origen en x, sus elevaciones a z son homótopas.

Demostración: Sea $\sigma : I \to B,\ \sigma(0 = x)$. Existe una partición finita de I, $0{=}t_0{<}t_1{<}...{<}t_r{=}1$ de modo que cada segmento $[t_{i-1}, t_i]$ está contenido en un abierto U_i de B bien cubierto por p, entonces existen abiertos de E, $\{V_i\}_{1\leq i\leq r}$ tales que:

- $p_i|_{V_i} : V_i \to U_i$ homeomorfismo $\forall i,\ 1 \leq i \leq r$.
- $x \in V_0,\ \sigma(t_i) \in V_{i-1} \cap V_i$.

Entonces σ se eleva obviamente a $\bigcup_0^r V_i$. La elevación es única aplicando 8.5 por ser I conexo.

La prueba de la elevación de la homotopía es similar descomponiendo $I \times I$ en una cuadrícula con sus cuadrados bien cubiertos por p □

Como consecuencia de esta proposición:

- Si (E,p) es un revestimiento de B, y $p(e) = x$, el homomorfismo $p_* : \pi_1(E,e) \to \pi_1(X,x)$ es inyectivo.
- El grupo $\pi_1(B,x)$ actúa por la derecha sobre la fibra $p^{-1}(x)$ por $e.[\sigma] = \sigma_e(1)$ siendo σ_e la elevación a E de σ con origen en e.
- En esta acción el estabilizador de un punto $e \in p^{-1}(x)$ es el subgrupo $p_*(\pi_1(E,e)) \subset \pi_1(B,x)$.
- Si E es conexo por caminos, como todo camino que une dos puntos de $p^{-1}(x)$ se proyecta en un lazo en x, el grupo $\pi_1(B,x)$ actúa transitivamente sobre $p^{-1}(x)$.
- Si E es conexo por caminos existe una correspondencia biunívoca entre la fibra $p^{-1}(x)$ y las clases por la derecha de $\pi_1(B,x)$ módulo $p_*(\pi_1(E,e))$, en particular si la fibra es finita $p_*(\pi_1(E,e))$ es un subgrupo de índice finito de $\pi_1(B,x)$.

Teorema 8.14.– *Dado un revestimiento (E,p) de B, con $p(e) = b$, si E es simplemente conexo y localmente conexo por caminos, el grupo G de transformaciones recubridoras de (E,p) es canónicamente isomorfo a $\pi_1(B,b)$.*

Demostración:

Sea $e \in E,\ p(e) = b$. Si $\theta \in G$, y $\theta(e) = e_1$, existe un camino:

$$(*) \qquad \sigma : I \longrightarrow E,\ \sigma(0) = e,\ \sigma(1) = e_1.$$

Su proyección $p_*(\sigma)$ es un lazo en X basado en b y define una clase $[p_*(\sigma)] \in \pi_1(B, b)$. Definimos:

$$\chi : G \longrightarrow \pi_1(B, x),\ \chi(\theta) = [p_+(\sigma)]$$

χ no depende de la elección de σ porque al ser E simplemente conexo, si τ verifica $(*)$ es homótopa a σ y sus proyecciones son también homótopas. Obviamente χ es homomorfismo de grupos y es inyectivo porque si $\chi(\theta) = 1$ $p_*(\sigma)$ es homótopa a la aplicación constante en b, y como p es un revestimiento, hay un entorno de e que solo corta a la fibra $p^{-1}(b)$ en e, luego $\sigma(0) = \sigma(1) = e$ y θ es una transformación recubridora con un punto fijo y por tanto es la identidad.

Para probar que χ es sobre, tomemos una clase de lazos $[\alpha] \in \pi_1(B, b)$, y vamos a definir $\theta \in G$.

1. Si $x \in p^{-1}(b)$, construimos un camino α_x en E, elevación de α con origen en x y definimos $\theta(x) = \alpha_x(1)$.

2. Si $x \in E \setminus p^{-1}(b)$, construimos un camino

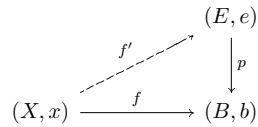
   $$\beta : I \to B,\ \beta(0) = b,\ \beta(1) = p(x)$$

   que da lugar a un lazo basado en $p(x)$, $\tau = \beta^{-1} * \sigma * \beta$ que tiene una elevación única con origen en x, β_x y llamamos $\theta(x) = \beta_x(1)$

Es obvio que θ depende solo de la clase de homotopía de α y que $\chi(\theta) = [\alpha]$, solo hay que probar que θ es continua, pero de la construcción se desprende que si $x, y \in E$ y δ es un camino en E con origen en x y extremo en y, si proyectamos δ y elevamos su proyección $p_*(\delta)$, con origen en $\theta(x)$ esta elevación tiene su extremo en $\theta(y)$, entonces al ser p un revestimiento, θ va siguiendo las hojas y es continua. □

Una vez que hemos relacionado el grupo de transformaciones recubridoras con el grupo fundamental, vamos a construir un revestimiento que juega en la teoría topológica el papel del cierre separable en la teoría algebraica. Para ello necesitamos un resultado previo que generaliza el teorema de elevación de caminos.

Lema 8.15.– *Si en el diagrama de espacios conexos y localmente conexos por caminos con un punto fijo:*



p es un revestimiento y f es continua. Existe la aplicación continua f' que hace conmutativo el diagrama si y solo si

$$f_*(\pi_1(X,x)) \subset p_*(\pi_1(E,e)).$$

Demostración: Por la funtorialidad del grupo fundamental, si existe f',

$$pf' = f \Rightarrow f_*(\pi_1(X,x)) = p_*f'_*(\pi_1(X,x)) \subset p_*(\pi_1(E,e))$$

Para probar el recíproco, construimos f'. Como X es conexo por caminos, dado un punto $z \in X$ existe un camino:

$$(**) \qquad \beta : I \to X,\ \beta(0) = x,\ \beta(1) = z$$

entonces $f.\beta$ une b con $f(z)$ y admite una elevación a E, β_z, con origen en e. Es decir:

$$p.\beta_z = f.\beta,\ \beta_z(0) = e.$$

Definimos entonces: $f'(z) = \beta_z(1)$, f' no depende de la elección de β, porque si τ cumple también las condiciones de $(**)$. $\beta * \tau^{-1}$ es un lazo en (X,x) y en consecuencia $f.(\beta*\tau) = (f.\beta)*(f.\tau)^{-1}$ es un lazo en (B,b) cuya clase de homotopía debe ser imagen por p_* de la de un lazo en (E,e), luego $(f.\tau)(1) = (f.\tau)^{-1}(0) = (f.\beta)(1)$ Desde aquí la prueba de que f' es continua es como la del teorema anterior □

Del lema se sigue una consecuencia inmediata:

Consecuencia 8.16.– *Si X es simplemente conexo, f' siempre existe, y si (X,f) y (E,p) son ambos revestimientos simplemente conexos de B, son isomorfos.*

Definición 8.17.– *Un revestimiento conexo y localmente conexo por caminos $(\widetilde{B},\widetilde{p})$ de un espacio B se llama revestimiento universal si para todo revestimiento conexo y localmente conexo por caminos (E,p), existe un morfismo $q : (\widetilde{B},\widetilde{p}) \to (E,p)$*

Entonces la consecuencia anterior se lee así:

Proposición 8.18.– *Si $(\widetilde{B},\widetilde{p})$ es un revestimiento de B con $\widetilde{B}$ localmente conexo por caminos y simplemente conexo $(\widetilde{B},\widetilde{p})$ es el revestimiento universal de B (que es necesariamente único salvo isomorfismos).*

No todo espacio X conexo y localmente conexo por caminos admite un revestimiento simplemente conexo,$\widetilde{X}$, ya que al ser $\widetilde{X}$ locamente homeomorfo a X, los lazos en X suficientemente pequeños deben se homotópicamente triviales. Así:

Ejemplo 8.19.– Si C_n es la circunferencia de $\mathbb{R}^2$ de centro $(1/n, 0)$ y radio $1/n$ para todo $n \in \mathbb{N}$, el subespacio de $\mathbb{R}^2$

$$\mathcal{X} = \bigcup_{n\in\mathbb{N}} C_n$$

no admite ningún revestimiento simplemente conexo

Definición 8.20.– *Un espacio X se dice semilocalmente simplemente conexo si todo punto $x \in X$ admite un entorno U_x tal que todo lazo en U_x basado en x es topológicamente trivial en X.*

Teorema 8.21.– *Si X es conexo, localmente conexo por caminos y semilocalmente simplemente conexo, admite un revestimiento universal.*

Demostración: Tomamos un punto $x_0 \in X$, y construimos el par $(\widetilde{X}, p)$, tomando como elementos de $\widetilde{X}$ las clase de homotopía de caminos en X que tienen origen en x_0, para cada clase $[\sigma] \in \widetilde{X}$ definimos $p([\sigma]) = \sigma(1)$.

La topología de $\widetilde{X}$ es la que tiene como base de abiertos los conjuntos:

$$\langle [\sigma], V\rangle = \{[\sigma * \tau] \mid \tau : I \to V,\ \sigma(1) = \tau(0)\}$$

donde $[\sigma] \in \widetilde{X}$ y V recorre los entornos conexos por caminos de $\sigma(1)$. De este modo:

- $p(\langle [\sigma], V\rangle) = V$.
- $[\tau] \in \langle [\sigma], V\rangle \Rightarrow [\tau] = [\sigma * \beta],\ \beta(I) \subset V,\ \sigma(1) = \beta(0)$, entonces $\tau(1) = \beta(1)$ y $[\sigma] = [\tau * \beta{-}1] \in \langle [\tau], V\rangle$ luego

$$\langle [\sigma], V\rangle = \langle [\tau], V\rangle.$$

- $[\gamma] \in \langle [\sigma], V\rangle \cap \langle [\tau], W\rangle \Rightarrow \langle [\gamma], T\rangle \subset \langle [\sigma], V \cap\rangle \langle [\tau], W\rangle$ donde T es un entorno conexo por caminos de $\gamma(1)$ en $V \cap W$.
- $p^{-1}(U) = \bigcup \tau(1) \in U \langle [\tau], U\rangle$.

En consecuencia los conjuntos elegidos son efectivamente base de abiertos para una topología de $\widetilde{X}$ y con ella p es continua y abierta.

Veamos que si U es un entorno de $x = \sigma(1)$ conexo por caminos y tal que todo lazo en U basado en x es topológicamente trivial en X, U está bien cubierto por p. Como hemos dicho:

$$p^{-1}(U) = \bigcup \tau(1) \in U \langle [\tau], U \rangle.$$

Los $\langle [\tau], U \rangle$ son disjuntos porque:

$$[\gamma] \in \langle [\delta], U \rangle \cap \langle [\beta], U \rangle \Rightarrow \langle [\gamma], U \rangle = \langle [\delta], U \rangle = \langle [\beta], U \rangle$$

y cada uno de ellos es homeomorfo por p a U.

El espacio $\widetilde{X}$ es conexo por caminos porque todo punto $[\sigma] \in \widetilde{X}$ se une a $[c_{x_0}] \in \widetilde{X}$ por el camino:

$$\widetilde{\sigma} : I \to \widetilde{X},\ \widetilde{\sigma}(s) = \sigma_s,\ \sigma_s : I \to X,\ \sigma_s(t) = \sigma(st)$$

Observemos que además $p\widetilde{\sigma} = \sigma$.

Por último $\widetilde{X}$ es simplemente conexo, ya que si θ es un lazo en $\widetilde{X}$ basado en $[c_{x_0}]$, su proyección $\sigma = p\theta$ es un lazo en x_0 que con la construcción anterior se eleva a un camino $\widetilde{\sigma}$ con origen en $[c_{x_0}]$, y, por la unicidad de la elevación, $\widetilde{\sigma} = \theta$, por tanto $[\sigma] = \widetilde{\sigma}(1) = \theta(1) = [c_{x_0}]$, luego σ es homótopo a c_{x_0} y por el teorema de elevación θ es homotópicamente trivial. □

Si fijamos un espacio topológico X podemos construir la subcategoría completa de $\mathfrak{T}/X$, $((Cov(X)))$, cuyos objetos son los revestimientos de X y para cada punto $x \in X$, y cada revestimiento (Z, p) de X, hemos visto que el grupo fundamental $\pi_1(X, x)$ actúa por la derecha sobre la fibra $p^{-1(x)} \subset Z$, llamado a este conjunto con su acción $Fib_x(Z, p)$ tenemos el llamado funtor fibra de la categoría $((Cov(X)))$ en la de conjuntos con $\pi_1(X, x)$- acción.

La construcción del revestimiento universal que acabamos de hacer, y que depende (varía en un isomorfismo) del punto $x \in X$ que hemos elegido para hacer la construcción significa en otros términos lo siguiente:

Proposición 8.22.– *Si X es conexo, localmente conexo por caminos y semilocalmente simplemente conexo, para cada $x \in X$ el funtor fibra Fib_x es representable.*

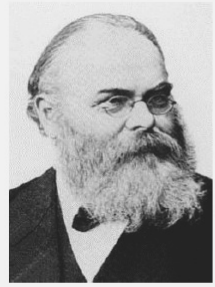
Demostración: Si llamamos $(\widetilde{X}_x, p_x)$ al revestimiento universal construido en el teorema 8.21, como $\widetilde{X}_x$ es simplemente conexo y localmente conexo pr caminos, $\pi_1(X, x)$ actúa transitivamente sobre la fibra $p_x^{-1}(x)$ y es isomorfo (con su acción) al grupo de transformaciones recubridoras, por tanto tenemos una biyección natural

$$Fib_x(\widetilde{X}_x) \simeq Hom_{\mathfrak{T}/X}((\widetilde{X}_x, p_x), (\widetilde{X}_x, p_x)),$$

en la cual a la transformación recubridora identidad le podemos hacer corresponder la clase de homotopía del lazo constante $[c_x] \in \widetilde{X}_x$, entonces el par $((\widetilde{X}_x, p_x), [c_x])$ dan la representación buscada. □

Podemos establecer ahora el teorema fundamental a la Grothendieck de la teoría de revestimientos:

Teorema 8.23.– *Si X es conexo, localmente conexo por caminos y semilocalmente simplemente conexo, y $x \in X$, el funtor Fib_x es una equivalencia entre la categoría de revestimientos de X y la de $\pi_1(X, x)$ -conjuntos. Los revestimientos conexos corresponden a conjuntos con acción transitiva del grupo y los revestimientos galoisianos a las acciones del grupo sobre sus cocientes por subgrupos normales.*



Schwarz regards the Riemann surface as being dissected in a suitable way, then infinitely often covered and now these different coverings glued together along the cross sections in sucha waythat there arises a total surface corresponding to all polygons lying side by side in the plane. This total surface is simply connected and has only one boundary component. Thus it is only necessary to verify that such a simply connected surface can be mapped in the well known way onto the interior of a disc.

Carta de Klein a Poincare citada por Remmert

9. Superficies de Riemann

Vamos a introducir ahora un campo en el que confluyen las teorías de Galois algebraica y topológica, el de las superficies de Riemann.

Definición 9.1.– *Sea X un espacio topológico Hausdorff.*

1. *Diremos que X es una variedad topologica n-dimensional, si todo punto de X tiene un entorno homeomorfo a un abierto de $\mathbb{R}^n$.*

2. *Si X es una variedad topológica bidimensional (superficie topológica), llamaremos carta compleja en X a todo homeomorfismo $\varphi : U \to V$ donde U es un abierto de X y V un abierto de $\mathbb{C}$, representaremos a la carta por (φ, U, V).*

3. *Dos cartas complejas de una superficie X, (φ_1, U_1, V_1) y (φ_2, U_2, V_2) se dicen compatibles si la aplicación:*

$$\varphi_2\varphi_1^{-1} : \varphi_1(U_1 \cap U_2) \to \varphi_2(U_1 \cap U_2)$$

es biholomorfa.

4. *Un atlas complejo en una superficie X es una familia de cartas complejas compatibles dos a dos:*
$$\mathfrak{A} = \{(\varphi_1, U_1, V_1)\}_{i\in I}, \text{ tales que } X = \bigsqcup_{i\in I} U_i.$$

5. *Dos atlas se dicen compatibles si cada carta de uno de ellos es compatible con todas las cartas del otro. La relación de compatibilidad es una relación de equivalencia en el conjunto de atlas complejos en X y cada clase contiene un único atlas maximal para la relación contenido.*

6. *Una estructura compleja en una superficie X es una clase de atlas complejos compatibles, o lo que es lo mismo, un atlas complejo maximal.*

7. *Una superficie de Riemann es un par (X, Σ) donde X es una superficie y Σ una estructura compleja en X.*

Ejemplos 9.2.–

Ejemplo. 9.2.1.- $\mathbb{C}$ con la estructura compleja definida por $Id : \mathbb{C} \to \mathbb{C}$ es una superficie de Riemann.

Ejemplo. 9.2.2.- Si U es un dominio (abierto conexo) de una superficie de Riemann (X, Σ) y llamamos $\Sigma|_U$ al atlas formado por las cartas contenidas en U, $(U, \Sigma|_U)$ es una superficie dr Riemann.

Ejemplo. 9.2.3.- $\mathbb{P}^1_{\mathbb{C}}$ con su atlas habitual es una superficie de Riemann a la que se llama *Esfera de Riemann*.

Ejemplo. 9.2.4.- Si $\omega_1,\ \omega_2$ son complejos $\mathbb{R}$-linealmente independientes, y consideramos el subgrupo aditivo de $\mathbb{C}$:
$$\Gamma = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$
se puede dotar $\mathbb{C}/\Gamma$ de la topología final del homomorfismo natural $\pi : \mathbb{C} \to \mathbb{C}/\Gamma$, con esta topología $\mathbb{C}/\Gamma$ es una superficie, cada uno de sus puntos tiene un único representante en:
$$T = \{a\omega_1 + b\omega_2 \mid a, b \in [0, 1)\}$$
y si cubrimos un punto de T con un abierto U de $\mathbb{C}$ tal que $\pi|_U$ sea inyectiva, $\pi(U)$ es abierto en $\mathbb{C}/\Gamma$ y las cartas $(\pi|_U^{-1}, \pi(U), U)$ definen una estructura de superficie de Riemann en $\mathbb{C}/\Gamma$.

Ejemplo. 9.2.5.- Si $f(x,y)$ es una función analítica en un dominio $U \subset \mathbb{C}^2$ y :

$$\left(\left(\frac{\partial f}{\partial x}\right)(a,b), \left(\frac{\partial f}{\partial y}\right)(a,b)\right) \neq (0,0),\ \forall (a,b) \in U,\ f(a,b) = 0$$

El teorema de existencia de funciones implícitas permite dotar a:

$$V(f) = \{(a,b) \in U \mid f(a,b) = 0\}$$

de una estructura de superficie de Riemann.

Ejercicio 9.3.– Completar los ejemplos anteriores.

Definición 9.4.– *Sean (X,Σ) (Y,Υ) superficies de Riemann y sea $f : X \to Y$ una apliacacion, se dice que f es una aplicación holomorfa, si para cada par de cartas complejas $(\varphi, U, V) \in \Sigma$, $(\phi, T, W) \in \Upsilon$ con $f(U) \subset T$ la función de variable compleja:*

$$\phi f \varphi^{-1} : V \to W$$

es holomorfa.
Si T es un abierto de X, una aplicación holomorfa de $(T, \Sigma|_T)$ en $\mathbb{C}$ se llama una función holomorfa o analítica en T.

Ejercicios 9.5.–

Ejercicio. 9.5.1.- Probar que las superficies de Riemann y las aplicaciones holomorfas forman una categoría.

Ejercicio. 9.5.2.- Probar que si (X,Σ) es una superficie de Riemann :

1. Para cada abierto T de X, el conjunto $\mathcal{O}(T)$ de funciones holomorfas en T, con las operaciones naturales es una $\mathbb{C}$ -álgebra.

2. Que si Si $T_1 \subset T_2$ son abiertos de X la restricciónA $\mathcal{O}(T_2) \to \mathcal{O}(T_1)$ es un homomorfismo de $\mathbb{C}$ -álgebras.

3. La correspondencia $T \mapsto \mathcal{O}(T)$ define un haz de $\mathbb{C}$ -álgebras en X y que las fibras de este haz son isomorfas a la $\mathbb{C}$ -álgebra de series convergentes $\mathbb{C}\{x\}$.

4. Una aplicación continua f de (X, Σ) en otra superficie de Riemann (Y, Γ) si y solo si el morfismo inducido entre los haces de funciones continuas (ver 4.8) induce un morfismo de haces $\mathcal{O}_Y \to f_*(\mathcal{O}_X)$.

Aceptaremos sin prueba los dos resultados siguientes que son extensión inmediata de los correspondientes teoremas de Riemann relativos a funciones de variable compleja:

Teorema 9.6.– *Si U es un abierto de una superficie de Riemann X y $a \in X$, toda función $f \in \mathcal{O}(U \setminus \{a\})$ acotada en un entorno de a se extiende en forma única a una función analítica en U.*

Teorema 9.7.– *[Principio de identidad] Si dos aplicaciones holomorfas entre las superficies de Riemann (X, Σ), (Y, Υ) coinciden en un subconjunto de X con un punto de acumulación, son iguales.*

Definición 9.8.– *Una función meromorfa sobre un abierto U de una superficie de Riemann (X, Σ) es una función holomorfa $f \in \mathcal{O}_X(V)$ tal que:*

1. *V es un abierto de U*
2. *$U \setminus V$ está formado por puntos aislados de U, a los que llamaremos polos de f*
3. *$\forall z \in U \setminus V$*

$$\lim_{x \to z} |f(x)| = \infty$$

Tampoco aquí hay diferencias entre la teoría clásica de funciones de una variable compleja y la teoría de funciones sobre una superficie de Riemann. Es facil probar que la correspondencia que asocia a cada abierto $U \subset X$ el conjunto de funciones meromorfas en U, $\mathcal{M}_X(U)$ es un haz de cuerpos cuyas fibras son isomorfas al cuerpo de series de Laurent en una variable con coeficientes complejos. Se prueba también fácilmente que si consideramos $\mathbb{P}^1_{\mathbb{C}} \equiv \mathbb{C} \cup \{\infty\}$ y para $f \in \mathcal{M}_X(U)$ y cada polo p de f definimos $f(p) = \infty$. Entonces $\mathcal{M}_X(U)$, se identifica con el conjunto de funciones holomorfas de U en la recta proyectiva compleja menos la función f_∞ que toma el valor constante ∞.

Desde el punto de vista local, las funciones holomorfas son muy simples, ya que si f es holomorfa en un punto x podemos elegir cartas locales de modo que x se lea como 0 y f se lea en esas cartas como una función que se anula en 0. Tomando el desarrollo en serie de f este se escribe como z^k por una serie de orden 0 que es por tanto potencia k-esima de una serie, entonces un cambio de variable permite considerar localmente la función como z^k, k se llama *orden de la función* en x. Observemos que esto no significa que las aplicaciones holomorfas tengan fibras finitas, porque nuestra afirmación anterior significa que en cada punto de la fibra en un punto y la función se porta como una potencia pero no dice nada de los puntos de la fibra. Así la aplicación $exp : \mathbb{C} \to \mathbb{C}^*$ tiene orden 1 y fibras infinitas en todos los puntos.

Consecuencias inmediatas de esta descripción son las siguientes:

- Todo polinomio se puede considerar como una función holomorfa en la recta proyectiva que lleva el infinito al infinito y su orden en infinito es su grado como polinomio.
- Toda aplicación holomorfa no constante es abierta.
- Una aplicación holomorfa inyectiva es necesariamente biholomorfa.
- Toda función meromorfa en la recta proyectiva es racional.

Hemos visto que si una funcion es holomorfa en un punto x, localmente en un entorno abierto U de x, la función se escribe como z^k. Entonces en el entorno reducido obtenido suprimiendo x de U, la función proporciona un revestimiento de k hojas.

Definición 9.9.– *Si $p : X \to Y$ es una aplicación holomorfa no constante entre superficies de Riemann un punto $x \in X$ se llama un punto de ramificación de f si el orden de f en x es mayor que uno; o lo que es lo mismo, si no existe ningún entorno U de x tal que $f|_U$ sea inyectiva. Una aplicación holomorfa no constante sin puntos de ramificación se llama función no ramificada.*

Proposición 9.10.– *Si $p : X \to Y$ es una aplicación holomorfa no constante entre superficies de Riemann p es abierta y discreta (es decir, sus fibras $p^{-1}(y)$ son discretas en X). p es no ramificada si y solo si es un homeomorfismo local.*

Demostración:

La condición de discreta es consecuencia del principio de identidad y las otras afirmaciones son consecuencia de que localmente las funciones holomorfas se portan como la función $x \mapsto x^r$ y si el punto en que nos situamos no es de ramificación $r = 1$ □

No es cierto que, como podría parecer a partir de este teorema, que una aplicación holomorfa no ramificada sea una proyección recubridora, por ejemplo la inmersión del disco abierto de radio 1, $\mathbb{D}$, en $\mathbb{C}$ no es una proyección recubridora porque ningún entorno de un complejo de módulo 1 está bien cubierto. Sin embargo si tenemos una superficie de Riemann, se pueden dotar de estructura de superficie de Riemann sus revestimientos como prueba el resultado siguiente:

Proposición 9.11.– *Si (X, Σ) es una superficie de Riemann, Y es un espacio Hausdorff y $p : X \to Y$ es un homeomorfismo local, existe una única estructura compleja en Y con la cual p es holomorfa.*

Demostración: podemos tomar un atlas de X compuesto por cartas $\{(U_{x,y}, V_{x,y}, \varphi_{x,y})\}_{x\in X, p(y)=x}$ de modo que:

$$\forall x \in X,\ \forall y \in p^{-1}(x),\ \exists W_y \text{ entorno abierto de y},\ p|_{W_y} : W_y \simeq U_{x,y}$$

Entonces:

$$\{(W_y, V_{x,y}, \varphi_{x,y} p|_{W_y})\}_{x\in X, p(y)=x}$$

es la estructura compleja buscada. □

Esencialmente por la misma razón, la elevación de una aplicación holomorfa respecto a una aplicación holomorfa no ramificada es también holomorfa. Si usamos este resultado para la exponencial obtenemos el logaritmo de cualquier función con valores en $\mathbb{C}^*$, como una función holomorfa multivalorada en $\mathbb{C}$.

Como hemos visto las aplicaciones holomorfas no ramificadas no son proyecciones recubridoras, para que lo sean, tienen que cumplir una condición adicional:

Definición 9.12.– *Una aplicación continua entre dos espacios topológicos se llama propia si la imagen recíproca de todo compacto es compacta.*

Ejercicios 9.13.–

Ejercicio. 9.13.1.- Probar que si $f : X \to Y$ es continua y X es compacto, f es propia. Probar que si X e Y son localmente compactos y f es propia, entonces f es cerrada.

Ejercicio. 9.13.2.- Probar que si $f : X \to Y$ es continua, propia y discreta y X e Y son localmente compactos las fibras de f son finitas y para todo $y \in Y$ y todo entorno abierto V de $p^{-1}(y)$ existe un entorno U de y con $p^{-1}(U) \subset V$.

Ejercicio. 9.13.3.- Probar que si $f : X \to Y$ es propia y homeomorfismo local y X e Y son localmente compactos p es una proyección recubridora. En particular toda aplicación holomorfa propia no ramificada entre superficies de Riemann es una proyección recubridora.

De ahora en adelante a los morfismos analíticos propios no ramificados, que son proyecciones recubridoras, les llamaremos *revestimientos analíticos no ramificados,* y a los que pueden tener puntos de ramificación les llamaremos *revestimientos analíticos ramificados*.

La confluencia de las teorías de Galois algebraica y topológica se obtiene si tomamos un polinomio de dos variables complejas y lo consideramos como un polinomio en una de las variables con coeficientes en el cuerpo de funciones racionales en la otra. Así tenemos un cuerpo de descomposición y un grupo de Galois algebraico del polinomio. Pero también el polinomio define una función multivalorada, ya que para cada valor de la variable secundaria, tenemos una ecuación algebraica con un conjunto finito de soluciones. Fuera de los ceros del discriminante y de los

del coeficiente del término de mayor grado tendremos un espacio recubridor que igualmente tiene un grupo de Galois topológico. Nuestro objetivo es formalizar estas afirmaciones y comprobar que ambos grupos coinciden, para ello necesitamos precisar las nociones de prolongación analítica y función algebraica.

Definición 9.14.– *Si X es una superficie analítica y $\gamma : [0,1] \to X$ es una curva (función continua), con extremos $a = \gamma(0),\ b = \gamma(1)$ un germen analítico $\psi \in \mathcal{O}_{X,b}$ se dice prolongación analítica a lo largo de γ de un germen $\varphi \in \mathcal{O}_{X,a}$ si existe una curva en el espacio etalé de $\mathcal{O}_X$, $\widetilde{\gamma} : [0,1] \to |\mathcal{O}_X|$ elevación de γ con origen en φ y extremo en ψ.*

$$\begin{array}{ccc} & & |\mathcal{O}_X| \\ & \overset{\widetilde{\gamma}}{\nearrow} & \Big\downarrow \pi \\ [0,1] & \xrightarrow{\gamma} & X \end{array} \qquad \widetilde{\gamma}(0) = \varphi,\ \widetilde{\gamma}(1) =$$

Los teoremas de unicidad de la elevación, aplicable porque π es homeomorfismo local y $|\mathcal{O}_X|$ es Hausdorff, y el de elevación de homotopías se verifica que la prolongación a lo largo de un camino, si existe, es única y que solo depende de la clase de homotopía del camino que sigue. En particular si X es simplemente conexo y un germen de $\mathcal{O}_{X,a}$ admite prolongación analítica a lo largo de todos los caminos que parten de a, existe una única función analítica en todo X que representa ese germen. Normalmente no es esta la situación pero podemos tratar de considerar la prolongación mayor posible de cada germen analítico.

Si $p : Y \to X$ es una aplicación holomorfa no ramificada, como p es localmente biholomorfa, para cada punto $y \in Y$ la composición con p da lugar a isomorfismos de $\mathbb{C}$- álgebras:

$$p_y^* : \mathcal{O}_{X,p(y)} \to \mathcal{O}_{Y,y},\ p_*^y = (p_y^*)^{-1} : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,p(y)}$$

Definición 9.15.– *Dados:*

- *Una superficie de Riemann X.*
- *Un punto $x \in X$.*
- *Un germen de función analítica $\varphi \in \mathcal{O}_{X,a}$.*

Se llama continuación analítica de φ a toda cuaterna (Y, p, f, b) tal que:

- *Y es una superficie de Riemann y $p : Y \to X$ es una aplicación holomorfa no ramificada.*
- *$f \in \mathcal{O}_Y(Y)$.*

- $b \in Y$ *con* $p(b) = a$ *y* $p_*^y([f]_b) = \varphi$.

Una continuación analítica se dice maximal si verifica la siguiente propiedad universal:
Para toda continuación analítica (Z, q, g, c) *de* φ *existe un único morfismo analítico* $F : Z \to X$ *tal que:*

- $p.F = q$.
- $F(c) = b$.
- $f.F = g$.

Si (Y, p, f, b) es una continuación analítica de $\varphi \in \mathcal{O}_{X,a}$ y si $\delta : [0, 1] \to Y$ es un camino con origen en b y extremo en y, el germen $\psi = p_*^y([f]_y)$ es prolongación analítica de φ a lo largo de la curva proyección $p\delta$. También se verifica que la continuación maximal, si existe, es única salvo isomorfismos.

Teorema 9.16.– *Todo germen analítico en una superficie de Riemann posee continuación analítica.*

Demostración: Dada la superficie de Riemann X y el germen analítico $\varphi \in \mathcal{O}_{X,x}$, tomamos la componente conexa de φ en $|\mathcal{O}_X|$, Y. En virtud de 9.11 Y se puede dotar de estructura de superficie de Riemann de modo que la proyección $\pi : Y \to X$ sea holomorfa, tomamos como punto $b = \varphi$ y construimos la función $f : Y \to \mathbb{C}$ asignando a cada germen $\psi \in \mathcal{O}_{X,y}$, es decir, tal que $\pi(\psi) = y$ el valor $\psi(y)$, es decir:

$$\forall \psi \in \mathcal{O}_{X,y},\ f(\psi) = \psi(y) = \psi(\pi(\psi))$$

De este modo f es holomorfa y (Y, p, f, b) es una continuación analítica maximal de φ □

Vamos a construir usando estos resultados la función algebraica asociada a un polinomio con coeficientes funciones analíticas de una variable. Comenzaremos haciendo ver el carácter casi-henseliano del anillo de funciones holomorfas en el disco, es decir a comprobar que si se puede encontrar la forma ininicial de una solución de una ecuación polinómica, se puede resolver la ecuación:

Proposición 9.17.– *Si* $c_1, ..., c_n$ *son funciones holomorfas en el disco de radio* $r > 0$*:*

$$\mathbb{D}_r(0) = \{z \in \mathbb{C},\ |z| < r\}$$

y si z_0 *es un cero simple del polinomio:*

$$X^n + c_1(0)X^{n-1} + ... + c_n(0) \in \mathbb{C}[X]$$

existe un número real $s,\ 0 < s \leq r$ *y una función* $\varphi \in \mathcal{O}_{\mathbb{C}}(\mathbb{D}_s(0))$ *tal que:*

$$\varphi^n + c_1\varphi^{n-1} + ... + c_n = 0,\ y\ \varphi(0) = z_0$$

Demostración: La función:

$$F : \mathbb{D}_r(0) \times \mathbb{C} \to \mathbb{C},\ F(w,z) = z^n + c_1(w)z^{n-1} + ... + c_n(w)$$

es una función analítica de dos variables. Como los ceros de un polinomio son aislados existe un $\varepsilon > 0$ tal que el polinomio $F(0,z)$ no tiene más ceros en el disco $\mathbb{D}_\varepsilon(z_0)$ que z_0, entonces al se F continua existe un $s,\ 0 < s \leq r$ tal que la función F no tiene ceros en:

$$\{(w,z) \in \mathbb{C}^2,\ |w| < s,\ |z - z_0| = \varepsilon\}$$

Para cada $w \in \mathbb{D}_s(0)$ el número de ceros de $F(w,z)$ en el disco $\mathbb{D}_\varepsilon(z_0)$ está dado por:

$$N(w) = \frac{1}{2\pi i}\oint_{|z-z_0|=\varepsilon} \frac{\partial_z F(w,z)}{F(w,z)}dz$$

como $N(0) = 1$ es $N(w) = 1$ para todo $w \in \mathbb{D}_s(0)$. Entonces por el teorema de los residuos el cero en z de $F(w,z)$ para cada $w \in \mathbb{D}_s(0)$ está dado por:

$$\varphi(w) = \frac{1}{2\pi i}\oint_{|z-z_0|=\varepsilon} z\frac{\partial_z F(w,z)}{F(w,z)}dz$$

esta función es holomorfa en w sobre el disco $\mathbb{D}_s(0)$ y claramente verifica que:

$$F(w, \varphi(w)) = 0,\ \forall w \in \mathbb{D}_s(0)$$

□

Como consecuencia, el anillo de gérmenes de funciones holomorfas en un punto de una superficie de Riemann, isomorfo al anillo de gérmenes en 0 de funciones analíticas de una variable compleja es henseliano y en particular:

Consecuencia 9.18.– *Si* X *es una superficie de Riemann,* $x \in X$ *y:*

$$P(T) = T^n + c_1T^{n-1} + ... + c_n \in \mathcal{O}_{X,x}[T]$$

verifica que el polinomio

$$p(T) = T^n + c_1(0)T^{n-1} + ... + c_n(0) \in \mathbb{C}[T]$$

tiene n raíces distintas $z_1, ..., z_n$, existen elementos $\varphi_1, ..., \varphi_n \in \mathcal{O}_{X,x}$ tales que:

$$P(T) = \prod_{i=1}^{n}(T - \varphi_i),\ \varphi_i(0) = z_i,\ \forall i,\ 1 \leq i \leq n.$$

Podemos probar ahora que dado un polinomio con coeficentes meromorfos sobre una superficie de Riemann, podemos *adjuntar* a esta superficie una raíz del polinomio.

Teorema 9.19.– *Sea X una superficie de Riemann y sea:*

$$P(T) = T^n + c_1 T^{n-1} + ... + c_n \in \mathcal{M}_X(X)[T]$$

un polinomio irreducible entonces existen:

- *Una superficie de Riemann Z*
- *Un revestimiento analítico ramificado de n hojas $\pi : Z \to X$*
- *Una función meromorfa $F \in \mathcal{M}_Y(Y)$ tales que $\pi^*(P)(F) = 0$. Los datos (Z, π, F) están unívocamente determinados salvo aplicaciones biholomorfas que conservan las fibras*

Demostración: Llamemos A al conjunto de ceros del discriminante de P, es decir, al lugar de los puntos de X en los cuales el polinomio tiene raíces multiple. Como P es irreducible $A \neq X$ y por tanto, A es un cerrado formado por puntos aislados, y en cada punto de $X' = X \setminus A$ el polinomio P tiene n raíces simples.

En consecuencia si llamamos:

$$Y' = \{\varphi \in \mathcal{O}_{X,x} \subset |\mathcal{O}_X|, x \in X', P(\varphi) = 0\}$$

se verifica, por la proposición anterior, que para todo $x \in X'$ existen un entorno abierto U de x y funciones en $\mathcal{O}_X(U)$, $\varphi_1, ..., \varphi_n$ tales que:

$$P(T) = \prod_{i=1}^{n}(T - \varphi_i), \text{en} U$$

Entonces en la topología étale,

$$\pi^{-1}U = \bigcup_{i=1}^{n} C_{U,\varphi_i}$$

y U es un entorno bien cubierto con lo cual Y' es un revestimiento no ramificado de X', la misma construcción de la prolongación anlatica proporciona la función f, y toda la estructura se extiende por el teorema de singularidades evitables a los puntos de ramificación. □

Si X es la recta proyectiva compleja, los coeficientes son necesariamente funciones racionales, el polinomio es entonces un polinomio en dos variables y además al ser el morfismo de proyección un morfismo propio, Y es una superficie de Riemann compacta. También se verifica el recíproco de este resultado, es decir, toda superficie de Riemann compacta es la superficie de Riemann de un polinomio.

Observemos que si $\sigma : Z \to X$ es una aplicación analítica no constante, induce, por composición, un homomorfismo no trivial entre los cuerpos de funciones meromorfas sobre X y sobre Z

$$\sigma^* : \mathcal{M}_X(X) \to \mathcal{M}_Z(Z),\ \sigma^*(f) = f\sigma$$

Veremos a continuación que si σ es propia la extensión es algebraica y que su grado es el número de hojas de σ. Para ello necesitamos un resultado complementario sobre la actuación de las funciones simétricas elementales.

Como notación, dadas variables $T, x_1, ..., x_n$, podemos formar el polinomio:

$$\prod_{i=1}^{n}(T - x_i) = T^n + c_1T^{n-1} + ... + c_n,\ c_i = (-1)^i s_i(x_1, ..., x_n)$$

donde las s_i son las funciones simétricas elementales. Sea $\pi : Y \to X$ un revestimiento analítico no ramificado y sea $f \in \mathcal{M}_Y(Y)$. Para cada punto $x \in X$ podemos tomar un abierto bien cubierto V, y llamamos:

$$\pi^{-1}(V) = \bigcup_{i=1}^{n} V_i;\ \tau_i = \pi|_{V_i}^{-1};\ f_i = f|_{V_i}.\tau_i.$$

Podemos escribir:

$$\prod_{i=1}^{n}(T - f_i) = T^n + c_1(f_1, ..., f_n)T^{n-1} + ... + c_n(f_1, ..., f_n)$$

Obviamente las funciones meromorfas $c_i(f_1, ..., f_n)$ pegan y definen funciones meromorfas en X a las que representaremos por $c_i(f)$ y llamaremos *funciones simétricas elementales* de f respecto del revestimiento.

Las funciones simétricas elementales están también bien definidas aunque se trate de un revestimiento ramificado a consecuencia del teorema de singularidades evitables de Riemann. La proposición siguiente es consecuencia inmediata de la construcción de las funciones simétricas elementales.

Proposición 9.20.– *Si $\sigma : Z \to X$ es una aplicación analítica propia de n hojas y si $f \in \mathcal{M}_Z(Z)$ entonces:*

$$f^n + \sigma^*(c_1(f))f^{n-1} + ... + \sigma^*(c_n(f)) = 0.$$

en consecuencia $\sigma^* : \mathcal{M}_X(X) \to \mathcal{M}_Z(Z)$ es una extensión algebraica de grado $\leq n$.

Un resultado de Riemann de existencia de funciones meromorfas, que no probaremos, permite asegurar que el grado de la extensión es precisamente n.

Se llaman *valores críticos* de un morfismo analítico ramificado $\sigma : Z \to X$ a las imágenes de los puntos de ramificación. Los valores críticos forman un conjunto discreto. Suprimiendo en X un cerrado discreto A que contenga a los valores críticos y llamando:

$$X' = X \setminus A,\ Z' = \sigma^{-1}(X'), \sigma' = \sigma|_{Z'}$$

el teorema de singularidades evitables de Riemann permite extender las transformaciones recubridoras del revestimiento $\sigma' : Z' \to X'$ a transformaciones biholomorfas que conservan las fibras de σ. Usando la notación clásica para superficies de Riemann, llamaremos al grupo formado por estas transformaciones $Deck(Z/X)$. Extendemos a los revestimientos ramificados la noción de revestimiento de Galois:

Definición 9.21.– *Con las notaciones anteriores el revestimiento ramificado $\sigma : Z \to X$ se dice de Galois si lo es el revestimiento $\sigma' : Z' \to X'$*

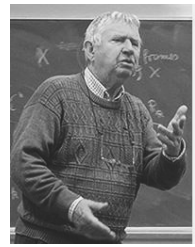
La combinación de estos resultados con el teorema 9.19 nos lleva al teorema central que es la justificación de esta sección y que establece que para las funciones algebraicas las teorías de Galois algebraica y topológica son la misma teoría:

Teorema 9.22.– *Si X es una superficie de Riemann, $P(T) \in \mathcal{M}_X(X)[T]$ es un polinomio irreducible de grado n, y (Y, π, F) es la función algebraica definida por $P(T)$:*

- *$\mathcal{M}_Y(Y)$ es una extensión algebraica de $\mathcal{M}_X(X)$ de grado n.*
- *$\mathcal{M}_Y(Y) \simeq \mathcal{M}_X(X)[T]/(P(T))$.*
- *Toda transformación recubridora $\sigma \in Deck(Y/X)$ induce un $\mathcal{M}_X(X)$-automorfismo de $\mathcal{M}_Y(Y)$ por $f \mapsto f.\sigma^{-1}$, asi tenemos un isomorfismo de grupos :*

$$Deck(Y/X) \simeq Gal_{\mathcal{M}_X(X)}(\mathcal{M}_Y(Y))$$

- *El revestimiento Y/X es de Galois si y solo si lo es la extensión correspondiente de los cuerpos de funciones meromorfas.*



Malgrange remarked that another way to "save" Schlesinger's theorem for non-Fuchsian linear differential equations - without adding new Galois ambiguities - is to replace algebraic groups by algebraic groupoids. This approach then generalizes to the non-linear case (foliations with singularities) if one further replace "algebraic groupoid" (defined by algebraic equations) by "algebraic D-groupoid" (defined by algebraic systems of partial differential equations, using jets).

Yves Andre

10. Hacia la Teoría de Galois-Grothendieck de foliaciones

Por limitaciones de tiempo daremos solamente una introducción a la Teoría de Galois de foliaciones regulares en la versión de Grothendieck. Comenzaremos con los conjuntos con acción de un grupo, para ellos también se pueden establecer las distintas teorías de Galois, ahora de un modo más simple y menos espectacular que en las superficies de Riemann, pero hacerlo nos va a servir para justificar la aparición de los grupoides en Teoría de Galois. En esta sección seguiremos la tesis de Viaud [37].

10.1. Conjuntos con acción de grupo

Sea G un grupo y sea $((G-Sets))$ la categoría de conjuntos con acción de G y aplicaciones G estables. Observemos que:

- Todo conjunto E se puede dotar de una estructura de G- conjunto con la *acción trivial*:

$$G \times E \xrightarrow{p_2} E,\ g.e = p_2(g,e) = e$$

- Un conjunto con un solo elemento $\{0\}$ y la acción trivial de G es un objeto final de $((G - Sets))$, es decir, para todo G-conjunto S la aplicación constante $S \to \{0\}$ es el único morfismo de G-conjuntos entre ellos.

- Si H es un subgrupo de G, el conjunto de clases por la izquierda de G respecto de H, G/H, se puede dotar de una acción natural de G-conjunto:

$$G \times G/H \to G/H,\ g.(rH) = (gr)H.$$

Definición 10.1.– *Sea E un G-conjunto:*

1. *Si $A \subset E$, se llama* estabilizador *de A al conjunto:*

$$S_A = \{g \in G \mid g.A = A\}.$$

   Si $x \in E$ escribiremos S_x por $S_{\{x\}}$.

2. *Diremos que la acción de G sobre E es simple si para todo $x \in E$:*

$$g.x \neq g'.x,\ \forall g, g' \in G,\ g \neq g'.$$

3. *Diremos que la acción de G sobre E es transitiva o que E es un G - conjunto homogéneo si:*

$$\forall x, y \in E,\ \exists g \in G,\ g.x = y.$$

4. *Diremos que E es un G-torsor si la acción de G sobre E es simple y transitiva.*

Si E es un G - conjunto, es inmediato que:

- S_A es un subgrupo de G para todo $A \subset E$.

- Para $x \in E,\ g \in G$,

$$S_{gx} = g.S_x.g^{-1}$$

- La acción de G sobre E es simple si y solo si todos los estabilizadores $\{S_x\}_{x \in E}$ son triviales.

- La acción G sobre E es transitiva si y solo si E no se puede descomponer en coproducto en la categoría $((G-sets))$ de dos G-conjuntos no vacíos. Por esa razón a los conjuntos con acción transitiva se les llama también G-conexos.
- Si H es un subgrupo de G la acción natural de G sobre G/H es transitiva.
- Si la acción de G sobre E es transitiva un G -morfismo de E en otro G -conjunto F queda unívocamente determinado por la imagen de un punto.
- La acción por producto por la izquierda de G sobre G, dota a G de una estructura de torsor

Con estas observaciones estamos en condiciones de establecer una correspondencia galoisiana entre G- conjuntos homogéneos y subgrupos de G.

Proposición 10.2.– *Si E es un conjunto G -homogéneo y S es el estabilizador de un elemento de E, E es isomorfo como G- conjunto a G/S con la acción natural.*

Demostración: Si S es el estabilizador de $e \in E$, definimos:

$$\forall x \in E,\ x = g.e \Leftrightarrow f(x) = g.S \in G/S$$

Entonces, f es un isomorfismo en $((G-sets))$. □

Obviamente si H es un subgrupo de G, G/H es homogéneo y el estabilizador de la clase $1_g.H$ es H, por tanto tenemos una correspondencia biunívoca entre clases de conjugación de subgrupos de G y conjuntos G-Homogeneos. La existencia de esta correspondencia no es propiamente un teorema de Galois ya que funcionamos con clases de isomorfía en lugar de hacerlo con objetos. La situación es más clara para el formalismo de recubrimientos.

Podemos tomar como funtor fibra el funtor de olvido de la categoría $((G-sets))$ en la de conjuntos, el funtor fibra es representable y su representante es el G- conjunto que jugara el papel de revestimiento universal.

Proposición 10.3.– *Si excepcionalmente representamos por Fib al funtor de olvido de $((G-sets))$ en $((sets))$, el funtor Fib es representable y el par $(G, 1_G)$ es uno de sus representantes.*

Demostración: basta probar que para todo G -conjunto E la correspondencia:

$$\varphi_E : Hom_{((G-sets))}(G, E) \to E,\ \varphi(f) = f(1_G)$$

es biyectiva. Pero esta correspondencia es obviamente aplicación y como la acción de G sobre si mismo es simple y transitiva, para cualquier $e \in E$ existe un único morfismo $f \in Hom_{((G-sets))}(G, E)$ tal que $f(1_G) = e$. □

Los automorfismos de G como G conjunto jugarían un papel similar al de las transformaciones recubridoras del recubrimiento universal o sea al del grupo fundamental del espacio base, veamos quien es ese grupo:

Proposición 10.4.–

$$G \simeq Aut_{((G-sets))}(G).$$

Demostración: acabamos de probar que existe una biyección conjuntista:

$$\varphi_E : Hom_{((G-sets))}(G, E) \to E,\ \varphi(f) = f(1_G)$$

que aplicada a $E = G$ da lugar a una biyección:

$$\varphi_G : Hom_{((G-sets))}(G, G) \to G,\ \varphi(f) = f(1_G).$$

Pero como la acción de G sobre G es simple y transitiva, si $f \in Hom_{((G-sets))}(G, G)$, $f(g) = gf(1_G)$. Luego:

- Todos los homomorfismos de G-conjuntos de G en G son automorfismos, es decir, $Hom_{((G-sets))}(G, G) = Aut_{((G-sets))}(G)$.
- Cada automorfismo de G corresponde a multiplicar por la derecha por un elemento de G.
- φ_G es un isomorfismo de grupos.

□

Ahora observemos que en cada conjunto E en el que hemos olvidado la estructura de G-conjunto, el grupo de automorfismos del funtor fibra actúa de modo natural porque si ϕ es un automorfismo de Fib, ϕ_E es una biyección de E en E y podemos definir la acción por:

$$\phi_E.x = \phi_E(x).$$

Entonces el funtor fibra es un funtor de la categoría de G-conjuntos en la categoría de $Aut(Fib)$-conjuntos, pero al ser representable y ser G su representante $Aut(Fib) \simeq Aut_{((G-sets))}(G) \simeq G$, tenemos así el teorema de Grothendieck para este funtor fibra. Los revestimientos galoisianos corresponden a los G- conjuntos de cocientes de G por un subgrupo normal, que son aquellos sobre los cuales su grupo de automorfismos actúa de modo simple y transitivo.

10.2. Grupoides

La primera definición de grupoide se debe a Brandt (v. [3]) y está motivada por la idea de generalizar la teoría de ideales de los anillos de enteros al caso no conmutativo (v. [4]). La definición inicial de Brandt era más restringida que la que usamos hoy, sus grupoides se conocen actualmente por grupoides transitivos o conexos.

Hoy en día el concepto de grupoide es un concepto ubicuo en Matemáticas, pero la aparición de los grupoides en topología y en Teoría de Galois está motivada esencialmente por el hecho de que si, en lugar de considerar el grupo fundamental de un espacio con base en un punto, se deslocaliza el grupo y se considera en su lugar el grupoide fundamental, se simplifican muchas de las pruebas en teoría de la homotopía.

Si X es un espacio topológico, el conjunto de clases de homotopía de caminos en X con la operación de concatenación es un grupoide. Los objetos del grupoide son los puntos de X, los elementos son las clases de homotopía de caminos, para cada clase de homotopía de caminos. su origen común es su dominio y su extremo su rango. La composición es la concatenación de caminos.

Es necesario tomar clase de homotopía porque $\sigma * 1_x \neq \sigma$ pero ambos caminos son homótopos. Este grupoide se llama grupoide de homotopía de X y se representa por $\pi_1(X)$. La substitución del grupo de Poincare por el grupoide fundamental evita la necesidad de elegir un punto base y eso no solo proporciona pruebas más fáciles de algunos teoremas (Van Kampen por ejemplo), sino también proporciona resultados nuevos interesantes. El survey de R.Brown [5] y su libro [6] proporcionan detalles de estos resultados

Usando las definiciones de las secciones anteriores podemos dar la siguiente:

Definición 10.5.– *Un grupoide es una categoría en la que todos los morfismos son isomorfismos*

Si substituimos la categoría por un par de conjuntos, la unión disjunta de sus conjuntos de morfismos a la que llamaremos G, y el conjunto O de sus objetos, y traducimos a términos de estos conjuntos el dominio y rango de un morfismo, la composición de morfismos y las unidades y los inversos. Podemos dar también la definición siguiente:

Definición 10.6.– *un grupoide es un par de conjuntos (G, O) junto con:*

1. *Una aplicación $u : O \to G$.*
2. *Dos aplicaciones $d, r : G \to O$ tales que $du = ru = 1_O$.*
3. *Una aplicación involutiva $i : G \to G$ tal que $di = r$.*

4. *Si* $P = \{(a,b) \in G \times G \mid r(a) = d(b)\} = G \times_O G$ *una aplicación* $p : P \to G$, $p(a,b) = ab$ *(notación).*

De modo que:

- *La operación parcial* p *es asociativa, es decir, si existen* ab *y* bc*, existen* $a(bc)$ *y* $(ab)c$ *y* $a(bc) = (ab)c$*.*
- $\forall a \in G, au(d(a)) = u(r(a))a = a$*.*
- i *es el inverso respecto a* p *es decir,* $\forall a \in G, ai(a) = u(r(a)),\ i(a)a = u(r(a))$*.*

Los objetos que intervienen en la definición tienen todo un surtido de nombres diferentes en diversos idiomas. Aquí usaremos los siguientes:

- Al conjunto G también le llamaremos *grupoide* y a O *conjunto base*, a los elementos de G les llamaremos indistintamente *elementos del grupoide* y *flechas* y a los de O les llamaremos *objetos* o *vértices*.
- A las aplicaciones d, r, les llamaremos respectivamente *dominio* y *rango*. A la aplicación u le llamaremos *aplicación unidad*, para cada objeto $x \in O$, llamaremos a $u(x)$ *unidad* de x y la representaremos por 1_x.
- Como $du = ru = 1_O$, d y r son sobreyectivas y u es inyectiva por lo que podemos identificar O con Imu
- A $u(r(a))$ y $u(d(a))$ les llamaremos respectivamente *unidad por la izquierda* y *unidad por la derecha* de a.
- A $i(a)$ le llamaremos *inverso* de a y lo representaremos por a^{-1}.
- Representaremos por:

$$\Omega_x = d^{-1}(x),\ \Omega^y = r^{-1}(y),\ \Omega_x^y = \Omega_x \cap \Omega^y$$

Cada Ω_x^x se llama *grupo vértice* del grupoide.

Ejercicios 10.7.–

Ejercicio. 10.7.1.-
Probar que las dos definiciones de grupoide son equivalentes.

Ejercicio. 10.7.2.-
Probar que:

1. $\forall g \in G,\ d(g) = x\mathrm{y}gh = g \Rightarrow h = 1_x$.
2. $\forall g \in G,\ d(g) = x\mathrm{y}hg = 1_x \Rightarrow h = g^{-1}$

y por simetría de las definiciones que:

1. $\forall g \in G,\ r(g) = x\mathrm{y}hg = g \Rightarrow h = 1_x$.
2. $\forall g \in G,\ r(g) = x\mathrm{y}gh = 1_x \Rightarrow h = g^{-1}$.

Ejercicio. 10.7.3.-
Probar que los grupos vértice son efectivamente grupos y que:

$$\Omega_x^y \neq \emptyset \Rightarrow \Omega_x^x \simeq \Omega_y^y.$$

Definición 10.8.– *Llamaremos morfismo entre dos grupoides* $(G_1, O_1, r_1, d_1, u_1, i_1, p_1)$ *y* $(G_2, O_2, r_2, d_2, u_2, i_2, p_2)$ *a todo par de aplicaciones:*

$$\chi : O_1 \to O_2,\ \psi : G_1 \to G_2$$

tales que:

1. $d_2\psi = \chi d_1$.
2. $r_2\psi = \chi r_1$.
3. $\forall g, h \in G_1$ *tales que* $r_1(g) = d_1(h))$ *es* $\psi(hg) = \psi(p_1(h, g)) = p_2(\psi(h), \psi(g)) = \psi(h)\psi(g)$.

Si ambas aplicaciones son biyectivas el morfismo se llama isomorfismo.

Ejercicios 10.9.–

Ejercicio. 10.9.1.- Probar que un morfismo de grupoides es lo mismo que un funtor entre ellos considerados como categoríias.

Ejercicio. 10.9.2.- Probar que si (χ, ψ) es un morfismo de grupoides:

$$\psi(1_x) = 1_{\chi(x),\ \psi(g^{-1}) = \psi(g)^{-1}}$$

Ejemplos 10.10.–

Ejemplo. 10.10.1.- [Estructura de grupoides].- En este primer ejemplo veremos tres modelos básicos de grupoide y daremos un teorema de estructura que prueba que esencialmente los grupoides no son sino una relación de igualdad y una familia de grupos:

1. Si $\{G_b\}_{b\in B}$ es una familia de grupos, su unión disjunta con las operaciones razonables es un grupoide con base B, cuyos grupos vértice son los G_b.

2. Si $R \subset B \times B$ es una relación de igualdad, R es un grupoide de base B, la operación se construye por la propiedad transitiva de la relación y las aplicaciones d y r son las proyecciones y los grupos vértice son todos triviales.

3. Si B es un conjunto y G un grupo el conjunto, $B \times G \times B$, se puede dotar de estructura de grupoide de base B y grupos vértice iguales todos a G por:

   a) Las aplicaciones r y d son las proyecciones sobre la primera y tercera componente respectivamente,

   b) $(y, h, z)(x, g, y) = (x, hg, z)$.

   c) $1_x = (x, 1, x),\ (x, g, y)^{-1} = (y, g^{-1}, x)$.

   Si $G = \{1\}$ este grupoide es el asociado a la relación de igualdad total de B.

Ejercicios 10.11.–

Ejercicio. 10.11.1.- Probar que un grupoide es el asociado a una relación de igualdad si y solo si todos sus grupos vértice son triviales.

Ejercicio. 10.11.2.- ¿Cuál es la suma directa (coproducto) de una familia de grupoides?

Ejercicio. 10.11.3.- Un grupoide de base B se llama *transitivo* si:

$$\forall x, y \in B,\ \Omega_x^y \neq \emptyset.$$

Probar que todo grupoide es suma directa de grupoides transitivos.

Ejercicio. 10.11.4.- Probar que todo grupoide transitivo G de base B es isomorfo a uno de la forma $B \times G \times B$ y en consecuencia que los grupoides de base B se corresponden con los pares $(R, \mathcal{G})$ donde R es una relación de igualdad en B y $\mathcal{G}$ una familia de grupos indexada por el conjunto cociente B/R.

Sugerencia: Fijo $x \in B$, consideramos la aplicación rango: $r : \Omega_x \to B$, como el grupoide es transitivo r es sobre y se puede construir una inversa por la izquierda $\tau : B \to \Omega_x$, probar que la aplicación:

$$: B \times \Omega_x^x \times B \to G,\ \psi((y,g,z)) = \tau(z) g \tau(y)^{-1}$$

verifica que $(1_B, \psi)$ es un isomorfismo.

Ejemplo. 10.11.1.- Si G es un grupo que actúa sobre un conjunto X, podemos dotar a $T = X \times G$ de estructura de grupoide:

- $O = X, u = X \equiv X \times \{1\}$
- $r(x,g) = gx, d(x,g) = x$
- $r(x,g) = d(y,h) \Leftrightarrow y = gx,\ (x,g).(y,h) = (x,hg)$

En términos de categorías los objetos de T son los elementos de X y los homomorfismos $Hom_T(x,y) = \{g \in G \mid gx = y\}$. Claramente en esta categoría:

$$x \simeq y \Leftrightarrow x, y \text{ están en la misma órbita para la acción de } G$$

de este modo las clases de isomorfía del grupoide son las órbitas.
Si G es un grupo en una categoría $\mathfrak{C}$, que actúa sobre un objeto X, para todo objeto S, $Hom_{\mathfrak{C}}(S,G) = G(S)$ es un grupo que actúa sobre el conjunto $Hom_{\mathfrak{C}}(S,X) = X(S)$, tenemos así para cada objeto S el grupoide $T(S)$ construido como en el ejemplo anterior.

Ejemplo. 10.11.2.- Si la acción de G sobre E es simple y transitiva, es decir, si $E \simeq G$ considerando la acción de G sobre si mismo por producto por la derecha, se dice que E es un G- torsor.
Dado un G-conjunto X, se llama G-torsor de X a un par (E,u) donde E es un G-torsor y $u : E \to X$ un morfismo equivariante. Un morfismo de G -torsores de X de (E,u) a (F,v) es un morfismo equivariante $\beta : E \to F$ tal que $v\beta = u$.
Observemos que:

- Los G-torsores de X y sus morfismos forman una categoría.
- Todo morfismo de G- torsores es un isomorfismo.
- Las imágenes en X de los G-torsores son las órbitas de X por la acción de G.
- Dos G- torsores de X son isomorfos si y solo si tienen como imagen la misma órbita.

Es decir, la categoría de G-torsores de X es también un grupoide cuyas clases de isomorfia de objetos se corresponden con las órbitas de X por la acción de G.
Para cada x de X tenemos el G-torsor de X, $\rho_x : G \to X,\ \rho_x(g) = xg$ tenemos así un funtor de la categoría T construida en el ejemplo anterior en la categoría de G-torsores de X que es fiel, completo y esencialmente suprayectivo, por tanto ambas categorías son equivalentes y equivalentes al grupoide asociado a la acción trivial de G sobre el espacio de órbitas X/G.

Ejemplo. 10.11.3.- Sea X un espacio topológico y sea $\{U_i\}_{i\in I}$ un recubrimiento abierto de X, podemos construir los conjuntos:

- $U = \coprod_{i\in I} U_i$.
- $G = U \times_X U = \coprod_{i,j\in I} U_i \cap U_j$.

y las aplicaciones siguientes dotan al par (G, U) de estructura de grupoide:

1. $u : U \to G,\ u(x) = x$, es decir, si $x \in U$ existe un único $i \in I$ con $x \in U_i = U_i \cap U_i \subset G$ y u está bien definida.
2. $d|_{U_i\cap U_j}$ es la inclusión $U_i \cap U_j \subset U_i$.
3. $r|_{U_i\cap U_j}$ es la inclusión $U_i \cap U_j \subset U_j$
4. $i|_{U_i\cap U_j}$ es la identidad $U_i \cap U_j = U_j \cap U_i$.
5. Si
$$(x, y) \in P, x \in U_i \cap U_j,\ y \in U_l \cap U_k$$
entonces
$$r(x) = x \in U_j,\ d(y) = y \in U_l,\ r(x) = d(y) \Rightarrow l = j,\ x = y$$
y definimos:
$$p(x, y) = x \in U_i \cap U_k.$$

En vez de un recubrimiento podríamos haber tomado un atlas de una variedad diferenciable o de un espacio analítico, substituyendo las identidades por los cambios de carta.

Definición 10.12.– *Un grupoide topológico es un grupoide en el que tanto el conjunto de flechas G como el de vértices O están dotados de una topología y se verifica que son continuas las aplicaciones*

- $u : O \to G$.

- $d, r : G \to O$.
- $i : G \to G$.
- $p : P \to G,\ p(a,b) = ab$ *donde* $P = \{(a,b) \in G \times G \ \mid \ r(a) = d(b)\} = G \times_O G$ *con la topología inducida.*

10.3. Relaciones locales

En esta última sección vamos a exponer de modo muy somero algunos aspectos de la propuesta de Grothendieck [19] para una Teoría de Galois de foliaciones regulares. Comencemos con el objeto topológico correspondiente a una foliación:

Si C es un conjunto una relación de equivalencia en C no es otra cosa que un subconjunto $R \subset C \times C$ tal que:

- $\Delta(C) = \{(x,x),\ \forall x \in C\} \subset R$.
- $(x,y) \in R \Rightarrow (y,x) \in R$.
- $(x,y) \in R,\ (y,z) \in R \Rightarrow (x,z) \in R$.

Es claro que si $\{R_i\}_{i \in I}$ son relaciones en C, $\cap_{i \in I} R_i$ es una relación de equivalencia en C, por tanto tiene sentido hablar de la mínima relación de equivalencia que contiene a un subconjunto S de $C \times C$, a la que llamaremos *relación de equivalencia generada por* S, y también es claro que si R es una relación de equivalencia en C y $T \subset C$, $R \cap T \times T$ es una relación de equivalencia en T a la que llamaremos *restricción* de R a T Si X es un espacio topológico, podemos construir para cada abierto U de X el conjunto $\mathbb{E}_X(U) \subset U \times U$ de relaciones de equivalencia en U, siempre que $U \subset V$ sean abiertos de X la restricción es una aplicación

$$\rho_{V,U} : \mathbb{E}_X(V) \to \mathbb{E}_X(U),\ \rho_{V,U}(R) = R \cap V \times V$$

Tenemos de esta forma un prehaz de conjuntos sobre X que en general no es un haz.

Ejercicio 10.13.– Poner un ejemplo que pruebe que $\mathbb{E}_X$ no es un haz (basta con un espacio con tres puntos)

Definición 10.14.– *Llamaremos relación de equivalencia local en X a toda sección global del haz $\mathcal{E}_X$ asociado al prehaz $\mathbb{E}_X$.*

Como consecuencia de la construcción del haz asociado a un prehaz, una relación de equivalencia local en X consiste en:

- Un recubrimiento abierto $\{U_i\}_{i\in I}$ de X
- Una familia de relaciones de igualdad $R_i \in \mathbb{E}_X(U_i),\ \forall i \in I$

Tales que:

$$(*) \quad \forall i,j \in I,\ \forall z \in U_i \cap U_j,\ \exists W \in \mathfrak{T}(X),\ z \in W \subset U_i \cap U_j,\ \rho_{U_i,W}(R_i) = \rho_{U_j,W}(R_j).$$

Hay que notar que no se puede establecer la compatibilidad por coincidencia en las fibras, y que la coincidencia de dos relaciones locales se mide por coincidencias en las restricciones a las intersecciones de los dominios. En particular un par (V, R) donde V es un abierto de X y R es una relación de equivalencia en V se dice que es *una carta local* para la relación de equivalencia local r definida por la familia $\{(U_i, R_i)\}_{i\in I}$ si:

$$\forall i \in I,\ \forall z \in U_i \cap V,\ \exists W \in \mathfrak{T}(X),\ z \in W \subset U_i \cap V,\ \rho_{U_i,W}(R_i) = \rho_{U,W}(R)$$

Un recubrimiento de X formado por cartas compatibles se llama un $atlas$ para la relación local.

Ejemplo 10.15.– El ejemplo más interesante de relación local es el de foliación (regular). Si X es una variedad C^∞ de dimensión $n = p + q,\ 0 < q < n$, una foliación de codimensión q en X es un objeto definido por:

- Un recubrimiento abierto $\{U_i\}_{i\in I}$ de X
- Para cada $i \in I$ un difeomorfismo $\varphi_i : \mathbb{R}^n = \mathbb{R}^p \times \mathbb{R}^q \to U_i$.

Tales que para todos i, j existan funciones C^∞,

$$\varphi_{i,j} : \mathbb{R}^n \to \mathbb{R}^p,\ \gamma_{ij} : \mathbb{R}^q \to \mathbb{R}^q$$

tales que el cambio de carta sea del tipo:

$$\varphi_j^{-1}\varphi_i : \varphi_i^{-1}(U_i \cap U_j) \to \varphi_j^{-1}(U_i \cap U_j)$$

$$\varphi_j^{-1}\varphi_i(\mathbf{x}, \mathbf{y}) = (\mathbf{x}', \mathbf{y}'),\ \mathbf{x}' = \varphi_{i,j}(\mathbf{x}, \mathbf{y}),\ \mathbf{y}' = \gamma_{i,j}(\mathbf{y}).$$

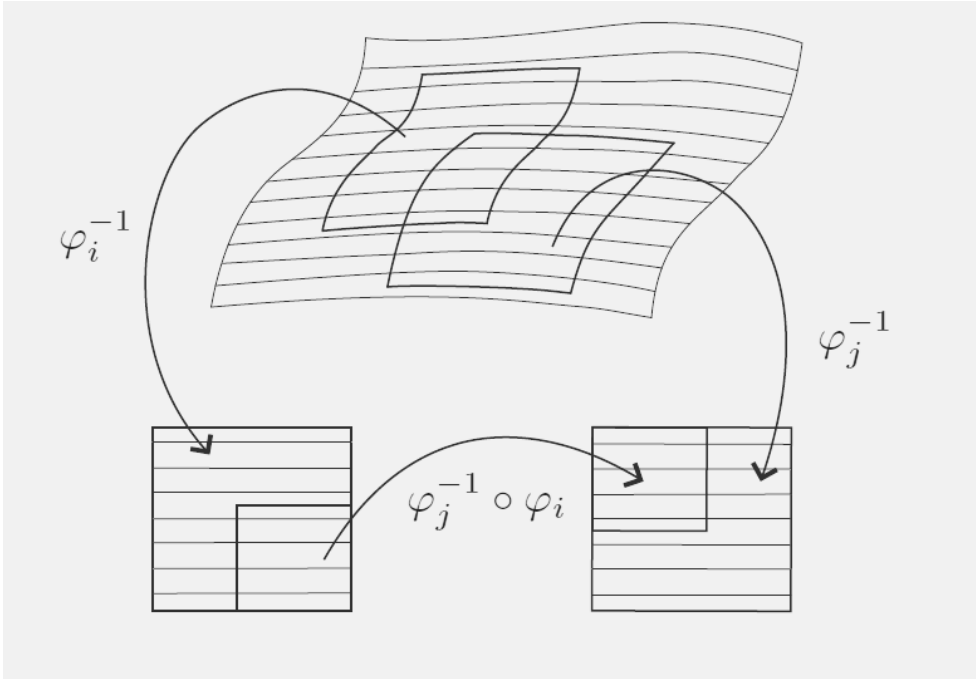


Figura 1: Representación gráfica del ejemplo 10.15

La foliación es un ejemplo de relación local. Sobre cada abierto del recubrimiento U_i la relación estaría definida por:

$$(A, B) \in R_i \Leftrightarrow \varphi_{i,j}\varphi_i^{-1}(A) = \varphi_{i,j}\varphi_i^{-1}(B)$$

Definición 10.16.– *Si R es una relación de equivalencia en un espacio topológico X, llamaremos R-topología en X a la que tiene como base de abiertos los conjuntos de la forma $U \cap xR$ donde U es un abierto de X y xR la clase en R de $x \in X$.*
Si r es una relación de equivalencia local en X, llamaremos r- topología de X, a la que tiene como base de abiertos los conjuntos $U \cap xR$ donde U es un abierto de X, (V, R) es una carta local de r y xR la clase en R de $x \in V$.

A X con la r-topología, lo representaremos por X_r.

Para mantener la analogía con las foliaciones, si $(U,\ R)$ es una carta de r las clases de U módulo R se llaman *placas* de la relación. Es claro que, puesto que $(U \cap V,\ R|_{U\cap V})$ es también un carta de r, podemos reescribir la definición anterior diciendo que la r- topología es la topología menos fina de entre las topologías más finas que la de X y tales que en ella las placas de la relación son abiertas.

Normalmente requeriremos a las relaciones unas propiedades topológicas que enunciamos a continuación:

Definición 10.17.– *Sea R una relación de equivalencia en un espacio topológico X:*

1. *Diremos que R es* abierta *si el saturado de cada abierto U por R:*

$$S_R(U) = \{x \in X \mid \exists y \in U,\ xRy\} = \bigcup_{y\in U} yR$$

   es abierto.

2. *Diremos que R es conexa si sus clase de equivalencia son conexas.*

3. *Diremos que R es localmente conexa, si si existe una base de la topología de X, $\{U_i\}_{i\in I}$ tal que las clases de $R|_{U_i}$ son conexas.*

4. *De modo similar a las dos definiciones anteriores se definen relaciones simplemente conexas, localmente simplemente conexas, conexas por caminos y localmente conexas por caminos.*

Estas definiciones se extienden a las relaciones locales por medio de sus atlas:

Definición 10.18.– *Sea r una relación de equivalencia local en un espacio topológico X:*

1. *Una carta (R, U) de r se dice* abierta *si R es abierta en U. Un atlas de r se dice abierto si sus cartas son todas abiertas.*

2. *De modo similar a la definición anterior se definen relaciones locales conexas simplemente conexas, localmente simplemente conexas, conexas por caminos y localmente conexas por caminos.*

Ejercicios 10.19.–

Ejercicio. 10.19.1.- .- Probar que la relación local asociada a una foliación regular es abierta, localmente conexa y localmente simplemente conexa.

Ejercicio. 10.19.2.- .- Probar que la relación definida en RR^2 por:

$$(x,y)R(z,t) \Leftrightarrow\ x^2+y^2=z^2+t^2$$

es abierta y localmente conexa pero no es localmente simplemente conexa.

A partir de ahora fijaremos en un espacio X una relación local r que será abierta, localmente simplemente conexa y localmente conexa por caminos y vamos a construir su grupoide de monodromía esencialmente como el grupoide de *clases de homotopía de caminos sobre las hojas de la relación*.

Sea X un espacio topológico y sea X^I el conjunto de caminos en X, es decir, el conjunto de aplicaciones continuas:

$$\sigma : [0,1] \longrightarrow X$$

La *topología compacta-abierta* de X^I es la topología que tiene como base de abiertos los conjuntos:

$$N_X(U_1,...,U_s) = \{\sigma \in X^I \mid \sigma([\frac{i-1}{s},\frac{i}{s}]) \subset U_i,\ 1 \leq i \leq s\}.$$

Donde los U_i recorren una base de la topología de X y s recorre $\mathbb{N}$.

La aplicación identidad $X_r \rightarrow X$ es continua y en consecuencia, tenemos una aplicación inyectiva $\delta : X_r^I \rightarrow X^I$; dotamos al espacio X^I de la topología compacta abierta, y esa topología induce una topología en la imagen de δ. Al espacio resultante lo representaremos por $P(X,r)$. Una base de la topología de $P(X,r)$ está formada por los conjuntos

$$N_X((U_1,R_1),...,(U_s,R_s)) = \{\sigma \in X^I \mid \sigma([\frac{i-1}{s},\frac{i}{s}]) \subset \sigma(\frac{i}{s})R_i,\ 1 \leq i \leq s\}$$

Donde los (U_i,R_i) recorren el conjunto de cartas compatibles con r.

Entonces $(P(X,r),X_r)$ se puede dotar de aplicaciones dominio y rango que son continuas, concatenación de caminos que también es continua, así como la inversión. Se pueden definir homotopías en X_r y clasificar $P(X,r)$ módulo homotopías. Tememos así el grupoide de Monodromía de la relación que es un grupoide topológico. No entraremos por las limitaciones del curso en la holonomía (espacio de hojas), el trasporte o la construccion de los recubrimientos y la Teoría de Galois que pueden verse en [21]

Referencias

[1] André, Y., *Ambiguity Theory, Old and New*, Bolletino U.M.I. (**8**),**I**(2008).

[2] Birkhoff, G.W. *Three Public Lectures on Scientific Subjects.The Principle of Sufficient Reason* Lectures delivered at the Rice Institute, March 6, 7, and 8, (1940).

[3] Brandt, H., *Uber eine Verallgemeinerung des Gruppenbegriffes*, Math. Ann. **96** (1926) 360-366.

[4] Brandt, H, *Idealtheorie in Quaternionenalgebren*, Math. Ann. **99** (1928) 1-29.

[5] Brown, R. *From groups to grupoids; A brief survey*. Bull. London Math. Soc. **19** (1987), 113-134.

[6] Brown, R. *Elements of modern topology*. McGraw Hill, Maidenhead, 1968.

[7] Cameron, P.J. *Sets, Logic and Categories*. Springer Verlag, Berlin. 1999.

[8] Casale, G. *Sur le grupoïde de Galois d'un feuilletage*. Thèse Univ Paul Sabatier Toulouse (2004).

[9] Dubuc, E.J. y De la Vega C.S. *On the Galois theory of Grothendieck*. Bol. Acad. Nac. Córdoba **65** (2000), 111 – 139.

[10] Dubuc, E.J., *Categorías los treinta primeros años*. arXiv 1404-6240v1. 24 de abril de 2014.

[11] Ehresmann, C. *Catégories topologiques et catégories différentiables*, Colloque Géom. Diff. Globale (Bruxelles, 1958), Centre Belgue Rech. Math. Louvain, 1959, 137 -150.

[12] Eilenberg B. y Mac Lane S. *General Theory of Natural Equivalences*, Transactions of the American Mathematical Society Vol. **58** (1945), 231 -294.

[13] Forster, O. *Lectures on Riemann surfaces*, Spriger Verlag, New York 1981.

[14] Gabriel, P. *Des catégories abeliénnes*. Bull. Soc. Math. France, Vol. **70**,(1962), 323 - 448.

[15] Galois, E. *Oeuvres mathématiques*. Gauthiers-Villars, 1951.

[16] Godement, R. *Théorie des faisceaux*, Hermann, Paris 1958.

[17] Grenberg, M.J. *Lectures on Algebraic Topology*. W.A. Benjamin, Reading Mass. 1973.

[18] Grothendieck, A. *Éléments de géométrie algébrique I (Le langage des schémas) (EGA 1)*. Pub. Math. I.H.E.S. **4**, Paris 1960.

[19] Grothendieck, A. *Revêtements étales et groupe fondamental (SGA 1)*. Springer Verlag, Berlin. 1971.

[20] Hofstadter, D.R. *Gödel, Escher, Bach: Un eterno y grácil bucle*. Tusquets. Barcelona 2007.

[21] Kock, A. y Moedijk, I. *Espaces with local equivalence relations and their monodromy*. Topology and its App. **72**,(1996), 47 - 78.

[22] Krull, W. *Galoische Theorie der unendlichen algebraischen erweiterungen*. Mat. Annalen Vol. **100**,(1928), 687 -698.

[23] Low, Zhen Lin, *Universes for Category Theory*.arXiv 1304-5227v2. 28 noviembre 2014.

[24] Mackenzie, K. C. H. *Lie grupoids and Lie algebroids in differential Geometry*. London Math. Soc. Lecture Notes vol(**124**) Cambridge Univ. Pres. (1987).

[25] Mackenzie, K. C. H. *General theory of Lie grupoids and Lie algebroids*. London Math. Soc. Lecture Notes vol(**213**) Cambridge Univ. Pres. (2005).

[26] Mac Lane, S. *One universe as a foundation for category theory*. Reports of the Midwest Category Seminar III. Springer Lect. Notes Math. **106** (1969): 192-200

[27] McCleary, J. *A history of Algebraic Topology*. 2009 Springsession Korean Colloquium.14 pp.

[28] Moschovakis, Y.N.*Notes on Set Theory* Undergraduate text in Math. Springer Verlag, Berlin (1994).

[29] Núñez, J., Tenorio A.F., Vilches, J.A.,*Elementos de la teoría de grupoides y algebroides* Serv. pub. Univ Cadiz (2006).

[30] Ramis, J. P., *La theorie de l'ambiguïté,: de Galois aux systèmes dynamiques*. Séance solennelle de l'Académie des sciences.Réception des Membres élus en 2005. Paris 2006.

[31] Ramis, J. P., *The theory of Ambiguity of E. Galois*. Conferencia en el CTRI-Uva, mayo 2011.

[32] Remmert, R., *From Riemann surfaces to complex spaces*. Seminaires et Congrés (Soc. Math. France) **3** (1998) pp 203 - 241.

[33] Ribes, L., Zaleskii, P., *Profinite Groups*. Ergebnisse der Math. vol. 40. Springer Verlag, Berlin (2000).

[34] Rosenthal K.I., *Local equivalence relations* Topology and its App. **13**, 1982, 167 -176.

[35] Szamuely, T.,*Galois Groups and Fundamental Groups* Cambridge studies in adv. math.Cambridge Univ. Pres. (2009).

[36] Velasco Lorenzo, E. *Teoría de Galois - Grothendieck*. T.F.M. Univ. Valladolid 2010.

[37] Viaud, J-F.,*Théories de Galois, relations d'équivalence locales et feuilletages* Thèse, Univ La Rochelle, (2007).