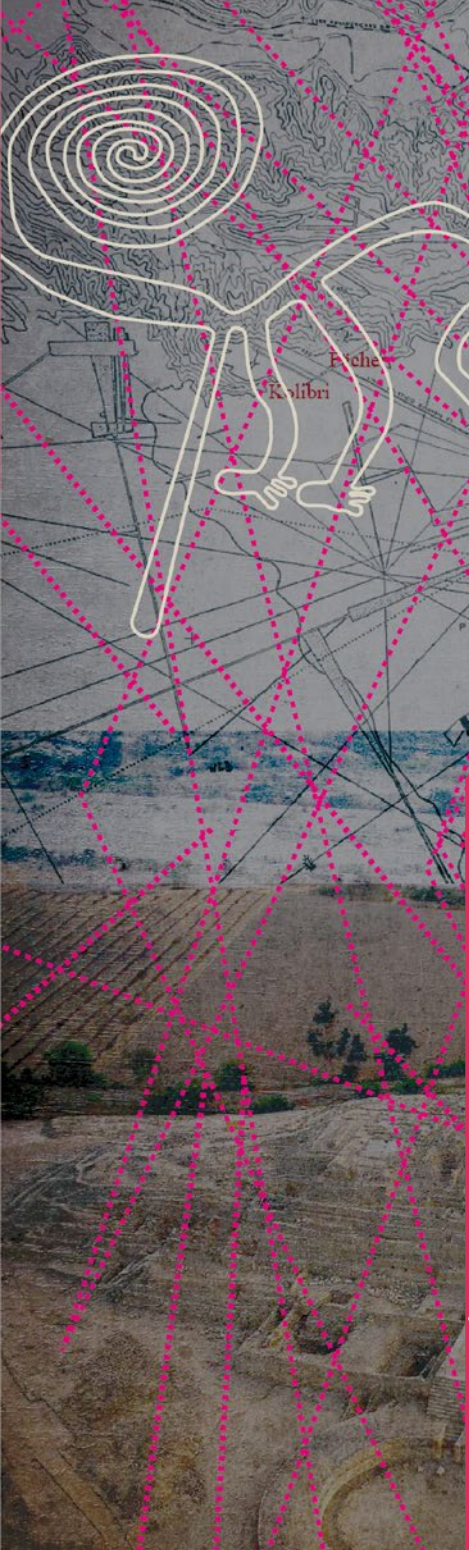


Francisco Ugarte Guerra
Nuria Corral Pérez
Editores

VIII Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2015

CIMPA RESEARCH SCHOOL

VIII Escuela Doctoral Intercontinental
de Matemáticas PUCP-UVA 2015

VIII Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2015

CIMPA RESEARCH SCHOOL

Francisco Ugarte Guerra
Nuria Corral Pérez
Editores

FONDO EDITORIAL
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

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

Índice

Presentación

La Pontificia Universidad Católica del Perú y la Universidad de Valladolid colaboran desde hace años organizando una Escuela Doctoral conjunta. En 2015, coincidiendo con la octava edición de esta escuela doctoral, se organizó una Escuela de investigación CIMPA. El CIMPA es un organismo dependiente de la Unesco cuyo objetivo es fomentar la investigación y la enseñanza superior de matemáticas fundamentales y aplicadas y sus interacciones. La principal actividad del CIMPA es apoyar la organización de escuelas de investigación y en este contexto se enmarcó la VIII Escuela Doctoral Intercontinental de Matemáticas.

Durante la escuela se impartieron cinco cursos:

- "Galois theories" por José Manuel Aroca Hernández-Ros (Universidad de Valladolid, España)
- "Galois grupoid of a racional transformation" por Guy Casale (Université de Rennes I, Francia)
- "About the Cremona group" por Julie Déserti (Université Paris 7, France)
- "Transformation groups of holomorphic foliations" por Percy Fernández Sánchez (Pontificia Universidad Católica del Perú)
- "Algebraic properties of groups of complex analytic local diffeomorphisms" por Lorena López Hernanz (Universidade de Minas Gerais, Brasil) and Javier Ribón Herguedas (Univesidade Federal Fluminense, Brasil)

así como varias conferencias, algunas de ellas impartidas por los estudiantes que asistieron a la Escuela. Este libro contiene las notas de cuatro de los cursos que se impartieron. Queremos aprovechar estas líneas para agradecer a los profesores J. M. Aroca, G. Casale, J. Déseti, P. Fernández, L. López y J. Ribón el haber aceptado impartir estos cursos y también a los participantes en la escuela por el buen ambiente de trabajo creado entre todos.

La realización de la Escuela pudo llevarse a cabo gracias a la financiación de los siguientes organismos: PUCP, CIMPA, Foundation Compositio Mathematica, International Mathematical Union, CNRS, Institut de Mathématiques de Jussieu Paris Rive Gauche, Ministerio de Economía y Competitividad de España y la Red Peruana de Universidades, a los cuales agradecemos su colaboración.

Santander y Lima, 30 de noviembre de 2015

Nuria Corral Pérez

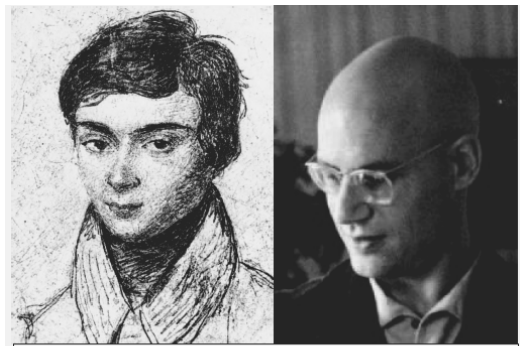
Francisco Ugarte Guerra

Participantes de la VIII Escuela Doctoral Intercontinental de Matemáticas PUCP-UVA 2015

Teorías de Galois

José Manuel Aroca

Sección Matemáticas - PUCP, CTRI-UVA
Lima 32 - Perú, Valladolid - España
E-mail address: aroca@uva.es



La filiation la la plus directe que je crois reconnaître à présent avec un mathématicien du passé, est bien celle qui me relie à Evariste Galois.

A tort ou à raison, il me semble que cette vision que j'ai développeé pendant quinze années de ma vie, et qui a continué encore à mûrir en moi et à s'enrichir pendant les seize années écoulées depuis mon départ de la scène mathématique, que cette vision est aussi celle que Galois n'aurait plus s'empêcher de développer, s'il s'etait trouvé dans les parages à ma ma place, et sans qu'une mort précoce ne vienne brutalement couper court un magnifique élan}

A. Grothendieck. *Récoltes et Semailles*

Índice

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:

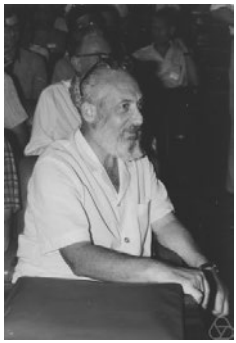
$$H = Gal_{L^H}(L) = \mathcal{I}\mathcal{V}(H)$$

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.*

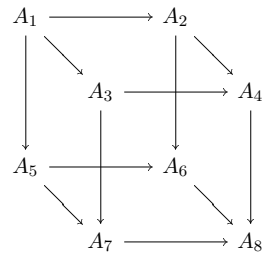
3. *Diremos que $I \in Ob(\mathfrak{C})$ es un* objeto inicial *si $Hom_{\mathfrak{C}}(I, A)$ tiene un solo elemento cualquiera que sea A.*

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 :

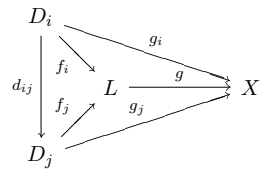
1. $\forall (i,j) \in \Delta, \quad f_j d_{i,j} = f_i$.

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 :

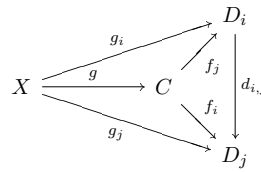
1. $\forall (i,j) \in \Delta, \quad d_{i,j} f_i = f_j$

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:

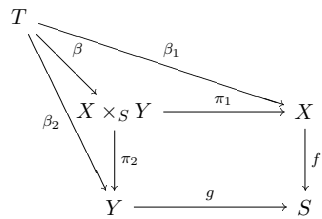
$$b = F(a) \Leftrightarrow b_j = \pi_j\beta\ \forall j \in I$$

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.

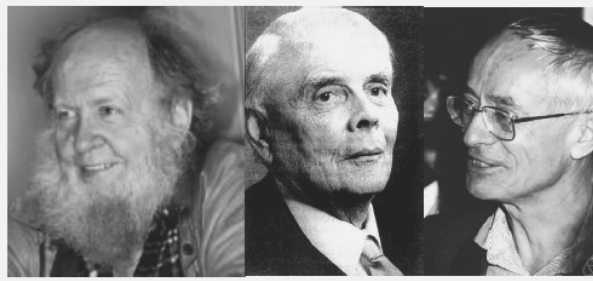
Ejemplo. 5.3.3.- La acción de un grupo de $\mathfrak{G}$ sobre un objeto X, se define como un morfismo:

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

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 $\sigma \notin Gal_M(K)$

□

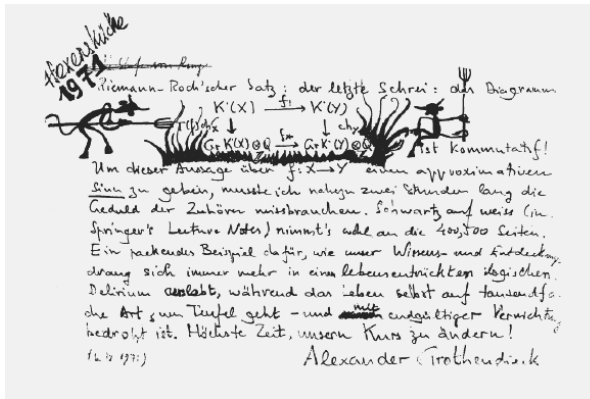
Veamos un ejemplo de grupo de Galois que admite subgrupos que no son cerrados, para probar que el teorema de Krull no es generalización trivial del de Galois. Si consideramos el cuerpo primo de característica p, $F_p = \mathbb{Z}/(p)$, su cierre separable $F_{p,s}$ contiene para cada n una subextensión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

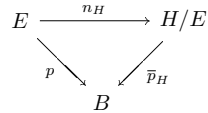
Demostración: Si $z \in Z$ podemos construir un entorno abierto conexo U de $q(z)$ en B bien cubierto por p y q, entonces tenemos un entorno abierto conexo W de z tal que $q|_W : W \to V$ es un homeomorfismo. Si las hojas de p sobre V son $\{T_i\}_{i\in I}$ y si

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

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

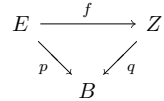
Teorema 8.11.– *[Teorema de Galois para revestimientos] Si (E,p) es un revestimiento de Galois de un espacio localmente conexo B y G es el grupo de transformaciones recubridoras de (E,p):*

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:*



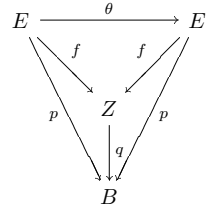
   entonces (E,f) es un revestimiento de Galois de X y si H_Z el grupo de transformaciones recubridoras (E,f), H_Z es un subgrupo de G y (Z,q) es isomorfo a $(H_Z/E, \overline{p}_{H_Z})$.

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



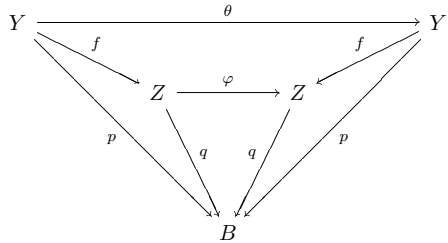
Solo queda probar que H_Z actúa transitivamente en las fibras de f y que en consecuencia (E, f) es galoisiano. Si $z \in Z$ y

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

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

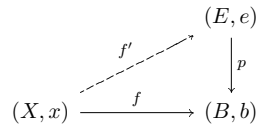
   $$\beta : I \to B,\ \beta(0) = b,\ \beta(1) = p(x)$$

   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.*

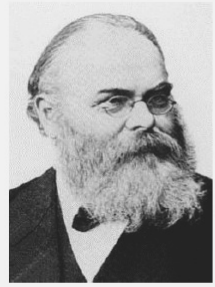
Demostración: Si llamamos $(\widetilde{X}_x, p_x)$ al revestimiento universal construido en el teorema 8.21, como $\widetilde{X}_x$ es simplemente conexo y localmente conexo pr caminos, $\pi_1(X, x)$ actúa transitivamente sobre la fibra $p_x^{-1}(x)$ y es isomorfo (con su acción) al grupo de transformaciones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

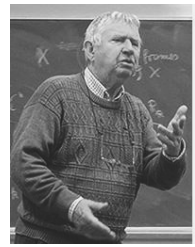
La combinación de estos resultados con el teorema 9.19 nos lleva al teorema central que es la justificación de esta sección y que establece que para las funciones algebraicas las teorías de Galois algebraica y topológica son la misma teoría:

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:

$$\varphi_j^{-1}\varphi_i : \varphi_i^{-1}(U_i \cap U_j) \to \varphi_j^{-1}(U_i \cap U_j)$$

$$\varphi_j^{-1}\varphi_i(\mathbf{x}, \mathbf{y}) = (\mathbf{x}', \mathbf{y}'),\ \mathbf{x}' = \varphi_{i,j}(\mathbf{x}, \mathbf{y}),\ \mathbf{y}' = \gamma_{i,j}(\mathbf{y}).$$

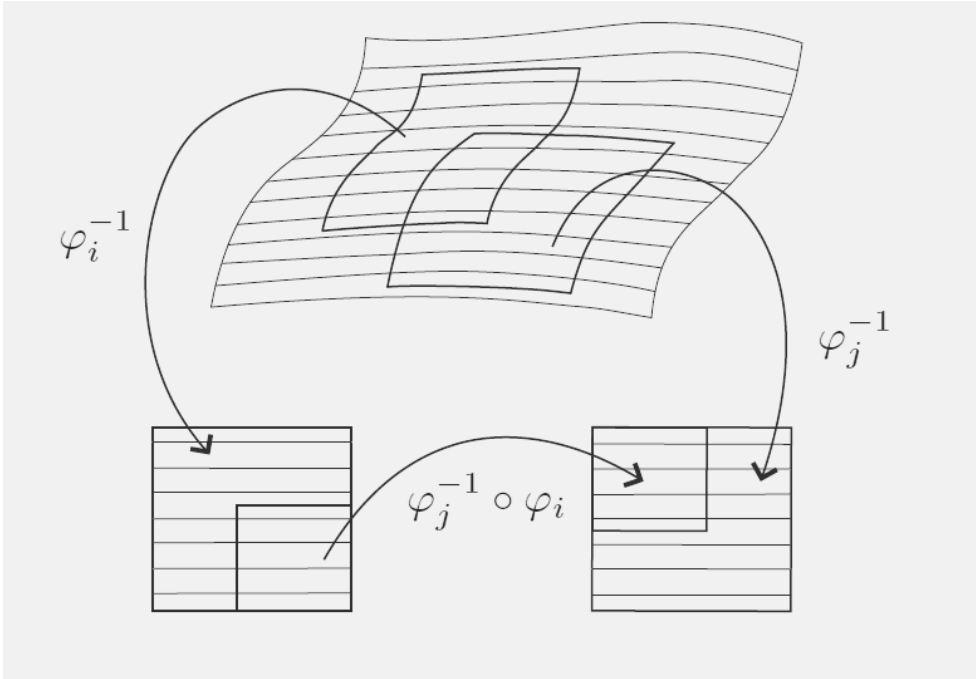


Figura 1: Representación gráfica del ejemplo 10.15

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).

El grupoide de Galois de una transformación racional

Guy Casale

Department of Mathematics, IRMAR, Université de Rennes 1,
35042 RENNES Cedex, France
E-mail address: guy.casale@univ-rennes1.fr

Índice

1 Introducción

Este curso tiene dos objetivos:

1. En primer lugar, definir el grupoide de Galois de una transformación racional:

$$f : \mathbb{C}^n \dashrightarrow \mathbb{C}^n$$
$$(z_1, \ldots, z_n) \mapsto (f_1(z), \ldots, f_n(z))$$

   con $f_i \in \mathbb{C}(z_1, \ldots z_n)$ tal que $\det Jac(f) \not\equiv 0$.

   Cuando f está dada por funciones lineales con respecto a $z_1, \ldots, z_n$, existe una teoría de Galois casi-completa (con una correspondencía de Galois ...). Se puede leer esta teoría en [15]. Para generalizar la definición a una transformación no lineal, necesitamos introducir un grupoide (más precisamente un pseudogrupo) siguiendo a B. Malgrange [10].

2. En segundo lugar, describir completamente el caso $n = 1$ para probar un teorema de Ritt sobre la trascendencia diferencial de la dinámica de f.

La prueba de Ritt utiliza la teoría de eliminación en los anillos de ecuaciones diferenciales. Nuestra demostración reemplaza la eliminación por argumentos de teoría de grupos.

1.1 El teorema de Ritt

El libro de J. Milnor [13] es nuestra referencia para los resultados de dinámica holomorfa en dimensión uno. Un teorema de Koenigs [13, capítulo 8] dice que si $f : \mathbb{C} \dashrightarrow \mathbb{C}$ tiene un punto fijo z_0 tal que $|f'(z_0)| > 1$ entonces existe $h \in \mathbb{C}\{w\}$ con $h(0) = z_0$ y $h'(0) = 1$ tal que $h^{-1} \circ f \circ h(w) = \lambda w$.

La construcción de la linealización h se hace por medio del límite de una sucesión de funciones holomorfas. Por eso podemos pensar que, generalmente, la linealización es trascendental. La linealización de un monomio $f(z) = z^k$ en el punto fijo $z_0 = 1$ es $h(w) = e^w$; los monomios son ejemplos de sistemas dinámicos con una linealización trascendental pero diferencialmente algebraica. El teorema de Ritt dice que no hay muchos más ejemplos de este tipo.

Definición 1. Una función holomorfa $f : U \to \mathbb{C}$ sobre un abierto U es *diferencialmente algebraica* si existe una ecuación diferencial $E \in \mathbb{C}[z, y, y', \ldots y^{(n)} \ldots]$ tal que

$$E(z, f(z), f'(z), \ldots, f^{(n)}(z)) = 0 \text{ sobre } U.$$

Una función que no es diferencialmente algebraica es *diferencialmente trascendental*.

Teorema 2 (Ritt [18]). *Si $f : \mathbb{C} \dashrightarrow \mathbb{C}$ tiene un punto fijo z_0 tal que $|f'(z_0)| > 1$ y su linealización h satisface una ecuación diferencial polinomial, entonces f es:*

- *una homografía*
- *o un monomio*
- *o un Chebyshev* [1]
- *o un Lattès* [2]

en una buena coordenada homográfica sobre $\mathbb{C}$.

La prueba la realizaremos será de la siguiente manera:

1. Daremos la definición del grupoide de Galois de una transformación f.
2. Probaremos que las transformaciones f con un grupoide "pequeño" están en la lista de Ritt .
3. Si f satisface las hipótesis de Ritt entonces su grupoide es "pequeño" .

Este lista aparece en otros teorema de Ritt ([17, 19])

1.2 Las ecuaciones en diferencias

Otra interpretación de este teorema es la siguiente.

Sean $f \in \mathbb{C}(z)$ y $\lambda \in \mathbb{C}$ con $|\lambda| > 1$. Si existe una solución meromorfa sobre $\mathbb{C}$ de la ecuación en diferencias multiplicativa $y(\lambda w) = f(y(w))$ que satisface una ecuación diferencial, entonces f está en la lista de Ritt. Para éstos f, la solución y está dada por funciones clásicas: $\exp(aw^k + b), \cos(aw^k + b), \mathcal{P}(aw^k + b)$ u otras funciones elípticas.

Desde este punto de vista, estamos mirando a las funciones que son soluciones de una ecuación diferencial y de una ecuación en diferencias. Las funciones que satisfacen ecuaciones diferenciales y en diferencias lineales son estudiadas de manera analítica en [16] y de manera muy diferente en [8] donde se hace uso de la teoría de Galois.

[1] 16 de Mayo de 1821 - 8 de diciembre de 1894, fue un matemático ruso. `https://es.wikipedia.org/wiki/Pafnuti_Chebyshov`

[2] 21 de Febrero de 1873 - 5 de julio de 1918, fue un matemático francès `https://de.wikipedia.org/wiki/Samuel_Lattès` y [1]

1.3 Otro teorema de tipo "Ritt"

Un teorema similar de Bergweiler-Aschenbrenner [4] puede demostrarse de manera análoga. Si $f : \mathbb{C} \dashrightarrow \mathbb{C}$ tiene un punto fijo z_0 tal que $f'(z_0) = 1$, entonces existe $k \in \mathbb{N}$, $c \in \mathbb{C}$ y $h \in \mathbb{C}[[z]]$ tal que $h^{-1} \circ f \circ h = \exp\left(\frac{z^{k+1}}{1-cz^k}\frac{d}{dz}\right)$ (ver [11, chap. I §§1,2]).

Teorema 3. *No existe $f : \mathbb{C} \dashrightarrow \mathbb{C}$ con un punto fijo z_0 tal que $f'(z_0) = 1$ y su normalización formal h satisfaga una ecuación diferencial.*

La organización del curso es la siguiente:

1. El ejemplo de una aplicación lineal.
2. El ejemplo de una aplicación lineal en las $n-1$ coordenadas últimas.
3. La definición del grupoide (o pseudogrupo) de Galois de f.
4. Los pseudogrupos en dimensión $n = 1$.
5. El pseudogrupo de Galois de f en dimensión $n = 1$.
6. El teorema de Ritt.

1.4 Agradecimientos

Quiero dar las gracias a Jesus David Piñeda Escobar para la ayudad a escribir las notas del curso en español. Muchas gracias a Nuria Corral y Francisco Ugarte para la organización de la escuela CIMPA "Transformation Groups and Dynamical Systems".

2 Transformaciones lineales y grupos algebraicos

Una transformación lineal es un elemento de un grupo, este último será utilizado para simplificar la definición general de grupoide de Galois, no obstante, esta simplificación es muy fuerte y muchas cosas parecerán artificiales.

Definición 4. Sean E un espacio vectorial y $A \in GL(E)$ una aplicación lineal invertible. La envolvente algebraica ("enveloppe" en francés) de A es el subgrupo algebraico minimal $G_A \subset GL(E)$ tal que $A \in G_A$.

Es posible leer una introducción sobre los aspectos básicos de los grupos algebraicos lineales en [6] o resultados más complejos en [9]. Aunque existe una amplia literatura acerca de grupos algebraicos, daremos una breve introducción.

2.1 Grupos algebraicos lineales

En adelante consideraremos conjuntos algebraicos sobre el cuerpo de los números complejos. El espacio $\mathbb{C}^n$ posee un álgebra de funciones polinomiales $\mathbb{C}[X_1, \ldots, X_n]$ con muy buenas propiedades, es por esto que le llamamos un conjunto algebraico o una variedad algebraica.
Podemos construir otros conjuntos algebraicos utilizando un ideal de polinomios $I \subset \mathbb{C}[X_1, \ldots, X_n]$. El conjunto $V_I = \{x \in \mathbb{C}^n \mid f(x) = 0 \text{ para todo } f \in I\}$ es un conjunto algebraico con álgebra de funciones polinomiales $\mathbb{C}[V] = \mathbb{C}[X_1, \ldots, X_n]/\sqrt{I}$. Una variedad algebraica es un objeto un poco más general pero no vamos a utilizarlas.

El conjunto algebraico minimal que contiene un subconjunto C de una variedad algebraica V se llama la clausura de Zariski de C o la clausura algebraica de C, se escribe $\overline{C}$. Un abierto de Zariski es el complementario de un conjunto algebraico.

El conjunto $GL_n(\mathbb{C})$ es un conjunto algebraico. Podemos verlo como el subconjunto de $\mathbb{C}^{n^2+1}$ de los ceros del polinomio $P(X_1^1, \ldots, X_n^n, t) = t \det X - 1$. Su álgebra de funciones es $\mathbb{C}[X_1^1, \ldots, X_n^n, \frac{1}{\det X}]$. El conjunto $GL_n(\mathbb{C})$ es también un grupo y las dos estructuras son compatibles: Si $g \mapsto P(g)$ es una función polinomial entonces

- $(g_1, g_2) \mapsto P(g_1 g_2)$ es una función polinomial sobre $GL_n \times GL_n$,
- $g \mapsto P(g^{-1})$ es una función polinomial sobre GL_n.

Definición 5. Un subgrupo $G \subset GL_n$ que es un conjunto algebraico es un subgrupo algebraico.

Ejercicio 6. Comparar con la definición del curso del Pr. Aroca y probar que las dos definiciones son compatibles.

Ejercicio 7. Probar que si $G \subset GL(E)$ es un subgrupo, entonces $\overline{G}$ es un grupo algebraico.

Ejemplo 8. El subgrupo $SL_n \subset GL_n$ es algebraico.
El grupo de las matrices triangulares superiores U_n es algebraico.

En general, si E es un espacio vectorial, podemos elegir una base $e_1, \ldots, e_n$ y el isomorfismo $e : \mathbb{C}^n \to E$ determina un isomorfismo de $GL_n \to GL(E)$ que hace de $GL(E)$ un grupo algebraico. Entonces podemos definir sus subgrupos algebraicos. Casi todos los teoremas básicos e importantes sobre grupos algebraicos se prueban utilizando la acción del grupo sobre $\mathbb{C}[GL(E)]$ por traslaciones. Para $g \in GL(E)$, escribiremos $T_g : g' \mapsto g'g$ para denotar la traslación y $T_g^* : \mathbb{C}[GL(E)] \to \mathbb{C}[GL(E)]$; $P \mapsto P \circ T_g$.

Definición 9. Un invariante (resp. invariante racional) de $g \in GL(E)$ es una función $H \in \mathbb{C}[GL(E)]$, (resp. $H \in \mathbb{C}(GL(E))$) tal que $H = H \circ T_g$. Un invariante de un subgrupo G de $GL(E)$ es un invariante común a todos los elementos de G.

El siguiente es el teorema más importante para este curso, es un teorema de Kolchin y Chevalley pero realizaremos una prueba de J. Drach [7, §§16 – 19 pp 466 – 474].

Teorema 10 ([5])**.** *Si $G \subset GL(E)$ es un grupo algebraico, entonces existen $H_1, \ldots, H_p \in \mathbb{C}(GL(E))$ en el cuerpo de funciones racionales tales que*

$$G = \{g \in GL(E) \mid H_i = H_i \circ T_g \text{ para todo } i\}.$$

Demostración. – Tenemos una acción lineal de G por $T_g^* : \mathbb{C}[GL(E)] \to \mathbb{C}[GL(E)]$. Utilizaremos algunos lemas sobre esta acción.

Lema 11. *El subespacio vectorial $I \subset \mathbb{C}[GL(E)]$ de las funciones que se anulan sobre G es estable por G.*

Ejercicio 12. Probar el lema precedente.

Ahora tenemos que el grupo

$$G = \{g \in GL(E) \mid T_g^*(I) \subset I\},$$

es el estabilizador de un subespacio vectorial I de $\mathbb{C}[GL(E)]$. El problema es que tenemos dos espacios vectoriales de dimensión infinita y para construir invariantes necesitamos espacios de dimensión finita. Vamos a construirlos.

Sean $F_1, \ldots, F_p$ generadores linealmente independientes del ideal I. Dado que $F_i(gg')$ es un polinomio,

$$\text{para todo } (g, g') \in GL(E) \times GL(E) \quad \text{se tiene} \quad F_i(gg') = \sum_{j=1}^{n} D_i^j(g') B_j(g),$$

para funciones D y B en $\mathbb{C}[GL(E)]$. Esta suma no es única, escribimos una suma con un número minimal de términos y $F_i = B_i$ para $i \leq p$.

Lema 13. *En virtud de la minimalidad del número de términos, los B_j para $j = 1, \ldots, n$ son linealmente independientes y las columnas $(D_i^j)_i$ para $j = 1, \ldots, n$ también.*

Ejercicio 14. Probar el lema precedente.

Sea V el espacio vectorial sobre $\mathbb{C}$ generado por los B_i, probaremos que V es estable por $GL(E)$. Tenemos

$$B_j(gg') = \sum_k \widetilde{D}_j^k(g')B_k(g) + \sum_\ell A_j^\ell(g')C_\ell(g)$$

con los B y C linealmente independientes. Las dos fórmulas y la asociatividad dan:

$$\sum_j D_i^j(g'g'')B_j(g) = F_i(gg'g'') = \sum_j D_i^j(g'')B_j(gg')$$

$$\sum_j D_i^j(g'g'')B_j(g) = \sum_j \widetilde{D}_i^j(g'')\left(\sum_k \widetilde{D}_j^k(g')B_k(g) + \sum_\ell A_j^\ell(g')C_\ell(g)\right)$$

Por la independencia de los B y C tenemos $\sum_{j,\ell} \widetilde{D}_i^j(g'')A_j^\ell(g')C_\ell(g) = 0$. En virtud del lema anterior tenemos que las columnas $(\widetilde{D}_i^j)_j$ son independientes, entonces $\sum_\ell A_j^\ell(g')C_\ell(g)$ son cero, para cada j. Tenemos un espacio de dimensión finita de V estable por T_g^* para cada $g \in GL(E)$. El subespacio $V \cap I$ es un subespacio estable de dimensión q, entonces

$$G = \{g \in GL(E) \mid T_g^*|_V(V \cap I) \subset V \cap I\}.$$

Ahora elegimos una base de V tal que los q primeros vectores sean una base de $V \cap I$. Definimos n^2 funciones $\widetilde{D}_j^k$ sobre $GL(E)$ por las fórmulas de arriba. Un elemento g está en G si y solo si la traslación T_q preserva las funciones $F_{K,L}$ siguientes:

$$\text{para } K \subset \{1, \ldots, n\}, L \subset \{1, \ldots, n\}, \#K = \#L = n - q :$$

$$F_{K,L} = \frac{\det(\widetilde{D}_j^k)_{\substack{j=q+1,\ldots n \\ k \in K}}}{\det(\widetilde{D}_j^k)_{\substack{j=q+1,\ldots n \\ k \in L}}}$$

□

Nota 15. En la prueba utilizamos las buenas propiedades del producto tensorial sobre un cuerpo.

2.2 La envolvente algebraica

Para entender una aplicación lineal A podemos estudiar el grupo algebraico generado por A.

Definición 16. La envolvente algebraica de $A \in GL(E)$ es el grupo algebraico minimal G_A que contiene A.

Lema 17. *El conjunto algebraico minimal que contiene todos los A^n para $n \in \mathbb{Z}$ es G_A.*

Ejercicio 18. Probar el lema precedente.

Lema 19. *La envolvente algebraica de A es el grupo de los elementos que preservan los invariantes racionales de A.*

Ejercicio 20. Probar el lema precedente.

2.3 Los grupos de Galois de A

Para entender una aplicación lineal A podemos estudiar su prolongación sobre espacios más grandes. El conjunto de todas las bases de E es un conjunto algebraico

$$BE = \{e = (e_1, \ldots, e_n) \in E^n | e_1 \wedge \ldots \wedge e_n \neq 0\}$$

con

- una acción de $g \in GL_n$, $T_g : (e_1, \ldots, e_n) \mapsto (e_1, \ldots, e_n)g$,
- una acción de A : $(e_1, \ldots, e_n) \mapsto (Ae_1, \ldots, Ae_n)$

que conmutan. Elegimos una base e y miramos su órbita $O(e) = \{A^n e, n \in \mathbb{Z}\}$ y su clausura algebraica $\overline{O(e)}$.

Definición 21. El estabilizador de $\overline{O(e)}$ en GL_n es $Gal(A, e)$, el grupo de Galois de A en e.

Lema 22. $\overline{O(eg)} = T_g(\overline{O(e)})$ *y* $Gal(A, eg) = gGal(A, e)g^{-1}$.

Ejercicio 23. Probar el lema precedente.

2.4 Comparación

Si $E = \mathbb{C}^n$ y $e = identidad$ entonces $Gal(A, e) = G_A = \overline{O(e)}$.

La envolvente G_A actúa a la izquierda sobre todos los $\overline{O(e)}$ para cualquier $e \in BE$. El grupo de Galois $Gal(A, e)$ actúa a la derecha sobre la subvariedad $\overline{O(e)}$. La envolvente es intrínseca pero se necesita poner A dentro de un grupo con una topología para definirla. El grupo de Galois depende de una base pero solo necesitamos una acción de A sobre un espacio suficientemente grande para "desarollar" la dinámica de A.

2.5 Ejercicios

Ejercicio 24. Sea $G \subset GL(E)$ un subgrupo conmutativo. Probar que $\overline{G}$ es conmutativo. Deducir que para $A \in GL(E)$, G_A es conmutativo.

Ejercicio 25. Dar los grupos algebraicos generados por

$$A = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \qquad \text{o} \qquad A = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}.$$

3 Ecuaciones en diferencias lineales

La recta compleja $\mathbb{C}$ será denotada por L. Para una aplicación racional $A : L \dashrightarrow GL(E)$ nos interesa la transformación

$$\begin{aligned} f_A : L \times E &\dashrightarrow L \times E \\ (z, x) &\mapsto (z + 1, A(z)x) \end{aligned}$$

Podemos pensar en cambiar de cuerpo y proceder de manera análoga al caso lineal con $A \in GL(E \otimes \mathbb{C}(z))$. Pero $f_A \circ f_A \neq f_{A^2}$, por eso no es fácil dotar a $GL(E \otimes \mathbb{C}(z))$ de una estructura de grupo compatible con f, salvo en el caso constante $A \in GL(E)$. Es más fácil definir los grupos de Galois.

Tradicionalmente se escriben las ecuaciones de las aplicaciones $Y : L \to E$ con grafo invariante por f_A :

$$Y(z + 1) = A(z)Y(z)$$

y los grupos de Galois son los grupos de Galois del sistema de ecuaciones en diferencias de [15]. Estos se definen de manera análoga al caso constante pero la definición de la envolvente necesita colocar f_A dentro de un grupoide.

3.1 Los grupos de Galois

Como en el caso constante, estudiamos la acción de f_A sobre las bases de E :

$$\begin{aligned} f_A : L \times BE &\dashrightarrow L \times BE \\ (z, e) &\mapsto (z+1, A(z)e) \end{aligned}.$$

Aún tenemos la acción de GL_n a la derecha que conmuta con f_A.

Elegimos un punto z_0, una base e_0 y $V(z_0, e_0)$ será el conjunto algebraico minimal de $L \times BE$ tal que:

- $(z_0, e_0) \in V(z_0, e_0)$,
- $f_A(V(z_0, e_0)) \subset V(z_0, e_0)$,
- $pr_1(V(z_0, e_0))$ es un abierto de L.

Básicamente la minimalidad y las dos primeros condiciones significan que miramos a la clausura de Zariski de la órbita de (z_0, e_0). La tercera significa que esta órbita no se encuentra con el espacio de indeterminación de f_A.

Definición 26. El estabilizador de $V(z_0, e_0)$ en GL_n es el grupo de Galois de f_A en e_0: $Gal(f_A, e_0)$.

3.2 La envolvente algebraica

Podemos definir la envolvente algebraica, pero no en un grupo sino dentro en un grupoide. El grupoide es $\mathcal{G}r = L \times GL(E) \times L$. La composición es $(z_1, g, z_2)(z_2, h, z_3) = (z_1, gh, z_3)$ y es compatible con las álgebras de funciones polinomiales. Por lo tanto es un grupoide algebraico.

Ejercicio 27. Probar que $\{(z_1, g, z_2) \in L \times GL_1(\mathbb{C}) \times L \mid z_1 g = z_2\}$ es un subgrupoide algebraico.

La transformación f_A da muchos elementos de este grupoide: para cada $z \in L$ tal que $A(z)$ existe, tenemos $A_z = (z+1, A(z), z) \in \mathcal{G}r$. Podemos intentar una definición análoga a la definición 16.

Definición 28 (mala)**.** La envolvente de A, $\mathcal{G}_A$, es el subgrupoide algebraico minimal tal que $A_z \in \mathcal{G}_A$ para todo $z \in L$.

Sobre ejemplos podemos ver que este objeto es bastante grande.

Definición 29 (buena)**.** La envolvente de A, $\mathcal{G}_A$, es el conjunto algebraico minimal tal que

- para todo $z \in dom(A) \subset L$ el dominio de A, $A_z \in \mathcal{G}_A$,
- existe $U \subset L$ un abierto de Zariski tal que $\mathcal{G}_A|_{U\times U}$ es un grupoide algebraico.

Tenemos teoremas análogos a los dos lemas de la parte 2.2.

Teorema 30. *$\mathcal{G}_A$ es la clausura de Zariski del conjunto*

$$\{(z, \prod_{i=0}^{n-1} A(z+i), z+n), n \in \mathbb{N}, z \in L^\circ\} \cup \{(z, Id, z), z \in L\} \cup$$

$$\{(z+n, \prod_{i=0}^{n-1} A^{-1}(z+n-1-i), z), n \in \mathbb{N}, z \in L^\circ\}.$$

siendo L° un subconjunto de L donde las fórmulas tienen sentido.

Definición 31. Un invariante racional de f_A es un $H \in \mathbb{C}(L \times BE)$ tal que $H \circ f_A = H$. El cuerpo de los invariantes de f_A será $Inv(A) \subset \mathbb{C}(L \times BE)$.

Teorema 32. *La envolvente de f_A está dada por sus invariantes:*

$$\mathcal{G}_A = \{(z_1, g, z_2) \in \mathcal{G}r \mid H(z_2, e) = H(z_1, g(e)) \text{ para todo } H \in Inv(A)\}.$$

Las pruebas de estos dos teoremas son difíciles y no son más fáciles que sus versiones no lineales, entonces no vamos a hacerles aquí.

3.3 Ejercicios

Ejercicio 33. Si $A : \mathbb{C} \dashrightarrow \mathbb{C}^*; z \to z$ y $f_A(z, x) = (z+1, zx)$.

Probar $Gal(T_A, e) = \mathbb{C}^*$.

Indicación: la ecuación en diferencias $y(z+1) = zy(z)$, es la ecuación de la función Γ. Calcular el grupo de Galois es equivalente a probar que Γ no es una función algebraica.

4 Los referentes y los invariantes diferenciales

Ahora queremos definir la envolvente algebraica de una aplicación racional $f : M \dashrightarrow M$. Necesitamos introducir los objetos que reemplazarán las bases de E: los referentes. Son versiones no lineales de los referentes móviles de E. Cartan.

Definición 34.

- Un referente $p \in M$ es un germen de coordenadas locales holomorfas: $r : (\mathbb{C}^n, 0) \to (M, p)$ invertible en 0.
- Un referente de orden k es el jet de orden k, $j_k(r)$, de un referente r.
- El conjunto de todos los referentes de orden k es una variedad algebraica R_kM.

Se puede escribir un referente como n series de potencias. Si $(t_1, \ldots, t_n)$ son coordenadas sobre $\mathbb{C}^n$ y $(z_1, \ldots, z_n)$ son coordenadas sobre M entonces un referente r se escribe $r(t) = (r_1(t), \ldots, r_n(t))$ donde

$$r_i(t) = \sum_{\alpha \in \mathbb{N}^n} \partial^\alpha r_i(0) \frac{t^\alpha}{\alpha!}.$$

Su jet de orden k es

$$j_k r_i = \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| \leq k}} \partial^\alpha r_i(0) \frac{t^\alpha}{\alpha!}.$$

Entonces el anillo de funciones polinomiales sobre R_kM es

$$\mathbb{C}[R_kM] = \mathbb{C}\left[z_i^\alpha | 1 \leq i \leq n, \alpha \in \mathbb{N}^n, |\alpha| \leq k\right] \left[\frac{1}{\det z_i^{\epsilon_j}}\right]$$

con

$$z_i^\alpha(j_k r) = \partial^\alpha r_i(0).$$

Definición 35. El conjunto de los referentes formales es $RM = \varprojlim R_kM$. Un referente formal $\widehat{r}$ está dado, en coordenadas locales, por n series de potencias $(\widehat{r}_1(t), \ldots \widehat{r}_n(t))$ pero sin ninguna condición de convergencia.

El espacio RM tiene muchas propiedades buenas que vamos a definir.

4.1 R_kM es un espacio natural

Significa que si $\varphi : U \to V$ es un biholomorfismo local entre abiertos de M entonces tenemos $R_k\varphi : R_kU \to R_kV$ un biholomorfismo local canónico entre el abierto de los referentes en U y el de los referentes en V definido por

$$R_k\varphi(j_k r) = j_k(\varphi \circ r_k).$$

La asociatividad de la composición da $R_k(\varphi_1 \circ \varphi_2) = R_r\varphi_1 \circ R_k\varphi_2$. En particular, f actúa sobre R_kM. La elevación $R\varphi$ de un biholomorphismo local φ se llama la prolongación de φ al espacio de los referentes.

Podemos también prolongar los campos de vectores: si X es un campo de vectores sobre M con flujo $\exp(\epsilon X)$ entonces R_kX es el generador infinitesimal de la familia $R_k(\exp(\epsilon X))$ para pequeños ϵ. Esta prolongación es compatible con el paréntesis de Lie $R_k[X_1, X_2] = [R_kX_1, R_kX_2]$.

4.2 R_kM es un fibrado principal

El grupo de cambio de coordenadas sobre $(\mathbb{C}^n, 0)$ actúa sobre los referentes.

Definición 36. El grupo $\Gamma_k = \{j_k\gamma \mid \gamma : (\mathbb{C}^n, 0) \to (\mathbb{C}^n, 0) \text{ invertible}\}$ es un grupo algebraico.

Ejercicio 37. Probar que Γ_k es un subgrupo algebraico de $GL(E)$ donde E es el espacio vectorial de los jets de orden k de funciones holomorfas sobre $(\mathbb{C}^n, 0)$.

Este grupo actúa sobre R_kM : si $j_k\gamma \in \Gamma_k$, $T_{j_k\gamma}(j_kr) = j_k(r \circ \gamma)$ y la acción satisface que

$$\begin{aligned} R_kM \times \Gamma_k &\to R_kM \underset{M}{\times} R_kM \\ (j_kr, j_k\gamma) &\mapsto (j_kr, T_{j_k\gamma}j_kr) \end{aligned}$$

es un isomorfismo de variedades algebraicas.

Lema 38. *Las aplicaciones $T_{j_k\gamma}$ y $R_k\varphi$ conmutan.*

Ejercicio 39. Probar el lema precedente.

4.3 $\mathbb{C}[RM]$ es un álgebra diferencial

El anillo de funciones sobre RM es

$$\lim_{\to}\mathbb{C}[R_kM] = \mathbb{C}\left[z_i^\alpha | 1 \le i \le n, \alpha \in \mathbb{N}^n\right]\left[\frac{1}{\det jac}\right].$$

Los operadores $\partial_i = \sum_{j,\alpha} z_j^{\alpha+\epsilon(i)} \frac{\partial}{\partial z_j^\alpha}$, donde $\epsilon(i) = (0 \ldots, 1, \ldots 0)$ es el multiíndice cuya única componente no nula es la i-esima, actúan sobre $\mathbb{C}[RM]$ como derivaciones :

$$\partial_i(P + Q) = \partial_i(P) + \partial_i(Q) \quad , \quad \partial_i(PQ) = \partial_i(P)Q + P\partial_i(Q).$$

Además satisfacen

$$\partial_i \circ (R_k\varphi)^* = (R_{k+1}\varphi)^* \circ \partial_i.$$

4.4 RM tiene una conexión de Cartan plana

Es una condición de compatibilidad de las estructuras de fibrado principal y de álgebra diferencial. La definición general puede encontrarse en el libro de Sharpe [20].

Para definir la condición de compatibilidad, necesitamos

- El álgebra de Lie $\widehat{\chi}$ de los campos de vectores formales :

$$\widehat{\chi} = \{\sum a_i(t)\frac{\partial}{\partial t_i} \mid a_i(t) \in \mathbb{C}[[t_1, \ldots, t_n]]\},$$

- un teorema que se puede probar leyendo el curso de los Profesores López-Hernanz y Ribón.

  Teorema 40.

  1. *Para cada $\widehat{\gamma}$ en el grupo Γ existe un campo vectorial formal $\widehat{a} = \sum a_i(t)\frac{\partial}{\partial t_i}$ tal que $\widehat{a}(0) = 0$ y para todo $F : (\mathbb{C}^n, 0) \to \mathbb{C}$; $\exp(\widehat{a}) \cdot F = F \circ \widehat{\gamma}$*
  2. *Para cada $\widehat{a}$ tal que $\widehat{a}(0) = 0$, existe un $\widehat{\gamma}$ tal que $\exp(\widehat{a}) \cdot F = F \circ \widehat{\gamma}$.*

Utilizando el teorema, cada $\widehat{a} = \sum a_i(t)\frac{\partial}{\partial t_i}$ tal que $\widehat{a}(0) = 0$ actúa sobre $R(M)$ por un campo vectorial $T_{\widehat{a}}$ que es el generador infinitesimal de la familia $T_{\exp \epsilon\widehat{a}}$ para pequeños ϵ: $T_{\widehat{a}} = \lim \frac{1}{\epsilon}(T_{\exp \epsilon\widehat{a}} - T_{id})$

Los campos $\frac{\partial}{\partial t_i}$ actúan también por ∂_i.

Proposición 41. Las dos acciones arriba definen un morfismo T de álgebras de Lie de $\widehat{\chi}$ en el álgebra de Lie de los campos vectoriales sobre RM.

Esta estructura no es importante para la definición del grupoide de Galois pero lo es para los cálculos.

4.5 Los invariantes diferenciales de f

La definición siguiente es muy similar a las definiciones anteriores.

Definición 42. Un invariante diferencial de f es una función racional $H \in \mathbb{C}(RM)$ tal que $H \circ Rf = H$.

Lema 43. *Si H es un invariante de f y $\gamma \in \Gamma$ entonces $H \circ T_\gamma$ es un invariante de f.*

Lema 44. *Si H es un invariante de f entonces $\partial_i H$ es un invariante de f.*

Ejercicio 45. Probar los lemas precedentes.

4.6 El estabilizador de una variedad de referentes

Los grupos de Galois son estabilizadores de subvariedades de un fibrado principal. Entonces antes de dar las definiciones de grupos y grupoide de Galois necesitamos especificar lo que son "los" estabilizadores de una subvariedad de RM.

Definición 46. El estabilizador de una subvariedad $V \subset RM$ es un par $(G, \mathfrak{g})$ donde

1. $G = \{\gamma \in \Gamma \mid T_\gamma(V) = V$ es el estabilizador de V por la acción de Γ,
2. $\mathfrak{g} = \{a \in \widehat{\chi} \mid T_a|_V \in TV\}$ es el estabilizador de V por la acción de $\widehat{\chi}$.

El álgera de Lie de G es una subalgebra de Lie de $\mathfrak{g}$.

4.7 Ejercicios

Ejercicio 47. Si f es la aplicación $(z, x) \mapsto (z + 1, zx)$.

- Calcular $R_1 f$.
- Probar que z^α son invariantes si $|\alpha| > 0$.
- Probar que $\frac{\det jac}{x}$ es un invariante.
- Calcular el estabilizador de un nivel común de los invariantes.

Ejercicio 48. Si $\widehat{a}$ es un campo de vectores formal que se anula dos veces en cero. Su flujo puede definirse como

$$(t_1, \ldots, t_n, \epsilon) \mapsto (\sum \frac{1}{\ell!}(\epsilon\widehat{a})^\ell t_1, \ldots, \sum \frac{1}{\ell!}(\epsilon\widehat{a})^\ell t_n)$$

- Probar que $(\widehat{a})^\ell t_1$ se anula para un orden mayor que $\ell + 1$ en cero.
- Probar que la fórmula está bien definida en el anillo $\mathbb{C}[[t_1, \ldots t_n]]$.

5 Los grupoides

5.1 El grupoide $\mathcal{A}utM$

Este grupoide es

$$\mathcal{A}ut(M) = \{(q, \widehat{\varphi}, p) \mid q \in M, p \in M, \widehat{\varphi} : (M, p) \to (M, q)\}$$

y $\widehat{\varphi}$ está dado por n series de potencias sin condiciones de convergencia tal que $\det Jac(\varphi)(p) \neq 0$.

$$\varphi = (\varphi_1, \ldots, \varphi_n) \text{ con } \varphi_i = q_i + \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| > 0}} \varphi_i^{\alpha} \frac{(z-p)^{\alpha}}{\alpha!}$$

La composición es $(q_1, \widehat{\varphi}, p)(p, \widehat{\psi}, q_2) = (q_1, \widehat{\varphi} \circ \widehat{\psi}, q_2)$. Gracias a las fórmulas de Faa di Bruno, este grupoide es un grupoide algebraico con anillo de funciones polinomiales

$$\mathbb{C}[\mathcal{A}utM] = \mathbb{C}[p_1, \ldots, p_n, q_1, \ldots, q_n, \ldots \varphi_i^{\alpha} \ldots][1/\det(\varphi_i^{\epsilon(j)})]$$

Este grupoide actúa sobre RM :

$$\begin{aligned} &\mathcal{A}utM \underset{M}{\times} RM \to RM \\ &(q, \varphi, p)(p, r) \mapsto R(q, \varphi, p)(p, r) = (q, \varphi \circ r) \end{aligned}$$

y conmuta con la acción de Γ.

5.2 Pseudogrupos algebraicos

Es posible dar una definición intrínseca de grupoide algebraico y probar el teorema de Drach:

Teorema 49. *Un grupoide algebraico es el grupoide de invarianza de sus invariantes sobre un abierto de Zariski $U \subset M$.*

La prueba del teorema de Drach es casi la misma que la prueba del teorema de Kolchin y Chevalley. La diferencia es que tenemos que trabajar con productos tensoriales sobre $\mathbb{C}[M]$. Para hacer la misma prueba necesitamos trabajar sobre $\mathbb{C}(M)$, *i.e.*, sobre un abierto de Zariski.

Utilizando este teorema podemos dar una definición alternativa.

Definición 50. Un subgrupoide $\mathcal{G}$ de $\mathcal{A}ut(M)$ tal que existe une subcuerpo $Inv \subset \mathbb{C}(RM)$ con

$$\mathcal{G} = \{\varphi \mid H \circ R\varphi = H \text{ para todo } H \in Inv\}$$

es un subgrupoide algebraico.

Definición 51. Un subgrupoide algebraico $\mathcal{G}$ de $\mathcal{A}ut(M)$ tal que su cuerpo de invariantes $Inv \subset \mathbb{C}(RM)$ es un subcuerpo diferencial es un pseudogrupo algebraico.

5.3 El grupoide de Galois

Este grupoide es el análogo no lineal de la envolvente algebraica. Existe también un análogo de los grupos de Galois. Son definidos por H. Umemura [21] y la definición puede resultar mucho más difícil que la definición del grupoide.

Para cada punto p tal que f es localmente invertible en p, podemos definir un punto $(f(p), \widehat{f}_p, p)$ de $\mathcal{A}ut(M)$ con el desarrollo de f en serie de potencias alrededor de p. De esta manera tenemos la definición topológica de la envolvente.

Definición 52. $\mathcal{G}al(f)$ es la subvariedad algebraica minimal de $\mathcal{A}ut(M)$ tal que para todo $n \in \mathbb{N}$, $f^{\circ n} \in \mathcal{G}al(f)$.

Esta fórmula significa que para cada $p \in M$ tal que $f^{\circ n}$ es localmente invertible en p, $(f^{\circ n}(p), \widehat{f^{\circ n}}_p, p) \in Gal(f)$. Los dos teoremas siguientes son análogos de las construcciones alternativas de la envolvente.

Teorema 53. *Existe un abierto de Zariski $U \subset M$ tal que $\mathcal{G}al(f)|_{U\times U}$ es un pseudogrupo algebraico.*

Teorema 54. *Si $Inv(f) \subset \mathbb{C}(RM)$ es el subcuerpo diferencial de los invariantes de f entonces*

$$\mathcal{G}al(f) = \{\varphi \mid \forall H \in Inv(f) \ ; \ H \circ R\varphi = H\}$$

La prueba del teorema 53 es difícil. Se necesita un teorema de Americ y Campana [2].

La prueba del teorema 54 es el teorema de Drach. En este curso es una consecuencia fácil de la definición.

5.4 Ejercicios

Ejercicio 55. Si f es la aplicación $(z, x) \mapsto (z + 1, zx)$.

- Probar que $\mathcal{G}al(f) \subset \{\varphi : (z, x) \mapsto (z + a, g(z)x) \mid a \in \mathbb{C} \text{ y } g \in \mathbb{C}[[z]], g(0) \neq 0\}$.
- Probar la igualdad (¡es difícil! y será necesario estudiar [8]).

Ejercicio 56. Probar que $\mathcal{A}ut(M)$ es el cociente de $RM \times RM$ por la acción diagonal de Γ.

6 Aplicación en dimensión 1: los pseudogrupos

Cuando M es la recta compleja L, solo miramos a funciones analíticas (o series de potencias) de una variable. Tenemos $\mathbb{C}[RL] = \mathbb{C}[z, z_1, z_2, \dots,][1/z_1]$, la derivación $\partial = \sum z_{i+1} \frac{\partial}{\partial z_i}$ y el álgebra de Lie $\widehat{\chi} = \mathbb{C}[[t]] \frac{d}{dt}$. No hay espacio para muchos invariantes :

Lema 57. *Si un pseudogrupo $\mathcal{G}$ tiene un invariante entonces el cuerpo de los invariantes es el cuerpo diferencial generado por un H de orden minimal k. Diremos que este H es* el invariante *de f.*

Demostración. – Sea k el orden minimal de los invariantes $Inv(f)$. La intersección $Inv(f) \cap \mathbb{C}(R_{k-1}) = \{0\}$, entonces el grado de trascendencia de $Inv(f) \cap \mathbb{C}(R_k)$ sobre $\mathbb{C}$ es 1. El teorema del elemento primitivo implica que $Inv(f) \cap \mathbb{C}(R_k)$ está generado por un elemento H. Las derivadas $\partial^p H$ son lineales en z_{k+p} entonces $Inv(f) = \mathbb{C}(H, \partial H, \dots)$. □

Vamos a estudiar un nivel común particular de los invariantes: la subvariedad $V = \cap_n \{\partial^n H = 0\} \subset RL$ y sus estabilizadores.

1. $G \subset \Gamma$ es $\{\gamma \mid T_\gamma(V) \subset V\}$
2. $\mathfrak{g} \subset \widehat{\chi}$ es $\{\widehat{a} \mid T_{\widehat{a}}|_V \in TV\}$

Lema 58. *El grupo G es un subgrupo algebraico de Γ de dimensión $k - 1$. El álgebra de Lie $\mathfrak{g}$ es una subálgebra de Lie de $\widehat{\chi}$ de dimensión k que contiene $\frac{d}{dt}$.*

Ejercicio 59. Probar el lema.

6.1 Un teorema de Lie

Teorema 60. *Si $\mathfrak{g}$ es una subalgebra de Lie de $\widehat{\chi} = \mathbb{C}[[t]]\frac{d}{dt}$ de dimensión finita que contiene $\frac{d}{dt}$, entonces existe $\gamma \in \Gamma$ tal que*

$$\gamma^*\mathfrak{g} \subset sl_2 = \{(c_0 + c_1 t + c_2\frac{t^2}{2})\frac{d}{dt} \mid c_0, c_1, c_2 \in \mathbb{C}\}.$$

Demostración. – Sea $\frac{d}{dt}, a_1(t)\frac{d}{dt}, \dots a_n(t)\frac{d}{dt}$ una base de $\mathfrak{g}$.

El paréntesis de Lie $[\frac{d}{dt}, a_i(t)\frac{d}{dt}] = a_i'(t)\frac{d}{dt}$ está en $\mathfrak{g}$, entonces $(1, a_1, \dots, a_n)$ satisface a un sistema diferencial lineal con coeficientes constantes.

Podemos resolver este sistema con exponenciales y polinomios.

En el caso semisimple $a_i(t) = \exp(\lambda_i t)$ y

$$\left[\exp(\lambda_i t)\frac{d}{dt}, \exp(\lambda_j t)\frac{d}{dt}\right] = (\lambda_j - \lambda_i)\exp((\lambda_i + \lambda_j)t)\frac{d}{dt},$$

dado que tenemos un número finito de λ's, tenemos menos de 3: $\lambda, 0, -\lambda$. El álgebra de Lie está dentro del algebra de Lie con base

$$\exp(\lambda t)\frac{d}{dt}, \frac{d}{dt}, \exp(-\lambda t)\frac{d}{dt}$$

i.e.,

$$\lambda(\exp(\lambda t))^2\frac{d}{d(\exp(\lambda t))}, \lambda\exp(\lambda t)\frac{d}{d(\exp(\lambda t))}, \lambda\frac{d}{d(\exp(\lambda t))}.$$

El cambio de variable $\gamma(t) = \exp\lambda t - 1$ conjuga estos campos a

$$\lambda(t+1)^2\frac{d}{dt}, \lambda(t+1)\frac{d}{dt}, \lambda\frac{d}{dt}$$

que generan sl_2.

Si el sistema no es semisimple tenemos que hacer cálculos parecidos. □

Ejercicio 61. Probar el teorema de Lie en el caso general.

Sea γ el cambio de variable del teorema de Lie. La variedad

$$V_0 = T_\gamma(V) = \{r \circ \gamma \mid r \in V\}$$

Sus estabilizadores son

1. $G_0 = \{\gamma \in \Gamma | T_\gamma(V_0) \subset V_0\} \subset \{\gamma : t \mapsto \frac{\alpha t}{1-\beta t} \mid \alpha \in \mathbb{C}^*, \beta \in \mathbb{C}\}$
2. $\mathfrak{g}_0 = \{\widehat{a} \in \widehat{\chi} \mid T_{\widehat{a}}|_{V_0} \in TV_0\} \subset sl_2$

6.2 Las ecuaciones de V_0

Supongamos que $\mathfrak{g}_0 = sl_2$ y escribimos $F(z, z_1, z_2, z_3) = \left(2\frac{z_3}{z_1} - 3\left(\frac{z_2}{z_1}\right)^2\right)\frac{1}{(z_1)^2} \in \mathbb{C}[R_3L]$.

Lema 62. *V_0 es un fibrado principal para el grupo G_0 sobre un abierto de Zariski de L.*

Lema 63. *Existe $\nu \in \mathbb{C}(z)$ tal que*

$$V_0 = \left\{ r \in RM \mid \left(2\frac{r'''}{r'} - 3\left(\frac{r''}{r'}\right)^2\right)\frac{1}{(r')^2} - \nu(r) = 0 \right\}.$$

Esta fórmula significa que el ideal de definición de V_0 está generado diferencialmente por $q(z)F(z, z_1, z_2, z_3) - p(z)$ donde $\nu = \frac{p}{q}$.

Los referentes de V_0 en un punto $p \in L$ son una órbita de la acción de G_0 sobre RL. Es fácil verificar que sus órbitas en R_3L son los niveles de F :
Si $r = r_0 + r_1 t + r_2\frac{t^2}{2} + r_3\frac{t^3}{6} + \dots$ y $\gamma = \alpha t + 2\alpha\beta\frac{t^2}{2} + 6\alpha\beta^2\frac{t^3}{6} + \dots$ entonces

$$r \circ \gamma = r_0 + r_1\alpha t + (r_2\alpha^2 + 2r_1\alpha\beta)\frac{t^2}{2} + (r_3\alpha^3 + 6r_2\alpha^2\beta + 6r_1\alpha\beta^2)\frac{t^3}{6} + \dots$$

y tenemos $F(r) = F(r\circ\gamma)$. La restricción de esta función sobre V_0 es una función invariante por G_0, entonces es una función racional en r_0.

6.3 Las ecuaciones de $\mathcal{G}$

Obtenemos las ecuaciones de $\mathcal{G}$ mirando las ecuaciones de V_0.

Lema 64. *Si $\mathcal{G}$ es un pseudogrupo con su invariante de orden 3 entonces*

$$\mathcal{G} = \{\varphi \mid 2\frac{\varphi'''}{\varphi'} - 3\left(\frac{\varphi''}{\varphi'}\right)^2 + \nu(\varphi)(\varphi')^2 = \nu(z)\}$$

Demostración. – Si

$$r = r_0 + r_1 t + r_2 \frac{t^2}{2} + r_3 \frac{t^3}{6} + \dots$$

y

$$\varphi = \varphi_0 + \varphi_1 (z - r_0) + \varphi_2 \frac{(z - r_0)^2}{2} + \varphi_3 \frac{(z - r_0)^3}{6} + \dots$$

tenemos

$$\varphi \circ r = \varphi_0 + (\varphi_1 r_1) t + (\varphi_2 (r_1)^2 + \varphi_1 r_2) \frac{t^2}{2} + (\varphi_3 (r_1)^3 + 3\varphi_2 r_1 r_2 + \varphi_1 r_3) \frac{t^3}{6} + \dots$$

Si $r \in V_0$ y $\varphi \circ r \in V_0$ podemos eliminar r y obtener ecuaciones en φ :

$$2\frac{\varphi_3}{\varphi_1} - 3\left(\frac{\varphi_2}{\varphi_1}\right)^2 + \nu(\varphi_0)(\varphi_1)^2 = \nu(r_0).$$

□

Llamaremos $\mathcal{G}_3(\nu)$ este tipo de pseudogrupos.

6.4 Ejercicios

Ejercicio 65. Probar que si $\mathfrak{g}_0 = (\mathbb{C} + \mathbb{C}t)\frac{d}{dt}$, entonces existe $\mu \in \mathbb{C}(z)$ tal que

$$\mathcal{G} = \{\varphi | \frac{\varphi''}{\varphi'} + \mu(\varphi)\varphi' = \mu(x)\}.$$

Ejercicio 66. Probar que si $\mathfrak{g}_0 = \mathbb{C}\frac{d}{dt}$ entonces tenemos dos casos

1. existe $\eta \in \mathbb{C}(z)$ y $k \in \mathbb{N}$ tal que
$$\mathcal{G} = \{\varphi | \eta(\varphi)(\varphi')^k = \eta(x)\},$$
2. existe $h \in \mathbb{C}(z)$ tal que
$$\mathcal{G} = \{\varphi | h(\varphi) = h(x)\}.$$

7 Aplicación en dimensión 1: el pseudogroupo de Galois de $f : \mathbb{C} \dashrightarrow \mathbb{C}$

Queremos probar el siguiente teorema:

Teorema 67. *Si $f : L \dashrightarrow L$ es tal que $\mathcal{G}al(f) \neq \mathcal{A}ut(L)$ entonces f está en la lista de Ritt: existe una homografía A tal que $A \circ f \circ A^{-1}$ es*

- *una homografía*
- *un monomio, $M_k(z) = z^k$,*
- *un Chebishev, $T_k(z) = \cos(k \arccos(z))$*
- *un Lattès, $L_e(z) = \mathcal{P}(e(\mathcal{P}^{-1}(z)))$ donde e es un endomorfismo de grado > 1 de la curva elíptica de la función elíptica $\mathcal{P}$.*

Utilizando la clasificación de los pseudogrupos, el problema es: dar los $f \in \mathbb{C}(z)$ tal que existe un $\nu \in \mathbb{C}(z)$ tal que $f \in \mathcal{G}_3(\nu)$, *i.e.*,

$$2\frac{f'''}{f'} - 3\left(\frac{f''}{f'}\right)^2 + \nu(f)(f')^2 - \nu(z) = 0.$$

7.1 La linealización de un punto fijo repulsivo

Para resolver la ecuación utilizaremos elementos de la dinámica de f.

Teorema 68 (Koenigs)**.** *Si $f : (\mathbb{C}, 0) \to (\mathbb{C}, 0)$ es tal que $\lambda = |f'(0)| > 1$ entonces existe $h \in \mathbb{C}\{w\}$ con $h(0) = 0, h'(0) = 1$ tal que $h^{-1} \circ f \circ h(w) = \lambda w$. Llamaremos a h una linealización de f.*

Teorema 69 ([13] chap. 10 corollary 10.16.)**.** *Si $f \in \mathbb{C}(z)$ pero no es una homografía entonces para cada $k \in \mathbb{N}$ existe $n \in \mathbb{N}$ tal que $f^{\circ n}$ tiene más de k puntos fijos repulsivos.*

La prueba del segundo teorema es más difícil. La cantidad de puntos fijos crece con n pero tenemos una cota sobre el número de puntos fijos que no son repulsivos.

Podemos suponer que $f : L \dashrightarrow L$ tiene un punto fijo repulsivo con linealización h que no es un polo de ν.

Lema 70. *La linealización $h : (\mathbb{C}, 0) \to L$ es el germen de una función meromorfa sobre $\mathbb{C}$.*

Demostración. – Si $w \in \mathbb{C}$, existe n tal que $\frac{w}{\lambda^n}$ está en el dominio de h. Si $h\left(\frac{w}{\lambda^n}\right)$ está en el dominio de $f^{\circ n}$, definimos $h(w)$ por

$$f^{\circ n} \circ h\left(\frac{w}{\lambda^n}\right).$$

□

Nota 71. Para f en la lista de Ritt, tenemos $\lambda = k$ y

$$h = A \circ \exp,\ A \circ \cos,\ A \circ \mathcal{P},\ A \circ \mathcal{P}^2, A \circ \mathcal{P}' \text{ o } A \circ \mathcal{P}'^2.$$

Éstas son funciones que realizan los cocientes de $\mathbb{C}$ por grupos discretos de transformaciones afines : $w \to aw + b$.

7.2 El pull-back de $\mathcal{G}al$ por h y la estructura de h

Queremos probar que los φ tal que $h \circ \varphi = h$ son aplicaciones afines. El pseudogrupo "pull-back" de $\mathcal{G}al$ por h,

$$\{\varphi \mid \text{ existe } \psi \in \mathcal{G}_3(\nu) \text{ t.q. } h \circ \varphi = \psi \circ h\},$$

es un pseudogrupo de tipo $\mathcal{G}_3(\widetilde{\nu})$ con

$$\widetilde{\nu}(w) = \nu(h(w))h'(w)^2 + 2\frac{h'''}{h'} - 3\left(\frac{h''}{h'}\right)^2.$$

Conocemos una solución $w \to \lambda w$ de $\mathcal{G}_3(\widetilde{\nu})$, entonces

$$\widetilde{\nu}(\lambda w)\lambda^2 = \widetilde{\nu}(w).$$

Por otro lado, la fórmula para $\widetilde{\nu}$ nos da que $\widetilde{\nu}$ es holomorfa en 0 y por eso $\widetilde{\nu} = 0$.

Los elementos $\varphi \in \mathcal{G}_3(0)$ son gérmenes de homografías. Probamos que h es el cociente por un grupo de homografía. Los grupos que aparecen son

- $\mathbb{Z}$
- $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $(\mathbb{Z} + \tau\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$
- $(\mathbb{Z} + i\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}$

- $(\mathbb{Z} + j\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$
- $(\mathbb{Z} + j\mathbb{Z}) \times \mathbb{Z}/6\mathbb{Z}$

y las funciones que realizan este cociente son exp, cos o las funciones elípticas.

Probamos que si f está dentro de un $\mathcal{G}_3(\nu)$ entonces $f^{\circ n}$ está en la lista de Ritt. Para finalizar la prueba tenemos que ver que:

1. los f de la lista de Ritt pertenecen a un $\mathcal{G}_3(\nu)$,
2. si $f^{\circ n}$ está en la lista entonces f también.

El primero es un ejercicio de cálculo. Para probar el segundo, tenemos que verificar que si h es una linealización de $f^{\circ n}$ entonces $f \circ h$ también.

8 Aplicación en dimensión 1: el teorema de Ritt

Teorema 72. *Si la linealización h de un punto fijo repulsivo de $f : L \dashrightarrow L$ satisface una ecuación diferencial polinomial entonces f está en la lista de Ritt: existe una homografía A tal que $A \circ f \circ A^{-1}$ es*

- *una homografía*
- *un monomio $M_k(z) = z^k$,*
- *un Tchebitchev $T_k(z) = \cos(k \arccos(z))$*
- *un Lattes $L_e(z) = \mathcal{P}(e(\mathcal{P}^{-1}(z)))$ donde e es un endomorfismo de grado > 1 de la curva elíptica de $\mathcal{P}$.*

8.1 La ecuación de h

La linealización h es una función meromorfa de $\mathbb{C}$ en L entonces sus series de potencias en cada punto de su dominio son elementos de

$$F(\mathbb{C}, L) = \{(z_0, \widehat{k}, w_0) \mid \widehat{k} : (\mathbb{C}, w_0) \to (L, z_0)\}$$

$$\widehat{k}(w) = z_0 + \sum_{n>1} k_n \frac{(w - w_0)^n}{n!}.$$

El anillo de funciones polinomiales sobre $F(\mathbb{C}, L)$ es $\mathbb{C}[F] = \mathbb{C}[w_0, z_0, k_1, k_2, \ldots]$.

Sea $I \subset \mathbb{C}[F]$ el ideal de las ecuaciones satisfechas por todos los desarrollos de series de potencias de h.

Lema 73. *El ideal I es un ideal estable por $D = \frac{\partial}{\partial w_0} + k_1 \frac{\partial}{\partial z_0} + \sum_{i>0} k_{i+1} \frac{\partial}{\partial k_i}$*

Lema 74. *Sea Z el conjunto de los ceros de I en $F(\mathbb{C}, L)$. Este conjunto es de dimensión finita*

Demostración. – Por hipótesis I contiene un polinomio que no es 0: si $E(w, h, h', \ldots h^{(p)}) = 0$ es una ecuación de h de orden minimál entonces la dimensión de Z es $p + 1$. □

8.2 Las acciones de f y $\mathbb{C}^*$

La transformación $f : L \dashrightarrow L$ actúa sobre $F(\mathbb{C}, L)$ por $Rf : \widehat{k} \mapsto f \circ \widehat{k}$. Pero no preserva Z. Queremos construir un conjunto algebraico de dimensión finita y invariante por Rf.

El grupo de transformaciones $\sigma_q : w \mapsto qw$ actúa sobre $F(\mathbb{C}, L)$ por cambios de variable. Si $\widehat{k} : (\mathbb{C}, w_0) \to (L, z_0)$ con

$$\widehat{k}(w) = z_0 + \sum_{n>1} k_n \frac{(w - w_0)^n}{n!}$$

entonces $T_q(\widehat{k}) : (\mathbb{C}, \frac{w_0}{q}) \to (L, z_0)$ está definida por

$$\widehat{k} \circ \sigma_q(w) = z_0 + \sum_{n>1} q^n k_n \frac{(w - \frac{w_0}{q})^n}{n!}.$$

La ecuación funcional de linealización es $Rf(\widehat{h}) = T_\lambda(\widehat{h})$. Vamos a construir un conjunto invariante utilizando esta igualdad y un teorema de Chevalley:

Teorema 75 ([12] por ejemplo)**.** *Si $f : X \to Y$ es una aplicación polinomial entre conjuntos algebraicos entonces existe un conjunto algebraico $S \subset \overline{f(X)}$ tal que*

- *$\overline{f(X)} - S$ es denso dentro de $\overline{f(X)}$,*
- *$\overline{f(X)} - S = f(X) - S$*

El conjunto $T_{\lambda^{-1}}(\overline{Rf(Z)})$ es un conjunto algébraico que contiene los desarrollos de h entonces contiene Z *i.e.* $\overline{Rf(Z)} \supset T_\lambda(Z)$. Como Rf y T_q conmutan $\overline{R_f(T_q Z)} \supset T_{q\lambda}(Z)$, el conjunto

$$V = \overline{\cup_{q\in\mathbb{C}^*} T_q(Z)}$$

es un conjunto algebraico invariante. Tenemos que probar que este conjunto es de dimensión finita.

Los invariantes de la acción de $\mathbb{C}^*$ sobre $F(\mathbb{C}, L)$ son

$$\begin{aligned} \pi : F(\mathbb{C}, L) &\to \mathbb{C}^{\mathbb{N}} \\ (w_0, z_0, h_1 \ldots) &\mapsto (z_0, w_0 h_1, (w_0)^2 h_2 \ldots) \end{aligned}$$

Los niveles de π son de dimensión uno. Por el teorema de Chevalley: $\overline{\pi(Z)}$ es un conjunto algebraico de dimensión más pequeña que la dimensión de Z y $V = \pi^{-1}(\overline{\pi(Z)})$ es un conjunto algebraico de dimensión menor que la dimensión de Z más uno, es el conjunto algebraico minimal $\mathbb{C}^*$-invariante que contiene Z, entonces

$$R_f(V) \subset V$$

La dimensión de V es finita y por lo tanto

$$\mathcal{G} = \left\{ \varphi \in \mathcal{A}ut(L) \;\middle|\; R\varphi(V) \subset V \right\}$$

es un pseudogrupo algebraico de dimensíon finita y contiene f. Por definición $\mathcal{G}al(f) \subset \mathcal{G}$. Entonces $\mathcal{G}al(f)$ es pequeño y el teorema de Ritt está probado.

Referencias

[1] Audin M. – Julia, Montel. The great prize of mathematical sciences of 1918, and beyond. Translated from the 2009 French original by the author. Lecture Notes in Mathematics, 2014. History of Mathematics Subseries. Springer, Heidelberg, 2011. viii+332 pp. 113

[2] Americ K. & Campana F. – Fibrations méromorphes sur certaines variétés à fibré canonique trivial. Pure Appl. Math. Q. 4 (2008), no. 2, Special Issue: In honor of Fedor Bogomolov. Part 1, 509–545. 125

[3] Bergweiler W. – Solution of a problem of Rubel concerning iteration and algebraic differential equations, Indiana Univ. Math. J. 44 (1995), 257–267;

[4] Bergweiler W. ;& Aschenbrenner M. – Julia's equation and differential transcendence 113

[5] Chevalley, C. & Kolchin, E. – Two proofs of a theorem on algebraic groups. Proc. Amer. Math. Soc. 2, (1951). 126–134. 115

[6] Crespo, T. & Hajto, Z. – Algebraic Groups and Differential Galois Theory, Graduate Studies in Mathematics 122, American Mathematical Society, 2011. 114

[7] Drach, J. – Sur l'intégration logique des équations différentielles ordinaires, Proceedings of the 5th international congress of mathematicians Cambrige university press (1913), Vol 1 pp 438–497 (available on `http://www.mathunion.org/ICM/`) 115

[8] Hardouin C. & Singer M.F. – Differential Galois theory of linear difference equations. Math. Ann. 342 (2008), no. 2, 333–377. 113, 125

[9] Hochschild, G. P. – Basic theory of algebraic groups and Lie algebras. Graduate Texts in Mathematics, 75. Springer-Verlag, New York-Berlin, 1981. viii+267 pp. 114

[10] Malgrange, B. – Le groupoïde de Galois d'un feuilletage. (French) [The Galois groupoid of a foliation] Essays on geometry and related topics, Vol. 1, 2, 465–501, Monogr. Enseign. Math., 38, Enseignement Math., Geneva, 2001. 112

[11] Martinet, J. & Ramis, J.-P. – Classification analytique des équations différentielles non linéaires résonnantes du premier ordre. Ann. Sci. École Norm. Sup. (4) 16 (1983), no. 4, 571–621 (1984). 113

[12] Matsumura H. – Commutative algebra, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980 131

[13] Milnor, J.W. – Dynamics in one complex variable. Introductory lectures. Ann. of Math. Studies 160 Princeton Univ. Press (2006) 112, 129

[14] Milnor J. W. – On Lattès maps. Dynamics on the Riemann sphere, 9–43, Eur. Math. Soc., Zürich, 2006.,

[15] van der Put, M. & Singer, M.F. – Galois theory of difference equations. Lecture Notes in Mathematics, 1666. Springer-Verlag, Berlin, 1997. viii+180 pp. 112, 118

[16] Ramis, J.-P. – About the growth of entire functions solutions of linear algebraic q-difference equations. Ann. Fac. Sci. Toulouse Math. (6) 1 (1992), no. 1, 53–94. 113

[17] Ritt, J. F. – Permutable rational functions. Trans. Amer. Math. Soc. 25 (1923), no. 3, 399–448. 113

[18] Ritt, J. F. – Transcendental transcendency of certain functions of Poincaré. Math. Ann. 95 (1926), no. 1, 671–682. 112

[19] Ritt, J. F. – Meromorphic functions with addition or multiplication theorems. Trans. Amer. Math. Soc. 29 (1927), no. 2, 341–360. 113

[20] Sharpe, R. W. – Differential geometry. Cartan's generalization of Klein's Erlangen program. With a foreword by S. S. Chern. Graduate Texts in Mathematics, 166. Springer-Verlag, New York, 1997. xx+421 pp. 122

[21] Umemura, H. – Differential Galois theory of infinite dimension. Nagoya Math. J. 144 (1996), 59–135. 124

About the Cremona group

Julie Déserti

Université Paris Diderot, Sorbonne Paris Cité, Institut De Mathématiques de Jussieu-Paris Rive Gauche, UMR 7586, CNRS, Sorbonne Universités, UPMC Univ Paris 06, F-75013 Paris, France

E-mail address: deserti@math.univ-paris-diderot.fr

Contents

1 First definitions and properties

1.1 Divisors and blow-ups

Definition 1.1. — Let X be an algebraic variety. A **prime divisor** on X is an irreducible closed subset of X of codimension 1.

Examples 1.2.
- If $\dim X = 2$, *i.e.* if X is a surface, then the prime divisors of X are the irreducible curves that lie on it.
- If $X = \mathbb{P}^n_{\mathbb{C}}$, then the prime divisors are given by the zero locus of irreducible homogeneous polynomials.

Let us set

$$\mathrm{Div}(X) = \Big\{ \sum_{i=1}^{m} a_i D_i \,|\, m \in \mathbb{N},\, a_i \in \mathbb{Z},\, D_i \text{ prime divisors on } X \Big\}.$$

An element $\sum_{i=1}^{m} a_i D_i$ of $\mathrm{Div}(X)$ is **effective** if $a_i \geq 0$ for any $1 \leq i \leq m$.

If f is a non zero rational function, and D a prime divisor of X, one can define the multiplicity $\nu_f(D)$ of f at D as follows

- $\nu_f(D) = k > 0$ if f vanishes on D at the order k;
- $\nu_f(D) = -k$ if f has poles of order k on D;
- $\nu_f(D) = 0$ otherwise.

To any rational function $f \in \mathbb{C}(X)^*$ one associates a divisor $\mathrm{div}\, f \in \mathrm{Div}(X)$ defined by

$$\mathrm{div}\, f = \sum_{\substack{D \text{ prime} \\ \text{divisor}}} \nu_f(D)\, D.$$

Such a divisor is called a **principal divisor**. Note that a principal divisor belongs to $\mathrm{Div}(X)$ as $\nu_f(D) = 0$ for all but finitely many D. Since $\mathrm{div}\, f + \mathrm{div}\, g = \mathrm{div}\, fg$ the set of principal divisors is a subgroup of $\mathrm{Div}(X)$.

Two divisors D, D' on an algebraic variety are **linearly equivalent** if $D - D'$ is a principal divisor. The set of equivalence classes corresponds to the quotient of $\mathrm{Div}(X)$ by the subgroup of principal divisors. When X is smooth, this quotient is isomorphic to the group of isomorphism classes of line bundles on X called the **Picard group** of X and denoted $\mathrm{Pic}(X)$.

Exercice 1. — Determine $\mathrm{Pic}(\mathbb{P}^n_{\mathbb{C}})$.

Exercice 2. — Determine $\mathrm{Pic}(\mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}})$.

There is a notion of intersection:

Proposition 1.3 ([26]). — *Let S be a smooth projective surface. There exists a unique bilinear symmetric form*

$$\mathrm{Div}(S) \times \mathrm{Div}(S) \to \mathbb{Z}, \qquad (D, D') \mapsto D \cdot D'$$

having the following properties:

- *if C and D are smooth curves meeting transversely, then $C \cdot D = \#(C \cap D)$;*
- *if C and C' are linearly equivalent, then $C \cdot D = C' \cdot D$.*

In particular this yields an intersection form

$$\mathrm{Pic}(S) \times \mathrm{Pic}(S) \to \mathbb{Z}, \qquad (D, D') \mapsto D \cdot D'.$$

Definition 1.4. — Let p be a point of a smooth surface S. We say that $\pi\colon Y \to S$ is a **blow-up** of $p \in S$ if

- Y is a smooth variety,
- $\pi_{|Y \smallsetminus \{\pi^{-1}(p)\}}\colon Y \smallsetminus \{\pi^{-1}(p)\} \to S \smallsetminus \{p\}$ is an isomorphism,
- $\pi^{-1}(p) \simeq \mathbb{P}^1_{\mathbb{C}}$.

The set $\pi^{-1}(p)$ is called the **exceptional divisor**.

Let us explain how to construct π. Assume for simplicity that $X = S$ is a surface. Take a neighborhood $\mathcal{U}$ of p on which there exist local coordinates x, y at p, that is the curves $x = 0$ and $y = 0$ intersects transversely at p. Up to shrinking $\mathcal{U}$ one has

$$(x = 0) \cap (y = 0) \cap \mathcal{U} = \{p\}.$$

Let us consider the subvariety $\widetilde{\mathcal{U}} \subset \mathcal{U} \times \mathbb{P}^1_{\mathbb{C}}$ defined by $xv - yu = 0$ where u and v are homogeneous coordinates on $\mathbb{P}^1_{\mathbb{C}}$. The projection $\pi\colon \widetilde{\mathcal{U}} \to \mathcal{U}$ is an isomorphism over the points of $\mathcal{U}$ where at most one of the coordinates x, y vanishes

$$\pi\big((0,y),(0:1)\big) = (0,y) \qquad \pi\big((x,0),(1:0)\big) = (x,0)$$

and $\pi^{-1}(p) = \{p\} \times \mathbb{P}^1_{\mathbb{C}}$. It follows from the construction that the points of E can be naturally identified with the tangent directions on S at p.

Remarks 1.5.
- If $\pi\colon Y \to S$ and $\pi'\colon Y' \to S$ are two blow-ups of p, then there exists an isomorphism $\varphi\colon Y \to Y'$ such that $\pi = \pi'\varphi$; we can thus speak about the blow-up of $p \in S$.
- Note that π is not an isomorphism: it contracts $E = \pi^{-1}(p) \simeq \mathbb{P}^1_{\mathbb{C}}$ onto p.

Let $\pi\colon \mathrm{Bl}_p S \to S$ be the blow-up of $p \in S$. The morphism π induces the map

$$\pi^*\colon \mathrm{Pic}(S) \to \mathrm{Pic}(\mathrm{Bl}_p S), \qquad C \mapsto \pi^{-1}C.$$

If S is a smooth algebraic surface and if $C \subset S$ is an irreducible curve, the **strict transform** of C is $\widetilde{C} = \overline{\pi^{-1}(C \smallsetminus \{p\})}$.

Let us recall that if Y is a quasi-projective variety, and if y is a point of Y, then $O_{y,Y}$ is the set of equivalence classes of pairs $(\mathcal{U}, f)$ where

- $\mathcal{U} \subset Y$ is an open subset,
- $y \in \mathcal{U}$,
- $f \in \mathbb{C}[\mathcal{U}]$.

Definition 1.6. — If S is a smooth algebraic surface, $C \subset S$ a curve on S, and p a point of S, we can define the **multiplicity** $m_p(C)$ **of** C **at** p.

Let $\mathfrak{m}$ be the maximal ideal of the ring of functions $O_{p,S}$. Let f be a local equation of C; then $m_p(C)$ can be defined as the integer k such that $f \in \mathfrak{m}^k \smallsetminus \mathfrak{m}^{k+1}$. For instance if S is rational, one can find a neighborhood $\mathcal{U}$ of p in S with

$$\begin{cases} \mathcal{U} \subset \mathbb{C}^2 \\ p = (0,0) \\ C \text{ is described by } \displaystyle\sum_{i=1}^{m} P_i(x,y) = 0 \end{cases}$$

where P_i denotes an homogeneous polynomial of degree i.

The multiplicity $m_p(C)$ is equal to the lowest i such that $P_i \not\equiv 0$. The following properties holds

$$\begin{cases} m_p(C) \geq 0 \\ m_p(C) = 0 \Longleftrightarrow p \notin C \\ m_p(C) = 1 \Longleftrightarrow p \text{ is a smooth point of } C \end{cases}$$

Take two distinct curves C and C' without common component. One can define an integer $(C \cdot C')_p$ which counts the intersection of C and C' at p:

- it is equal to 0 if either C, or C' does not pass through p,
- otherwise let f, resp. g be some local equation of C, resp. C' in a neighborhood of p and define $(C\cdot C')_p$ to be $\dim \frac{O_{p,S}}{(f,g)}$.

This number is related to $C\cdot C'$ as follows (*see* [26, Chapter V, Proposition 1.4]): if C and C' are two distinct curves without common irreducible component on a smooth surface, then

$$C\cdot C' = \sum_{p\in C\cap C'} (C\cdot C')_p.$$

In particular $C\cdot C' \geq 0$.

Lemma 1.7. — *Let $\pi\colon \mathrm{Bl}_p S \to S$ be the blow-up of $p\in S$. Then*

$$\pi^* C = \widetilde{C} + m_p(C)E$$

where $\widetilde{C}$ is the strict transform of C, and $E=\pi^{-1}(p)$.

Proof. Let us fix some local coordinates (x,y) such that

$$\begin{cases} p=(0,0) \\ k=m_p(C) \\ C \text{ is given by} \\ \qquad P_k(x,y)+P_{k+1}(x,y)+\ldots+P_{k+\ell}(x,y)=0 \\ \text{where } P_i \text{ denotes a homogeneous polynomial of degree } i \end{cases}$$

The blow-up of p can be viewed as $(u,v)\mapsto(uv,v)$; hence the pull-back of C is given by

$$v^k\big(P_k(u,1)+vP_{k+1}(u,1)+\ldots+v^\ell P_{k+\ell}(u,1)\big)=0$$

i.e. it decomposes into k times the exceptional divisor $\pi^{-1}(0,0)=(v=0)$ and the strict transform of C. □

Let S be a compact, complex surface, and let ω_S be the line bundle of differential 2-forms on S. The **canonical divisor** K_S of S is such that $O_S(K_S)=\omega_S$.

Example 1.8. The canonical divisor of $\mathbb{P}^2_{\mathbb{C}}$ is

$$K_{\mathbb{P}^2_{\mathbb{C}}} = [-3H]$$

where H denotes a generic hyperplane of $\mathbb{P}^2_{\mathbb{C}}$.

Proposition 1.9 ([26]). — *Let S be a smooth surface, p be a point of S, and $\pi\colon \mathrm{Bl}_p S \to S$ be the blow-up of p. Set $E = \pi^{-1}(p) \simeq \mathbb{P}^1_{\mathbb{C}}$. One has*

$$\mathrm{Pic}(\mathrm{Bl}_p S) = \pi^*\mathrm{Pic}(S) + \mathbb{Z}\cdot E.$$

The intersection form on $\mathrm{Bl}_p S$ is induced by the intersection form on S via

$$\begin{cases} \pi^*C \cdot \pi^*C' = C \cdot C' \quad \forall C, C' \in \mathrm{Pic}(S) \\ \pi^*C \cdot E = 0 \quad \forall C \in \mathrm{Pic}(S) \\ E^2 = E \cdot E = -1 \\ \widetilde{C}^2 = C^2 - 1 \quad \forall C \ni p, C \text{ smooth} \end{cases}$$

Furthermore, $K_{\mathrm{Bl}_p S} = \pi^* K_S + E$.

The proof is decomposed in the following exercises:

Exercice 3. Prove the following equalities

$$\begin{cases} \pi^*C \cdot \pi^*C' = C \cdot C' \quad \forall C, C' \in \mathrm{Pic}(S) \\ \pi^*C \cdot E = 0 \quad \forall C \in \mathrm{Pic}(S) \\ E^2 = E \cdot E = -1 \\ \widetilde{C}^2 = C^2 - 1 \quad \forall C \ni p, C \text{ smooth} \end{cases}$$

Exercice 4. Prove that

$$\mathrm{Pic}(\mathrm{Bl}_p S) = \pi^*\mathrm{Pic}(S) + \mathbb{Z}\cdot E.$$

Exercice 5. Prove that $K_{\mathrm{Bl}_p S} = \pi^* K_S + E$.

1.2 Rational and birational maps

1.2.1 First Definitions

Consider two irreducible varieties X and Y. A **rational map** $\phi\colon X \dashrightarrow Y$ is a morphism from an open subset $\mathcal{U}$ of X to Y which cannot be extended to any larger open subset; ϕ is **defined** at x if x belongs to $\mathcal{U}$. The set $X \smallsetminus \mathcal{U}$ is the **indeterminacy set** of ϕ; it is denoted $\mathrm{Ind}\,\phi$.

Suppose that $X = S$ is a smooth surface, then $\mathrm{Ind}\,\phi$ is the union of a finite number of points. One has

- if C is an irreducible curve on S, then ϕ is defined on $C \smallsetminus \mathrm{Ind}\,\phi$; the image of C is $\overline{\phi(C \smallsetminus \mathrm{Ind}\,\phi)}$ and is still denoted $\phi(C)$.

- restriction induces an isomorphism between the divisors groups of $S \smallsetminus \operatorname{Ind}\phi$ and S, which induces an isomorphism between $\operatorname{Pic}(S)$ and $\operatorname{Pic}(S \smallsetminus \operatorname{Ind}\phi)$. We can thus speak of the inverse image $\phi^* D$ under ϕ of a divisor D on Y.

Example 1.10. — Let $S \subset \mathbb{P}^n_{\mathbb{C}}$ be a surface, and p be a point of S. The set of lines through p can be identified with a projective space $\mathbb{P}^{n-1}_{\mathbb{C}}$. To any point q of $S \smallsetminus \{p\}$ we associate the line through p and q; this yields a rational map $S \dashrightarrow \mathbb{P}^{n-1}_{\mathbb{C}}$ (the projection away from p). It is defined outside p and extends to a morphism $\mathrm{Bl}_p S \to \mathbb{P}^{n-1}_{\mathbb{C}}$.

A **birational map** $\phi\colon X \dashrightarrow Y$ is a rational map such that there exists a rational map $\psi\colon Y \dashrightarrow X$ such that $\phi\psi = \psi\phi = \mathrm{id}$.

1.2.2 Linear systems

Consider a divisor D on a surface S; we denote by $|D|$ the set of all effective divisors on S linearly equivalent to D. Every non-vanishing section of $O_s(D)$[1] defines an element of $|D|$, namely its divisor of zeros. Conversely any element of $|D|$ is the divisor of zeros of a non-vanishing section of $O_S(D)$, defined up to scalar multiplication. Therefore $|D|$ can be naturally identified with the projective space associated to the vector space[2] $\mathrm{H}^0(O_S(D))$. A linear subspace $\mathscr{S}$ of $|D|$ is called a **linear system** on S; equivalently $\mathscr{S}$ can be defined by a vector subspace of $\mathrm{H}^0(O_S(D))$.

The **dimension** of $\mathscr{S}$ is by definition its dimension as a projective space. A 1-dimensional linear system is a **pencil**.

A curve C is a **fixed component** of $\mathscr{S}$ if any divisor of $\mathscr{S}$ contains C.

The **fixed part** of $\mathscr{S}$ is the biggest divisor F that is contained in every element of $\mathscr{S}$.

A point p of S is a **base point** or **fixed point** of $\mathscr{S}$ if every divisor of $\mathscr{S}$ contains p. If the linear system $\mathscr{S}$ has no fixed part, then it has only a finite number, say b, of fixed points; clearly $b < D^2$, for $D \in \mathscr{S}$.

Let S be a surface. Then there is a bijection between the set

$$\left\{ \text{rational maps } \phi\colon S \dashrightarrow \mathbb{P}^n_{\mathbb{C}} \text{ such that } \phi(S) \text{ is contained in no hyperplane} \right\}$$

and the set

$$\left\{ \text{linear systems on } S \text{ without fixed part and of dimension } n \right\}.$$

Indeed, to the map ϕ we associate the linear system $\phi^*|H|$, where $|H|$ is the system of hyperplanes in $\mathbb{P}^n_{\mathbb{C}}$. Conversely, let $\mathscr{S}$ be a linear system on S with no fixed part and denote by $\mathscr{S}^\vee$

[1] Recall that $O_S(D)$ denotes the invertible sheaf corresponding to D.

[2] Recall that $\mathrm{H}^i(O_S(D))$ is the i-th cohomology group of $O_S(D)$.

the projective space dual to $\mathscr{S}$. Now define a rational map $\phi\colon S \dashrightarrow \mathscr{S}^\vee$ by sending $x \in S$ to the hyperplane in $\mathscr{S}$ consisting of the divisors passing through x; the map ϕ is defined at x if and only if x is not a base point of $\mathscr{S}$.

1.2.3 Cremona maps

If $S = \mathbb{P}^2_{\mathbb{C}}$, then a birational self-map ϕ of S can be written

$$(z_0 : z_1 : z_2) \dashrightarrow \big(\phi_0(z_0,z_1,z_2) : \phi_1(z_0,z_1,z_2) : \phi_2(z_0,z_1,z_2)\big)$$

where the ϕ_i's denote homogeneous polynomials of the same degree without common factor (of positive degree). The set of all birational maps of $\mathbb{P}^2_{\mathbb{C}}$ is called the **Cremona group**, and is denoted $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$. The indeterminacy set $\mathrm{Ind}\,\phi$ of ϕ is the finite set given by

$$\big\{p \in \mathbb{P}^2_{\mathbb{C}} \,|\, \phi_0(p) = \phi_1(p) = \phi_2(p) = 0\big\}.$$

The **exceptional set** $\mathrm{Exc}\,\phi$ **of** ϕ is the set of curves blown down by ϕ; one has

$$\mathrm{Exc}\,\phi = \big\{\det \mathrm{jac}\,\phi = 0\big\}.$$

The **degree of** ϕ is defined by: $\deg\phi = \deg\phi_i$. Let d be a positive integer. The set $\mathrm{Bir}_d(\mathbb{P}^2_{\mathbb{C}})$ of plane birational maps of degree d is quasi-projective: it is a Zariski open subset in the subvariety of the projective space made of triples of homogeneous polynomials of degree d modulo scalar multiplication. The group $\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}})$ acts on $\mathrm{Bir}_d(\mathbb{P}^2_{\mathbb{C}})$ as follows

$$\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}) \times \mathrm{Bir}_d(\mathbb{P}^2_{\mathbb{C}}) \times \mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}) \to \mathrm{Bir}_d(\mathbb{P}^2_{\mathbb{C}}), \qquad (A,\phi,B) \mapsto A\phi B^{-1}.$$

If ϕ is an element of $\mathrm{Bir}_d(\mathbb{P}^2_{\mathbb{C}})$, then $O(\phi)$ denotes the orbit of ϕ under this action.

The linear system $\mathscr{S}$ defined by any element $\phi = (\phi_0 : \phi_1 : \phi_2)$ of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ is given by

$$\big\{\lambda_0\phi_0 + \lambda_1\phi_1 + \lambda_2\phi_2 = 0 \,|\, (\lambda_0 : \lambda_1 : \lambda_2) \in \mathbb{P}^2_{\mathbb{C}}\big\}.$$

It is the reciprocical image by ϕ of the net of lines

$$\big\{\lambda_0 z_0 + \lambda_1 z_1 + \lambda_2 z_2 = 0 \,|\, (\lambda_0 : \lambda_1 : \lambda_2) \in \mathbb{P}^2_{\mathbb{C}}\big\}.$$

In particular any curve of $\mathscr{S}$ is a rational one. Take a base point p of ϕ; the **multiplicity** of ϕ at p is the multiplicity of a generic curve of $\mathscr{S}$ at p, that is the order of a generic element of $\mathscr{S}$ at p.

The degree is not a birational invariant: there exist ϕ and ψ in $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ such that $\deg(\psi\phi\psi^{-1}) \neq \deg\phi$. Nevertheless the **dynamical degree**

$$\lambda(\phi) = \lim_{n\to+\infty} (\deg \phi^n)^{1/n}$$

of a birational map ϕ is. More generally consider a projective surface S, a birational self-map ϕ of S, and $||\cdot||$ any norm of the Néron-Severi real vector space $\mathrm{NS}(S)$; we can define

$$\lambda(\phi) = \lim_{n\to+\infty} ||(\phi^n)^*||^{1/n}$$

where ϕ^* is the induced action on $\mathrm{NS}(S)$.

Note that $1 \leq \lambda(\phi) \leq d$. When ϕ is an automorphism with $\lambda(\phi) > 1$, then $\lambda(\phi)$ is algebraic but never rational; in particular $\lambda(\phi) < d$. Let ω denote any Kähler form (for instance the Fubini Study form) with $\int_S \omega^2 = 1$. For any generic line L one has

$$\begin{aligned}
\lambda(\phi) &= \lim_k ||(\phi^k)^*||^{1/k} \\
&= \lim_k \Big(\int_S \beta \wedge (\phi^k)^*\beta \Big)^{1/k} \\
&= \lim_k \Big(\int_{\phi^{-k}L} \beta \Big)^{1/k} \\
&= \lim_k \big(\mathrm{vol}(\phi^{-k}L) \big)^{1/k}
\end{aligned}$$

so the dynamical degree also measures the exponential rate of growth of $(k-1)$-dimensional volume under pullback. It would be convenient if we could have $(\phi^*)^k = (\phi^k)^*$. Diller and Favre showed there is a finite sequence of blow-ups $\pi\colon S' \to S$ such that the induced map $\phi_{S'} = \pi^{-1}\phi\pi$ satisfies $(\phi^k_{S'})^* = (\phi^*_{S'})^k$ (*see* [18]). Set $\omega_{S'} = \pi^*\omega$; then

$$\begin{aligned}
\lambda(\phi) &= \lim_k \Big(\int_S \omega \wedge (\phi^k)^*\omega \Big)^{1/k} \\
&= \lim_k \Big(\int_{S'} \omega_{S'} \wedge (\phi^k_{S'})^*\omega_{S'} \Big)^{1/k} \\
&= \lim_k \Big(\int_{S'} \omega_{S'} \wedge (\phi^*_{S'})^k\omega_{S'} \Big)^{1/k}
\end{aligned}$$

The form $\omega_{S'}$ is a Kähler form so as soon as $\lambda(\phi) > 1$ the growth of $\omega_{S'}$ under $(\phi^*_{S'})^k$ gives the growth of $|(\phi^k_{S'})^*|$ and $\lambda(\phi)$ coincides with the spectral radius of $\phi^*_{S'}$, *i.e.* the modulus of the largest eigenvalue.

Definition 1.11. — Let ϕ be an element of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$.

If $(\deg\phi^n)_n$ is bounded, we say that ϕ is **elliptic**.

If $(\deg\phi^n)_n$ grows linearly, then ϕ is a **Jonquières twist**.

If $(\deg\phi^n)_n$ grows quadratically, then ϕ is a **Halphen twist**.

If $(\deg\phi^n)_n$ grows exponentially, then ϕ is **hyperbolic**.

Examples 1.12. • Birational self-maps of $\mathbb{P}^2_{\mathbb{C}}$ of degree 1 are maps of the type

$$\big(a_0z_0+a_1z_1+a_2z_2 : a_3z_0+a_4z_1+a_5z_2 : a_6z_0+a_7z_1+a_8z_2\big)$$

with $\det(a_i)\neq 0$; they form the group $\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}})$. They are elliptic maps.

• The set $\mathrm{Bir}_2(\mathbb{P}^2_{\mathbb{C}})$ is an irreducible algebraic variety of dimension 14. Set

$$\begin{cases} \sigma=(z_1z_2 : z_0z_2 : z_0z_1)\\ \rho=(z_0z_2 : z_0z_1 : z_2^2)\\ \tau=(z_0z_2+z_1^2 : z_1z_2 : z_2^2)\end{cases}$$

One has ([11])

$$\begin{cases} \mathrm{Bir}_2(\mathbb{P}^2_{\mathbb{C}})=O(\sigma)\cup O(\phi)\cup O(\tau)\\ \mathrm{Bir}_2(\mathbb{P}^2_{\mathbb{C}})=\overline{O(\sigma)}\\ \dim O(\sigma)=14,\ \dim O(\rho)=13,\ \dim O(\tau)=12\end{cases}$$

• Denote by $\mathcal{J}_d$ the set of birational maps of degree d of $\mathbb{P}^2_{\mathbb{C}}$ that preserve the pencil of lines through $p_0=(1:0:0)$. These maps are called **Jonquières maps** of degree d. The **Jonquières group** is the group $\mathcal{J}=\cup_d\mathcal{J}_d$. In affine coordinates an element ϕ of $\mathcal{J}_d$ has the following form

$$\phi(z_0,z_1)=\left(\frac{a(z_1)z_0+b(z_1)}{c(z_1)z_0+d(z_1)},\frac{\alpha z_1+\beta}{\gamma z_1+\delta}\right)$$

with

$$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\in\mathrm{PGL}(2,\mathbb{C})\qquad \begin{bmatrix}a(z_1) & b(z_1)\\ c(z_1) & d(z_1)\end{bmatrix}\in\mathrm{PGL}(2,\mathbb{C}(z_1)).$$

Cleaning denominators we may assume that a, b, c and d are polynomials of respective degree $d-1$, d, $d-2$, and $d-1$. The base points of ϕ are

$$\begin{cases}\text{the point } p_0=(1:0:0) \text{ with multiplicity } d-1\\ 2d-2 \text{ single points } p_1,\ p_2,\ \ldots,\ p_{2d-2}\end{cases}$$

The same holds for ϕ^{-1}.

Remarks that the set of Jonquières twist is contained in $\mathcal{J}$ but the inclusion is strict (for instance σ is elliptic and belongs to $\mathcal{J}$).

- A **polynomial automorphism** ϕ of $\mathbb{C}^2$ is a bijective map of the form

$$\phi\colon \mathbb{C}^2 \to \mathbb{C}^2, \quad (z_0,z_1) \mapsto \big(\phi_0(z_0,z_1),\phi_1(z_0,z_1)\big), \quad \phi_i \in \mathbb{C}[z_0,z_1].$$

  The set of polynomial automorphisms of $\mathbb{C}^2$ form a group denoted $\mathrm{Aut}(\mathbb{C}^2)$. According to Friedland and Milnor if ϕ belongs to $\mathrm{Aut}(\mathbb{C}^2)$, then up to conjugacy ([20])

  (i) either $\phi = (\alpha x + P(y), \beta y + \gamma)$ with α, β, $\gamma \in \mathbb{C}$, $\alpha\beta \neq 0$, $P \in \mathbb{C}[y]$,

  (ii) or

$$\phi = h_1 h_2 \dots h_k$$

  with $h_i = (y, P_i(y) - \delta_i x)$, $\delta_i \in \mathbb{C}^*$, $P_i \in \mathbb{C}[y]$, $\deg P_i \geq 2$.

  In case (i), then ϕ is elliptic; in case (ii) ϕ is hyperbolic.

Exercice 6. — Give a description of the indeterminacy set, and the exceptional set of an automorphism of $\mathbb{P}^2_{\mathbb{C}}$.

Exercice 7. — Give a description of the indeterminacy set, and the exceptional set of σ, resp. ρ, resp. τ.

Exercice 8. — Give a description of the linear systems associated to σ, ρ and τ.

There is a "classification" of the birational maps of $\mathbb{P}^2_{\mathbb{C}}$:

Theorem 1.13 ([18, 25, 4])**.** — *Let ϕ be an element of the Cremona group. Then exactly one of the following holds*

- *ϕ is elliptic, furthermore either ϕ is of finite order, or ϕ is conjugate to an automorphism of $\mathbb{P}^2_{\mathbb{C}}$;*
- *ϕ is a Jonquières twist, ϕ preserves a unique fibration that is rational and ϕ is non conjugate to an automorphism;*
- *ϕ is a Halphen twist, ϕ preserves a unique fibration that is elliptic, and ϕ is conjugate to an automorphism;*
- *ϕ is a hyperbolic map.*

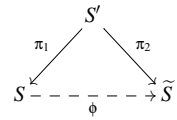
In the first three cases $\lambda(\phi) = 1$, in the last one $\lambda(\phi) > 1$.

Exercice 9. Give an example of an elliptic map, a Jonquières twist, a Halphen twist, and a hyperbolic map.

1.3 Zariski theorem

Let us recall the following statement.

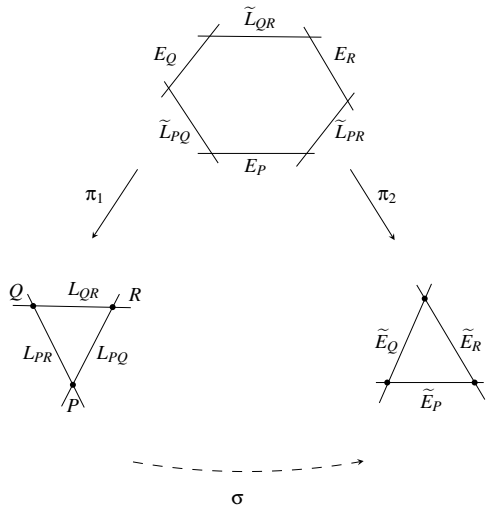
Theorem 1.14 (Zariski)**.** *Let S, $\widetilde{S}$ be two smooth projective surfaces and $\phi\colon S \dashrightarrow \widetilde{S}$ be a birational map. There exists a smooth projective surface S' and two sequences of blow-ups $\pi_1\colon S' \to S$, $\pi_2\colon S' \to \widetilde{S}$ such that $\phi = \pi_2\pi_1^{-1}$*



Example 1.15. The involution

$$\sigma\colon \mathbb{P}^2_{\mathbb{C}} \dashrightarrow \mathbb{P}^2_{\mathbb{C}}, \qquad (z_0 : z_1 : z_2) \dashrightarrow (z_1z_2 : z_0z_2 : z_0z_1)$$

is the composition of two sequences of blow-ups



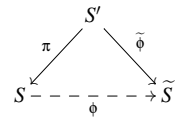
with

$$P = (1:0:0), \qquad Q = (0:1:0), \qquad R = (0:0:1),$$

L_{PQ} (resp. L_{PR}, resp. L_{QR}) the line passing through P and Q (resp. P and R, resp. Q and R) E_P (resp. E_Q, resp. E_R) the exceptional divisor obtained by blowing up P (resp. Q, resp. R) and $\widetilde{L}_{PQ}$ (resp. $\widetilde{L}_{PR}$, resp. $\widetilde{L}_{QR}$) the strict transform of L_{PQ} (resp. L_{PR}, resp. L_{QR}).

We will prove Theorem 1.14 in the following exercises. There are two steps:

- the first one is to compose ϕ with a sequence of blow-ups in order to remove all the points of indeterminacy, we thus have

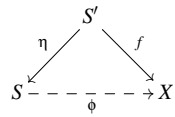


  where π_1 is a finite sequence of blow-ups and $\widetilde{\phi}$ a birational morphism;

- the second step can be stated as follows: let $\phi\colon S \to S'$ be a birational morphism between two surfaces S and S'. Assume that ϕ^{-1} is not defined at a point p of S'; then ϕ can be written $\pi\psi$ where $\pi\colon \mathrm{Bl}_p S' \to S'$ is the blow-up of $p \in S'$ and ψ a birational morphism from S to $\mathrm{Bl}_p S'$.

Remark 1.16. The first step is also possible with a rational map, and can be adapted in higher dimension whereas the second one isn't.

Exercice 10. Let $\phi\colon S \dashrightarrow X$ be a rational map from a surface to a projective variety. Then there exists a surface S', a morphism $\eta\colon S' \to S$ which is the composition of a finite number of blow-ups, and a morphism $f\colon S' \to X$ such that

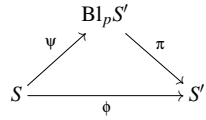


commutes.

The second step is decomposed in the two following exercises.

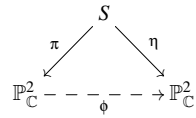
Exercice 11. Let $\phi\colon S \dashrightarrow S'$ be a birational map between two surfaces S and S'. If there exists a point $p \in S$ such that ϕ is not defined at p there exists a curve $\mathcal{C}$ on S' such that $\phi^{-1}(\mathcal{C}) = p$.

Exercice 12. Let $\phi\colon S \to S'$ be a birational morphism between two surfaces S and S'. Assume that ϕ^{-1} is not defined at a point p of S'; then ϕ can be written $\pi\psi$ where $\pi\colon \mathrm{Bl}_p S' \to S'$ is the blow-up of $p \in S'$ and ψ a birational morphism from S to $\mathrm{Bl}_p S'$



1.4 Exceptional configurations and characteristic matrices

Let $\phi \in \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ be a birational map of degree ν. By Theorem 1.14 there exist a smooth projective surface S' and π, η two sequences of blow-ups such that



We can rewrite π as follows

$$\pi\colon S = S_k \overset{\pi_k}{\to} S_{k-1} \overset{\pi_{k-1}}{\to} \ldots \overset{\pi_2}{\to} S_1 \overset{\pi_1}{\to} S_0 = \mathbb{P}^2_{\mathbb{C}}$$

where π_i is the blow-up of the point p_{i-1} in S_{i-1}. Let us set

$$\mathrm{E}_i = \pi_i^{-1}(p_i), \qquad\qquad \mathcal{E}_i = (\pi_{i+1} \circ \ldots \circ \pi_k)^* \mathrm{E}_i.$$

The divisors $\mathcal{E}_i$ are called the **exceptional configurations** of π and the p_i base-points of ϕ.

An **ordered resolution** of ϕ is a decomposition $\phi = \eta\pi^{-1}$ where η and π are ordered sequences of blow-ups. An ordered resolution of ϕ induces two basis of $\mathrm{Pic}(S)$

- $\mathcal{B} = \big\{e_0 = \pi^*\mathrm{H}, e_1 = [\mathcal{E}_1], \ldots, e_k = [\mathcal{E}_k]\big\}$,
- $\mathcal{B}' = \big\{e'_0 = \eta^*\mathrm{H}, e'_1 = [\mathcal{E}'_1], \ldots, e'_k = [\mathcal{E}'_k]\big\}$,

where H is a generic line. We can write e'_i as follows

$$e'_0 = \nu e_0 - \sum_{i=1}^{k} m_i e_i, \qquad\qquad e'_j = \nu_j e_0 - \sum_{i=1}^{k} m_{ij} e_i,\ j \geq 1.$$

The matrix of change of basis

$$M = \begin{bmatrix} \nu & \nu_1 & \dots & \nu_k \\ -m_1 & -m_{11} & \dots & -m_{1k} \\ \vdots & \vdots & & \vdots \\ -m_k & -m_{k1} & \dots & -m_{kk} \end{bmatrix}$$

is called **characteristic matrix** of ϕ. The first column of M, which is the **characteristic vector** of ϕ, is the vector $(\nu, -m_1, \dots, -m_k)$. The other columns

$$(\nu_i, -m_{1i}, \dots, -m_{ki})$$

describe the "behavior of $\mathcal{E}_i'$": if $\nu_j > 0$, then $\pi(\mathcal{E}_j')$ is a curve of degree ν_j in $\mathbb{P}^2_{\mathbb{C}}$ through the points p_ℓ of ϕ with multiplicity $m_{\ell j}$.

Example 1.17. Consider the birational map

$$\sigma\colon \mathbb{P}^2_{\mathbb{C}} \dashrightarrow \mathbb{P}^2_{\mathbb{C}}, \qquad (z_0 : z_1 : z_2) \dashrightarrow (z_1z_2 : z_0z_2 : z_0z_1).$$

The points of indeterminacy of σ are

$$P = (1:0:0), \quad Q = (0:1:0), \quad R = (0:0:1)$$

and the exceptional set is the union of the three following lines

$$\Delta = \{z_0 = 0\}, \quad \Delta' = \{z_1 = 0\}, \quad \Delta'' = \{z_2 = 0\}.$$

First we blow up P; let us denote E the exceptional divisor and $\mathcal{D}_1$ the strict transform of $\mathcal{D}$. Set

$$\begin{cases} z_1 = u_1 \\ z_2 = u_1v_1 \end{cases} \qquad \begin{cases} z_1 = r_1s_1 \\ z_2 = s_1 \end{cases}$$

In the coordinates (u_1, v_1) (resp. (r_1, s_1)) the exceptional divisor E is given by $\{u_1 = 0\}$ (resp. $\{s_1 = 0\}$) and Δ_1'' (resp. Δ_1') by $\{v_1 = 0\}$ (resp. $\{r_1 = 0\}$).

On the one hand

$$(u_1, v_1) \to (u_1, u_1v_1)_{(z_1,z_2)} \to (u_1v_1 : v_1 : 1) = \left(\frac{1}{u_1}, \frac{1}{u_1v_1}\right)_{(z_1,z_2)} \to \left(\frac{1}{u_1}, \frac{1}{v_1}\right)_{(u_1,v_1)}$$

and on the other hand

$$(r_1,s_1)\to(r_1s_1,s_1)_{(z_1,z_2)}\to(r_1s_1:1:r_1)=\left(\frac{1}{r_1s_1},\frac{1}{s_1}\right)_{(z_1,z_2)}\to\left(\frac{1}{r_1},\frac{1}{s_1}\right)_{(r_1,s_1)}.$$

Hence E is sent on Δ_1; as σ is an involution Δ_1 is sent on E.

Now blow up Q_1; this time let us denote F the exceptional divisor and $\mathcal{D}_2$ the strict transform of $\mathcal{D}_1$:

$$\begin{cases} z_0=u_2\\ z_2=u_2v_2\end{cases}\qquad\qquad\begin{cases} z_0=r_2s_2\\ z_2=s_2\end{cases}$$

In the coordinates (u_2,v_2) (resp. (r_2,s_2)) one has $\mathrm{F}=\{u_2=0\}$ and $\Delta_2''=\{v_2=0\}$ (resp. $\mathrm{F}=\{s_2=0\}$ and $\Delta_2=\{r_2=0\}$).

We have

$$(u_2,v_2)\to(u_2,u_2v_2)_{(z_0,z_2)}\to(v_2:u_2v_2:1)=\left(\frac{1}{u_2},\frac{1}{u_2v_2}\right)_{(z_0,z_2)}\to\left(\frac{1}{u_2},\frac{1}{v_2}\right)_{(u_2,v_2)}$$

and

$$(r_2,s_2)\to(r_2s_2,s_2)_{(z_0,z_2)}\to(1:r_2s_2:r_2)=\left(\frac{1}{r_2s_2},\frac{1}{s_2}\right)_{(z_0,z_2)}\to\left(\frac{1}{r_2},\frac{1}{s_2}\right)_{(r_2,s_2)}.$$

Therefore F is sent on Δ_2' and Δ_2' on F.

Finally we blow up R_2; let us denote G the exceptional divisor and set

$$\begin{cases} z_0=u_3\\ z_1=u_3v_3\end{cases}\qquad\qquad\begin{cases} z_0=r_3s_3\\ z_2=s_3\end{cases}$$

Note that

$$(u_3,v_3)\to(u_3,u_3v_3)_{(z_0,z_1)}\to(v_3:1:u_3v_3)=\left(\frac{1}{u_3},\frac{1}{u_3v_3}\right)_{(z_0,z_1)}\to\left(\frac{1}{u_3},\frac{1}{v_3}\right)_{(u_3,v_3)}$$

and

$$(r_3,s_3)\to(r_3s_3,s_3)_{(z_0,z_1)}\to(1:r_3:r_3s_3)=\left(\frac{1}{r_3s_3},\frac{1}{s_3}\right)_{(z_0,z_1)}\to\left(\frac{1}{r_3},\frac{1}{s_3}\right)_{(r_3,s_3)}.$$

One has $\mathrm{G}=\{u_3=0\}$ and $\Delta_3'=\{v_3=0\}$ (resp. $\mathrm{G}=\{s_3=0\}$ and $\Delta_3=\{r_3=0\}$).

Thus $\mathrm{G}\to\Delta_3'$ and $\Delta_3'\to\mathrm{G}$. There are no more point of indeterminacy, no more exceptional curve; in other words σ is conjugate to an automorphism of $\mathrm{Bl}_{P,Q_1,R_2}\mathbb{P}^2_{\mathbb{C}}$.

Let H be a generic line. Note that $\mathcal{E}_1 = \mathrm{E}$, $\mathcal{E}_2 = \mathrm{F}$, $\mathcal{E}_3 = \mathrm{H}$. Consider the basis $\{\mathrm{H}, \mathrm{E}, \mathrm{F}, \mathrm{G}\}$. After the first blow-up Δ and E are swapped; the point blown up is the intersection of Δ' and Δ'' so $\Delta \to \Delta + \mathrm{F} + \mathrm{G}$. Then $\sigma^*\mathrm{E} = \mathrm{H} - \mathrm{F} - \mathrm{G}$. Similarly we have

$$\begin{cases} \sigma^*\mathrm{F} = \mathrm{H} - \mathrm{E} - \mathrm{G} \\ \sigma^*\mathrm{G} = \mathrm{H} - \mathrm{E} - \mathrm{F} \end{cases}$$

It remains to determine $\sigma^*\mathrm{H}$. The image of a generic line by σ is a conic hence $\sigma^*\mathrm{H} = 2\mathrm{H} - m_1\mathrm{E} - m_2\mathrm{F} - m_3\mathrm{G}$. Let L be a generic line given by $a_0z_0 + a_1z_1 + a_2z_2$. A computation shows that

$$(u_1, v_1) \to (u_1, u_1v_1)_{(z_1,z_2)} \to (u_1^2v_1 : u_1v_1 : u_1) \to u_1(a_0v_2 + a_1u_2v_2 + a_2)$$

vanishes to order 1 on $\mathrm{E} = \{u_1 = 0\}$ thus $m_1 = 1$. Note also that

$$(u_2, v_2) \to (u_2, u_2v_2)_{(z_0,z_2)} \to (u_2v_2 : u_2^2v_2 : u_2) \to u_2(a_0v_2 + a_1u_2v_2 + a_2),$$

respectively

$$(u_3, v_3) \to (u_3, u_3v_3)_{(z_0,z_1)} \to (u_3v_3 : u_3 : u_3^2v_3) \to u_3(a_0v_3 + a_1 + a_2u_3v_3)$$

vanishes to order 1 on $\mathrm{F} = \{u_2 = 0\}$, resp. $\mathrm{G} = \{u_3 = 0\}$ so $m_2 = 1$, resp. $m_3 = 1$. Therefore $\sigma^*\mathrm{H} = 2\mathrm{H} - \mathrm{E} - \mathrm{F} - \mathrm{G}$ and the characteristic matrix of σ in the basis $\{\mathrm{H}, \mathrm{E}, \mathrm{F}, \mathrm{G}\}$ is

$$M_\sigma = \begin{bmatrix} 2 & 1 & 1 & 1 \\ -1 & 0 & -1 & -1 \\ -1 & -1 & 0 & -1 \\ -1 & -1 & -1 & 0 \end{bmatrix}.$$

Exercice 13. Let us consider the involution given by

$$\rho\colon \mathbb{P}^2_{\mathbb{C}} \dashrightarrow \mathbb{P}^2_{\mathbb{C}}, \qquad (z_0 : z_1 : z_2) \dashrightarrow (z_0z_1 : z_2^2 : z_1z_2).$$

We can show that $M_\rho = M_\sigma$.

Exercice 14. Consider the birational map

$$\tau\colon \mathbb{P}^2_{\mathbb{C}} \dashrightarrow \mathbb{P}^2_{\mathbb{C}}, \qquad (z_0 : z_1 : z_2) \dashrightarrow (z_0^2 : z_0z_1 : z_1^2 - z_0z_2).$$

We can verify that $M_\tau = M_\sigma$.

Solution 1. — Let us determine $\mathrm{Pic}(\mathbb{P}^n_{\mathbb{C}})$. Consider the homomorphism of groups given by

$$\theta\colon \mathrm{Div}(\mathbb{P}^n_{\mathbb{C}}) \to \mathbb{Z}, \qquad D \mapsto \deg D.$$

Let D be in $\ker\theta$; write D as $\sum_i a_i D_i$ where D_i denotes a prime divisor given by a homogeneous polynomial $f_i \in \mathbb{C}[z_0, z_1, \ldots, z_n]$ of some degree d_i. Since $\sum_i a_i d_i = 0$ one has: $f = \prod_i f_i^{a_i}$ belongs to $\mathbb{C}(\mathbb{P}^n_{\mathbb{C}})^*$, and by construction $D = \mathrm{div}\, f$ so D is a prime divisor.

Conversely any prime divisor is equal to $\mathrm{div}\,\frac{g}{h}$ where g, h are polynomials of the same degree; any principal divisor thus belongs to $\ker\theta$.

In other words $\ker\theta$ is the subgroup of principal divisors. So $\mathrm{Div}(\mathbb{P}^n_{\mathbb{C}})\big/_{\ker\theta} \simeq \mathbb{Z}$.

Solution 2. — Let us determine $\mathrm{Pic}(\mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}})$? Set

$$h_1 = \{0\} \times \mathbb{P}^1_{\mathbb{C}} \qquad h_2 = \mathbb{P}^1_{\mathbb{C}} \times \{0\} \qquad \mathcal{U} = \mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}} \smallsetminus (h_1 \cup h_2).$$

Since $\mathcal{U}$ is isomorphic to the affine space $\mathbb{A}^2$, every divisor on $\mathcal{U}$ is the divisor of a rational function. Let us consider a divisor on $\mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$, then $D_{|\mathcal{U}} = \mathrm{div}\,\phi$ so

$$D = \mathrm{div}\,\phi + nh_1 + mh_2$$

for some integers n and m. Furthermore $D \sim nh_1 + mh_2$. Hence $\mathrm{Pic}(\mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}})$ is generated by the classes of h_1 and h_2. Obviously $h_1 \cdot h_2 = 1$. Moreover

$$h_1 \cdot h_1 \sim h_1 \cdot (\{\infty\} \times \mathbb{P}^1_{\mathbb{C}})$$

as $h_1 \sim \{\infty\} \times \mathbb{P}^1_{\mathbb{C}}$. Since $h_1 \cap (\{\infty\} \times \mathbb{P}^1_{\mathbb{C}}) = \emptyset$ one gets $h_1^2 = 0$. Similarly $h_2^2 = 0$.

Solution 3. We can replace C and C' by linearly equivalent divisors and so assume that p lies on no component of C nor C'. Therefore obviously $\pi^*C \cdot \pi^*C' = C \cdot C'$, and $\pi^*C \cdot E = 0$.

Take C a curve passing through p with multiplicity 1. Its strict transform $\widetilde{C}$ meets E transversely at one point which corresponds in E to the tangent direction defined at p by C. Thus $C \cdot E = 1$. From $\widetilde{C} = \pi^*C - E$ (Lemma 1.7) and $\pi^*C \cdot E = 0$ we get $E^2 = -1$.

Solution 4. Let us prove that

$$\phi\colon \mathrm{Pic}(S) \oplus \mathbb{Z} \to \mathrm{Pic}(\mathrm{Bl}_p S) \qquad (D, n) \mapsto \pi^*D + nE$$

is an isomorphism. Every irreducible curve on $\mathrm{Bl}_p S$ except E is a strict transform of its image in S, hence ϕ is surjective. Assume that there is a divisor D on S such that $\pi^*D + nE = 0$. Taking the intersection with E we get that $n = 0$ and upon applying π_* we see that $D = 0$.

Solution 5. Recall that if $D = \sum_i a_i D_i$ is a divisor, and if all the a_i are non zero, the **support** $\mathrm{Supp}\, D$ of D is $\cup_i D_i$.

Consider a differential form $\omega \in \Omega^2(S)$ such that p does not belong to $\mathrm{Supp}(\mathrm{div}\,\omega)$. Since $\pi\colon \mathrm{Bl}_p S \smallsetminus E \to S \smallsetminus \{p\}$ is an isomorphism, obviously $\mathrm{div}(\pi^*\omega) = \pi^*(\mathrm{div}\omega)$ over $\mathrm{Bl}_p S \smallsetminus E$. If x and y are local parameters at p then $\omega = f\,dx \wedge dy$ where f denotes an element of $\mathcal{O}_p$ such that $f(p) \neq 0$. Let us blow up p: set

$$\begin{cases} x = u \\ y = uv \end{cases}$$

Then $\pi^*\omega = \pi^*(f)u\,du \wedge dv$ on S, and since $\pi^*(f) \neq 0$ on E we get

$$\mathrm{div}(\pi^*\omega) = \pi^*(\mathrm{div}\omega) + E$$

that is $K_{\mathrm{Bl}_p S} = \pi^* K_S + E$.

Solution 6. — Any element ϕ of $\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}})$ satisfies $\mathrm{Ind}\,\phi = \mathrm{Exc}\,\phi = \emptyset$.

Solution 7. — One has

$$\begin{cases} \mathrm{Ind}\,\sigma = \{(1:0:0),(0:1:0),(0:0:1)\},\ \mathrm{Exc}\,\sigma = \{z_0 = 0\} \cup \{z_1 = 0\} \cup \{z_2 = 0\} \\ \mathrm{Ind}\,\rho = \{(1:0:0),(0:1:0)\},\ \mathrm{Exc}\,\rho = \{z_0 = 0\} \cup \{z_2 = 0\} \\ \mathrm{Ind}\,\tau = \{(1:0:0)\},\ \mathrm{Exc}\,\tau = \{z_2 = 0\} \end{cases}$$

Solution 8. — The linear system defined by σ is the set of conics in $\mathbb{P}^2_{\mathbb{C}}$ passing through $(1:0:0)$, $(0:1:0)$ and $(0:0:1)$.

The linear system defined by ρ is the set of conics in $\mathbb{P}^2_{\mathbb{C}}$ passing through $(1:0:0)$, $(0:1:0)$ and tangent to $z_2 = 0$.

The linear system defined by τ is the set of conics in $\mathbb{P}^2_{\mathbb{C}}$ passing through $(1:0:0)$ that are tangent to $z_2 = 0$, and osculate it.

Solution 9. —

- Any birational map of finite order is elliptic; any element of the following groups

$$\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}), \quad \{(\alpha z_0 + P(z_1), \beta z_1 + \gamma) \,|\, \alpha, \beta \in \mathbb{C}^*, \gamma \in \mathbb{C}, P \in \mathbb{C}[z_1]\}$$

  is elliptic.

- Any element of $\mathcal{J}$ of the form

$$\left(\frac{a(z_1)z_0+b(z_1)}{c(z_1)z_0+d(z_1)}, z_1\right)$$

with $\frac{(\mathrm{tr}M)^2}{\det M} \in \mathbb{C}(z_1) \smallsetminus \mathbb{C}$ where M denotes the matrix defined by

$$\begin{bmatrix} a(z_1) & b(z_1) \\ c(z_1) & d(z_1) \end{bmatrix}$$

is a Jonquières twist ([10]).

- Let ϕ be the birational self-map of $\mathbb{P}^2_{\mathbb{C}}$ given by

$$\phi = (z_0z_2^2+z_1^3-2z_1z_2^2 : z_1z_2^2 : z_0z_2^2+z_1^3+z_1z_2^2-z_2^3).$$

One has $\deg \phi^n \sim n^2$.

- Consider the family of birational maps (f_ε) given by ([18])

$$f_\varepsilon = \left(z_1+1-\varepsilon, z_0\frac{z_1-\varepsilon}{z_1+1}\right).$$

If

  - $\varepsilon = -1$, then f_ε is elliptic,
  - $\varepsilon \in \{0,1\}$, then f_ε is a Jonquières twist,
  - $\varepsilon \in \{1/2, 1/3\}$, then f_ε is a Halphen twist,
  - $\varepsilon \in \{\cup_{k\geq 4} 1/k\}$, then f_ε is hyperbolic.

Solution 10 ([2], Theorem 2.7)**.** As X lies in some projective space, one can assume that $X = \mathbb{P}^m_{\mathbb{C}}$. Of course one can suppose that $\phi(S)$ lies in no hyperplane of $\mathbb{P}^m_{\mathbb{C}}$. Hence ϕ corresponds to a linear system $\mathscr{S} \subset |D|$ of dimension m on S.

If $\mathscr{S}$ has no base point, then ϕ is a morphism, and we are done.

Consider now the case where ϕ has a base point p_1. Let $\pi_1 \colon \mathrm{Bl}_{p_1} S \to S$ be the blow-up of p_1. Then the exceptional curve E_1 occurs in the fixed part of the linear system $\pi_1^*\mathscr{S} \subset |\pi_1^*D|$ with some multiplicity $k_1 \geq 1$. That is the system $\mathscr{S}_1 \subset |\pi_1^*D - k_1E_1|$ obtained by subtracting k_1E_1 from each element of $\pi_1^*\mathscr{S}$ has no fixed component. It thus defines a rational map $\phi_1 = \phi\pi_1 \colon S_1 \dashrightarrow \mathbb{P}^m_{\mathbb{C}}$. If ϕ_1 is a morphism, then we are done. Otherwise we repeat the process. Hence by induction we

get a sequence $\pi_n \circ \pi_{n-1} \circ \ldots \circ \pi_1$ of blow-ups and a linear system $\mathscr{S}_n \subset |D_n = \pi_n^* D_{n-1} - k_n E_n|$ on S_n with no fixed part. Note that

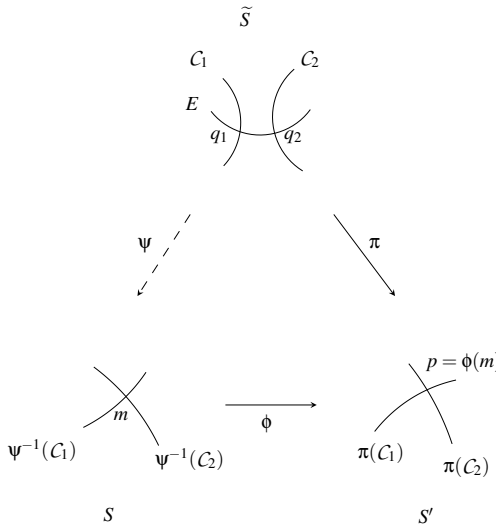
$$D_n^2 = D_{n-1}^2 - k_n^2 < D_{n-1}^2.$$

Since $\mathscr{S}_k$ has no fixed part $D_k^2 \geq 0$ for all k and so a finite number of blow-ups is needed. In other words after a finite number of blow-ups one gets a linear system with no base points which defines a morphism $S_N \to \mathbb{P}^m_{\mathbb{C}}$.

Solution 11 ([2], Lemma 2.9)**.** Suppose S affine, with $\pi^{-1}(p) \neq \emptyset$, so that there is an embedding $\iota\colon S \hookrightarrow \mathbb{A}^n$. The rational map $\iota \circ \phi^{-1}\colon S' \dashrightarrow \mathbb{A}^n$ is defined by rational functions ψ_1, …, ψ_n; furthermore one of them, for instance ψ_1, is not defined at p, that is $\psi_1 \notin \mathcal{O}_{S',p}$. One can write ψ_1 as $\frac{u}{v}$ with u, v in $\mathcal{O}_{S',p}$, u and v coprime, and $v(p) = 0$. Let us consider the curve $\mathcal{C}$ on S defined by $\phi^* v = 0$. Denote by x_1 the first coordinate function on $S \subset \mathbb{A}^n$; on S one has $\phi^* u = x_1 \phi^* v$. It follows that $\phi^* u = \phi^* v = 0$ on $\mathcal{C}$ so that $\mathcal{C} = \phi^{-1}(\{u = v = 0\})$. Since u and v are coprime the set $\{u = v = 0\}$ is finite. Shrinking S' if needed one can assume that $\{u = v = 0\} = \{p\}$, and thus $\mathcal{C} = \phi^{-1}(p)$.

Solution 12 ([30])**.** Assume that $\psi = \pi^{-1}\phi$ is not a morphism. Let m be a point of S such that ψ is not defined at m. On the one hand $\phi(m) = p$ and ϕ is not locally invertible at m, on the other hand there exists a curve in $\mathrm{Bl}_p S'$ contracted on m by ψ^{-1} (Exercise 11). This curve is necessarily the exceptional divisor E obtained by blowing up.

Let q_1, q_2 be two different points of E at which ψ^{-1} is well defined and let $\mathcal{C}_1$, $\mathcal{C}_2$ be two germs of smooth curves transverse to E. Then $\pi(\mathcal{C}_1)$ and $\pi(\mathcal{C}_2)$ are two germs of smooth curve transverse at p which are the image by ϕ of two germs of curves at m. The differential of ϕ at m is thus of rank 2: contradiction with the fact that ϕ is not locally invertible at m.



Solution 13. — We can show that $M_\rho = M_\sigma$.

Solution 14. — We can verify that $M_\tau = M_\sigma$.

2 Generation of the Cremona group in any dimension

2.1 In dimension 2

Recall that σ and ρ are the elements of $\mathrm{Bir}(\mathbf{P}^2_{\mathbb{C}})$ given by

$$\sigma = (z_1 z_2 : z_0 z_2 : z_0 z_1), \qquad \rho = (z_0 z_2 : z_0 z_1 : z_2^2).$$

Theorem 2.1 ([31, 9]). — *The group* $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ *is generated by* $\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}) = \mathrm{PGL}(3,\mathbb{C})$ *and* σ*:*

$$\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}}) = \langle \mathrm{PGL}(3,\mathbb{C}), \sigma \rangle.$$

Let us remark that $\sigma = (z_1 : z_2 : z_0)\rho(z_1 : z_2 : z_0)\rho$, hence

$$\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}}) = \langle \mathrm{PGL}(3,\mathbb{C}), \rho \rangle.$$

Definition 2.2. — Let $\phi_0, \phi_1, \ldots, \phi_n \in \mathbb{C}(z_0, z_1, \ldots, z_n)$ be some rational functions; we define

$$\mathrm{jac}(\phi_0, \phi_1, \ldots, \phi_n) = \det\left(\left[\frac{\partial \phi_i}{\partial z_j} \right]_{0 \leq i,\, j \leq n} \right) \in \mathbb{C}(z_0, z_1, \ldots, z_n).$$

Definition 2.3. — If $\phi = (\phi_0 : \phi_1 : \ldots : \phi_n)$ is a birational self-map of $\mathbb{P}^n_{\mathbb{C}}$, the **jacobian determinant** of ϕ is defined to be $\mathrm{jac}(\phi_0, \phi_1, \ldots, \phi_n)$. It is defined up to multiplication with the $(n+1)$-th power of an element of $\mathbb{C}^*$, and has degree $(n+1)(d-1)$.

Remark 2.4. — The jacobian determinant of $\phi \in \mathrm{Bir}(\mathbb{P}^n_{\mathbb{C}})$ is a polynomial which determines the hypersurfaces of $\mathbb{P}^n_{\mathbb{C}}$ where the map ϕ is not locally an isomorphism.

One can check that $\det \mathrm{jac}\, \tau$ is a perfect cube, and the jacobian determinant of any element ϕ in $\langle \mathrm{PGL}(3,\mathbb{C}), \tau \rangle$ is a perfect cube ([24]); therefore

$$\langle \mathrm{PGL}(3,\mathbb{C}), \tau \rangle \subsetneq \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}}).$$

Alexander showed Theorem 2.1; we will follow its proof ([1]). Let us first introduce some definitions and notations. Let us consider a birational map ϕ of $\mathbb{P}^2_{\mathbb{C}}$ of degree $d > 1$ (note that if $d = 1$, then according to Lemma 2.5 the map ϕ is an automorphism of $\mathbb{P}^2_{\mathbb{C}}$, and thus satisfies Theorem 2.1). Denote by p_0, p_1, …, p_k the base points of ϕ, and by m_i the multiplicity of p_i. Assume up to reindexation that

$$m_0 \geq m_1 \geq \ldots \geq m_k.$$

Let S be a surface, and let p be a point of S. The exceptional divisor obtained by blowing up p is called **first infinitesimal neighborhood**, and the points of E are called **infinitely near** p.

The k**-th infinitesimal neighborhood of** p is the set of points contained in the first infinitesimal neighborhood of a point of the $(k-1)$-th infinitesimal neighborhood of p. On the contrary the points of S are called **proper point**. The **general quadratic birational map** centered at p, q, and r is the application (defined up to automorphism) $\psi \in O(\sigma)$ such that $\mathrm{Ind}\,\psi = \{p, q, r\}$.

In his proof Noether showed that for any $\phi \in \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ one can find a general quadratic birational map ψ such that $\deg \phi\psi < \deg \phi$, and so by induction proved that $\phi = \psi_1\psi_2 \dots \psi_\ell$ up to automorphism of $\mathbb{P}^2_{\mathbb{C}}$ where ψ_i are general quadratic birational maps. But it is false for instance if one of the base points is proper and the others in its infinitesimal neighborhoods. To give a complete proof Alexander introduces the **complexity of the linear system** associated to ϕ defined by

$$2c = d - m_0.$$

Geometrically it is the number of points except p_0 that belong to the intersection of a generic line through p_0 and a curve of the linear system. Denote by C the set of points defined by

$$C = \{p_i \,|\, i \geq 1, m_i > c\}$$

and by n the cardinal of C. Alexander's idea is the following: apply to ϕ a sequence of general quadratic birational maps in order to decrease the complexity c until $c = 1$ and the cardinal n until $n = 0$.

Lemma 2.5. — *Let ϕ be a birational self-map of $\mathbb{P}^2_{\mathbb{C}}$ of degree d. Let p_0, p_1, …, p_k be the base points of ϕ, and m_0, m_1, …, m_k be their multiplicity. Then*

$$\sum_{j=0}^{k} m_j^2 = d^2 - 1 \tag{2.1}$$

$$\sum_{j=0}^{k} m_j(m_j - 1) = (d-1)(d-2) \tag{2.2}$$

$$\sum_{j=0}^{k} m_j = 3d - 3 \tag{2.3}$$

Proof. One gets (2.3) from (2.1) and (2.2) as follows :

$$\begin{aligned} \sum_{j=0}^{k} m_j &= -\sum_{j=0}^{k} m_j(m_j-1) + \sum_{j=0}^{k} m_j^2 \\ &= -(d-1)(d-2) + d^2 - 1 \\ &= 3d - 3 \end{aligned}$$

Exercice 15. — Prove relation (2.1).

Exercice 16. — Prove equality (2.2).

□

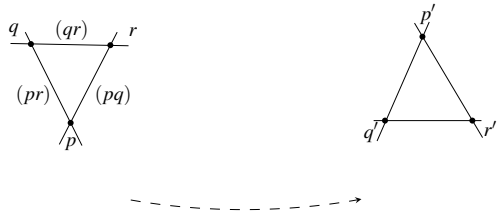
Exercice 17. Prove that $2c \geq 0$.

Exercice 18. Prove the following inequality: $2c \geq 1$.

Exercice 19. Prove that

$$2c \geq m_1 \geq m_2 \geq \ldots \geq m_n > c.$$

Take a general quadratic birational map ψ centered at p, q, and r; the lines (pq), (qr), and (pr) are blown down by ψ onto r', p', and q':



Lemma 2.6. *If $d > 1$, then $n \geq 2$. Hence $m_0 > \frac{d}{3}$.*

Furthermore if $n \geq 3$, then the points p_i with $i \in \{1, 2, \ldots, k\}$ are not all aligned.

Exercice 20. Prove Lemma 2.6

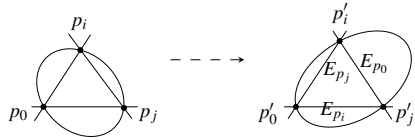
Lemma 2.7. *Compose ϕ with a general quadratic birational map centered at p_0, q, and r; the complexity of the system is constant if and only if the point p_0' is the point of maximal multiplicity. Otherwise the complexity of the system decreases.*

Exercice 21. Prove Lemma 2.7

Lemma 2.8. *Assume that there exist two points p_i and p_j in C which are not infinitely near, and not infinitely near p_0. After composition with a general quadratic map centered at p_0, p_i, and p_j then*

- *either the complexity of the system decreases,*
- *or the cardinal of C decreases by 2.*

Proof. Let us compose ϕ with a general quadratic birational map whose base points are p_0, p_i and p_j



Denote by L' the new linear system; the degree d' of L' is

$$d' = 2d - m_0 - m_i - m_j$$

furthermore

$$\begin{cases} m_j' = d - m_0 - m_i < c \\ m_0' = d - m_i - m_j \\ m_i' = d - m_0 - m_j < c \end{cases}$$

Let C' be the set of base points with multiplicity strictly larger than c'. One has

$$d' = d + (d - m_0 - m_i - m_j) = d + (2c - m_i - m_j).$$

In particular $d' < d$.

After this composition

- p_0, p_i, and p_j are not base points anymore (they have been blown up on lines);
- the other base points don't change, and their multiplicity remains constant;
- there are three new base points p_0', p_i', and p_j'.

The multiplicity of the new base points is equal to the number of intersections (counted with multiplicity) of the corresponding line (that is contracted) and the strict transform of a general curve of the linear system. According to Bezout theorem one has

$$\begin{cases} m_0' = d - m_i - m_j \\ m_i' = d - m_0 - m_j \\ m_j' = d - m_0 - m_i \end{cases}$$

Let us now distinguish two cases: the case where p_0' is not the point of highest multiplicity and the case where it is:

- if p'_0 is not the point of highest multiplicity, then the complexity of the system decreases (Lemma 2.7);
- otherwise p'_0 is the point of highest multiplicity, then the complexity of the system remains constant (Lemma 2.7). According to Lemma 2.6 the point p'_0 belongs to C'. Moreover since $m_i > c$, $m_j > c$, and $d - m_0 = 2c$ then $m'_i < c$, $m'_j < c$ that is p'_i and p'_j don't belong to C'. Hence $n' = n-2$.

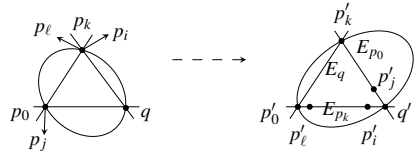
□

Lemma 2.9. *Suppose that there exists a base point p_k in C which is not infinitely near p_0. After composition with a general quadratic birational map*

- *there is no infinitely near base points above p_0 (resp. p_k),*
- *there is no infinitely near base points above p'_0,*
- *the complexity of the linear system remains constant,*
- *the cardinal of C remains constant.*

Proof. Let us compose ϕ with a general quadratic birational map centered at p_0, p_k, and q such that

- the lines (p_0q) and (p_kq) don't contain base points;
- there is no base point infinitely near p_k in the direction of the line (p_kq);
- there is no base point infinitely near p_0 in the direction of the line (p_0q).



Remark that the degree increases; indeed, the degree of the new system is

$$d' = 2d - m_0 - m_k = d + 2c - m_k \geq d$$

and

$$\begin{cases} m'_0 = d - m_k \geq d - m_0 = 2c \geq m_1 \\ m'_q = d - m_0 - m_k = 2c - m_k < c \\ m'_k = d - m_0 = 2c > c \end{cases}$$

In particular the base point p_0' is the point of highest multiplicity. The complexity remains constant (Lemma 2.7). The cardinal of C is equal to the cardinal of C': we blow up two points of C and get two new points.

We don't transform a point infinitely near p_k (resp. p_0) in a point infinitely near p_0' nor q'. Indeed assume by contradiction that we transform a point p_i infinitely near p_k in a point infinitely near q'. It means that p_k is in the direction of the line (p_0p_k). Denoting by D the divisor representing (p_0p_k) one has

$$(C\cdot D)_{p_k} = m_k + m_i$$

so

$$C\cdot D = m_0 + m_k + m_i > m_0 + 2c = d$$

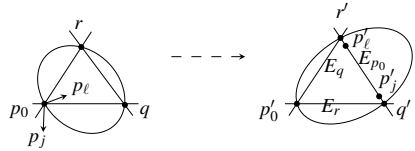
which is impossible by Bezout theorem. The same holds if we consider a point infinitely near p_0. □

Lemma 2.10. *Assume that all points of C are infinitely near p_0. After composing with a general quadratic birational map*

- *there is no infinitely near base point above the point of highest multiplicity p_0',*
- *the complexity of the linear system remains constant,*
- *the cardinal of C decreases by 2.*

Proof. Compose ϕ with a general quadratic birational map centered at p_0, r, and q such that

- the lines (p_0r), (p_0q), and (rq) don't contain base points of the new system;
- the lines (p_0r), (p_0q), and (rq) are not in the direction of the points infinitely near p_0.



The degree strictly increases; indeed $d' = 2d - m_0 > d$. Since the elements of the linear system don't pass through r and q hence according to Bezout theorem p_0' is a point of multiplicity d. It is thus the point of highest multiplicity. Moreover the complexity of the system is

$$2c' = 2d - m_0 - d = d - m_0 = 2c.$$

Any curve of the linear system intersects (p_0r) and (p_0q) at $d-m_0=2c$ points so q' and r' become base points of the system, and $m'_r=m'_q=2c>c=c'$. As a consequence $n'=n+2$.

The points infinitely near p_0 are dispersed on the line $(r'q')$; thanks to the assumption on the line (rq) there is no base point infinitely near p'_0. □

Proof of Theorem 2.1. Let us first describe the two keysteps:

Step a: if there is one base point in C that is not infinitely near the base point p_0 of highest multiplicity go to "Step b"; otherwise let us apply Lemma 2.10 to ϕ. We thus get that there is no more infinitely near base points above p'_0, and n increases by 2. Then since there is no more infinitely near base points above p'_0 one can apply Lemma 2.9 until all the points of C are distinct. The complexity and the number of base points with multiplicity $>c$ except p'_0 remain constant (still by Lemma 2.9). But now $n\geq 3$ and so the base points of C are not aligned (Lemma 2.6). Take two points p_i and p_j such that p_ℓ and p_q don't belong to (p'_0p_i), (p'_0p_j) and (p_ip_j). Let us now apply two times Lemma 2.8 to p_ℓ and p_q. If the complexity decreases come back to the beginning of "Step a"; otherwise $n+2$ decreases by 4 and p'_0 has no more infinitely near base points with multiplicity $>c$ so let us go on with "Step b".

Step b is decomposed in two cases:

- either C contains two base points that aren't infinitely near and one applies Lemma 2.8; if the complexity decreases come to "Step a", otherwise come back to the beginning of "Step b";
- or one applies Lemma 2.9 then the base points are "separated" and one comes back to "Step b".

Using this strategy one gets first that the complexity decreases until 1, and then that the cardinal of C is zero. We thus have a system with at most one base point p'_0, *i.e.* using Lemma 2.5 and the definition of c the two following equalities hold

$$\begin{cases} m_0=3d-3 \\ 1=d-m_0 \end{cases}$$

Therefore $d=1$ and $m_0=0$, that is after composing ϕ with well choosen general quadratic birational maps ϕ is an automorphism of $\mathbb{P}^2_{\mathbb{C}}$. □

2.2 In higher dimensions

Theorem 2.11 ([27, 32]). — *Let $n \geq 3$ be an integer. Any set of generators of* $\mathrm{Bir}(\mathbb{P}^n_{\mathbb{C}})$ *contains an infinite uncountable number of elements of* $\mathrm{Bir}(\mathbb{P}^n_{\mathbb{C}}) \smallsetminus \mathrm{Aut}(\mathbb{P}^n_{\mathbb{C}})$.

We follow Cantat's notes based on the proof of Pan ([32]).

2.2.1 Exceptional hypersurfaces

Definition 2.12. — Let ϕ be a birational map of $\mathbb{P}^n_{\mathbb{C}}$, and let X be an irreducible hypersurface of $\mathbb{P}^n_{\mathbb{C}}$. We say that X is **ϕ-exceptional** if there exists an open subset $\mathcal{U}$ of X which is mapped onto a subset of codimension ≥ 2 by ϕ.

Lemma 2.13. — *Let ϕ_1, ϕ_2, …, ϕ_m be some birational self-maps of $\mathbb{P}^n_{\mathbb{C}}$. Consider*

$$\phi = \phi_m \phi_{m-1} \dots \phi_1.$$

The irreducible hypersurface X of $\mathbb{P}^n_{\mathbb{C}}$ is ϕ-exceptional if there exist an integer i between 1 and m, and a ϕ_i-exceptional hypersurface X_i such that X_i is birational equivalent to X.

2.2.2 Jonquières maps with prescribed exceptional set

Consider the homogeneous coordinates $(z_0 : z_1 : \dots : z_{n-1})$ on $\mathbb{P}^{n-1}_{\mathbb{C}}$, and the homogeneous coordinates $(u : v)$ on $\mathbb{P}^1_{\mathbb{C}}$. Let Y be an irreducible hypersurface of degree d in $\mathbb{P}^{n-1}_{\mathbb{C}}$, distinct from $z_0 = 0$. Assume that $h = 0$ is a reduced homogeneous equation of Y. Consider the birational map

$$\psi_Y : \mathbb{P}^{n-1}_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}} \dashrightarrow \mathbb{P}^{n-1}_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$$

defined by

$$\big((z_0 : z_1 : \dots : z_{n-1}), (u : v)\big) \dashrightarrow \big((z_0 : z_1 : \dots : z_{n-1}), (uz_0^d : vh(z_0, z_1, \dots, z_{n-1})\big).$$

The map ψ_Y is birational, and ψ_Y contracts the generic points of $Y \times \mathbb{P}^1_{\mathbb{C}}$ onto the codimension 2 subset $Y \times \{(1:0)\}$ of $\mathbb{P}^{n-1}_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$.

The projective variety $\mathbb{P}^{n-1}_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$ is birationally equivalent to $\mathbb{P}^n_{\mathbb{C}}$; an explicit birational map from $\mathbb{P}^{n-1}_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$ to $\mathbb{P}^n_{\mathbb{C}}$ is

$$\eta : \mathbb{P}^{n-1}_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}} \dashrightarrow \mathbb{P}^n_{\mathbb{C}}, \quad \big((z_0 : z_1 : \dots : z_{n-1}), (u : v)\big) \dashrightarrow \big(uz_0 : vz_0 : vz_1 : \dots : vz_{n-1}\big).$$

Conjugate ψ_Y by η, and set $X = \eta(Y \times \mathbb{P}^1_{\mathbb{C}})$; since η blows down

$$\big(Y \times \{(1:0)\}\big) \smallsetminus \{u = 0\}$$

onto $(1 : 0 : 0 : \dots : 0) \in \mathbb{P}^n_{\mathbb{C}}$ one gets:

Lemma 2.14. — *For any irreducible hypersurface Y of $\mathbb{P}^{n-1}_{\mathbb{C}}$ of degree d there exist a birational self-map ϕ_Y of $\mathbb{P}^n_{\mathbb{C}}$ of degree $d+1$, and a hypersurface X of $\mathbb{P}^n_{\mathbb{C}}$ such that*

- *X is birationally equivalent to $Y \times \mathbb{P}^1_{\mathbb{C}}$,*
- *X is ϕ_Y-exceptional.*

In case $n = 3$ the previous statement says that: for any irreducible curve C in $\mathbb{P}^2_{\mathbb{C}}$ of degree ℓ there exists $\phi_C \in \mathrm{Bir}(\mathbb{P}^3_{\mathbb{C}})$ of degree $d+1$, and a hypersurface X in $\mathbb{P}^3_{\mathbb{C}}$ such that

- X is birationally equivalent to $C \times \mathbb{P}^1_{\mathbb{C}}$,
- and X is ϕ_C-exceptional.

Consider now the particular case of smooth plane cubics: the set of these curves is a one-parameter family so according to Lemma 2.13 one gets Theorem 2.11 for $n = 3$. More generally one concludes as follows.

2.2.3 Stable equivalence

Definition 2.15. — Let Y, and Y' be two varieties; Y is **m-stably equivalent** to Y' if there exists a birational map from $Y \times \mathbb{P}^m_{\mathbb{C}}$ to $Y' \times \mathbb{P}^m_{\mathbb{C}}$.

Remark 2.16. — Be careful there exist complex projective varieties Y of dimension $n \geq 3$ such that Y is not rational but Y is stably equivalent to $\mathbb{P}^n_{\mathbb{C}}$.

Lemma 2.17. — *Let Y and Y' be two smooth irreducible hypersurfaces of $\mathbb{P}^{n-1}_{\mathbb{C}}$ of degree $\geq n+1$. If Y and Y' are m-stably equivalent, then Y and Y' are isomorphic.*

Lemmas 2.13, 2.14, and 2.17 imply Theorem 2.11.

2.2.4 A similar argument to Gizatullin's one

Let us consider the birational involution σ_n of $\mathbb{P}^n_{\mathbb{C}}$ defined by

$$\sigma_n = \Big(\prod_{\substack{i=0 \\ i \neq 0}}^{n} z_i : \prod_{\substack{i=0 \\ i \neq 1}}^{n} z_i : \ldots : \prod_{\substack{i=0 \\ i \neq n}}^{n} z_i \Big).$$

Definition 2.18. — A **monomial map** of $\mathbb{P}^n_{\mathbb{C}}$ is a birational self-map of $\mathbb{P}^n_{\mathbb{C}}$ of the form

$$\big(\alpha_1 z_1^{a_{11}} z_2^{a_{12}} \ldots z_n^{a_{1n}}, \alpha_2 z_1^{a_{21}} z_2^{a_{22}} \ldots z_n^{a_{2n}}, \ldots, \alpha_n z_1^{a_{n1}} z_2^{a_{n2}} \ldots z_n^{a_{nn}} \big)$$

in the affine chart $z_0 = 1$ with $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in (\mathbb{C}^*)^n$ and $\big[a_{ij}\big]_{1 \leq i,j \leq n} \in \mathrm{GL}(n, \mathbb{Z})$.

Blanc and Heden prove that $\langle \sigma_n, \mathrm{Aut}(\mathbb{P}^n_{\mathbb{C}})\rangle \neq \mathrm{Bir}(\mathbb{P}^n_{\mathbb{C}})$ for n odd:

Theorem 2.19 ([5]). — *If n is odd, there are monomial maps of $\mathbb{P}^n_{\mathbb{C}}$ which do not belong to $\langle \sigma_n, \mathrm{Aut}(\mathbb{P}^n_{\mathbb{C}})\rangle$.*

The idea of the proof is the same as Gizatullin's. They prove the following statement:

Proposition 2.20 ([5]). — *Assume n odd. The jacobian determinant of any element of $\langle \sigma_n, \mathrm{Aut}(\mathbb{P}^n_{\mathbb{C}})\rangle$ is equal to αP^2 for some $\alpha \in \mathbb{C}^*$ and some homogeneous polynomial $P \in \mathbb{C}[z_0, z_1, \ldots, z_n]$.*

Corollary 2.21. — *Suppose n odd. The quadratic birational involution of $\mathbb{P}^n_{\mathbb{C}}$ given by*

$$\big(z_1 z_2 : z_0 z_1 : z_0 z_2 : \ldots : z_0 z_n\big)$$

does not belong to $\langle \sigma_n, \mathrm{Aut}(\mathbb{P}^n_{\mathbb{C}})\rangle$.

Exercice 22. Let $\psi \in \mathbb{C}[z_0, z_1, \ldots, z_n]_d$ be a homogeneous polynomial of degree $d \in \mathbb{N}$, and ϕ_0, ϕ_1, …, $\phi_n \in \mathbb{C}(z_0, z_1, \ldots, z_n)_e$ be homogeneous rational functions of degree $e \in \mathbb{Z} \smallsetminus \{0\}$. Prove that

$$\mathrm{jac}(\psi\phi_0, \psi\phi_1, \ldots, \psi\phi_n) = \left(1 + \frac{d}{e}\right) \mathrm{jac}(\phi_0, \phi_1, \ldots, \phi_n)\psi^{n+1}.$$

Exercice 23. Using Exercice 22 prove that $\mathrm{jac}\,\sigma_n = n(-1)^n \prod_{i=0}^{n} z_i^{n-1}$.

Exercice 24. Let $\phi = (\phi_0 : \phi_1 : \ldots : \phi_n)$ and $\psi = (\psi_0 : \psi_1 : \ldots : \psi_n)$ be two birational self-maps of $\mathbb{P}^n_{\mathbb{C}}$. Set $d_1 = \deg \phi$, and $d_2 = \deg \psi$.

Assume that $\deg(\phi\psi) = d_1 d_2$; then the chain rule states that

$$\mathrm{jac}(\phi\psi) = \psi^*(\mathrm{jac}\,\phi)\,\mathrm{jac}\,\psi$$

where $\psi^*(\mathrm{jac}\,\phi)$ is obtained by replacing each z_i with ψ_i in $\mathrm{jac}\,\phi$.

If $\deg(\phi\psi) = d_1 d_2 - m$ for $m > 0$ there exists a homogeneous polynomial Q of degree m that divides the formal composition of ϕ and ψ. Prove that

$$\mathrm{jac}(\phi\psi) = \left(\frac{d_1 d_2 - m}{d_1 d_2}\right) \frac{\psi^*(\mathrm{jac}\,\phi)\,\mathrm{jac}\,\psi}{Q^{n+1}}.$$

Deduce from it the Proposition 2.20.

Exercice 25. Prove Corollary 2.21 : compute the jacobian determinant of

$$\big(z_1 z_2 : z_0 z_1 : z_0 z_2 : \ldots : z_0 z_n\big)$$

and conclude with Proposition 2.20.

Solution 15. — Let $\mathscr{S}$ be the linear system defined by ϕ. Consider two curves C and D of $\mathscr{S}$. According to Bezout theorem one has $C \cdot D = d^2$. Blow up $\mathbb{P}^2_{\mathbb{C}}$ at p_0, and denote by C', resp. D' the strict transform of C, resp. D; according to Lemma 1.7

$$C' \cdot D' = (\pi^* C - m_0 E) \cdot (\pi^* D - m_0 E)$$

so

$$C' \cdot D' = \pi^* C \cdot \pi^* D - \pi^* C \cdot m_0 E - m_0 E \cdot \pi^* D + m_0 E \cdot m_0 E$$

that is

$$C' \cdot D' = \pi^* C \cdot \pi^* D - \pi^* C \cdot m_0 E - m_0 E \cdot \pi^* D - m_0^2$$

hence

$$C' \cdot D' = C \cdot D - m_0^2$$

and finally

$$d^2 = C \cdot D = C' \cdot D' + m_0^2.$$

The points p_1, p_2, …, p_k are still points of multiplicity m_1, m_2, …, m_k. By induction one has

$$d^2 = \widetilde{C} \cdot \widetilde{D} + \sum_{j=0}^{k} m_j^2$$

where $\widetilde{C}$, resp. $\widetilde{D}$ is the strict transform of C, resp. D after the blow up of p_0, p_1, …, p_k. Moreover the curves $\widetilde{C}$ and $\widetilde{D}$ intersect at only one point that does not belong to $\{p_0, p_1, \ldots, p_k\}$; hence $\widetilde{C} \cdot \widetilde{D} = 1$. Therefore

$$d^2 = 1 + \sum_{j=0}^{k} m_j^2.$$

Solution 16. — Consider a curve C in $\mathbb{P}^2_{\mathbb{C}}$ that belongs to the linear system defined by ϕ. Let $\pi\colon \mathrm{Bl}_{p_0}\mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ be the blow-up of p_0, and C' be the strict transform of C. One has (Proposition 1.9)

$$K_{\mathrm{Bl}_{p_0}\mathbb{P}^2_{\mathbb{C}}} = \pi^* K_{\mathbb{P}^2_{\mathbb{C}}} + E$$

and so

$$K_{\mathrm{Bl}_{p_0}\mathbb{P}^2_{\mathbb{C}}} \cdot C' = \pi^* K_{\mathbb{P}^2_{\mathbb{C}}} \cdot C + m_0.$$

By induction one gets

$$K_S \cdot \widetilde{C} = K_{\mathbb{P}^2_{\mathbb{C}}} \cdot C + \sum_{j=0}^{k} m_j$$

where $S = \mathrm{Bl}_{p_0,p_1,\ldots,p_k}\mathbb{P}^2_{\mathbb{C}}$, and $\widetilde{C}$ is the strict transform of C. The curve $\widetilde{C}$ is smooth so according to Riemann-Roch theorem and adjunction formula one obtains

$$K_S \cdot \widetilde{C} = 2g(\widetilde{C}) - 2 - \widetilde{C}^2$$

where $g(C)$ denotes the real genus of C, that is the topological genus of a desingularization of C. So

$$K_{\mathbb{P}^2_{\mathbb{C}}} \cdot C + \sum_{j=0}^{k} m_j = 2g(\widetilde{C}) - 2 - \widetilde{C}^2.$$

Since $g(\widetilde{C}) = 0$ one has

$$K_{\mathbb{P}^2_{\mathbb{C}}} \cdot C + \sum_{j=0}^{k} m_j = -2 - \widetilde{C}^2 \tag{2.4}$$

But $\widetilde{C}^2 = C^2 - \sum_{j=0}^{k} m_j^2$ and $K_{\mathbb{P}^2_{\mathbb{C}}} = -3H$ thus

$$\begin{aligned}
(2.4) \quad &\Leftrightarrow \quad -3d + \sum_{j=0}^{k} m_j = -2 - C^2 + \sum_{j=0}^{k} m_j^2 \\
&\Leftrightarrow \quad -3d + \sum_{j=0}^{k} m_j = -2 - d^2 + \sum_{j=0}^{k} m_j^2 \\
&\Leftrightarrow \quad d^2 - 3d + 2 = \sum_{j=0}^{k} m_j(m_j - 1) \\
&\Leftrightarrow \quad (d-1)(d-2) = \sum_{j=0}^{k} m_j(m_j - 1)
\end{aligned}$$

Solution 17. The degree of elements of the linear system defined by ϕ is d, hence the multiplicity of a point is bounded by d.

Solution 18. If an homogeneous polynomial P of degree d has a point of multiplicity d then $(P = 0)$ is not irreducible, it is the union of d lines.

Solution 19. According to Bezout's theorem the line through p_0 and p_1 intersects any curve of the linear system at d points counted with multiplicity. But the line through p_0 and p_1 intersects any curve of the system at p_0 with multiplicity m_0 so $m_1 \leq d - m_0 = 2c$. We thus have the inequalities

$$2c \geq m_1 \geq m_2 \geq \ldots \geq m_n > c.$$

Solution 20. One has: $c\,(2.2)-(c-1)\,(2.1)$ gives on the one hand

$$c\sum_{i=0}^{k} m_i(m_i-1)-(c-1)\sum_{i=0}^{k} m_i^2=\sum_{i=0}^{k} m_i(m_i-c)$$

and on the other hand

$$c(d-1)(d-2)-(c-1)(d^2-1)=(d-1)(d-3c+1).$$

Hence

$$\sum_{i=0}^{k} m_i(m_i-c)=(d-1)(d-3c+1) \tag{2.5}$$

Since $3c-1\geq\frac{1}{2}>0$ and $m_{n+i}-c<0$ for all $i>0$ then

$$\sum_{i=0}^{n} m_i(m_i-c)\geq\sum_{i=0}^{k} m_i(m_i-c)$$

and according to 2.5

$$\sum_{i=0}^{n} m_i(m_i-c)\geq(d-1)(d-3c+1)$$

so $\sum_{i=0}^{n} m_i(m_i-c)>d(d-2c)=d(m_0-c)$. But

$$\sum_{i=0}^{n} m_i(m_i-c)=m_0(m_0-c)+\sum_{i=1}^{n} m_i(m_i-c)$$

therefore

$$\sum_{i=1}^{n} m_i(m_i-c)>d(m_0-c)-m_0(m_0-c)=(d-m_0)(m_0-c)=2c(m_0-c).$$

Since $2c\geq m_1\geq m_2\geq\ldots\geq m_n\geq c$ one has

$$2c\sum_{i=1}^{n}(m_i-c)>2c(m_0-c)$$

and as $c>0$

$$\sum_{i=1}^{n}(m_i-c)>m_0-c.$$

But $m_1\leq m_0$ thus $n\geq 2$.

From $m_0\geq m_i$ for all i one has

$$0\geq\sum_{i=0}^{n} m_i(m_i-m_0)=\sum_{i=0}^{n} m_i^2-m_0\sum_{i=0}^{n} m_i=(d-1)(d+1-3m_0).$$

So $d+1-3m_0\leq 0$, and $m_0>\frac{d}{3}$.

Solution 21. The complexity of the system after composing with a general quadratic birational map centered at p_0, q, and r is

$$\begin{aligned} 2c' = d' - m'_{\max} &= 2d - m_0 - m_q - m_r - m'_{\max} \\ &= d - m_0 + m'_0 - m'_{\max} \\ &= 2c + m'_0 - m'_{\max} \end{aligned}$$

where $m'_{\max}$ denotes the highest multiplicity of the base points of the new system. Therefore $c' \leq c$ and $c = c'$ if and only if $m'_0 = m'_{\max}$.

Solution 22. *See* [5, Lemma 2.3]

Solution 23. [5, Corollary 2.4] Since $\sigma_n = \left(\frac{\psi}{z_0} : \frac{\psi}{z_1} : \ldots : \frac{\psi}{z_n}\right)$ with $\psi = \prod_{i=0}^{n-1}(z_i)^{n-1}$. It follows by Exercice 22 that

$$\operatorname{jac}(\sigma_n) = \left(1 + \frac{n+1}{-1}\right) \operatorname{jac}\left(z_0^{-1}, z_1^{-1}, \ldots, z_n^{-1}\right) \psi^{n+1} = n(-1)^n \prod_{i=0}^{n} (z_i)^{n-1}.$$

Solution 24. [5, Proposition 2.6] The formula

$$\operatorname{jac}(\phi\psi) = \left(\frac{d_1 d_2 - m}{d_1 d_2}\right) \frac{\psi^*(\operatorname{jac}\phi)\operatorname{jac}\psi}{Q^{n+1}}$$

directly follows from Exercice 22.

Since n is odd, we see that if the result is true for ϕ and ψ, then it is true for the composition $\phi\psi$. It remains to note that

- as we have seen $\operatorname{jac}(\sigma_n) = n(-1)^n \prod_{i=0}^{n}(z_i)^{n-1}$, that is $\operatorname{jac}(\sigma_n)$ is a square multiplied by a constant when n is odd,
- if ϕ is an automorphism of $\mathbb{P}^n_{\mathbb{C}}$, then$\operatorname{jac}(\phi)$ belongs to $\mathbb{C}$.

Solution 25. [5, Corollary 2.7] Since

$$\operatorname{jac}\left(z_1 z_2 : z_0 z_1 : z_0 z_2 : \ldots : z_0 z_n\right) = -2 z_0^{n-1} z_1 z_2$$

the result follows then from Proposition 2.20.

3 Action of the Cremona group on the Picard-Manin space and applications

3.1 Picard-Manin space and Bubble space

Let S, S_i be some complex projective surfaces. Any $\pi_i\colon S_i \to S$ birational morphism induces an embedding

$$\pi^*\colon \mathrm{NS}(S) \to \mathrm{NS}(S_i)$$

of Néron-Severi groups. We say that π_2 is **above** π_1 if $\pi_1^{-1}\pi_2$ is regular. Starting with two birational morphisms one can always find a third one that covers the two first. Therefore the inductive limit of all groups $\mathrm{NS}(S_i)$ for all surfaces S_i above S is well-defined. It is the **Picard-Manin space** $\mathcal{Z}_S$ of S. Structures invariant by the morphisms π_i^* go through the limit and so $\mathcal{Z}_S$ is provided with

- an intersection form,
- a nef cone $\mathcal{Z}_S^+ = \varinjlim \mathrm{NS}^+(S_i)$,
- a canonical class which can be seen as a linear form $\mathcal{Z}_S \to \mathbb{Z}$.

Consider all surfaces S_i above S that is all birational morphisms $\pi_i\colon S_i \to S$. Take $\pi_1\colon S_1 \to S$, $\pi_2\colon S_2 \to S$, and $p_1 \in S_1$, $p_2 \in S_2$. The point p_1 is **identified with** p_2 if $\pi_1^{-1}\pi_2$ is a local isomorphism that sends p_2 onto p_1. The **Bubble space** $\mathcal{B}(S)$ of S is the union of all points of all surfaces above S modulo the equivalence relation induced by this identification.

If $p \in \mathcal{B}(S)$ is represented by a point p on a surface $S_i \to S$ we denote by e_p the divisor class of the exceptional divisor of the blow-up of p. Then

$$\begin{cases} e_p \cdot e_p = -1 \\ e_p \cdot e_q = 0 \text{ if } p \neq q \end{cases}$$

Exercice 26. — Prove the previous formulas in case where p is a point of $\mathbb{P}^2_{\mathbb{C}}$, $S_1 = \mathrm{Bl}_p\mathbb{P}^2_{\mathbb{C}}$, q is a point on E_p, and $S_2 = \mathrm{Bl}_q S_1$.

Embed $\mathrm{NS}(S)$ as a subgroup of $\mathcal{Z}_S$. This finite dimensional lattice is orthogonal to e_p for any $p \in \mathcal{B}(S)$. Furthermore

$$\mathcal{Z}_S = \Big\{ D + \sum_{p \in \mathcal{B}(S)} a_p e_p \,|\, D \in \mathrm{NS}(S),\, a_p \in \mathbb{R} \Big\}$$

note that $a_p = 0$ except finitely many. The **completed Picard-Manin space** $\overline{\mathcal{Z}_S}$ of S is the L^2-completion of $\mathcal{Z}_S$, that is

$$\overline{\mathcal{Z}}_S = \Big\{ D + \sum_{p\in\mathcal{B}(S)} a_p e_p \,|\, D \in \mathrm{NS}(S), a_p \in \mathbb{R}, \sum a_p^2 < \infty \Big\}.$$

Furthermore the intersection form on $\mathrm{NS}(S_i)$ induces an intersection form with signature $(1,\infty)$ on $\overline{\mathcal{Z}}_S$. Let $\overline{\mathcal{Z}}_S^+$ be the **nef cone** of $\overline{\mathcal{Z}}_S$, and $\mathcal{L}\overline{\mathcal{Z}}_S = \big\{ d \in \overline{\mathcal{Z}}_S \,|\, d\cdot d = 0 \big\}$ be the **light cone** of $\mathcal{Z}_S$.

3.2 Hyperbolic space and isometries

The **hyperbolic space** $\mathbb{H}_S$ of S is then defined by

$$\mathbb{H}_S = \big\{ d \in \overline{\mathcal{Z}}_S^+ \,|\, d\cdot d = 1 \big\}.$$

Note that $\mathbb{H}_S$ is an infinite dimensional analogue of the classical hyperbolic space $\mathbb{H}^n$. The distance on $\mathbb{H}_S$ is defined by: for $d, d' \in \mathbb{H}_S$

$$\cosh(\mathrm{dist}(d,d')) = d\cdot d'.$$

The **geodesics** are intersections of $\mathbb{H}_S$ with planes. The projection $\mathbb{H}_S \to \mathbb{P}(\overline{\mathcal{Z}}_S)$ is one-to-one, the boundary of its image is the projection of the cone of isotropic vectors of $\overline{\mathcal{Z}}_S$. Hence

$$\partial\mathbb{H}_S = \big\{ \mathbb{R}^+ d \,|\, d \in \overline{\mathcal{Z}}_S^+, d\cdot d = 0 \big\}.$$

If $\pi\colon S' \to S$ is a birational morphism, we get an isometry π^* (and not simply an embedding) between $\mathbb{H}_S$ and $\mathbb{H}_{S'}$. This allows to define an action of $\mathrm{Bir}(S)$ on $\mathbb{H}_S$. Let $\phi\colon S \to S$ be a birational map; there exists S' a surface and $\pi_1\colon S' \to S$, $\pi_2\colon S' \to S$ two birational morphisms such that $\phi = \pi_2\pi_1^{-1}$ (*see for example* [2]). One can define the isometry $\phi_\bullet$ of $\mathbb{H}_S$ by

$$\phi_\bullet = (\pi_2^*)^{-1}\pi_1^*.$$

The isometries of $\mathbb{H}_S$ are classified in three types ([6, 23]). The **translation length** of an isometry $\phi_\bullet$ of $\mathbb{H}_S$ is defined by

$$L(\phi_\bullet) = \inf\big\{ \mathrm{dist}(p, \phi_\bullet(p)) \,|\, p \in \mathbb{H}_S \big\}.$$

If the infimum is a minimum, then

- either it is equal to 0 and $\phi_\bullet$ has a fixed point in $\mathbb{H}_S$, $\phi_\bullet$ is thus **elliptic**,

- or it is positive and $\phi_\bullet$ is **hyperbolic**. Hence the set of points $p \in \mathbb{H}_S$ such that $\mathrm{dist}(p, \phi_\bullet(p))$ is equal to $L(\phi_\bullet)$ is a geodesic line $\mathrm{Ax}(\phi_\bullet) \subset \mathbb{H}_S$. Its boundary points are represented by isotropic vectors $\omega(\phi_\bullet)$ and $\alpha(\phi_\bullet)$ in $\overline{Z}_S$ such that

$$\phi_\bullet(\omega(\phi_\bullet)) = \lambda(\phi)\,\omega(\phi_\bullet) \qquad\qquad \phi_\bullet(\alpha(\phi_\bullet)) = \frac{1}{\lambda(\phi)}\alpha(\phi_\bullet).$$

  The axis of $\phi_\bullet$ is the intersection of $\mathbb{H}_S$ with the plane containing $\omega(\phi_\bullet)$ and $\alpha(\phi_\bullet)$. Forall $p \in \mathbb{H}_S$ one has

$$\lim_{k\to+\infty} \frac{\phi_\bullet^{-k}(p)}{\lambda(\phi)} = \alpha(\phi_\bullet) \qquad\qquad \lim_{k\to+\infty} \frac{\phi_\bullet^{k}(p)}{\lambda(\phi)} = \omega(\phi_\bullet).$$

When the infimum is not realized, $L(\phi_\bullet) = 0$ and $\phi_\bullet$ is **parabolic**: $\phi_\bullet$ fixes a unique line in $\mathcal{L}\overline{Z}_S$; this line is fixed pointwise, and all orbits $\phi_\bullet^n(p)$ in $\mathbb{H}_S$ accumulate to the corresponding boundary point when n goes to $\pm\infty$.

Exercice 27. — Let $\phi_\bullet$ be a hyperbolic isometry; it acts as a translation along $\mathrm{Ax}(\phi_\bullet)$. Let us prove that this length of translation is $L(\phi_\bullet) = \log\lambda(\phi)$.

One can normalize $\alpha(\phi_\bullet)$ and $\omega(\phi_\bullet)$ such that $\alpha(\phi_\bullet) = \omega(\phi_\bullet) = \frac{1}{2}$; one has

$$\mathrm{Ax}(\phi_\bullet) = \left\{u\alpha(\phi_\bullet) + v\omega(\phi_\bullet) \,|\, uv = 1\right\}.$$

Set $p = \alpha(\phi_\bullet) + \omega(\phi_\bullet)$; the point p lies on $\mathrm{Ax}(\phi_\bullet)$. Compute $2\cosh(\mathrm{dist}(p, \phi_\bullet(p)))$, and $2\cosh(L(\phi_\bullet))$. Conclude.

There is a strong relationship between classification of birational maps of $\mathbb{P}^2_{\mathbb{C}}$ and the classification of isometries of $\mathbb{H}_{\mathbb{P}^2_{\mathbb{C}}}$:

Theorem 3.1 ([7]). — *Let ϕ be a birational map of the complex projective plane. Then*

- *ϕ is a elliptic map if and only if $\phi_\bullet$ is an elliptic isometry;*
- *ϕ is a twist if and only if $\phi_\bullet$ is a parabolic isometry;*
- *ϕ is a hyperbolic map if and only if $\phi_\bullet$ is a hyperbolic isometry.*

Remark 3.2. — Let ϕ be an element of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$, and let h be the class of a line viewed as a point in $\mathbb{H}_{\mathbb{P}^2_{\mathbb{C}}}$. Then

$$\phi_\bullet(h) = (\deg\phi)h - \sum a_p e_p$$

where a_p is the multiplicity of the linear system $\phi_*|O(1)|$ at the point p. Since h does not intersect any of the e_p one gets

$$\cosh(\mathrm{dist}(h,\phi_\bullet(h))) = h\cdot\phi_\bullet(h) = \deg\phi$$

this establishes a link between $\deg\phi^n$ and $\mathrm{dist}\big(h,\phi_\bullet^n(h)\big)$.

Exercice 28. — Take a generic element ϕ in $\mathrm{Bir}_2(\mathbb{P}^2_{\mathbb{C}})$. Then

$$\begin{cases} \mathrm{Ind}\,\phi = \{p_0,p_1,p_2\}, & \mathrm{Exc}\,\phi = \{L_{p_0p_1},L_{p_1p_2},L_{p_0p_2}\},\\ \mathrm{Ind}\,\phi^{-1} = \{q_0,q_1,q_2\}, & \mathrm{Exc}\,\phi^{-1} = \{L_{q_0q_1},L_{q_1q_2},L_{q_0q_2}\}\end{cases}$$

Let h be the class of a line in $\mathbb{P}^2_{\mathbb{C}}$. Determine $\phi_\bullet(h)$.
Assume ϕ is an isomorphism on a neighborhood of p, and $\phi(p)=q$; determine $\phi_\bullet(e_p)$.
Suppose $L_{q_1q_2}$ is blown down onto p_0 by ϕ^{-1} ; determine $\phi_\bullet(e_{p_0})$.

Exercice 29. — Any set $\{p_0=(1:0:0),p_1,p_2\}$ of three distinct and non colinear points is the indeterminacy set of a Jonquières map of degree 2. Any set $\{p_0=(1:0:0),p_1,p_2,p_3\}$ of four distinct points such that

- no three of them are on a line through p_0, and
- there is no line containing p_1, p_2 and p_3

is the indeterminacy set of a Jonquières map of degree 3. More generally on the complement of a strict Zariski closed subset of $\mathcal{J}_d$ the points p_0, p_1, …, p_{2d-2} form a set of $2d-1$ distinct points in the complex projective plane. Hence the base points of a generic element ϕ of $\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}})\times\mathcal{J}_d\times\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}})$ are $p_0=(1:0:0)$ and $2d-1$ distinct points p_1, p_2, …, p_{2d-2} of $\mathbb{P}^2_{\mathbb{C}}$.

Determine $\phi_\bullet(h)$.

3.3 Some applications

3.3.1 Tits alternative

Linear groups satisfy Tits alternative. Recall that a group G is **solvable** if there exists an integer k such that $G^{(k)}=\{\mathrm{id}\}$ where $G^{(0)}=G$ and for $k\geq 1$

$$G^{(k)} = [G^{(k-1)},G^{(k-1)}] = \langle aba^{-1}b^{-1}\,|\,a,b\in G^{(k-1)}\rangle.$$

Theorem 3.3 ([35]). *Let $\Bbbk$ be a field of characteristic 0, and Γ be a finitely generated subgroup of $\mathrm{GL}(n,\Bbbk)$. Then*

- *either* Γ *contains a non abelian, free group;*

- *or* Γ *contains a solvable subgroup of finite index.*

The group of diffeomorphisms of a real manifold of dimension ≥ 1 does not satisfy Tits alternative ([22]). The group of polynomial automorphisms of $\mathbb{C}^2$ satisfies Tits alternative ([29]); to prove it Lamy uses the structure of amalgamated product of $\mathrm{Aut}(\mathbb{C}^2)$ that implies that $\mathrm{Aut}(\mathbb{C}^2)$ acts on a tree ([34]). Using the action of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ on $\overline{\mathcal{Z}}_{\mathbb{P}^2_{\mathbb{C}}}$ Cantat studied the finitely generated subgroups of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ and establishes the following statement

Theorem 3.4 ([7])**.** *The Cremona group* $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ *satisfies Tits alternative.*

3.3.2 Simplicity

Let us recall that a group is **simple** if it has no non trivial, proper and normal subgroup. The **normal subgroup of** G **generated by** $f \in G$ is

$$\langle hfh^{-1} \,|\, h \in G \rangle.$$

Remark that $\mathrm{Aut}(\mathbb{C}^2)$ is not simple: let Ψ be the morphism defined by

$$\mathrm{Aut}(\mathbb{C}^2) \to \mathbb{C}^* \qquad \phi \mapsto \det \mathrm{jac}\, \phi$$

its kernel is a proper normal subgroup of $\mathrm{Aut}(\mathbb{C}^2)$. Danilov has established that $\ker \Psi$ is not simple ([13]); more precisely using [33] he proved that the normal subgroup generated by $(ea)^{13}$ where

$$a = (y, -x) \qquad\qquad e = (x, y + 3x^5 - 5x^4)$$

is a strict subgroup of $\left\{\phi \in \mathrm{Aut}(\mathbb{C}^2) \,|\, \Psi(\phi) = 1\right\}$. More recently Furter and Lamy gave a more precise statement ([21]).

What about the Cremona group ? A birational map ϕ is **tight** if

- $\phi_\bullet$ is hyperbolic;

- there exists a positive number ε such that: if ψ is a birational map, and if $\psi_\bullet(\mathrm{Ax}(\phi_\bullet))$ contains two points at distance ε which are at distance at most 1 from $\mathrm{Ax}(\phi_\bullet)$ then $\psi_\bullet(\mathrm{Ax}(\phi_\bullet)) = \mathrm{Ax}(\phi_\bullet)$;

- if ψ is a birational map and $\psi_\bullet(\mathrm{Ax}(\phi_\bullet)) = \mathrm{Ax}(\phi_\bullet)$, then $\psi\phi\psi^{-1} = \phi^{\pm 1}$.

Using the action of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ on $\overline{\mathcal{Z}}_{\mathbb{P}^2_{\mathbb{C}}}$ Cantat and Lamy proved that:

Theorem 3.5 ([8]). *Let ϕ be an element of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$. If ϕ is tight, then ϕ^k generates a non trivial, strict and normal subgroup of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ for some positive integer k.*

As a consequence:

Corollary 3.6 ([8]). *The Cremona group $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ contains an uncountable number of strict normal subgroups.*

In particular $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ is not simple.

3.3.3 Homomorphisms from lattices into the Cremona group

Using the embedding of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ into the Picard-Manin space, Cantat proved the following result:

Theorem 3.7 ([7]). *Any homomorphism with infinite image from a discrete Kazhdan group into $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ is conjugate to a homomorphism into $\mathrm{PGL}(3,\mathbb{C})$.*

In particular, this result applies to any lattice Γ in a connected simple Lie group with property (T)[3] but left open the problem of classifying homomorphisms from lattices in the groups $\mathrm{SO}(n,1)$ and $\mathrm{SU}(n,1)$ into $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$. There exist, for some values of n, injective homomorphisms from lattices in $\mathrm{SO}(n,1)$ to the Cremona group ([8, 19]). Delzant and Py focus on the case $\mathrm{SU}(n,1)$:

Theorem 3.8 ([15]). *Let Γ be a cocompact lattice in the group $\mathrm{SU}(1,n)$ with $n \geq 2$. If $\rho\colon \Gamma \to \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ is an injective homomorphism, then one of the following two possibilities holds*

- *the group $\rho(\Gamma)$ fixes a point in the Picard-Manin space;*
- *the group $\rho(\Gamma)$ fixes a unique point in the boundary of the Picard-Manin space.*

3.3.4 Solvable subgroups

The study of solvable groups started a long time ago, and any linear solvable subgroup is up to finite index triangularizable (Lie-Kolchin theorem, [28, Theorem 21.1.5]). The assumption "up to finite index" is essential: for instance the subgroup of $\mathrm{PGL}(2,\mathbb{C})$ generated by the matrices

$$\begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \qquad \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$$

is isomorphic to $\mathfrak{S}_3$ so is solvable but is not triangularizable.

[3] Informally, a locally compact topological group G has property (T) if it satisfies the following property: if G acts unitarily on a Hilbert space and has "almost invariant vectors", then it has a nonzero invariant vector.

Theorem 3.9 ([16]). *Let G be an infinite, solvable, non virtually abelian subgroup of* $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$. *Then, up to finite index, one of the following holds*

1. *any element of G is either of finite order, or conjugate to an automorphism of $\mathbb{P}^2_{\mathbb{C}}$;*
2. *G preserves a unique fibration that is rational, in particular G is, up to conjugacy, a subgroup of* $\mathrm{PGL}(2,\mathbb{C}(y)) \rtimes \mathrm{PGL}(2,\mathbb{C})$;
3. *G preserves a unique fibration that is elliptic;*
4. *G is, up to birational conjugacy, a subgroup of*

$$\left\{(x^p y^q, x^r y^s),\ (\alpha x, \beta y) \,|\, \alpha, \beta \in \mathbb{C}^*\right\}$$

where $M = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ *denotes an element of* $\mathrm{GL}(2,\mathbb{Z})$ *with spectral radius* > 1. *The group G preserves the two holomorphic foliations defined respectively by the* 1*-forms*

$$\alpha_1\, x\mathrm{d}y + \beta_1\, y\mathrm{d}x \qquad \alpha_2\, x\mathrm{d}y + \beta_2\, y\mathrm{d}x$$

where (α_1,β_1) *and* (α_2,β_2) *denote the eigenvectors of* ${}^tM$.

Furthermore if G is uncountable, case 3. does not hold.

Examples 3.10.

- Denote by S_3 the group generated by the matrices

$$\begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \qquad \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$$

  As we recall before $\mathrm{S}_3 \simeq \mathfrak{S}_3$. Consider now the subgroup G of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ whose elements are the monomial maps $(x^p y^q, x^r y^s)$ with $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \mathrm{S}_3$. Then any element of G has finite order, and G is solvable; it gives an example of case 1.

- The centralizer of a birational map of $\mathbb{P}^2_{\mathbb{C}}$ that preserves a unique fibration that is rational is virtually solvable ([10, Corollary C]); this example falls in case 2 (we will give some details in Example 3.17).

- In [12, Proposition 2.2] Cornulier proved that the group

$$\langle (x+1,y),\ (x,y+1),\ (x,xy) \rangle$$

  is solvable of length 3, and is not linear over any field; this example falls in case 2. The invariant fibration is given by $x = \mathrm{cst}$.

Exercice 30. Give a subgroup of $\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}})$ that illustrates case 1.

Exercice 31. Give a subgroup of $\mathrm{Aut}(\mathbb{C}^2)$ that illustrates case 1.

Remark 3.11. In case 1. if there exists an integer d such that $\deg\phi \leq d$ for any ϕ in G, then there exists a birational map $\psi\colon M \dashrightarrow \mathbb{P}^2_{\mathbb{C}}$ such that $\psi^{-1}G\psi$ is a solvable subgroup of $\mathrm{Aut}(M)$ (see the end of the section for more details). But there is some solvable subgroups G with only elliptic elements that do not satisfy this property: the group

$$\mathrm{E} = \left\{(\alpha x + P(y), \beta y + \gamma) \,|\, \alpha, \beta \in \mathbb{C}^*, \gamma \in \mathbb{C}, P \in \mathbb{C}[y]\right\} \subset \mathrm{Aut}(\mathbb{C}^2).$$

We will prove Theorem 3.9: we first assume that our solvable, infinite and non virtually abelian, subgroup G contains a hyperbolic map, then that it contains a twist and no hyperbolic map, and finally that all elements of G are elliptic.

A. Solvable groups of birational maps containing a hyperbolic map

Let us recall the following criterion (for its proof see for example [14]) used on many occasions by Klein, and also by Tits ([35]):

Lemma 3.12 (Ping-Pong Lemma)**.** *Let* H *be a group acting on a set* X*, let* Γ_1*,* Γ_2 *be two subgroups of* H*, and let* Γ *be the subgroup generated by* Γ_1 *and* Γ_2*. Assume that* Γ_1 *contains at least three elements, and* Γ_2 *at least two elements. Suppose that there exist two non-empty subsets* X_1*,* X_2 *of* X *such that* $X_2 \not\subset X_1$*, and for any* $\gamma \in \Gamma_1 \smallsetminus \{\mathrm{id}\}$ *and any* $\gamma' \in \Gamma_2 \smallsetminus \{\mathrm{id}\}$

$$\gamma(X_2) \subset X_1 \qquad \gamma'(X_1) \subset X_2.$$

Then Γ *is isomorphic to the free product* $\Gamma_1 * \Gamma_2$*.*

The Ping-Pong argument allows us to prove the following:

Lemma 3.13 ([16])**.** *A solvable, non abelian, subgroup of* $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ *cannot contain two hyperbolic maps* ϕ *and* ψ *such that* $\left\{\omega(\phi_\bullet), \alpha(\phi_\bullet)\right\} \neq \left\{\omega(\psi_\bullet), \alpha(\psi_\bullet)\right\}$.

Proof. Assume by contradiction that $\left\{\omega(\phi_\bullet), \alpha(\phi_\bullet)\right\} \neq \left\{\omega(\psi_\bullet), \alpha(\psi_\bullet)\right\}$. Then the Ping-Pong argument implies that there exist two integers n and m such that ψ^n and ϕ^m generate a subgroup of G isomorphic to the free group F_2 (*see* [7]). But $\langle\phi, \psi\rangle$ is a solvable group: contradiction. □

Let G be an infinite solvable, non virtually abelian, subgroup of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$. Assume that G contains a hyperbolic map ϕ. Let $\alpha(\phi_\bullet)$ and $\omega(\phi_\bullet)$ be the two fixed points of $\phi_\bullet$ on $\partial\mathbb{H}_{\mathbb{P}^2_{\mathbb{C}}}$, and $\mathrm{Ax}(\phi_\bullet)$ be the geodesic passing through these two points. As G is solvable there exists a subgroup

of G of index 2 that preserves $\alpha(\phi_\bullet)$, $\omega(\phi_\bullet)$, and $\mathrm{Ax}(\phi_\bullet)$ (*see* [7, Theorem 6.4]); let us still denote by G this subgroup. One thus has a morphism $\kappa\colon G \to \mathbb{R}_+^*$ such that

$$\psi_\bullet(\ell) = \kappa(\psi)\ell$$

for any ℓ in $\overline{\mathcal{Z}}_{\mathbb{P}^2_{\mathbb{C}}}$ lying on $\mathrm{Ax}(\phi_\bullet)$.

Gap property:

If $\phi \in \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ is a hyperbolic map, then $\lambda(\phi)$ is an algebraic integer with all Galois conjugates in the unit disk, that is a Salem number, or a Pisot number. The smallest known number is the Lehmer number $\lambda_L \simeq 1,176$ which is a root of

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

Blanc and Cantat prove in [3, Corollary 2.7] that there is a gap in the dynamical spectrum $\Lambda = \{\lambda(\phi) \,|\, \phi \in \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})\}$: there is no dynamical degree in $]1, \lambda_L[$.

The gap property implies that in fact $\kappa\colon \psi \to \kappa(\psi)$ such that $\psi_\bullet(\ell) = \kappa(\psi)\ell$ for any ℓ in $\overline{\mathcal{Z}}_{\mathbb{P}^2_{\mathbb{C}}}$ lying on $\mathrm{Ax}(\phi_\bullet)$ is a morphism from G to $\mathbb{Z}$. Furthermore $\ker\kappa$ is an infinite subgroup that contains only elliptic maps. Indeed it is clear that the set of elliptic elements of G coincides with $\ker\alpha$; and $[G,G] \subset \ker\alpha$ so if $\ker\alpha$ is finite, G is abelian up to finite index which is impossible.

Elliptic subgroups of the Cremona group with a large normalizer:

Consider in $\mathbb{P}^2_{\mathbb{C}}$ the complement of the union of the three lines $\{x = 0\}$, $\{y = 0\}$ and $\{z = 0\}$. Denote by $\mathcal{U}$ this open set isomorphic to $\mathbb{C}^* \times \mathbb{C}^*$. One has an action of $\mathbb{C}^* \times \mathbb{C}^*$ on $\mathcal{U}$ by translation. Furthermore $\mathrm{GL}(2,\mathbb{Z})$ acts on $\mathcal{U}$ by monomial maps

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix} \mapsto \big((x,y) \mapsto (x^p y^q, x^r y^s)\big)$$

One thus has an injective morphism from $(\mathbb{C}^* \times \mathbb{C}^*) \rtimes \mathrm{GL}(2,\mathbb{Z})$ into $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$. Let G_{toric} be its image.

One can now apply [15, Theorem 4] that says that if there exists a short exact sequence

$$1 \longrightarrow \mathrm{A} \longrightarrow \mathrm{N} \longrightarrow \mathrm{B} \longrightarrow 1$$

where $\mathrm{N} \subset \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ contains at least one hyperbolic element, and $\mathrm{A} \subset \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ is an infinite and that fixes a point in $\mathbb{H}_{\mathbb{P}^2_{\mathbb{C}}}$, then N is up to conjugacy a subgroup of G_{toric}. Hence up to birational conjugacy $G \subset G_{\mathrm{toric}}$.

One can now state:

Proposition 3.14 ([16]). *Let G be an infinite solvable, non virtually abelian, subgroup of* $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$. *If G contains a hyperbolic birational map, then G is, up to conjugacy and finite index, a subgroup of*

$$\langle (x^p y^q, x^r y^s), (\alpha x, \beta y) \,|\, \alpha, \beta \in \mathbb{C}^* \rangle$$

where $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ *denotes an element of* $\mathrm{GL}(2,\mathbb{Z})$ *with spectral radius* > 1.

B. Solvable groups with a twist

Consider a solvable, non abelian, subgroup G of $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$. Let us assume that G contains a twist ϕ; the map ϕ preserves a unique fibration $\mathcal{F}$ that is rational or elliptic. Let us prove that any element of G preserves $\mathcal{F}$. Denote by $\alpha(\phi_\bullet) \in \partial\mathbb{H}_{\mathbb{P}^2_{\mathbb{C}}}$ the fixed point of $\phi_\bullet$. Take one element in $\mathcal{LZ}_{\mathbb{P}^2_{\mathbb{C}}}$ still denoted $\alpha(\phi_\bullet)$ that represents $\alpha(\phi_\bullet)$. Take $\varphi \in G$ such that $\varphi(\alpha(\phi_\bullet)) \neq \alpha(\phi_\bullet)$. Then $\psi = \varphi\phi\varphi^{-1}$ is parabolic and fixes the unique element $\alpha(\psi_\bullet)$ of $\mathcal{LZ}_{\mathbb{P}^2_{\mathbb{C}}}$ proportional to $\varphi(\alpha(\phi_\bullet))$. Take $\varepsilon > 0$ such that $\mathcal{U}(\alpha(\phi_\bullet),\varepsilon) \cap \mathcal{U}(\alpha(\psi_\bullet),\varepsilon) = \emptyset$ where

$$\mathcal{U}(\alpha,\varepsilon) = \big\{ \ell \in \mathcal{LZ}_{\mathbb{P}^2_{\mathbb{C}}} \,|\, \alpha \cdot \ell < \varepsilon \big\}.$$

Since $\psi_\bullet$ is parabolic, then for n large enough the inclusion

$$\psi_\bullet^n\big(\mathcal{U}(\alpha(\phi_\bullet),\varepsilon)\big) \subset \mathcal{U}(\alpha(\psi_\bullet),\varepsilon)$$

holds. For m sufficiently large

$$\phi_\bullet^m\psi_\bullet^n\big(\mathcal{U}(\alpha(\phi_\bullet),\varepsilon)\big) \subset \big(\mathcal{U}(\alpha(\phi_\bullet),\varepsilon/2)\big) \subsetneq \big(\mathcal{U}(\alpha(\phi_\bullet),\varepsilon)\big).$$

Hence $\phi_\bullet^m\psi_\bullet^n$ is hyperbolic. You can by this way build two hyperbolic maps whose sets of fixed points are distinct: this gives a contradiction with Lemma 3.13. So for any $\varphi \in G$ one has : $\alpha(\phi_\bullet) = \alpha(\varphi_\bullet)$; one can thus state the following result.

Proposition 3.15 ([16]). *Let G be a solvable, non abelian, subgroup of* $\mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ *that contains a twist ϕ. Then*

- *if ϕ is a Jonquières twist, then G preserves a rational fibration, that is up to birational conjugacy G is a subgroup of* $\mathrm{PGL}(2,\mathbb{C}(y)) \rtimes \mathrm{PGL}(2,\mathbb{C})$,
- *if ϕ is a Halphen twist, then G preserves an elliptic fibration.*

If G is uncountable, then ϕ is a Jonquières twist.

Remark 3.16. Both cases are mutually exclusive.

Example 3.17. If $\phi \in \mathrm{Bir}(\mathbb{P}^2_{\mathbb{C}})$ preserves a unique fibration that is rational then one can assume that up to birational conjugacy this fibration is given, in the affine chart $z = 1$, by $y = \mathrm{cst}$. If ϕ preserves $y = \mathrm{cst}$ fiberwise, then

- ϕ is contained in a maximal abelian subgroup denoted $\mathrm{Ab}(\phi)$ that preserves $y = \mathrm{cst}$ fiberwise ([17]),
- the centralizer of ϕ is a finite extension of $\mathrm{Ab}(\phi)$ (*see* [10, Theorem B]).

This allows us to establish that if ϕ preserves a fibration not fiberwise, then the centralizer of ϕ is virtually solvable ([10, Corollary C]). For instance if $\phi = \big(x + a(y), y + 1\big)$ (resp. $\big(b(y)x, \beta y\big)$ or $\big(x + a(y), \beta y\big)$ with $\beta \in \mathbb{C}^*$ of infinite order) preserves a unique fibration, then the centralizer of ϕ is solvable and metabelian ([10, Propositions 5.1 and 5.2]).

C. Solvable groups with no hyperbolic map, and no twist

Let M be a smooth, irreducible, complex, projective variety of dimension n. Fix a Kähler form ω on M. If ℓ is a positive integer, denote by $x_i \colon M^\ell \to M$ the projection onto the i-th factor. The manifold M^ℓ is then endowed with the Kähler form $\sum_{i=1}^{\ell} x_i^* \omega$ which induces a Kähler metric. To any $\phi \in \mathrm{Bir}(M)$ one can associate its graph $\Gamma_\phi \subset M \times M$ defined as the Zariski closure of

$$\big\{(z, \phi(z)) \in M \times M \,|\, z \in M \smallsetminus \mathrm{Ind}\,\phi\big\}.$$

By construction Γ_ϕ is an irreducible subvariety of $M \times M$ of dimension n. Both projections x_1, $x_2 \colon M \times M \to M$ restrict to birational morphisms $x_1, x_2 \colon \Gamma_\phi \to M$.

The **total degree** $\mathrm{tdeg}\,\phi$ of $\phi \in \mathrm{Bir}(M)$ is defined as the volume of Γ_ϕ with respect to the fixed metric on $M \times M$:

$$\mathrm{tdeg}\,\phi = \int_{\Gamma_\phi} \big(x_1^*\omega + x_2^*\omega\big)^n = \int_{M \smallsetminus \mathrm{Ind}\,\phi} \big(\omega + \phi^*\omega\big)^n.$$

Let $d \geq 1$ be a natural integer, and set

$$\mathrm{Bir}_d(M) = \big\{\phi \in \mathrm{Bir}(M) \,|\, \mathrm{tdeg}\,\phi \leq d\big\}.$$

A subgroup G of $\mathrm{Bir}(M)$ has **bounded degree** if it is contained in $\mathrm{Bir}_d(M)$ for some $d \in \mathbb{N}^*$.

Any subgroup G of $\mathrm{Bir}(M)$ that has bounded degree can be regularized, that is up to birational conjugacy all indeterminacy points of all elements of G disappear simultaneously:

Theorem 3.18 ([36])**.** *Let M be a complex projective variety, and let G be a subgroup of* $\mathrm{Bir}(M)$*. If G has bounded degree, there exists a smooth, complex, projective variety M', and a birational map $\psi \colon M' \dashrightarrow M$ such that $\psi^{-1} G \psi$ is a subgroup of* $\mathrm{Aut}(M')$*.*

Solution 26. — Let p be a point of $\mathbb{P}^2_{\mathbb{C}}$, let S_1 be the surface obtained by blowing up $\mathbb{P}^2_{\mathbb{C}}$ at p, and let E_p be the exceptional divisor of this blow-up. Consider a point q on E_p; denote by S_2 the surface obtained by blowing up q and by E_q the associated exceptional divisor. Both e_p and e_q belong to the image of $\mathrm{NS}(S_2)$ in $\mathcal{Z}_{\mathbb{P}^2_{\mathbb{C}}}$. Let $\widetilde{E}_p$ be the strict transform of E_p in S_2. Then e_p corresponds to $\widetilde{E}_p+E_q$ and e_q to E_q. Hence

$$\begin{cases} e_p\cdot e_p=\widetilde{E}_p^2+E_q^2+2\widetilde{E}_p\cdot E_q=-2-1+2=-1\\ e_p\cdot e_q=(\widetilde{E}_p\cdot E_q)+E_q^2=1-1=0 \text{ if } p\neq q\end{cases}$$

Solution 27. — As $p=\alpha(\phi_\bullet)+\omega(\phi_\bullet)\in \mathrm{Ax}(\phi_\bullet)$ then

$$\phi_\bullet(p)=\frac{\alpha(\phi_\bullet)}{\lambda(\phi)}+\lambda(\phi)\omega(\phi_\bullet).$$

Since $\phi_\bullet\big(\alpha(\phi_\bullet)\big)=\frac{\alpha(\phi_\bullet)}{\lambda(\phi)}$ and $\phi_\bullet\big(\omega(\phi_\bullet)\big)=\lambda(\phi)\omega(\phi_\bullet)$ we have:

$$2\cosh(\mathrm{dist}(p,\phi_\bullet(p)))=2p\cdot\phi_\bullet(p)=\lambda(\phi)+\frac{1}{\lambda(\phi)}.$$

Furthermore

$$2\cosh(L(\phi_\bullet))=e^{L(\phi_\bullet)}+\frac{1}{e^{L(\phi_\bullet)}}$$

Solution 28. — If ϕ is an isomorphism on a neighborhood of p, and $\phi(p)=q$, then $\phi_\bullet(e_p)=e_q$.

If $L_{q_1q_2}$ is blown down onto p_0 by ϕ^{-1}, then

$$\phi_\bullet(e_{p_0})=h-e_{q_1}-e_{q_2}\qquad \phi_\bullet(h)=2h-e_{q_0}-e_{q_1}-e_{q_2}$$

where h is the class of a line in $\mathbb{P}^2_{\mathbb{C}}$.

Solution 29. — One has

$$\phi_\bullet(h)=dh-(d-1)e_{p_0}-\sum_{i=1}^{2d-2}e_{p_i}$$

where the p_i's are generic distinct points of $\mathbb{P}^2_{\mathbb{C}}$.

Solution 30. A subgroup of $\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}})$ that illustrates case 1. is

$$\big\{(\alpha x+\beta y+\gamma,\delta y+\varepsilon)\,|\,\alpha,\delta\in\mathbb{C}^*,\beta,\gamma,\varepsilon\in\mathbb{C}\big\}\subset\mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}).$$

Solution 31. A subgroup of $\mathrm{Aut}(\mathbb{C}^2)$ that illustrates case 1. is

$$\mathrm{E}=\big\{(\alpha x+P(y),\beta y+\gamma)\,|\,\alpha,\beta\in\mathbb{C}^*,\gamma\in\mathbb{C},P\in\mathbb{C}[y]\big\}\subset\mathrm{Aut}(\mathbb{C}^2).$$

References

[1] J. W. Alexander, *On the factorization of Cremona plane transformations*, Trans. Amer. Math. Soc. **17** (1916), no. 3, 295–300. MR 1501043

[2] A. Beauville, *Complex algebraic surfaces*, second ed., London Mathematical Society Student Texts, vol. 34, Cambridge University Press, Cambridge, 1996, Translated from the 1978 French original by R. Barlow, with assistance from N. I. Shepherd-Barron and M. Reid. MR 1406314 (97e:14045)

[3] J. Blanc and S. Cantat, *Dynamical degrees of birational transformations of projective surfaces*, J. Amer. Math. Soc. (To appear).

[4] J. Blanc and J. Déserti, *Degree growth of birational maps of the plane*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **14** (2015), no. 5, 1–27.

[5] J. Blanc and I. Hedén, *The group of Cremona transformations generated by linear maps and the standard involution,* arXiv:1405.2746, Ann. Inst. Fourier (Grenoble) (To appear).

[6] M. R. Bridson and A. Haefliger, *Metric spaces of non-positive curvature*, Grundlehren der Mathematischen Wissenschaften, vol. 319, Springer-Verlag, Berlin, 1999. MR 1744486 (2000k:53038)

[7] S. Cantat, *Sur les groupes de transformations birationnelles des surfaces*, Ann. of Math. (2) **174** (2011), no. 1, 299–340. MR 2811600 (2012g:14015)

[8] S. Cantat and S. Lamy, *Normal subgroups in the Cremona group*, Acta Math. **210** (2013), no. 1, 31–94, With an appendix by Yves de Cornulier. MR 3037611

[9] G. Castelnuovo, *Le trasformationi generatrici del gruppo cremoniano nel piano*, Atti R. Accad. Sci. Torino **36** (1901), 861–874.

[10] D. Cerveau and J. Déserti, *Centralisateurs dans le groupe de Jonquières*, Michigan Math. J. **61** (2012), no. 4, 763–783. MR 3049289

[11] ———, *Transformations birationnelles de petit degré*, Cours Spécialisés, vol. 19, Société Mathématique de France, Paris, 2013. MR 3155973

[12] Y. Cornulier, *Nonlinearity of some subgroups of the planar Cremona group*, Unpublished manuscript, 2013, `http://www.normalesup.org/~cornulier/crelin.pdf`.

[13] V. I. Danilov, *Non-simplicity of the group of unimodular automorphisms of an affine plane*, Mat. Zametki **15** (1974), 289–293. MR 0357626 (50 #10094)

[14] P. de la Harpe, *Topics in geometric group theory*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2000. MR 1786869 (2001i:20081)

[15] T. Delzant and P. Py, *Kähler groups, real hyperbolic spaces and the Cremona group*, Compos. Math. **148** (2012), no. 1, 153–184. MR 2881312

[16] J. Déserti, *On solvable subgroups of the Cremona group* , arXiv:1503.02121.

[17] J. Déserti, *Sur les automorphismes du groupe de Cremona*, Compos. Math. **142** (2006), no. 6, 1459–1478. MR 2278755 (2007g:14008)

[18] J. Diller and C. Favre, *Dynamics of bimeromorphic maps of surfaces*, Amer. J. Math. **123** (2001), no. 6, 1135–1169. MR 1867314 (2002k:32028)

[19] I. V. Dolgachev and D.-Q. Zhang, *Coble rational surfaces*, Amer. J. Math. **123** (2001), no. 1, 79–114. MR 1827278 (2002e:14061)

[20] S. Friedland and J. Milnor, *Dynamical properties of plane polynomial automorphisms*, Ergodic Theory Dynam. Systems **9** (1989), no. 1, 67–99. MR 991490 (90f:58163)

[21] J.-P. Furter and S. Lamy, *Normal subgroup generated by a plane polynomial automorphism*, Transform. Groups **15** (2010), no. 3, 577–610. MR 2718938 (2012b:14122)

[22] É. Ghys, *Groups acting on the circle*, Enseign. Math. (2) **47** (2001), no. 3-4, 329–407. MR 1876932 (2003a:37032)

[23] É. Ghys and P. de la Harpe (eds.), *Sur les groupes hyperboliques d'après Mikhael Gromov*, Progress in Mathematics, vol. 83, Birkhäuser Boston, Inc., Boston, MA, 1990, Papers from the Swiss Seminar on Hyperbolic Groups held in Bern, 1988. MR 1086648 (92f:53050)

[24] M. Gizatullin, *On some tensor representations of the Cremona group of the projective plane*, New trends in algebraic geometry (Warwick, 1996), London Math. Soc. Lecture Note Ser., vol. 264, Cambridge Univ. Press, Cambridge, 1999, pp. 111–150. MR 1714823 (2000i:14018)

[25] M. H. Gizatullin, *Rational G-surfaces*, Izv. Akad. Nauk SSSR Ser. Mat. **44** (1980), no. 1, 110–144, 239. MR 563788 (81d:14020)

[26] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116)

[27] H. P. Hudson, *Cremona Transformations in Plane and Space*, Cambridge University Press, 1927.

[28] M. I. Kargapolov and Ju. I. Merzljakov, *Fundamentals of the theory of groups*, Graduate Texts in Mathematics, vol. 62, Springer-Verlag, New York-Berlin, 1979, Translated from the second Russian edition by Robert G. Burns. MR 551207 (80k:20002)

[29] S. Lamy, *L'alternative de Tits pour* Aut$[\mathbb{C}^2]$, J. Algebra **239** (2001), no. 2, 413–437. MR 1832900 (2002d:14102)

[30] ———, *Une preuve géométrique du théorème de Jung*, Enseign. Math. (2) **48** (2002), no. 3-4, 291–315. MR 1955604 (2003m:14099)

[31] M. Noether, *Zur theorie der eindentigen ebenentrasformationen*, Math. Ann. **5** (1872), no. 4, 635–639.

[32] I. Pan, *Une remarque sur la génération du groupe de Cremona*, Bol. Soc. Brasil. Mat. (N.S.) **30** (1999), no. 1, 95–98. MR 1686984 (2000b:14015)

[33] P. E. Schupp, *Small cancellation theory over free products with amalgamation*, Math. Ann. **193** (1971), 255–264. MR 0291298 (45 #392)

[34] J.-P. Serre, *Arbres, amalgames,* SL_2, Société Mathématique de France, Paris, 1977, Avec un sommaire anglais, Rédigé avec la collaboration de Hyman Bass, Astérisque, No. 46. MR 0476875 (57 #16426)

[35] J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270. MR 0286898 (44 #4105)

[36] A. Weil, *On algebraic groups of transformations*, Amer. J. Math. **77** (1955), 355–391. MR 0074083 (17,533e)

Algebraic properties of groups of complex analytic local diffeomorphisms

Javier Ribón

Instituto de Matemática, Universidade Federal Fluminense, Rua Mário Santos Braga S/N Valonguinho, Niterói, Rio de Janeiro, Brasil 24020-140.

E-mail address: javier@mat.uff.br

Contents

1 Introduction

We study in these notes the algebraic properties of groups of holomorphic local diffeomorphisms. In this spirit we introduce the basic notions of the theory of pro-algebraic groups. Pro-algebraic groups are the analogue of algebraic linear groups in the infinite dimensional setting of groups of holomorphic local diffeomorphisms. They are very useful to study properties that determine groups defined by algebraic equations in every space of jets.

Let us indicate some examples of the study of algebraic group properties that can be found in the literature. The first example is the study of integrability properties of holomorphic foliations. Given a holomorphic foliation and a leaf we obtain a holonomy group as an image of a representation of the fundamental group of a leaf. It is possible to relate the properties of the derived series of these groups with existence of first integrals or integrating factors. Initially this point of view was developed to study codimension 1 foliations [15, Mattei-Moussu], [16, Paul]... and it has been applied more recently to one-dimensional foliations [18, Rebelo-Reis] [4, Câmara-Scardua]...

Another example is provided by groups of real analytic diffeomorphisms of compact surfaces. The properties of groups of local diffeomorphisms are crucial to show that any nilpotent group of real analytic diffeomorphisms of the sphere is always metabelian, i.e. its first derived group is abelian [7, Ghys]. It is interesting that algebraic properties can be exploited to deduce dynamical properties of groups [19, Rebelo-Reis] [20]. Other applications of the algebraic techniques are the study of the existence of faithful analytic actions of mapping class groups of surfaces on surfaces [5, Cantat-Cerveau], local intersection dynamics [23, Seigal-Yakovenko] [2, Binyamini], derived length [13, Martelo-Ribón] [21]...

We try to give a glimpse of the power of the theory of pro-algebraic groups of formal diffeomorphisms. We lay the groundwork for the study of the derived length of solvable subgroups of local diffeomorphisms in section 4. The fruits of this approach are the sharp bounds for the derived length presented in the results at the end of section 4. We did not prove such theorems in order to keep the text as elementary as possible. The text contains other examples of the utility of pro-algebraic groups in sections 3.6, 3.7, 3.8 and 3.9 that hopefully will motivate the reader. Sometimes we provide a more conceptual interpretation of well-known properties. But we also give very simple proofs of sophisticated results. For instance we show that a group of local diffeomorphisms in dimension n whose elements leave invariant n independent first integrals is necessarily finite (cf. Proposition 3.46).

Another good application is the uniform bound of the period of periodic analytic curves, i.e. invariant by an iterate of a fixed local diffeomorphism.

Let us outline the notes. Section 2 is devoted to explain basic properties of linear groups and to make the reader familiar with these concepts before generalizing them in the setting of local diffeomorphisms. We introduce pro-algebraic groups, explain their properties and how to find examples in section 3. We study the properties of the derived series of a group of local diffeomorphisms in section 4. We define an analogue of the derived series that is more suitable for algebraic groups than the derived series itself and study the properties of a group in terms of its Lie algebra. We classify the pro-algebraic subgroups in dimension 1 modulo formal conjugacy in section 5. Finally we provide an example of a pathological phenomenon of pro-algebraic groups in section 5.

2 Linear groups

We study the algebraic structure of groups of local complex analytic diffeomorphisms. Our point of view involves applying techniques of linear algebraic groups to obtain analogues for groups of local diffeomorphisms. In the next section we introduce linear algebraic groups and stress some properties that will be revisited later on in the context of diffeomorphisms.

Let us consider subgroups of the linear group $\mathrm{GL}(n,\mathbb{C})$. The elements of $\mathrm{GL}(n,\mathbb{C})$ can be considered as points in $\mathbb{C}^{n^2}$ by identifying each matrix with its list of coefficients. In this way it makes sense to consider the algebraic closure $\overline{G}^z$ of a subgroup G of $\mathrm{GL}(n,\mathbb{C})$. The z superindex stands for Zariski-closure.

Proposition 2.1. *Let G be a subgroup of $\mathrm{GL}(n,\mathbb{C})$. The algebraic closure $\overline{G}^z$ of G in $\mathrm{GL}(n,\mathbb{C})$ is a group.*

A proof of this result can be found in [3, Proposition 1.3(b), p. 47].

Let us calculate some examples so that we get familiarized with the algebraic closure. It is natural to start our study with cyclic groups.

Definition 2.2. Let $A \in \mathrm{GL}(n,\mathbb{C})$. We say that A is *unipotent* if $A - Id$ is nilpotent or equivalently if $\mathrm{spec}(A) = \{1\}$.

2.1 Example

Let

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \exp \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ -1/2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let us denote by B the matrix in the right hand side so that we have $A = \exp(B)$. The matrix B is nilpotent whereas A is unipotent. Let us calculate the one parameter group $\{\exp(tB) : t \in \mathbb{C}\}$. We have

$$\exp(tB) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ t & 1 & 0 & 0 & 0 & 0 \\ \frac{t^2-t}{2} & t & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & t & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Clearly $\{\exp(tB) : t \in \mathbb{C}\}$ is an algebraic group given by

$$a_{jj} = 1 \text{ for all } j \in \{1, \dots, 6\},\ a_{21} = a_{32} = a_{54},\ a_{31} = \frac{a_{21}^2 - a_{21}}{2}$$

and $a_{ij} = 0$ for any coefficient that does not appear in the previous equations.

Since $\exp((s+t)B) = \exp(sB)\exp(tB)$ for $s, t \in \mathbb{C}$, we deduce that $A^k = \exp(kB)$ for any $k \in \mathbb{Z}$. Let P be a polynomial on the coefficients of the matrices of $\mathrm{GL}(n, \mathbb{C})$ that vanishes on the elements of the cyclic group $\langle A \rangle$. The expression $Q(t) := P(\exp(tB))$ is polynomial in t. Moreover it vanishes for $t \in \mathbb{Z}$ since $P(A^k) = 0$ for $k \in \mathbb{Z}$. A complex polynomial that vanishes on the integer numbers is necessarily 0. Thus P vanishes on $\{\exp(tB) : t \in \mathbb{C}\}$. We deduce

$$\langle A \rangle \subset \{\exp(tB) : t \in \mathbb{C}\} \subset \overline{\langle A \rangle}^z$$

and then $\overline{\langle A \rangle}^z = \{\exp(tB) : t \in \mathbb{C}\}$ since $\{\exp(tB) : t \in \mathbb{C}\}$ is algebraic.

2.2 The closure of the group generated by a unipotent matrix

Let us generalize the previous example. Given a unipotent matrix $A \in \mathrm{GL}(n, \mathbb{C})$ we consider the unique nilpotent matrix B such that $A = \exp(B)$.

How to calculate B?

- We can write A in Jordan normal form and then to obtain B by using indeterminate coefficients.
- Alternatively the formula $\log(1+x) = \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} x^j$ motivates us to define $B = \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} (A - Id)^j$.

The sum defining B has only finitely many non-vanishing terms since $A - Id$ is nilpotent.

The 1-dimensional complex vector space generated by B is the Lie algebra of the group $\overline{\langle A \rangle}^z$.

Definition 2.3. We denote $\log A = B$. We say that $\log A$ is the *infinitesimal generator* of A. We denote $A^t = \exp(tB)$ for $t \in \mathbb{C}$.

The group $\{A^t : t \in \mathbb{C}\}$ is algebraic. The proof is similar as in the example since we can write B in Jordan normal form. The same argument of the example shows that any polynomial on the coefficients of $\mathrm{GL}(n, \mathbb{C})$ vanishing on $\langle A \rangle$ also vanishes on $\{A^t : t \in \mathbb{C}\}$. As a consequence we obtain

Proposition 2.4. *Let A be a unipotent element of $\mathrm{GL}(n, \mathbb{C})$. Then $\overline{\langle A \rangle}^z$ is equal to $\{A^t : t \in \mathbb{C}\}$*

2.3 The closure of the group generated by a semisimple matrix

Let us consider a diagonal matrix $A = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) \in \mathrm{GL}(n, \mathbb{C})$. The algebraic closure $\overline{\langle A \rangle}^z$ is contained in the algebraic group of diagonal matrices. Let us calculate $\overline{\langle A \rangle}^z$.

Definition 2.5. Given $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ we associate the morphism of groups

$$\begin{array}{rccc} \chi_{k_1,\ldots,k_n} & : & (\mathbb{C}^*)^n & \to & \mathbb{C}^* \\ & & (\lambda_1, \ldots, \lambda_n) & \mapsto & \lambda_1^{k_1} \ldots \lambda_n^{k_n} \end{array} .$$

We say that $\{\chi_{k_1,\ldots,k_n} : (k_1, \ldots, k_n) \in \mathbb{Z}^n\}$ is the group of *characters* of the complex torus $(\mathbb{C}^*)^n$.

Remark 2.6. The group operation is the multiplication of characters. Indeed the map $(k_1, \ldots, k_n) \mapsto \chi_{k_1,\ldots,k_n}$ is an isomorphism from $\mathbb{Z}^n$ onto the group of characters.

Definition 2.7. Let $\underline{\lambda} = (\lambda_1, \ldots, \lambda_n) \in (\mathbb{C}^*)^n$. We define

$$J_{\underline{\lambda}} = \{\underline{k} \in \mathbb{Z}^n : \chi_{\underline{k}}(\underline{\lambda}) = 1\} \text{ and } G_{\underline{\lambda}} = \{\underline{\mu} \in (\mathbb{C}^*)^n : \chi_{\underline{k}}(\underline{\mu}) = 1 \text{ for all } \underline{k} \in J_{\underline{\lambda}}\}.$$

Let us calculate the Zariski-closure of the group generated by a diagonal matrix. The arguments are presented in a series of exercises.

Exercise 2.1. Consider a subset J of $\mathbb{Z}^n$. Show that

$$\{(\lambda_1,\dots,\lambda_n)\in(\mathbb{C}^*)^n : \chi_{k_1,\dots,k_n}(\lambda_1,\dots,\lambda_n)=1 \text{ for all } (k_1,\dots,k_n)\in J\}$$

is an algebraic group (we are identifying $(\mathbb{C}^*)^n$ with the diagonal matrices). Deduce that $G_{\underline{\lambda}}$ is an algebraic group containing $\underline{\lambda}$.

Exercise 2.2. Let $\mu_1,\dots\mu_p$ pairwise different non-vanishing complex numbers. Suppose that

$$c_1\mu_1^k+\ldots+c_p\mu_p^k=0$$

for all $k\in\mathbb{Z}$. Show that $c_1=\ldots=c_p=0$.

Exercise 2.3. Let $P=\sum_{i_1,\dots,i_n} a_{i_1\dots i_n}x_1^{i_1}\dots x_n^{i_n}\in\mathbb{C}[x_1,\dots,x_n]$ be a polynomial such that $P(\lambda_1^k,\dots,\lambda_n^k)=0$ for some $(\lambda_1,\dots,\lambda_n)\in(\mathbb{C}^*)^n$ and any $k\in\mathbb{Z}$. We define

$$S=\{\lambda_1^{i_1}\dots\lambda_n^{i_n} : a_{i_1\dots i_n}\neq 0\}.$$

We write P in the form $\sum_{\mu\in S}\sum_{\lambda_1^{i_1}\dots\lambda_n^{i_n}=\mu} a_{i_1\dots i_n}x_1^{i_1}\dots x_n^{i_n}$. Show $\sum_{\lambda_1^{i_1}\dots\lambda_n^{i_n}=\mu} a_{i_1\dots i_n}=0$ for any $\mu\in S$.

Exercise 2.4. Let $\underline{\lambda}=(\lambda_1,\dots,\lambda_n)\in(\mathbb{C}^*)^n$. Consider

$$I(\langle(\lambda_1,\dots,\lambda_n)\rangle)=\{P\in\mathbb{C}[x_1,\dots,x_n] : P(\lambda_1^k,\dots,\lambda_n^k)=0 \text{ for all } k\in\mathbb{Z}\}$$

and

$$V(I(\langle\underline{\lambda}\rangle))=\{\underline{\mu}\in(\mathbb{C}^*)^n : P(\underline{\mu})=0 \text{ for all } P\in I(\langle\underline{\lambda}\rangle)\}.$$

Show $G_{\underline{\lambda}}=V(I(\langle\underline{\lambda}\rangle))$.

Proposition 2.8. $\overline{\langle\underline{\lambda}\rangle}^z=G_\lambda$.

Proposition 2.8 is a consequence of Exercise 2.4.

Corollary 2.9. *Let $\underline{\lambda}=(\lambda_1,\dots,\lambda_n)\in(\mathbb{C}^*)^n$ such that $\log\lambda_1,\dots,\log\lambda_n$, $2\pi i$ are $\mathbb{Q}$-linearly independent (notice that the condition does not depend on the choice of $\log\lambda_j$ for $1\leq j\leq n$). Then $\overline{\langle\underline{\lambda}\rangle}^z=(\mathbb{C}^*)^n$.*

2.4 The closure of a cyclic group

So far we calculated $\overline{\langle A\rangle}^z$ for $A \in \mathrm{GL}(n,\mathbb{C})$ in two cases, namely if A is diagonalizable or if A is unipotent. What happens in the general case? Let us see that it can be reduced to the previous ones.

Let us introduce the so called Jordan multiplicative decomposition, it is a diagonalizable-unipotent decomposition.

Proposition 2.10. *Let $A \in \mathrm{GL}(n,\mathbb{C})$. There exist unique commuting matrices $A_s, A_u \in \mathrm{GL}(n,\mathbb{C})$ such that A_s is diagonalizable, A_u is unipotent and $A = A_sA_u = A_uA_s$.*

The s in the subindex of A_s stands for semisimple. Indeed since A_s is diagonalizable there exists a direct sum $\bigoplus_{j=1}^n V_j$ where V_j is a vector subspace of dimension 1 of eigenvectors of A_s. Each action $(A_s)_{|V_j} : V_j \to V_j$ is simple, meaning that it can not be decomposed anymore or more rigorously that it is irreducible for any $1 \leq j \leq n$. Since V is decomposed into a sum of simple objects for the action of A_s we say that A_s is semisimple. Anyway, we use diagonalizable and semisimple as synonyms.

The proof is an exercise in linear algebra (cf. [3, Corollary 1, p. 81]). The existence of the decomposition is very easy to prove. Given any matrix the Jordan normal form theorem implies that up to linear change of coordinates it can be decomposed in diagonal blocks. For instance a 3×3 block is of the form

$$\begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ \lambda^{-1} & 1 & 0 \\ 0 & \lambda^{-1} & 1 \end{pmatrix}.$$

The right hand side is the multiplicative Jordan decomposition of the block. Proceeding analogously for each block we obtain the Jordan decomposition for the initial matrix.

This decomposition is also called Jordan-Chevalley decomposition. It is due to the following result:

Theorem 2.11 (Chevalley, cf. [3, section I.4.4, p. 83])**.** *Let G be a linear algebraic subgroup of $\mathrm{GL}(n,\mathbb{C})$. Given any $A \in G$ both the semisimple and the unipotent parts A_s and A_u of A also belong to G.*

This result is extremely important and very useful to calculate invariance groups associated to geometrical actions. Later on we will see some examples in the context of groups of diffeomorphisms.

The Chevalley's theorem implies that $\overline{\langle A\rangle}^z$ contains A_s and A_u and then the group generated by $\overline{\langle A_s\rangle}^z$ and $\overline{\langle A_u\rangle}^z$. Are we missing some elements? The answer is no!

Proposition 2.12. *Let $A \in \mathrm{GL}(n,\mathbb{C})$. Then $\overline{\langle A\rangle}^z$ is equal to the abelian group generated by $\overline{\langle A_s\rangle}^z$ and $\overline{\langle A_u\rangle}^z$. In particular $\overline{\langle A\rangle}^z$ is isomorphic to the direct product $\overline{\langle A_s\rangle}^z \times \overline{\langle A_u\rangle}^z$.*

How to prove Proposition 2.12? It is known that algebraic properties of groups do not change when considering the algebraic closure, so since $\langle A\rangle$ is abelian the closure $\overline{\langle A\rangle}^z$ is also abelian. Anyway, let us prove such result in order to gain some familiarity with these concepts.

Lemma 2.13. *Let G be a commutative linear algebraic subgroup of $\mathrm{GL}(n,\mathbb{C})$. Then $\overline{G}^z$ is commutative.*

Proof. We define

$$Z(G) = \{A \in \mathrm{GL}(n,\mathbb{C}) : AB - BA = 0 \text{ for all } B \in G\}.$$

Clearly $Z(G)$ is a group (the so called centralizer of G) and it is algebraic since fixed $B \in G$ the equation $AB - BA = 0$ is linear in the coefficients of A. Since G is abelian, $Z(G)$ contains G. We obtain $\overline{G}^z \subset \overline{Z(G)}^z = Z(G)$. In particular G is contained in $Z(\overline{G}^z)$ and since the latter group is algebraic we deduce $\overline{G}^z \subset Z(\overline{G}^z)$. The latter property is equivalent to $\overline{G}^z$ being abelian. □

Exercise 2.5. Lemma 2.13 and Chevalley's theorem imply that the group generated by $\overline{\langle A_s\rangle}^z$ and $\overline{\langle A_u\rangle}^z$ is abelian. Show this result without using Chevalley's theorem.

How to find an algebraic group that contains $\overline{\langle A_s\rangle}^z \cup \overline{\langle A_u\rangle}^z$? We can consider a morphism

$$\begin{array}{rccc} \times & : & \overline{\langle A_s\rangle}^z \times \overline{\langle A_u\rangle}^z & \to & \mathrm{GL}(n,\mathbb{C}) \\ & & (B,C) & \mapsto & BC \end{array}.$$

The group $\overline{\langle A_s\rangle}^z \times \overline{\langle A_u\rangle}^z$ can be interpreted as a linear matrix group, for instance as a subgroup of $\mathrm{GL}(2n,\mathbb{C})$ making $\overline{\langle A_s\rangle}^z$ (resp. $\overline{\langle A_u\rangle}^z$) act on the first (resp. last) n coordinates. We claim that it is a morphism of groups and an algebraic morphism, i.e. a morphism of algebraic groups. It is clear that $\times$ is an algebraic morphism. Moreover $\times$ is a morphism of groups since the elements of $\overline{\langle A_s\rangle}^z$ commute with the elements of $\overline{\langle A_u\rangle}^z$. Now we can use the following result:

Proposition 2.14 (cf. [3, Corollary 1.4, p. 47])**.** *Let $\alpha : G \to G'$ be a morphism of matrix algebraic groups. Then $\alpha(G)$ is an algebraic group.*

Remark 2.15. Given a subset M of $\mathrm{GL}(n,\mathbb{C})$ we denote by $\mathcal{A}(M)$ the intersection of the algebraic groups containing M. Clearly $\mathcal{A}(M)$ is an algebraic group, the smallest one containing M. Let $\alpha : G \to G'$ be a morphism of matrix algebraic groups and $M \subset G$. We obtain $\alpha(\mathcal{A}(M)) = \mathcal{A}(\alpha(M))$. Indeed $\alpha(\mathcal{A}(M))$ is an algebraic group containing $\alpha(M)$ by Proposition 2.14 and then $\mathcal{A}(\alpha(M)) \subset \alpha(\mathcal{A}(M))$. Moreover since α is continuous in the Zariski topology we obtain that $\alpha^{-1}(\mathcal{A}(\alpha(M)))$ is an algebraic group containing M and then $\mathcal{A}(M)$. We deduce $\alpha(\mathcal{A}(M)) \subset \mathcal{A}(\alpha(M))$.

Proof of Proposition 2.12. This is just a recap of the discussion above. The semisimple and unipotent parts A_s and A_u of A belong to $\overline{\langle A\rangle}^z$ by Chevalley's theorem. Thus $\overline{\langle A_s\rangle}^z$, $\overline{\langle A_u\rangle}^z$ and then $\times(\overline{\langle A_s\rangle}^z \times \overline{\langle A_u\rangle}^z)$ are contained in $\overline{\langle A\rangle}^z$. Since $\times(\overline{\langle A_s\rangle}^z \times \overline{\langle A_u\rangle}^z)$ is algebraic and contains the matrix A, we obtain

$$\times(\overline{\langle A_s\rangle}^z \times \overline{\langle A_u\rangle}^z) = \overline{\langle A\rangle}^z.$$

The map $\times$ is injective. Indeed if $\times(B,C) = BC = Id$ for some $B \in \overline{\langle A_s\rangle}^z$ and $C \in \overline{\langle A_u\rangle}^z$ then BC is a Jordan-Chevalley decomposition of the identity map. Therefore we obtain $B = Id$ and $C = Id$. As a consequence $\overline{\langle A\rangle}^z$ is isomorphic to $\overline{\langle A_s\rangle}^z \times \overline{\langle A_u\rangle}^z$. □

Exercise 2.6. Let G be an abelian subgroup of $\mathrm{GL}(n,\mathbb{C})$. Show

- The set of semisimple elements of G is a group.
- The set of unipotent elements of G is a group.
- Every semisimple element of G commutes with every unipotent element of G.

The group $\overline{\langle A\rangle}^z$ satisfies the conditions of Exercise 2.6 by Proposition 2.12. The goal of the exercise is extending this property to every abelian matrix group.

Remark 2.16. Is there any other distinguished class of groups that satisfies the properties in Exercise 2.6? Nilpotent groups do (Suprunenko and Tyskevic, cf. [27, Theorem 7.11, p. 97]).

2.5 Some elementary properties of linear algebraic groups

Let G be a linear algebraic matrix subgroup of $\mathrm{GL}(n,\mathbb{C})$. We introduce some properties of algebraic matrix groups that generalize in the setting of local diffeomorphisms. By no means the list is supposed to be exhaustive.

Definition 2.17. We denote by G_0 the connected component of the identity transformation Id.

Proposition 2.18 (cf. [3, Chapter I.1, p. 46])**.** *Let G be a linear algebraic matrix subgroup of $\mathrm{GL}(n,\mathbb{C})$. Then*

- *G is a smooth manifold.*
- *G_0 is a closed finite index normal subgroup of G.*
- *Every algebraic subgroup of G of finite index contains G_0.*

In particular G_0 is a linear algebraic group.

Remark 2.19. When we use topological terms as "closed" or "connected" in Proposition 2.18 we are referring to the Zariski topology. Anyway, an algebraic set is connected in the Zariski topology if and only if it is connected in the usual topology. This can be deduced from the connectedness in the usual topology of irreducible algebraic sets (cf. [25, Chapter VII.2.2, Theorem 1]).

Definition 2.20. Let G be a linear algebraic group (or a Lie group). We define

$$L(G) = \{A \in \mathrm{End}(\mathbb{C}^n) : \exp(tA) \in G \text{ for all } t \in \mathbb{C}\}.$$

Equivalently $L(G)$ is the tangent space $T_{Id}G$ of G at Id. We say that $L(G)$ is the Lie algebra of the group G.

Exercise 2.7. Show the equivalence between the two definitions of $L(G)$.

The definition is justified by the next result.

Proposition 2.21. *$L(G)$ is a complex Lie algebra where the Lie bracket $[A,B]$ is defined by $AB-BA$.*

The definition implies that the set $\exp(L(G))$ is contained in G_0. Even if these sets can be different we have

Proposition 2.22 (cf. [26, section 8.6, p. 177])**.** *Let G be a linear algebraic group (or more generally a Lie group). Then $G_0 = \langle \exp(L(G)) \rangle$.*

Exercise 2.8. Show that the Lie algebra of the algebraic group

$$\mathrm{SL}(2,\mathbb{C}) = \{A \in \mathrm{GL}(2,\mathbb{C}) : \det A = 1\}$$

is equal to $\mathrm{sl}(2,\mathbb{C}) = \{A \in \mathrm{End}(\mathbb{C}^2) : \mathrm{Tr}(A) = 0\}$.

Exercise 2.9. Show that any matrix in $\exp(\mathrm{sl}(2,\mathbb{C}))$ has Jordan normal form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Show that

$$\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$$

does not belong to $\exp(\mathrm{sl}(2,\mathbb{C}))$ and that $\exp : \mathrm{sl}(2,\mathbb{C}) \to \mathrm{SL}(2,\mathbb{C})$ is not surjective.

Let us applicate the previous definitions to our test examples.

Remark 2.23. Let $A \in \mathrm{GL}(n,\mathbb{C})$ be unipotent. The Lie algebra of $\overline{\langle A\rangle}^z$ is the 1-dimensional complex vector space generated by the infinitesimal generator $\log A$ of A. The group $\overline{\langle A\rangle}^z$ is connected, indeed it is isomorphic to $\mathbb{C}$.

Exercise 2.10. Let G be a linear algebraic group. Consider a unipotent element A of G. Show that A belongs to G_0.

Exercise 2.11. Consider the diagonal matrix $A = \mathrm{diag}(\underline{\lambda})$ where $\underline{\lambda} = (\lambda_1, \ldots, \lambda_n) \in (\mathbb{C}^*)^n$. Let $J_{\underline{\lambda}}$ the subgroup of $\mathbb{Z}^n$ of definition 2.7. We define $J'_{\underline{\lambda}}$ as the intersection of the $\mathbb{Q}$-vector space generated by $J_{\underline{\lambda}}$ and $\mathbb{Z}^n$. Show that the group

$$\{\underline{\mu} \in (\mathbb{C}^*)^n : \chi_{k_1,\ldots,k_n}(\underline{\mu}) = 1 \text{ for all } (k_1,\ldots,k_n) \in J'_{\underline{\lambda}}\}$$

is equal to the connected component of the identity of $\overline{\langle A\rangle}^z$. Show

$$L(\overline{\langle A\rangle}^z) = \{\mathrm{diag}(\mu_1,\ldots,\mu_n) : k_1\mu_1 + \ldots + k_n\mu_n = 0 \text{ for all } (k_1,\ldots,k_n) \in J_{\underline{\lambda}}\}.$$

Let us show a result that will be useful later on. We obtain the Zariski-closure of $\langle A\rangle$ as a Zariski-closure of groups generated by iterates of A.

Proposition 2.24. *Let $A \in \mathrm{GL}(n,\mathbb{C})$. Consider $k \in \mathbb{Z} \setminus \{0\}$ such that $A^k \in \overline{\langle A\rangle}_0^z$. Then we obtain $\overline{\langle A^k\rangle}^z = \overline{\langle A\rangle}_0^z$.*

Proof. We denote $H = \overline{\langle A^k\rangle}^z$. Since $A\langle A^k\rangle A^{-1} = \langle A^k\rangle$ we deduce $AHA^{-1} = H$. The group H is a finite index subgroup of $\langle H, A\rangle$. Morever since H is algebraic, the group $\langle H, A\rangle$ is algebraic; indeed $\langle H, A\rangle$ is the algebraic closure of $\langle A\rangle$. The last item of Proposition 2.18 implies $\overline{\langle A\rangle}_0^z \subset H$. Since $H \subset \overline{\langle A\rangle}_0^z$ by the choice of k, we obtain $\overline{\langle A^k\rangle}^z = \overline{\langle A\rangle}_0^z$. □

Let $\mathfrak{g}$ be a Lie subalgebra of $\mathrm{End}(\mathbb{C}^n)$. When is $\mathfrak{g}$ algebraic? More precisely, when is $\mathfrak{g}$ the Lie algebra of an algebraic matrix group? There is a complete answer for this question (cf. [3, Chapter II, section 7]). Let us focus though on a simpler problem in the next exercise.

Exercise 2.12. Let $\underline{\mu} = (\mu_1, \dots, \mu_n) \in \mathbb{C}^n$. Suppose that $\mu_1, \dots, \mu_n$ are $\mathbb{Q}$-linearly independent. Show that the Lie algebra generated by $\mathrm{diag}(\underline{\mu})$ is non-algebraic.

2.6 Classical results

Let us introduce well-known results by Lie and Kolchin about the structure of groups of unipotent elements and solvable groups.

Theorem 2.25 (Kolchin, cf. [24, chapter V, p. 35])**.** *Let V be a finite dimensional vector space over a field K. Let G be a subgroup of $\mathrm{GL}(V)$ such that each element $g \in G$ is unipotent. Then up to a change of base G is a group of upper triangular matrices.*

Theorem 2.26 (Lie-Kolchin, cf. [8, section 17.6, p. 113])**.** *Let G be a solvable connected subgroup of $\mathrm{GL}(n, F)$ where F is an algebraically closed field. Then up to a change of base G is a group of upper triangular matrices.*

2.7 More properties of algebraic groups

We continue describing the properties of the algebraic closure of a subgroup of $\mathrm{GL}(n, \mathbb{C})$.

Definition 2.27. Let G be a subgroup of $\mathrm{GL}(n, \mathbb{C})$. We denote by G_u the subset of G of unipotent transformations. We say that the group G is *unipotent* if $G = G_u$.

Definition 2.28. Let G be a group. We define the *derived group* $G^{(1)}$ (or $[G, G]$) of G as

$$G^{(1)} = \langle fgf^{-1}g^{-1} : f, g \in G \rangle,$$

i.e. $G^{(1)}$ is the subgroup generated by the commutators of elements of G. We define $G^{(2)} = [G^{(1)}, G^{(1)}]$, $G^{(3)} = [G^{(2)}, G^{(2)}], \dots$ recursively. We denote $G^{(0)} = G$.

Definition 2.29. We say that G is *solvable* if there exists $p \in \mathbb{N} \cup \{0\}$ such that $G^{(p)} = \{1\}$. Moreover the minimum such p is called the *derived length* $\ell(G)$ of G. We define $\ell(G) = \infty$ if G is non-solvable.

Lemma 2.30. *Let G be a subgroup of $\mathrm{GL}(n, \mathbb{C})$. Then*

- $\ell(\overline{G}^z) = \ell(G)$.
- $(\overline{G}^z)_u \subset (\overline{G}^z)_0$.
- $\overline{G}^z = (\overline{G}^z)_u$ *if* G *is unipotent.*
- $(\overline{G}^z)_u$ *is a closed normal connected subgroup of the group* $\overline{G}^z$ *if* G *is solvable.*

Proof. Since $\ell(G) \leq \ell(\overline{G}^z)$ it suffices to prove that $G^{(p)} = \{Id\}$ implies $(\overline{G}^z)^{(p)} = \{Id\}$. The property $G^{(p)} = \{Id\}$ is equivalent to a system of algebraic equations. The system is also satisfied for $\overline{G}^z$ by definition of the Zariski-closure. Hence we obtain $(\overline{G}^z)^{(p)} = \{Id\}$.

The second item is a consequence of Exercise 2.10.

We claim that $(\overline{G}^z)_u$ is an algebraic subset of $\overline{G}^z$. Indeed it is the subset of $\overline{G}^z$ defined by the equation $(A - Id)^n = 0$ that is algebraic in the coefficients of A. Let G be a unipotent group. We have $G \subset (\overline{G}^z)_u \subset \overline{G}^z$. Since $\overline{G}^z$ is the minimal algebraic set containing G, we deduce $(\overline{G}^z)_u = \overline{G}^z$.

Let us show the last item. We already proved that $(\overline{G}^z)_u$ is closed (or equivalently algebraic). Given $A \in (\overline{G}^z)_u$ we have

$$\{A^t : t \in \mathbb{C}\} = \overline{\langle A \rangle}^z \subset \overline{(\overline{G}^z)_u}^z = (\overline{G}^z)_u$$

and $\{A^t : t \in \mathbb{C}\}$ is a connected set containing Id and A. Therefore $(\overline{G}^z)_u$ coincides with its connected component of Id and it is connected. It is clear that $(\overline{G}^z)_u$ is normal as a set, meaning $A(\overline{G}^z)_u A^{-1} = (\overline{G}^z)_u$ since a conjugate of a unipotent matrix is also unipotent. Notice that we did not use so far that G is solvable, we will use it now to show that $(\overline{G}^z)_u$ is a subgroup.

The group $\overline{G}^z$ is solvable by the first item and $(\overline{G}^z)_0$ is solvable too since it is a subgroup of $\overline{G}^z$. The group $(\overline{G}^z)_0$ is connected by definition, hence we apply Lie-Kolchin's theorem; we can suppose that it is a group of upper triangular matrices up to linear conjugacy. The eigenvalues of an upper triangular matrix are exactly the coefficients in the principal diagonal of the matrix. Thus the elements of $(\overline{G}^z)_u$ are the elements of $(\overline{G}^z)_0$ that have all the elements of the diagonal principal equal to 1. The product of two elements of $(\overline{G}^z)_u$ is still an upper triangular matrix whose principal diagonal coefficients are all equal to 1 and in particular belongs to $(\overline{G}^z)_u$. Analogously the inverse of an element of $(\overline{G}^z)_u$ also belongs to $(\overline{G}^z)_u$. We deduce that $(\overline{G}^z)_u$ is a group. □

Exercise 2.13. Show that the subset of unipotent elements of the algebraic group $\mathrm{GL}(n, \mathbb{C})$ is not a group.

3 Pro-algebraic groups

Inspired by matrix groups we want to define the algebraic closure of a group of local diffeomorphisms. The main problem is that groups of diffeomorphisms can be infinite dimensional. Indeed an element ϕ of $\mathrm{Diff}\,(\mathbb{C}^n,0)$ is of the form

$$\phi(x_1,\dots,x_n)=(\sum_{i_1+\dots+i_n\geq 1} a^1_{i_1\dots i_n}x_1^{i_1}\dots x_n^{i_n},\dots,\sum_{i_1+\dots+i_n\geq 1} a^n_{i_1\dots i_n}x_1^{i_1}\dots x_n^{i_n})$$

where the linear part $D_0\phi$ at 0 is an invertible matrix and there are infinitely many coefficients in the power series defining ϕ. Anyway given any degree there are finitely many coefficients up to that degree. This suggests that it could be interesting to truncate a group of diffeomorphisms up to any degree, considering the algebraic closure in each of them and then pasting the information obtained. Let us explain how to execute this strategy in this section.

The first idea is forgetting for a minute that a diffeomorphism is a dynamical object. Let us interpret a diffeomorphism as an operator in a space of functions.

Definition 3.1. We denote by $\hat{\mathcal{O}}_n$ be the local ring $\mathbb{C}[[x_1,\dots,x_n]]$ of complex formal power series in n variables. We denote by $\mathfrak{m}$ the maximal ideal of $\hat{\mathcal{O}}_n$.

Every local diffeomorphism $\phi\in\mathrm{Diff}\,(\mathbb{C}^n,0)$ induces two morphisms of $\mathbb{C}$-algebras by composition in $\hat{\mathcal{O}}_n$ and $\mathfrak{m}$ respectively:

$$\begin{array}{ccc}\hat{\mathcal{O}}_n & \to & \hat{\mathcal{O}}_n\\ f & \mapsto & f\circ\phi\end{array}\quad\text{and}\quad\begin{array}{ccc}\mathfrak{m} & \to & \mathfrak{m}\\ f & \mapsto & f\circ\phi.\end{array}\tag{1}$$

The map that associates to any $\phi\in\mathrm{Diff}\,(\mathbb{C}^n,0)$ the operator induced by ϕ in $\mathfrak{m}$ or $\hat{\mathcal{O}}_n$ is injective since ϕ is determined by the compositions $x_1\circ\phi,\dots,x_n\circ\phi$.

Instead of considering the action of $\phi\in\mathrm{Diff}\,(\mathbb{C}^n,0)$ on $\mathfrak{m}$ let us consider the action induced on the finite dimensional vector complex space $\mathfrak{m}/\mathfrak{m}^{k+1}$, i.e. on the space of k-jets. We remind the reader that $\mathfrak{m}^{k+1}$ is the $(k+1)$th-power of the ideal $\mathfrak{m}$. Intuitively we are considering the power series expansion of ϕ up to order k. More precisely we consider the element $\phi_k\in\mathrm{GL}(\mathfrak{m}/\mathfrak{m}^{k+1})$ defined by

$$\begin{array}{ccc}\mathfrak{m}/\mathfrak{m}^{k+1} & \stackrel{\phi_k}{\to} & \mathfrak{m}/\mathfrak{m}^{k+1}\\ g+\mathfrak{m}^{k+1} & \mapsto & g\circ\phi+\mathfrak{m}^{k+1}.\end{array}\tag{2}$$

Definition 3.2. We define $D_k=\{\varphi_k:\varphi\in\mathrm{Diff}(\mathbb{C}^n,0)\}$.

Remark 3.3. D_k is a subgroup of the linear group $\mathrm{GL}(\mathfrak{m}/\mathfrak{m}^{k+1})$.

Exercise 3.1. Show that D_k is the group of isomorphisms of the $\mathbb{C}$-algebra $\mathfrak{m}/\mathfrak{m}^{k+1}$.

The group D_k can be understood as an algebraic group of matrices by noticing that we have

$$D_k = \{\alpha \in \mathrm{GL}(\mathfrak{m}/\mathfrak{m}^{k+1}) : \alpha(gh) = \alpha(g)\alpha(h) \text{ for all } g, h \in \mathfrak{m}/\mathfrak{m}^{k+1}\}$$

and that fixed $g, h \in \mathfrak{m}/\mathfrak{m}^{k+1}$ the equation $\alpha(gh) = \alpha(g)\alpha(h)$ is algebraic on the coefficients of α.

3.1 Example

Let us illustrate the algebraic nature of D_2 for $n = 2$. We denote $x = x_1$ and $y = x_2$. A base of $\mathfrak{m}/\mathfrak{m}^3$ is given by the classes of the monomials of degree 1 and 2, namely x, y, x^2, xy and y^2. Any element A of $\mathrm{GL}(\mathfrak{m}/\mathfrak{m}^3)$ is represented by a 5×5 invertible matrix

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix}$$

in such a basis. Notice that

$$A(x + \mathfrak{m}^3) = a_{11}x + a_{21}y + a_{31}x^2 + a_{41}xy + a_{51}y^2 + \mathfrak{m}^3$$

and

$$A(y + \mathfrak{m}^3) = a_{12}x + a_{22}y + a_{32}x^2 + a_{42}xy + a_{52}y^2 + \mathfrak{m}^3$$

determine an element A of D_2 since x^2, xy and y^2 are products of x and y. The equation $A(x^2 + \mathfrak{m}^3) = A(x + \mathfrak{m}^3)A(x + \mathfrak{m}^3)$ implies

$$a_{13}x + a_{23}y + a_{33}x^2 + a_{43}xy + a_{53}y^2 = (a_{11}x + a_{21}y + a_{31}x^2 + a_{41}xy + a_{51}y^2)^2$$

modulo $\mathfrak{m}^3$, i.e. modulo discarding the terms of degree greater or equal than 3. In particular we obtain

$$a_{13} = 0,\ a_{23} = 0, a_{33} = a_{11}^2,\ a_{43} = 2a_{11}a_{21},\ a_{53} = a_{21}^2. \tag{3}$$

By analyzing $A(xy+\mathfrak{m}^3)=A(x+\mathfrak{m}^3)A(y+\mathfrak{m}^3)$ and $A(y^2+\mathfrak{m}^3)=A(y+\mathfrak{m}^3)A(y+\mathfrak{m}^3)$ we obtain

$$a_{14}=0,\ a_{24}=0, a_{34}=a_{11}a_{12},\ a_{44}=a_{11}a_{22}+a_{21}a_{12},\ a_{54}=a_{21}a_{22} \tag{4}$$

and

$$a_{15}=0,\ a_{25}=0, a_{35}=a_{12}^2,\ a_{45}=2a_{12}a_{22},\ a_{55}=a_{22}^2 \tag{5}$$

respectively. Equations (3), (4) and (5) determine the algebraic group D_2.

3.2 The group of formal diffeomorphisms

We can think of D_k as the truncation of the group $\mathrm{Diff}\,(\mathbb{C}^n,0)$ up to the order k. Let us study the relations between the groups D_k for $k\in\mathbb{N}$.

Consider $l\geq k\geq 1$. We want to define a natural map $\pi_{l,k}: D_l\to D_k$ for $l\geq k\geq 1$. The idea is that the truncation of a diffeomorphism up to order l provides all truncations of orders less than l. The map $\pi_{l,k}$ strips the elements of D_l of the information associated to the levels higher than k.

Definition 3.4. Given $l\geq k\geq 1$ and $A\in D_l$ we define $\pi_{l,k}(A)$ as the unique element of D_k such that

$$\begin{array}{ccc} \mathfrak{m}/\mathfrak{m}^{l+1} & \xrightarrow{A} & \mathfrak{m}/\mathfrak{m}^{l+1} \\ \downarrow & & \downarrow \\ \mathfrak{m}/\mathfrak{m}^{k+1} & \xrightarrow{\pi_{l,k}(A)} & \mathfrak{m}/\mathfrak{m}^{k+1} \end{array}$$

is commutative where the vertical arrows are the natural projections.

The map $\pi_{l,k}: D_l\to D_k$ is well-defined since every element of D_l leaves invariant every subspace of the form $\mathfrak{m}^p/\mathfrak{m}^{l+1}$ for $1\leq p\leq l+1$ and in particular $\mathfrak{m}^{k+1}/\mathfrak{m}^{l+1}$.

Exercise 3.2. Let $\phi\in\mathrm{Diff}\,(\mathbb{C}^n,0)$. Show $\pi_{l,k}(\phi_l)=\phi_k$ for $l\geq k\geq 1$.

Lemma 3.5. *The pair $((D_k)_{k\in\mathbb{N}},(\pi_{l,k})_{l\geq k\geq 1})$ is an inverse system of algebraic groups and morphisms of algebraic groups. Moreover $\pi_{l,k}$ is surjective for any $l\geq k\geq 1$.*

sketch of proof. It is a simple exercise to check out that $\pi_{l,k}$ is a morphism of algebraic groups. We are just forgetting the action of an element of D_l on $\mathfrak{m}^{k+1}/\mathfrak{m}^{l+1}$.

We have $\pi_{p,p}=Id_{|D_p}$ and $\pi_{j,l}\circ\pi_{l,k}=\pi_{j,k}$ for all $p\in\mathbb{N}$ and $j\geq l\geq k\geq 1$ by Definition 3.4.

Fix $l\geq k\geq 1$. The map $\pi_{l,k}$ is surjective, in fact given $A\in D_k$ there exists by definition $\phi\in\mathrm{Diff}\,(\mathbb{C}^n,0)$ such that $\phi_k=A$ and we have $\pi_{l,k}(\phi_l)=\phi_k=A$. □

Definition 3.6. We define the group $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ of formal diffeomorphisms as the projective limit $\varprojlim_{k\in\mathbb{N}} D_k$.

Remark 3.7. Let us remind that the elements of $\varprojlim_{k\in\mathbb{N}} D_k$ are of the form $(A_k)_{k\geq 1}$ where $A_k \in D_k$ and $\pi_{l,k}(A_l) = A_k$ for all $l \geq k \geq 1$. In particular the map

$$\begin{array}{ccc} \mathrm{Diff}\,(\mathbb{C}^n,0) & \to & \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0) \\ \phi & \mapsto & (\phi_k)_{k\geq 1} \end{array}$$

is an injective morphism of groups. In this way we see $\mathrm{Diff}\,(\mathbb{C}^n,0)$ as a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$.

Let us give a (maybe) more pleasant presentation of the group of formal diffeomorphism in which it is clear that $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ is the formal completion of $\mathrm{Diff}\,(\mathbb{C}^n,0)$.

We consider the notation $\sum a_{\underline{i}}\underline{x}^{\underline{i}}$ for formal power series where $\underline{i} = (i_1,\ldots,i_n)$ is a multi-index of degree $|\underline{i}| = i_1 + \ldots + i_n$ and $\underline{x}^{\underline{i}} = x_1^{i_1}\ldots x_n^{i_n}$. Given a power series $\sum a_{\underline{i}}\underline{x}^{\underline{i}}$ we define $j^k(\sum a_{\underline{i}}\underline{x}^{\underline{i}}) = \sum_{|\underline{i}|\leq k} a_{\underline{i}}\underline{x}^{\underline{i}}$. We define $j^k(f_1,\ldots,f_n) = (j^k f_1,\ldots,j^k f_n)$ for a n-uple of power series.

Consider the set $\overline{\mathrm{Diff}}(\mathbb{C}^n,0)$ of elements $(\phi_1,\ldots,\phi_n)$ of $\mathfrak{m}^n$ such that $(j^1\phi_1,\ldots,j^1\phi_n)$ is an invertible linar map. The set of elements of $\overline{\mathrm{Diff}}(\mathbb{C}^n,0)$ such that all their coordinates are convergent power series coincides with the group $\mathrm{Diff}\,(\mathbb{C}^n,0)$ by the inverse function theorem. It would be natural to define $\overline{\mathrm{Diff}}(\mathbb{C}^n,0)$ as the group of formal diffeomorphisms too. This is not an issue in our approach since $\varprojlim_{k\in\mathbb{N}} D_k$ and $\overline{\mathrm{Diff}}(\mathbb{C}^n,0)$ can be identified.

Exercise 3.3. Define a group operation in $\overline{\mathrm{Diff}}(\mathbb{C}^n,0)$ such that $\mathrm{Diff}\,(\mathbb{C}^n,0)$ is a subgroup of $\overline{\mathrm{Diff}}(\mathbb{C}^n,0)$.

Given

$$\overline{\eta} = \left(\sum_{|\underline{i}|\geq 1} a^1_{\underline{i}}\underline{x}^{\underline{i}},\ldots,\sum_{|\underline{i}|\geq 1} a^n_{\underline{i}}\underline{x}^{\underline{i}}\right) \in \overline{\mathrm{Diff}}(\mathbb{C}^n,0)$$

let us construct an element of $\varprojlim D_k$. The diffeomorphisms $j^l\overline{\eta}, j^k\overline{\eta} \in \mathrm{Diff}\,(\mathbb{C}^n,0)$ satisfy $(j^l\overline{\eta})_k = (j^k\overline{\eta})_k$ for any $l \geq k \geq 1$ (the action on $\mathfrak{m}/\mathfrak{m}^{k+1}$ depends on the power expansion of the diffeomorphism up to order k). We define $\eta_k = (j^k\overline{\eta})_k$ for $k \in \mathbb{N}$ and $\eta = (\eta_k)_{k\geq 1}$. Then η belongs to $\varprojlim D_k$ since

$$\pi_{l,k}(\eta_l) = \pi_{l,k}((j^l\overline{\eta})_l) = (j^l\overline{\eta})_k = (j^k\overline{\eta})_k = \eta_k$$

for all $l \geq k \geq 1$. The second equality is a consequence of $j^l\overline{\eta} \in \mathrm{Diff}\,(\mathbb{C}^n,0)$ and Remark 3.7. Resuming we associate $\eta \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ to $\overline{\eta} \in \overline{\mathrm{Diff}}(\mathbb{C}^n,0)$.

Let us describe the inverse process. Given $\eta \in \varprojlim_{k\in\mathbb{N}} D_k$ we want to interpret it in some way closer to our intuition of what a diffeomorphism is. Indeed if $\eta \in \mathrm{Diff}\,(\mathbb{C}^n,0)$ then the image of x_j by the operator defined by η (cf. Equation (1)) is the jth coordinate $x_j \circ \eta$ of η. How to obtain the jth coordinate of an element $(A_k)_{k\geq 1}$ of $\varprojlim_{k\in\mathbb{N}} D_k$? We consider the sequence $(A_k(x_j+\mathfrak{m}^{k+1}))_{k\geq 1}$. Since it belongs to $\mathfrak{m} = \varprojlim \mathfrak{m}/\mathfrak{m}^{k+1}$, we can interpret $(A_k(x_j+\mathfrak{m}^{k+1}))_{k\geq 1}$ as an element η_j of $\mathfrak{m}$. Moreover $j^1\eta_1+\mathfrak{m}^2,\dots,j^1\eta_n+\mathfrak{m}^2$ is the image by A_1 of the basis $x_1+\mathfrak{m}^2,\dots,x_n+\mathfrak{m}^2$. Since A_1 is invertible, $(j^1\eta_1,\dots,j^1\eta_n)$ is also an invertible linear map. We deduce that

$$\overline{\eta}(x_1,\dots,x_n) := (\eta_1(x_1,\dots,x_n),\dots,\eta_n(x_1,\dots,x_n))$$

belongs to $\overline{\mathrm{Diff}}(\mathbb{C}^n,0)$.

Exercise 3.4. Show that the correspondences $\overline{\eta} \to \eta$ and $\eta \to \overline{\eta}$ described above are inverses of each other. Deduce that $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ and $\overline{\mathrm{Diff}}(\mathbb{C}^n,0)$ are isomorphic groups.

3.3 The Jordan-Chevalley decomposition

Let us see that the Jordan-Chevalley decomposition is compatible with the inverse system $((D_k)_{k\in\mathbb{N}},(\pi_{l,k})_{l\geq k\geq 1})$ and as a consequence formal diffeomorphisms possess a multiplicative Jordan decomposition.

Let $\phi \in \mathrm{Diff}\,(\mathbb{C}^n,0)$ (or $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$). We already know that ϕ defines an element $(\phi_k)_{k\geq 1}$ of $\varprojlim D_k$. (cf. Equation (2)). Since $\phi_k \in \mathrm{GL}(\mathfrak{m}/\mathfrak{m}^{k+1})$ we can consider its semisimple-unipotent decomposition $\phi_k = \phi_{k,s}\phi_{k,u} = \phi_{k,u}\phi_{k,s}$. The elements of the decomposition belong to D_k by Chevalley's theorem.

Exercise 3.5. Let $l \geq k \geq 1$ and $A \in D_l$. Show that $\pi_{l,k}(A_s)$ is semisimple and $\pi_{l,k}(A_u)$ is unipotent.

Exercise 3.6. Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Show $\pi_{l,k}(\phi_{l,s}) = \phi_{k,s}$ and $\pi_{l,k}(\phi_{l,u}) = \phi_{k,u}$ for $l \geq k \geq 1$. Deduce that $(\phi_{k,s})_{k\geq 1}$ and $(\phi_{k,u})_{k\geq 1}$ define elements of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$.

Definition 3.8. Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. We say that ϕ is semisimple if ϕ_k is semisimple (cf. Equation (2)) for any $k \in \mathbb{N}$.

Definition 3.9. Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. We say that ϕ is unipotent if ϕ_k is unipotent (cf. Equation (2)) for any $k \in \mathbb{N}$. Given a subgroup G of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ we define G_u as its subset of unipotent elements. We say that G is unipotent if $G = G_u$. We denote by $\widehat{\mathrm{Diff}}_u(\mathbb{C}^n,0)$ the subset of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ consisting of unipotent formal diffeomorphisms.

Definition 3.10. We denote by ϕ_s (resp. ϕ_u) the element $(\phi_{k,s})_{k\geq 1}$ (resp. $(\phi_{k,u})_{k\geq 1}$) of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$.

We can summarize the previous discussion in the following result:

Proposition 3.11. *Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. There exist unique elements ϕ_s, ϕ_u of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ such that $\phi = \phi_s \circ \phi_u = \phi_u \circ \phi_s$, ϕ_s is semisimple and ϕ_u is unipotent.*

We generalized the multiplicative Jordan decomposition for diffeomorphisms. Anyway, it is difficult to check out whether a diffeomorphism is semisimple or unipotent by applying the definition since it depends on their actions on all the jet spaces. Let us characterize the decomposition in simpler terms.

Proposition 3.12. *Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Then ϕ is unipotent if and only if $j^1\phi$ is unipotent.*

Proof. The matrix of $j^1\phi$ is the transposed of the matrix of ϕ_1. Thus ϕ_1 is unipotent if and only if $j^1\phi$ is unipotent.

We have to show that ϕ_k is unipotent for any $k \in \mathbb{N}$ if and only if ϕ_1 is unipotent. Let us prove the non-trivial implication. Consider the operator $\Delta : \mathfrak{m} \to \mathfrak{m}$ defined by $\Delta(f) = f \circ \phi - f$. The unipotence of ϕ_k is equivalent to the existence of some $l = l(k)$ such that $\Delta^l(\mathfrak{m}) \subset \mathfrak{m}^{k+1}$. Hence it suffices to show that given $k \in \mathbb{N}$ there exists $j_k \in \mathbb{N}$ such that $\Delta^{j_k}(\mathfrak{m}^k) \subset \mathfrak{m}^{k+1}$. The existence of j_1 is a consequence of the unipotence of ϕ_1.

We have

$$\Delta(fg) = (fg)\circ\phi - fg = (f\circ\phi - f)(g\circ\phi - g) + (f\circ\phi - f)g + f(g\circ\phi - g)$$

and then $\Delta(fg) = \Delta(f)\Delta(g) + \Delta(f)g + f\Delta(g)$. Given $j \geq 1$ we obtain

$$\Delta^j(fg) = \sum_{j\leq m+l,\ 0\leq m\leq j,\ 0\leq l\leq j} c_{jml}\Delta^m(f)\Delta^l(g) \tag{6}$$

where c_{jml} is a positive integer number independent of f and g for $j \leq m+l$, $0 \leq m \leq j$ and $0 \leq l \leq j$.

Suppose $\Delta^{j_k}(\mathfrak{m}^k) \subset \mathfrak{m}^{k+1}$ for some $k \in \mathbb{N}$. We define $j_{k+1} = j_k + j_1$. Let $f \in \mathfrak{m}^k$ and $g \in \mathfrak{m}$. Consider a non-vanishing coefficient $c_{j_{k+1}ml}$ in Equation (6). Then we have either $m \geq j_k$ or $l \geq j_1$. In the former case the term $c_{j_{k+1}ml}\Delta^m(f)\Delta^l(g)$ belongs to $\mathfrak{m}^{k+2} = \mathfrak{m}^{k+1}\mathfrak{m}$ whereas it belongs to $\mathfrak{m}^{k+2} = \mathfrak{m}^k\mathfrak{m}^2$ in the latter case. Anyway $\Delta^{j_{k+1}}(fg)$ belongs to $\mathfrak{m}^{k+2}$. Since any element of $\mathfrak{m}^{k+1}$ is of the form $f_1g_1 + \ldots + f_ag_a$ where $f_1,\ldots,f_a \in \mathfrak{m}^k$ and $g_1,\ldots,g_a \in \mathfrak{m}$, we deduce $\Delta^{j_{k+1}}(\mathfrak{m}^{k+1}) \subset \mathfrak{m}^{k+2}$. □

Next we see that a diffeomorphism is semisimple if and only if it is diagonalizable.

Proposition 3.13. *Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Then ϕ is semisimple if and only if there exists $\psi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ such that $\psi\circ\phi\circ\psi^{-1}=(\lambda_1 x_1,\dots,\lambda_n x_n)$ for some $(\lambda_1,\dots,\lambda_n)\in(\mathbb{C}^*)^n$.*

Proof. Let us prove the necessary condition. The formula $\eta(x_1,\dots,x_n)=(\lambda_1 x_1,\dots,\lambda_n x_n)$ defines an element η of $\mathrm{Diff}\,(\mathbb{C}^n,0)$. We claim that the transformation η_k is semisimple for any $k\in\mathbb{N}$. Indeed $x_1^{i_1}\dots x_n^{i_n}+\mathfrak{m}^{k+1}$ is an eigenvector of η_k of eigenvalue $\lambda_1^{i_1}\dots\lambda_n^{i_n}$ for $1\leq i_1+\ldots+i_n\leq k$. Since the classes of the monomials define a basis of $\mathfrak{m}/\mathfrak{m}^{k+1}$, we deduce that there exists a basis of eigenvectors for η_k. Since ϕ_k is conjugated to η_k by a linear map, ϕ_k is semisimple for any $k\in\mathbb{N}$.

Let us show the sufficient condition. Since ϕ_1 is semisimple there exists a linear map ψ_1 such that $\psi_1\circ j^1\phi\circ\psi_1^{-1}=(\lambda_1 x_1,\dots,\lambda_n x_n)$ for some $(\lambda_1,\dots,\lambda_n)\in(\mathbb{C}^*)^n$. We denote $\eta(x_1,\dots,x_n)=(\lambda_1 x_1,\dots,\lambda_n x_n)$. Let us see that if there exists $\psi_k\in\mathrm{Diff}\,(\mathbb{C}^n,0)$ such that $\psi_k\circ\phi\circ\psi_k^{-1}$ is equal to η modulo $\mathfrak{m}^{k+1}$ (or in other words $(\psi_k\circ\phi\circ\psi_k^{-1})_k=\eta_k$) then there exists $\psi_{k+1}\in\mathrm{Diff}\,(\mathbb{C}^n,0)$ such that $\psi_{k+1}\circ\phi\circ\psi_{k+1}^{-1}$ is equal to η modulo $\mathfrak{m}^{k+2}$. Moreover we can choose ψ_{k+1} such that it is equal to ψ_k modulo $\mathfrak{m}^{k+1}$. This result implies that $(\psi_k)_{k\geq 1}$ defines an element of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ such that $\psi\circ\phi\circ\psi^{-1}=\eta$.

We replace ϕ with $\psi_k\circ\phi\circ\psi_k^{-1}$ without lack of generality. We say that $(i_1\dots i_n;l)$ is resonant and we denote $(i_1\dots i_n;l)\in R$ if $\lambda_l=\lambda_1^{i_1}\dots\lambda_n^{i_n}$. We define

$$S=\left(\lambda_1 x_1+\sum_{|\underline{i}|=k+1,\ (\underline{i};1)\notin R} a^1_{\underline{i}}\underline{x}^{\underline{i}},\dots,\lambda_n x_n+\sum_{|\underline{i}|=k+1,\ (\underline{i};n)\notin R} a^n_{\underline{i}}\underline{x}^{\underline{i}}\right)$$

and

$$U=\left(x_1+\sum_{|\underline{i}|=k+1,\ (\underline{i};1)\in R}\lambda_1^{-1}a^1_{\underline{i}}\underline{x}^{\underline{i}},\dots,x_n+\sum_{|\underline{i}|=k+1,\ (\underline{i};n)\in R}\lambda_n^{-1}a^n_{\underline{i}}\underline{x}^{\underline{i}}\right).$$

We have $j^{k+1}\phi=j^{k+1}(S\circ U)=j^{k+1}(U\circ S)$. It is clear that U_{k+1} is unipotent by Proposition 3.12. Suppose that we prove the existence of $\alpha_{k+1}\in\mathrm{Diff}\,(\mathbb{C}^n,0)$ that is equal to Id modulo $\mathfrak{m}^{k+1}$ and such that $\alpha_{k+1}\circ S\circ\alpha_{k+1}^{-1}$ coincides with η modulo $\mathfrak{m}^{k+2}$. Then it is clear that S_{k+1} is semisimple by the necessary condition and $S_{k+1}U_{k+1}$ is the Jordan-Chevalley decomposition of ϕ_{k+1}. Since ϕ_{k+1} is semisimple by hypothesis, we obtain $U_{k+1}\equiv Id$ and then $U\equiv Id$. In particular $\alpha_{k+1}\circ\phi\circ\alpha_{k+1}^{-1}$ coincides with η modulo $\mathfrak{m}^{k+2}$.

Let us diagonalize S modulo $\mathfrak{m}^{k+2}$. We define

$$\alpha_{k+1}=\left(x_1+\sum_{|\underline{i}|=k+1,\ (\underline{i};1)\notin R}\frac{a^1_{\underline{i}}}{\lambda_1-\underline{\lambda}^{\underline{i}}}\underline{x}^{\underline{i}},\dots,x_n+\sum_{|\underline{i}|=k+1,\ (\underline{i};n)\notin R}\frac{a^n_{\underline{i}}}{\lambda_n-\underline{\lambda}^{\underline{i}}}\underline{x}^{\underline{i}}\right).$$

The diffeomorphism $\alpha_{k+1} \circ S \circ \alpha_{k+1}^{-1}$ coincides with η modulo $\mathfrak{m}^{k+2}$. □

3.4 Formal vector fields

We want to apply the theory of linear algebraic groups to subgroups of Diff $(\mathbb{C}^n, 0)$. We will associate Lie algebras to (yet to be defined) Zariski-closures of subgroups of Diff $(\mathbb{C}^n, 0)$. The algebraic closures are not necessarily contained in Diff $(\mathbb{C}^n, 0)$ even for subgroups of Diff $(\mathbb{C}^n, 0)$; we need to consider divergent formal diffeomorphisms in the Zariski-closure. As a consequence the Lie algebras of the Zariski-closure of a subgroup of Diff $(\mathbb{C}^n, 0)$ can not be considered in general as Lie algebras of analytic vector fields. It is necessary to consider formal vector fields.

Let us denote by $\mathfrak{X}(\mathbb{C}^n, 0)$ the Lie algebra of (singular) local vector fields defined in the neighborhood of 0 in $\mathbb{C}^n$. An element X of $\mathfrak{X}(\mathbb{C}^n, 0)$ can be interpreted as a derivation of the $\mathbb{C}$-algebra $\mathcal{O}_n$ such that X preserves the maximal ideal of $\mathcal{O}_n$. Naturally the Lie algebra $\hat{\mathfrak{X}}(\mathbb{C}^n, 0)$ of formal vector fields in n variables is the set of derivations X of $\hat{\mathcal{O}}_n$ such that $X(\mathfrak{m}) \subset \mathfrak{m}$. A formal vector field $X \in \hat{\mathfrak{X}}(\mathbb{C}^n, 0)$ is determined by $X(x_1), X(x_2), \ldots, X(x_n)$. We obtain

$$X = X(x_1)\frac{\partial}{\partial x_1} + \ldots + X(x_n)\frac{\partial}{\partial x_n}. \tag{7}$$

Definition 3.14. We define L_k as the Lie algebra of derivations of the $\mathbb{C}$-algebra $\mathfrak{m}/\mathfrak{m}^{k+1}$.

Exercise 3.7. Show that L_k is the Lie algebra of D_k for any $k \in \mathbb{N}$.

Analogously as for formal diffeomorphisms the Lie algebra $\hat{\mathfrak{X}}(\mathbb{C}^n, 0)$ can be understood as a projective limit $\varprojlim_{k\in\mathbb{N}} L_k$. Given $X \in \hat{\mathfrak{X}}(\mathbb{C}^n, 0)$ consider the element $(X_k)_{k\geq 1}$ that defines in $\varprojlim L_k$. Since L_k is the Lie algebra of D_k for any $k \in \mathbb{N}$, we obtain that $(\exp(X_k))_{k\geq 1}$ is a formal diffeomorphism φ. Equivalently given $t \in \mathbb{C}$ the expression

$$\exp(tX) = \left(\sum_{j=0}^{\infty} \frac{t^j}{j!} X^j(x_1), \ldots, \sum_{j=0}^{\infty} \frac{t^j}{j!} X^j(x_n)\right) \tag{8}$$

defines the exponential of tX where $X^0(f) = f$ and $X^{j+1}(f) = X(X^j(f))$ for all $f \in \hat{\mathcal{O}}_n$ and $j \geq 0$. Equation (8) has to be interpreted as an equality of operators. On the one hand the image of x_k by the operator defined by $\exp(tX)$ is equal to $x_k \circ \exp(tX)$ by definition of operator induced by a (maybe formal) diffeomorphism. On the other hand it has to be $\sum_{j=0}^{\infty}(tX)^j(x_k)/j!$ by definition of the exponential of the operator tX.

Definition 3.15. We say that a formal vector field $X \in \hat{\mathfrak{X}}(\mathbb{C}^n, 0)$ is nilpotent if $j^1 X$ is a linear nilpotent vector field (cf. Equation (7)). We denote by $\hat{\mathfrak{X}}_N(\mathbb{C}^n, 0)$ the set of nilpotent formal vector fields.

Remark 3.16. Let $X = (X_k)_{k\geq 1} \in \hat{\mathfrak{X}}(\mathbb{C}^n, 0)$. Then X_k is nilpotent (as an element of L_k) for any $k \in \mathbb{N}$ if and only if X_1 is nilpotent. This result is the analogue of Proposition 3.12 for formal vector fields. The proof is similar (but simpler) than for diffeomorphisms.

It is easier to deal with unipotent diffeomorphisms, instead of general ones, since the formal properties of formal unipotent diffeomorphisms and formal nilpotent vector fields are analogous.

Proposition 3.17 (cf. [6, 14])**.** *The image of $\hat{\mathfrak{X}}_N(\mathbb{C}^n, 0)$ by the exponential map is equal to $\widehat{\mathrm{Diff}}_u(\mathbb{C}^n, 0)$ and $\exp : \hat{\mathfrak{X}}_N(\mathbb{C}^n, 0) \to \widehat{\mathrm{Diff}}_u(\mathbb{C}^n, 0)$ is a bijection.*

Proof. The fundamental remark behind the proof is that the exponential establishes a bijection from nilpotent matrices to unipotent matrices. The other ingredient is that L_k is the Lie algebra of D_k.

Consider $X = (X_k)_{k\geq 1} \in \hat{\mathfrak{X}}_N(\mathbb{C}^n, 0)$. Its exponential $\exp(X) = (\exp(X_k))_{k\geq 1}$ is a unipotent formal diffeomorphism since $\exp(X_k)$ is unipotent and belongs to D_k for any $k \in \mathbb{N}$.

Let $\phi \in \widehat{\mathrm{Diff}}_u(\mathbb{C}^n, 0)$. The map ϕ_k is unipotent for $k \geq 1$ by definition. The infinitesimal generator $\log \phi_k$ is nilpotent by construction. Moreover $\log \phi_k$ is in the Lie algebra of $\overline{\langle \phi_k \rangle}^z$ since this group is equal to $\{\exp(t \log \phi_k) : t \in \mathbb{C}\}$ by Proposition 2.4. Since $\overline{\langle \phi_k \rangle}^z \subset D_k$, $\log \phi_k$ belongs to the Lie algebra L_k of D_k. Therefore $(\log \phi_k)_{k\geq 1}$ is a nilpotent element of $\hat{\mathfrak{X}}(\mathbb{C}^n, 0)$ whose exponential is equal to ϕ.

It is clear that the correspondences that we defined are inverse of each other. □

Definition 3.18. Given $\varphi \in \widehat{\mathrm{Diff}}_u(\mathbb{C}^n, 0)$ we define its *infinitesimal generator* $\log \varphi$ as the unique element of $\hat{\mathfrak{X}}_N(\mathbb{C}^n, 0)$ such that $\varphi = \exp(\log \varphi)$. We define the 1-parameter group $(\varphi^t)_{t\in\mathbb{C}}$ by $\varphi^t = \exp(t \log \varphi)$.

It is known by results of Baker, Ecalle and Liverpool that generically the infinitesimal generator of a local diffeomorphism is a divergent vector field [1] [6] [10] (cf. Remark 3.31).

3.5 Construction of the algebraic closure

In this section we construct the Zariski-closure of a subgroup of $\widehat{\mathrm{Diff}}(\mathbb{C}^n, 0)$ and describe its basic properties.

Definition 3.19. We consider the $\mathfrak{m}$-adic topology, also known as the Krull topology, in $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. The sets of the form

$$U_{k,\varphi}=\{\eta\in\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0):j^k\eta=j^k\varphi\}$$

for $k\in\mathbb{N}$ and $\varphi\in\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ provide a fundamental system of open sets of the topology. A sequence $(\eta(j))_{j\in\mathbb{N}}$ in $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ converges to $\eta\in\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ if given any $k\in\mathbb{N}$ then there exists $m(k)$ such that $j^k\eta(m)=j^k\eta$ for any $m\geq m(k)$.

Definition 3.20. Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. We define $G_k=\overline{\{\phi_k:\phi\in G\}}^z$.

Lemma 3.21. *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Then we obtain $\pi_{l,k}(G_l)=G_k$ for all $l\geq k\geq 1$.*

Proof. The map $\pi_{l,k}:D_l\to D_k$ is a surjective morphism of algebraic groups for $l\geq k$ by Lemma 3.5. Moreover the image by $\pi_{l,k}$ of the smallest algebraic group of $\mathrm{GL}(\mathfrak{m}/\mathfrak{m}^{l+1})$ containing $\{\varphi_l:\varphi\in G\}$ is the smallest algebraic group of $\mathrm{GL}(\mathfrak{m}/\mathfrak{m}^{k+1})$ that contains $\{\varphi_k:\varphi\in G\}$ by Remark 2.15. Hence we have $\pi_{l,k}(G_l)=G_k$ if $l\geq k$. □

Definition 3.22. Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. We define $\overline{G}^z$ (or $\overline{G}^{(0)}$) as $\varprojlim_{k\in\mathbb{N}}G_k$, more precisely $\overline{G}^z$ is the subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ defined by

$$\overline{G}^z=\{\varphi\in\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0):\varphi_k\in G_k\text{ for all }k\in\mathbb{N}\}.$$

We say that G is *pro-algebraic* if $G=\overline{G}^z$.

The group $\overline{G}^z$ is the (pro-)algebraic closure of G. It is a projective limit of algebraic groups.

Exercise 3.8. Show that the pro-algebraic closure of a subgroup G of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ is pro-algebraic.

The next results are technical lemmas that we use to characterize the pro-algebraic subgroups of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$.

Lemma 3.23. *Let H_k be an algebraic subgroup of D_k for $k\in\mathbb{N}$. Suppose $\pi_{l,k}(H_l)=H_k$ for all $l\geq k\geq 1$. Then $\varprojlim_{k\in\mathbb{N}}H_k$ is a pro-algebraic subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Moreover the natural map $\varprojlim H_j\to H_k$ is surjective for any $k\in\mathbb{N}$.*

Proof. The inverse limit $\varprojlim H_k$ is contained in $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0) = \varprojlim D_k$.

An inverse system $(S_k)_{k\in\mathbb{N}}$ of non-empty sets and surjective maps indexed by the natural numbers satisfies that the natural projections $\varprojlim_{j\in\mathbb{N}} S_j \to S_k$ are surjective for any $k \in \mathbb{N}$. Since $(\pi_{l,k})_{|H_l} : H_l \to H_k$ is surjective for $l \geq k \geq 1$, the natural map $\varprojlim_{j\in\mathbb{N}} H_j \to H_k$ is surjective for any $k \in \mathbb{N}$. In particular we have $\{\varphi_k : \varphi \in \varprojlim H_j\} = H_k$ for $k \in \mathbb{N}$ and then $\overline{(\varprojlim H_k)}^{(0)} = \varprojlim H_k$. □

Remark 3.24. Let us consider an example. Consider the group

$$\widehat{\mathrm{Diff}}_1(\mathbb{C}^n,0) := \{\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0) : j^1\phi = Id\}$$

of formal tangent to the identity diffeomorphisms. Denote $H_k = \{A \in D_k : \pi_{k,1}(A) = Id\}$. It is an algebraic subgroup of D_k for any $k \in \mathbb{N}$. Moreover we have $\pi_{l,k}(H_l) = H_k$ for all $l \geq k \geq 1$. Since $\widehat{\mathrm{Diff}}_1(\mathbb{C}^n,0) = \varprojlim H_j$, it is a pro-algebraic group by Lemma 3.23.

Corollary 3.25. *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Then the natural map $\varprojlim G_j \to G_k$ is surjective for any $k \in \mathbb{N}$.*

Proof. We have $\pi_{l,k}(G_l) = G_k$ if $l \geq k$ by Lemma 3.21. The result is a consequence of Lemma 3.23. □

We provide two characterizations of pro-algebraic groups in next proposition.

Proposition 3.26. *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Then the following conditions are equivalent:*

1. *G is pro-algebraic.*
2. *$\{\varphi_k : \varphi \in G\}$ is an algebraic matrix group for any $k \in \mathbb{N}$ and G is closed in the Krull topology.*
3. *G is of the form $\varprojlim_{k\in\mathbb{N}} H_k$ where H_k is an algebraic subgroup of D_k and $\pi_{l,k}(H_l)$ is contained in H_k for all $l \geq k \geq 1$.*

Proof. Let us prove (1) $\implies$ (2). Suppose $G = \overline{G}^{(0)}$. We obtain $\{\varphi_k : \varphi \in G\} = G_k$ by Corollary 3.25. Moreover since $\overline{G}^{(0)}$ is closed in the Krull topology by construction, G is closed in the Krull topology.

Let us show (2) $\implies$ (1). The group G_k is equal to $\{\varphi_k : \varphi \in G\}$ by hypothesis for any $k \in \mathbb{N}$. We claim $\overline{G}^{(0)} \subset G$. Indeed given $\varphi \in \overline{G}^{(0)}$ and $k \in \mathbb{N}$ there exists $\eta(k) \in G$ such that $\varphi_k = (\eta(k))_k$ for any $k \in \mathbb{N}$ since $\overline{G}^{(0)} = \varprojlim\{\varphi_k : \varphi \in G\}$. In particular

$\varphi = \lim_{k\to\infty} \eta(k)$ where the limit is considered in the Krull topology. Since G is closed in the Krull topology, we obtain $\varphi \in G$. The inclusion $\overline{G}^{(0)} \subset G$ implies $G = \overline{G}^{(0)}$ and hence G is pro-algebraic. Moreover we obtain $G = \overline{G}^{(0)} = \varprojlim G_k$ and then G is the form in item (3) by Lemma 3.21. We just proved (2) $\implies$ (3).

Finally let us prove (3) $\implies$ (1). We define $H_{l,k} = \pi_{l,k}(H_l)$ for $l \geq k \geq 1$. The group $H_{l,k}$ is algebraic since it is the image of an algebraic group by a morphism of algebraic groups. Since $\pi_{l',k} = \pi_{l,k} \circ \pi_{l',l}$ for $l' \geq l \geq k \geq 1$, the sequence $(H_{l,k})_{l\geq k}$ is decreasing for any $k \in \mathbb{N}$. The sequence stabilizes by the noetherianity of the ring of regular functions of an affine algebraic variety. We denote $K_k = \cap_{l\geq k} H_{l,k}$. Given $l \geq k \geq 1$ we consider $l' \geq l$ such that $K_l = H_{l',l}$ and $K_k = H_{l',k}$. Since $\pi_{l',k} = \pi_{l,k} \circ \pi_{l',l}$, we deduce $\pi_{l,k}(K_l) = K_k$ for all $l \geq k \geq 1$. The construction implies $\varprojlim K_k = \varprojlim H_k$. Thus $\varprojlim H_k$ is pro-algebraic by Lemma 3.23. □

Remark 3.27. Proposition 3.26 is very useful to show that certain groups are pro-algebraic. For example consider a family $\{G_j\}_{j\in J}$ of pro-algebraic subgroups of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Let us see that $\cap_{j\in J} G_j$ is pro-algebraic. We have

$$\pi_{l,k}(\cap_{j\in J}(G_j)_l) \subset \cap_{j\in J}(G_j)_k \text{ for all } l \geq k \geq 1 \text{ and } \cap_{j\in J} G_j = \varprojlim \cap_{j\in J}(G_j)_k.$$

Since the intersection of algebraic matrix groups is an algebraic group, the group $\cap_{j\in J} G_j$ is pro-algebraic by item (3) of Proposition 3.26.

Remark 3.28. Invariance properties typically define pro-algebraic groups. Item (3) of Proposition 3.26 provides an easy way of proving such property. Let us present an example. Consider $f_1, \ldots, f_p \in \hat{\mathcal{O}}_n$ and

$$G = \{\varphi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0) : f_j \circ \varphi \equiv f_j \text{ for all } 1 \leq j \leq p\}.$$

We define

$$H_k = \{A \in D_k : A(f_j + \mathfrak{m}^{k+1}) = f_j + \mathfrak{m}^{k+1} \text{ for all } 1 \leq j \leq p\}$$

for $k \in \mathbb{N}$. It is clear that H_k is an algebraic subgroup of D_k for $k \in \mathbb{N}$. Moreover we have $\pi_{l,k}(H_l) \subset H_k$ for $l \geq k \geq 1$. Since $f \circ \phi - f = 0$ is equivalent to $f \circ \phi - f \in \mathfrak{m}^k$ for any $k \in \mathbb{N}$, the group $\varprojlim H_k$ is equal to G. Moreover G is pro-algebraic by Lemma 3.23.

The power of item (3) of Proposition 3.26 is that in order to show that G is pro-algebraic we do not need to find $\{\varphi_k : \varphi \in G\}$ explicitly; in particular we could have $\{\varphi_k : \varphi \in G\} \subsetneq H_k$. Moreover, it allows us to exploit that a pro-algebraic group can be expressed in several ways as an inverse limit of algebraic groups.

Let us check out that the Jordan-Chevalley decomposition holds in the context of pro-algebraic groups.

Proposition 3.29. *Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ be an element of a pro-algebraic group G. Then ϕ_s, ϕ_u belong to G.*

Proof. We have

$$\phi \in G = \overline{G}^z = \{\varphi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0) : \varphi_k \in G_k \text{ for all } k \in \mathbb{N}\}.$$

The transformations $\phi_{k,s}$ and $\phi_{k,u}$ belong to G_k for any $k \in \mathbb{N}$ by Chevalley's theorem. Thus $\phi_s = (\phi_{k,s})_{k\geq 1}$ and $\phi_u = (\phi_{k,u})_{k\geq 1}$ belong to $\varprojlim G_k$. □

Next we calculate the algebraic closure of a cyclic unipotent group.

Remark 3.30. Let us calculate $\overline{\langle\phi\rangle}^z$ for $\phi \in \widehat{\mathrm{Diff}}_u(\mathbb{C}^n,0)$. We denote $G = \langle\phi\rangle$. Since ϕ_k is unipotent for any $k \in \mathbb{N}$, the group $G_k = \overline{\langle\phi_k\rangle}^z$ is equal to the 1-parameter group $\{\phi_k^t : t \in \mathbb{C}\}$. Clearly we obtain

$$\{\exp(t\log\phi) : t \in \mathbb{C}\} \subset \overline{\langle\phi\rangle}^z.$$

Let us show the reverse inclusion. An element ψ of $\varprojlim G_j$ is of the form $(\exp(t_j \log\phi)_j)_{j\geq 1}$. In order to obtain $\overline{G}^z = \{\exp(t\log\phi) : t \in \mathbb{C}\}$ it suffices to show that $\{\exp(t\log\phi) : t \in \mathbb{C}\}$ is closed in the Krull topology. This is a consequence of the injectivity of the map

$$\begin{array}{rccc} \pi_k & : & \{\exp(t\log\phi) : t \in \mathbb{C}\} & \to & D_k \\ & & \exp(t\log\phi) & \mapsto & (\exp(t\log\phi))_k \end{array}$$

for some $k \in \mathbb{N}$. The map π_k is trivially injective for any $k \in \mathbb{N}$ if $\log\phi \equiv 0$. Otherwise consider $k \in \mathbb{N}$ such that $(\log\phi)_k \not\equiv 0$. The map π_k is injective since $(\exp(t\log\phi))_k = Id$ implies $t(\log\phi)_k = 0$ and then $t = 0$.

Remark 3.31. Let $\phi \in \widehat{\mathrm{Diff}}_u(\mathbb{C}^n,0)$. Since $j^1\log\phi$ is nilpotent, it is equal to $\sum_{j=1}^{n-1}\delta_j x_{j+1}\frac{\partial}{\partial x_j}$ up to a linear change of coordinates where $\delta_j \in \{0,1\}$ for any $1 \leq j < n$. Let us define $\mathrm{ord}(x_j) = n-1+j$ for $1 \leq j \leq n$, $\mathrm{ord}(0) = \infty$ and then

$$\mathrm{ord}\left(\sum_{|\underline{i}|\geq 1} a_{\underline{i}} x^{\underline{i}}\right) = \min\left\{\sum_{j=1}^{n} i_j(n-1+j) : a_{\underline{i}} \neq 0\right\} \text{ if } \sum_{|\underline{i}|\geq 1} a_{\underline{i}} x^{\underline{i}} \neq 0.$$

The property $\mathrm{ord}(x_1) < \ldots < \mathrm{ord}(x_n) < 2\mathrm{ord}(x_1)$ implies $\mathrm{ord}(f) < \mathrm{ord}((\log\phi)(f))$ for any $f \in \mathfrak{m}$. The minimum possible order for a monomial is n whereas the maximum possible

order for a monomial of degree less or equal than j is $(2n-1)j$. Since applying $\log\phi$ increases the order, we obtain $(\log\phi)^{(2n-1)j-n+1}(\mathfrak{m}) \subset \mathfrak{m}^{j+1}$. Thus

$$\exp(t\log\phi) = \left(\sum_{|\underline{i}|\geq 1} a^1_{\underline{i}}(t)x^{\underline{i}}, \ldots, \sum_{|\underline{i}|\geq 1} a^n_{\underline{i}}(t)x^{\underline{i}}\right)$$

satisfies $a^k_{\underline{i}}(t) \in \mathbb{C}[t]$ and $\deg a^k_{\underline{i}} \leq |\underline{i}|(2n-1) - n$ for every choice of $\underline{i}$ and k. The degree of $a^k_{\underline{i}}$ is bounded by a linear function of $|\underline{i}|$. This property induces a dichotomy: either $\exp(t\log\phi)$ converges only for t in a polar set (that is, a set of logarithmic capacity 0) or $\log\phi$ converges [17], cf. [22]. A polar set has vanishing Hausdorff dimension and in particular zero Lebesgue measure. Generically $\overline{\langle\phi\rangle}^z$ contains (many) divergent elements.

Remark 3.32. Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ be a semisimple formal diffeomorphism. There exists a formal change of coordinates $\psi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ such that $\psi\circ\phi\circ\psi^{-1} = (\lambda_1 x_1, \ldots, \lambda_n x_n)$ for some $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{C}^*)^n$ The group $\overline{\langle\phi\rangle}^z$ is equal to $\psi^{-1}\circ G_{\underline{\lambda}}\circ\psi$ (cf. Definition 2.7).

Exercise 3.9. Show the analogue of Proposition 2.12 for formal diffeomorphisms. More precisely, given $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ prove that all elements of $\overline{\langle\phi_s\rangle}^z$ commute with all elements of $\overline{\langle\phi_u\rangle}^z$ and that $\overline{\langle\phi\rangle}^z$ is the group generated by $\overline{\langle\phi_s\rangle}^z$ and $\overline{\langle\phi_u\rangle}^z$.

Definition 3.33. Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Since G_k is an algebraic group of matrices and in particular a Lie group, we can define the conected component $G_{k,0}$ of the identity in G_k. We also consider the set $G_{k,u}$ of unipotent elements of G_k.

Definition 3.34. Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. We define

$$\overline{G}^z_0 = \{\varphi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0) : \varphi_k \in G_{k,0} \text{ for all } k \in \mathbb{N}\}$$

and

$$\overline{G}^z_u = \{\varphi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0) : \varphi_k \in G_{k,u} \text{ for all } k \in \mathbb{N}\}.$$

The group $\overline{G}^z_0$ is the natural candidate to connected component of Id of $\overline{G}^z$. Such a component is an algebraic group in the linear case; the analogue in the pro-algebraic case is the subject of next proposition. Moreover we will show that membership in $\overline{G}^z_0$ can be checked out on the linear part.

Proposition 3.35. *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Then $\overline{G}^z_0$ is a pro-algebraic subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ such that $\overline{G}^z_0 = \{\varphi \in \overline{G}^z : \varphi_1 \in G_{1,0}\}$.*

Proof. Let $l \geq k \geq 1$. Since $G_{l,0}$ is algebraic, $\pi_{l,k}(G_{l,0})$ is algebraic by Proposition 2.14. The dimension of $G_k = \pi_{l,k}(G_l)$ is equal to the dimension of $\pi_{l,k}(G_{l,0})$. Since $G_{l,0}$ is connected, $\pi_{l,k}(G_{l,0})$ is connected and hence contained in $G_{k,0}$. On top of that the algebraic groups $\pi_{l,k}(G_{l,0})$ and $G_{k,0}$ have the same dimension and $G_{k,0}$ is connected, we obtain $\pi_{l,k}(G_{l,0}) = G_{k,0}$ (we just proved that given a morphism $\alpha : H \to H'$ of algebraic groups then $\alpha(H)_0 = \alpha(H_0)$, cf. [3, Chapter I.1, Corollary 1,.4, p. 47]). In particular the image by $\pi_{l,k}$ of a connected component of G_l is a connected component of G_k. The map $\pi_{l,k}$ induces a map between connected components of G_l and connected components of G_k that is clearly surjective since $\pi_{l,k}$ is surjective by Lemma 3.5. Let us show that such correspondence is injective. Consider a connected component C of G_l such that $\pi_{l,k}(C) = G_{k,0}$. Then there exists $A \in C$ such that $\pi_{l,k}(A) = Id$. Thus A is unipotent by Proposition 3.12 and it belongs to $G_{l,0}$ by Exercise 2.10. Obviously we obtain $C = G_{l,0}$.

The discussion above implies $\pi_{l,k}^{-1}(G_{k,0}) = G_{l,0}$ and $\pi_{l,k}(G_{l,0}) = G_{k,0}$ for all $l \geq k \geq 1$. We deduce $\overline{G}_0^z = \{\varphi \in \overline{G}^z : \varphi_1 \in G_{1,0}\}$.

Since $\overline{G}_0^z = \varprojlim_{k\in\mathbb{N}} G_{k,0}$ and $\pi_{l,k} : G_{l,0} \to G_{k,0}$ is surjective for all $l \geq k \geq 1$, the group $\overline{G}_0^z$ is pro-algebraic by Lemma 3.23. □

We prove next that $\overline{G}_u^z$ is a pro-algebraic group if G is solvable. The next lemma is the analogue of Lemma 2.30 for groups of local diffeomorphisms.

Lemma 3.36. *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Then*

- $\ell(\overline{G}^z) = \ell(G)$.
- $\exp(t \log \varphi) \in \overline{G}_u^z$ *for all* $\varphi \in \overline{G}_u^z$ *and* $t \in \mathbb{C}$.
- $\overline{G}^z = \overline{G}_u^z$ *if G is unipotent.*
- *Suppose G is solvable. Then $\overline{G}_u^z$ is a pro-algebraic normal subgroup of $\overline{G}^z$.*

The three first items were proved in [13].

Proof. We have

$$\ell(G) = \max_{k\in\mathbb{N}} \ell(\{\phi_k : \phi \in G\}) = \max_{k\in\mathbb{N}} \ell(G_k) = \ell(\overline{G}^z).$$

The first and third equalities are immediate. The second equality is a consequence of the first item of Lemma 2.30.

Given $\varphi \in \overline{G}_u^z$ the group $\overline{\langle\varphi\rangle}^z$ is contained in $\overline{G}^z$ and it is equal to $\{\exp(t\log\varphi) : t \in \mathbb{C}\}$ by Remark 3.30. Since $t\log\varphi$ is nilpotent for $t \in \mathbb{C}$, the elements of $\overline{\langle\varphi\rangle}^z$ are contained in $\overline{G}_u^z$ by Proposition 3.17.

Suppose G is unipotent. Since $\{\phi_k : \phi \in G\}$ is unipotent, its Zariski-closure G_k is unipotent for any $k \in \mathbb{N}$ by Lemma 2.30. Thus $\overline{G}^z = \varprojlim G_k$ is unipotent by Proposition 3.12.

Suppose G is solvable. The set $G_{k,u}$ is an algebraic normal connected subgroup of the solvable group G_k for any $k \in \mathbb{N}$ by Lemma 2.30. We have $\pi_{l,k}^{-1}(G_{k,u}) = G_{l,u}$ for all $l \geq k \geq 1$ by Proposition 3.12. Since $\pi_{l,k}(G_l) = G_k$ by Lemma 3.21, hence $\pi_{l,k}(G_{l,u}) = G_{k,u}$ for all $l \geq k \geq 1$. Therefore $\overline{G}_u^z = \varprojlim G_{k,u}$ is a pro-algebraic group by Lemma 3.23. Moreover since $G_{k,u}$ is normal in G_k for any $k \in \mathbb{N}$, the group $\overline{G}_u^z$ is normal in $\overline{G}^z$. □

Remark 3.37. Let G be a solvable subgroup of $\mathrm{Diff}(\mathbb{C}^n, 0)$. Since membership in $\overline{G}_0^z$ and $\overline{G}_u^z$ can be checked out in the first jet, these groups have finite codimension in $\overline{G}^z$. Indeed the kernels of the natural maps

$$\overline{G}^z \to G_1/G_{1,u} \quad \text{and} \quad \overline{G}^z \to G_1/G_{1,0}$$

are equal to $\overline{G}_u^z$ and $\overline{G}_0^z$ respectively by Propositions 3.12 and 3.35. In particular $\overline{G}^z/\overline{G}_0^z$ is a finite group.

Proposition 3.38. *Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Consider $m \in \mathbb{Z} \setminus \{0\}$ such that $\phi^m \in \overline{\langle\phi\rangle}_0^z$. Then we obtain $\overline{\langle\phi^m\rangle}^z = \overline{\langle\phi\rangle}_0^z$.*

Proof. We denote $G = \langle\phi\rangle$. We have $\phi_k^m \in G_{k,0}$ for any $k \in \mathbb{N}$ by definition of $\overline{G}_0^z$. Proposition 2.24 implies $\overline{\langle\phi_k^m\rangle}^z = G_{k,0}$ for any $k \in \mathbb{N}$. We obtain $\overline{\langle\phi^m\rangle}^z = \overline{G}_0^z = \overline{\langle\phi\rangle}_0^z$ by construction of the pro-algebraic closure and definition of $\overline{G}_0^z$. □

We keep reproducing parts of the theory of algebraic matrix groups for formal diffeomorphisms. Next we associate Lie algebras to pro-algebraic groups.

Definition 3.39. Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. We define the set

$$\mathfrak{g} = \{X \in \hat{\mathfrak{X}}(\mathbb{C}^n, 0) : X_k \in \mathfrak{g}_k \text{ for all } k \in \mathbb{N}\}$$

where $\mathfrak{g}_k$ is the Lie algebra of G_k. We say that $\mathfrak{g}$ is the Lie algebra of $\overline{G}^z$.

Suppose G is solvable, we define

$$\mathfrak{g}_N = \{X \in \hat{\mathfrak{X}}(\mathbb{C}^n, 0) : X_k \in \mathfrak{g}_{k,u} \text{ for all } k \in \mathbb{N}\}$$

where $\mathfrak{g}_{k,u}$ is the Lie algebra of $G_{k,u}$. We say that $\mathfrak{g}_N$ is the Lie algebra of $\overline{G}_u^z$.

Remark 3.40. There are several possible definitions of Lie algebra of $\overline{G}^z$. Namely we can proceed as in Definition 3.39 or we can consider $\{X \in \hat{\mathfrak{X}}(\mathbb{C}^n,0) : \exp(tX) \in \overline{G}^z \ \forall\, t \in \mathbb{C}\}$. We show in next proposition that both choices are equivalent.

The Lie algebra of a pro-algebraic subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ shares analogous properties with the finite dimensional case.

Proposition 3.41 ([13, Proposition 2])**.** *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Then $\mathfrak{g}$ is equal to $\{X \in \hat{\mathfrak{X}}(\mathbb{C}^n,0) : \exp(tX) \in \overline{G}^z \ \forall\, t \in \mathbb{C}\}$ and $\overline{G}^z_0$ is generated by the set $\{\exp(X) : X \in \mathfrak{g}\}$. Moreover if G is unipotent then the map*

$$\exp : \mathfrak{g} \to \overline{G}^z$$

is a bijection and $\mathfrak{g}$ is a Lie algebra of nilpotent formal vector fields.

Proof. The first statement is a consequence of the definition of Lie algebra of an algebraic matrix group applied to G_k for $k \in \mathbb{N}$.

Given the map $\pi_{l,k} : G_l \to G_k$ for $l \geq k \geq 1$ we can consider the map $(d\pi_{l,k})_{Id} : \mathfrak{g}_l \to \mathfrak{g}_k$ given by the differential of $\pi_{l,k}$ at Id. It is the restriction to $\mathfrak{g}_l$ of the forgetful natural map $L_{k+1} \to L_k$. The map $(d\pi_{l,k})_{Id}$ satisfies $(d\pi_{l,k})_{Id}(\mathfrak{g}_l) \subset \mathfrak{g}_k$.

Let $A \in G_l$. The image of a small neighborhood U of A in G_l is a manifold whose dimension is the rank of $(d\pi_{l,k})_{Id}$ by the constant rank theorem (the rank of the maps $(d\pi_{l,k})_B$ for $B \in G_l$ is constant by the homogeneity of algebraic groups). We deduce that G_k is the union of countably closed (in the usual topology) sets contained in manifolds of dimension $\mathrm{rk}((d\pi_{l,k})_{Id})$. Since G_k is a smooth manifold of dimension $\dim(\mathfrak{g}_k)$ we deduce $\mathrm{rk}((d\pi_{l,k})_{Id}) = \dim(\mathfrak{g}_k)$. Otherwise we have $\mathrm{rk}((d\pi_{l,k})_{Id}) < \dim(\mathfrak{g}_k)$ and G_k is the union of countably nowhere-dense closed sets; this contradicts the Baire category theorem. Since $(d\pi_{l,k})_{Id}(\mathfrak{g}_l) \subset \mathfrak{g}_k$ and both complex vector spaces have the same dimension we obtain $(d\pi_{l,k})_{Id}(\mathfrak{g}_l) = \mathfrak{g}_k$. The last two paragraphs again describe a well-known fact about algebraic groups: the surjectivity of the differential map at Id of a surjective morphism of algebraic groups in characteristic 0 (cf. [3, Chapter II.7, p. 105]).

Since $\mathfrak{g} = \{X \in \hat{\mathfrak{X}}(\mathbb{C}^n,0) : \exp(tX) \in \overline{G}^z \text{ for all } t \in \mathbb{C}\}$, the set $\{\exp(X) : X \in \mathfrak{g}\}$ is contained in $\overline{G}^z_0$. Let us show that $\overline{G}^z_0$ is generated by $\{\exp(X) : X \in \mathfrak{g}\}$. Let $\phi \in \overline{G}^z_0$. Then ϕ_1 belongs to $G_{1,0}$ and as a consequence ϕ_1 is of the form $\exp(Y_1) \circ \ldots \circ \exp(Y_p)$ for some $Y_1, \ldots, Y_p$ in $\mathfrak{g}_1$ by Proposition 2.22. Since all the maps $(d\pi_{l,k})_{Id} : \mathfrak{g}_l \to \mathfrak{g}_k$ are surjective for $l \geq k \geq 1$, the natural projection $\varprojlim \mathfrak{g}_k = \mathfrak{g} \to \mathfrak{g}_1$ is surjective. Thus there exists $X_j \in \mathfrak{g}$ such that it induces the derivation Y_j of $\mathfrak{m}/\mathfrak{m}^2$ for any $1 \leq j \leq p$. The

diffeomorphism

$$\psi := \exp(-X_p) \circ \ldots \exp(-X_1) \circ \phi$$

has identity linear part by construction. We are done since $\log \psi$ belongs to $\mathfrak{g}$ by Remark 3.30.

Suppose G is unipotent. Hence $\overline{G}^z$ is unipotent by Lemma 3.36. The Lie algebra $\mathfrak{g}_1$ of the unipotent group G_1 consists of nilpotent matrices. Since $\varprojlim \mathfrak{g}_k = \mathfrak{g}$ we deduce that all elements of $\mathfrak{g}$ are nilpotent by Remark 3.16. The map $\exp : \mathfrak{g} \to \overline{G}^z$ is injective since $\exp : \hat{\mathfrak{X}}_N(\mathbb{C}^n, 0) \to \widehat{\mathrm{Diff}}_u(\mathbb{C}^n, 0)$ is injective (Proposition 3.17). Finally $\exp : \mathfrak{g} \to \overline{G}^z$ is is surjective since $\log \phi \in \mathfrak{g}$ for any $\phi \in \overline{G}^z$ by Remark 3.30. □

Remark 3.42. The term "connected component of the identity of $\overline{G}^z$" for $\overline{G}^z_0$ is completely justified. On the one hand $\overline{G}^z/\overline{G}^z_0$ is a finite group by Remark 3.37. On the other hand every element φ of $\overline{G}^z_0$ is of the form $\exp(X_1) \circ \ldots \circ \exp(X_k)$ where $X_1, \ldots, X_k \in \mathfrak{g}$ by Proposition 3.41. Hence $\exp(tX_1) \circ \ldots \circ \exp(tX_k)$ describes a path connecting the identity with φ in $\overline{G}^z_0$ when t varies in $[0, 1]$.

Corollary 3.43. *Let G be a solvable subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Then $\mathfrak{g}_N$ is a complex Lie algebra of nilpotent formal vector fields such that*

$$\exp : \mathfrak{g}_N \to \overline{G}^z_u$$

is a bijection.

Proof. Denote $H = \overline{G}^z_u$. Then H is a solvable unipotent pro-algebraic group by Lemma 3.36. Since $\mathfrak{g}_N$ is the Lie algebra of H, the result is a consequence of Proposition 3.41. □

3.6 Normal forms

Let us present in the next sections some simple consequences of the previous constructions. They are easily deduced from the Jordan-Chevalley decomposition and the properties of pro-algebraic groups.

Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}, 0)$. We can obtain a weak formal normal form for ϕ by linearizing its semisimple part. Next, we use this strategy to obtain the theorem of formal diagonalization of local diffeomorphisms with almost no calculations.

Proposition 3.44. *Let $(\lambda_1, \ldots, \lambda_n) \in (\mathbb{C}^*)^n$. Then there exists a non-semisimple $\phi \in \mathrm{Diff}\,(\mathbb{C}^n, 0)$ such that $j^1\phi = (\lambda_1 x_1, \ldots, \lambda_n x_n)$ if and only if there exists a multi-index $\underline{i} \in (\mathbb{N} \cup \{0\})^n$ such that $|\underline{i}| \geq 2$ and $\underline{\lambda}^{\underline{i}} = \lambda_j$ for some $1 \leq j \leq n$.*

Proof. We denote $L(x_1,\dots,x_n)=(\lambda_1 x_1,\dots,\lambda_n x_n)$. Let us show the necessary condition. We have that for

$$\phi := L\circ(x_1,\dots,x_{j-1},x_j+x^{\underline{i}},x_{j+1},\dots,x_n)$$

the right hand side is its Jordan-Chevally decomposition since the diffeomorphisms in the right hand side commute. Hence ϕ is not semisimple.

Suppose there exists a non-semisimple $\phi\in\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ with $j^1\phi=L$. By Proposition 3.13 (and its proof) there exists $\psi\in\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ such that $j^1\psi=Id$ and $\psi\circ\phi_s\circ\psi^{-1}=L$. We denote $\hat{\phi}_u=\psi\circ\phi_u\circ\psi^{-1}$. The formal diffeomorphism

$$\hat{\phi}_u(x_1,\dots,x_n)=\left(x_1+\sum_{|\underline{i}|\geq 2}a^1_{\underline{i}}(t)x^{\underline{i}},\dots,x_n+\sum_{|\underline{i}|\geq 2}a^n_{\underline{i}}(t)x^{\underline{i}}\right)$$

is non-trivial and commutes with L. Hence we obtain $\underline{\lambda}^{\underline{i}}=\lambda_j$ for any multi-index $\underline{i}$ such that $a^j_{\underline{i}}\neq 0$. □

Let us consider the case $n=1$. Fix $\lambda\in\mathbb{C}^*$. Then any element ϕ of $\mathrm{Diff}\,(\mathbb{C},0)$ (or $\widehat{\mathrm{Diff}}\,(\mathbb{C},0)$) such that $j^1\phi=\lambda x$ is formally linearizable if and only if λ is not a root of the unit.

3.7 Transferring properties to infinitesimal generators

Let us show a well-known property of unipotent diffeomorphisms. The result can be easily proved without considering pro-algebraic groups, but anyway the theory provides an easy conceptual proof.

Lemma 3.45. *Let $\phi,\psi\in\widehat{\mathrm{Diff}}_u(\mathbb{C}^n,0)$. Then $[\log\phi,\log\psi]=0$ if and only if ϕ commutes with ψ.*

Proof. The definition of Lie bracket implies that $[\log\phi,\log\psi]=0$ if and only if

$$\exp(t\log\phi)\circ\exp(s\log\psi)=\exp(s\log\psi)\circ\exp(t\log\phi)$$

for all $t,s\in\mathbb{C}$. This implies immediately the sufficient condition. Let us show the necessary condition.

The centralizer $Z(\psi)=\{\eta\in\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0):\psi\circ\eta\equiv\eta\circ\psi\}$ is a pro-algebraic group containing ϕ (cf. Remark 3.28). In particular it contains $\overline{\langle\phi\rangle}^z$. Thus we obtain

$$\psi\circ\exp(t\log\phi)=\exp(t\log\phi)\circ\psi$$

for any $t\in\mathbb{C}$. We deduce $\exp(t\log\phi)\circ\exp(s\log\psi)=\exp(s\log\psi)\circ\exp(t\log\phi)$ for all $t,s\in\mathbb{C}$ analogously. Therefore $[\log\phi,\log\psi]$ vanishes. □

3.8 First integrals

Let us see how the theory of pro-algebraic groups can dramatically simplify some proofs regarding invariance properties.

Proposition 3.46. *Let us consider n elements $f_1, \ldots, f_n$ of the field of fractions of $\hat{\mathcal{O}}_n$. Suppose $df_1 \wedge \ldots \wedge df_n \not\equiv 0$. Then the group*

$$G = \{\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0) : f_j \circ \phi \equiv f_j \text{ for all } 1 \leq j \leq n\}$$

is finite.

Proof. The group G is pro-algebraic. This result is proved for $f_1, \ldots, f_n \in \hat{\mathcal{O}}_n$ in Remark 3.28. The general case can be showed analogously.

Consider an element $X = \sum_{j=1}^{n} a_j \partial/\partial x_j$ in the Lie algebra $L(G)$ of G. By definition we have

$$f_j \circ \exp(tX) \equiv f_j \text{ for all } t \in \mathbb{C} \implies X(f_j) = \lim_{t \to 0} \frac{f_j \circ \exp(tX) - f_j}{t} \equiv 0$$

for any $1 \leq j \leq n$. The property $X(f_j) = 0$ for any $1 \leq j \leq n$ is equivalent to

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_n} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since $df_1 \wedge \ldots \wedge df_n \not\equiv 0$, the $n \times n$ matrix in the previous equation has a non-vanishing determinant and then $X \equiv 0$. Hence $L(G)$ is trivial and $\overline{G}_0^z$ is the trivial group by Proposition 3.41. Since $G/\overline{G}_0^z$ is finite by Remark 3.37, G is finite. □

3.9 Finding invariant curves

Let us see that the Jordan-Chevalley decomposition can be used to find invariant curves for a local diffeomorphism or one of its iterates.

Let us consider first an example. We define

$$\phi(x, y) = (iye^{-xy}, ixe^{xy}).$$

Does ϕ have invariant curves? And what about ϕ^p where $p \in \mathbb{N}$?

Let $X = xy(x\partial/\partial x - y\partial/\partial y)$. Since

$$\phi(x,y) = (iy, ix) \circ (xe^{xy}, ye^{-xy}) = (xe^{xy}, ye^{-xy}) \circ (iy, ix),$$

we have $\phi_s(x,y) = (iy,ix)$ and $\phi_u(x,y) = (xe^{xy}, ye^{-xy}) = \exp(X)$. Consider $p \in \mathbb{N}$ and a germ of curve γ at $(0,0)$ such that $\phi^p(\gamma) = \gamma$. Then $G_\gamma = \{\psi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^2,0) : \psi(\gamma) = \gamma\}$ is a pro-algebraic group containing ϕ^p. Since $\phi_s^p \circ \phi_u^p$ is the Jordan-Chevalley decomposition of ϕ^p, we obtain $\phi_s^p, \phi_u^p \in G_\gamma$ by Proposition 3.29. Remark 3.30 implies

$$\overline{\langle \phi_u^p \rangle}^z = \overline{\langle \phi_u \rangle}^z = \{\exp(t \log \phi_u) : t \in \mathbb{C}\};$$

in particular $\phi_u \in G_\gamma$ and γ is an invariant curve of the formal vector field $\log \phi_u$. Since $\log \phi_u = X$ and $X(xy) \equiv 0$, we deduce that the axis are the unique curves that are invariant by $\log \phi_u$. Therefore both axis are 2-periodic and no other curve is invariant or even periodic by ϕ.

Let us show that the periods of periodic curves are uniformly bounded.

Proposition 3.47. *Let $\phi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. There exists $p \in \mathbb{N}$ such that $\phi^p(\gamma) = \gamma$ for any formal periodic curve γ. Moreover every formal periodic curve is invariant if $\phi \in \overline{\langle \phi \rangle}_0^z$.*

Proof. Let $p \in \mathbb{N}$ such that $\phi^p \in \overline{\langle \phi \rangle}_0^z$. Given a formal periodic curve γ consider the pro-algebraic group $G_\gamma = \{\eta \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0) : \eta(\gamma) = \gamma\}$. There exists $q \in \mathbb{N}$ such that $\phi^{pq} \in G_\gamma$. In particular we obtain $\overline{\langle \phi^{pq} \rangle}^z \subset G_\gamma$. Since $\overline{\langle \phi^{pq} \rangle}^z = \overline{\langle \phi \rangle}_0^z$ by Proposition 3.38, we deduce $\phi^p \in G_\gamma$. □

4 Derived series

Solvable subgroups of $\mathrm{Diff}\,(\mathbb{C}^n,0)$ provide geometrical actions on a neighborhood of a point by solvable groups. A natural question is how the dimension n restricts the complexity of such actions. A simpler problem is studying wether or not the derived lengths of solvable subgroups of $\mathrm{Diff}\,(\mathbb{C}^n,0)$ is bounded by a function of n and if that is the case then finding the sharpest upper bound. Since a pro-algebraic group G of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ and its pro-algebraic closure $\overline{G}^{(0)}$ have the same derived length by Lemma 3.36 and the properties of $\overline{G}_0^{(0)}$ can be understood in terms of its Lie algebra, it is natural to consider this problem in the context of pro-algebraic groups.

We will see later on that the derived group of a pro-algebraic subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ is not necessarily pro-algebraic (section 5). We need to define the analogue of the derived group in the context of pro-algebraic groups.

Definition 4.1 ([13])**.** Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. By induction we define the j-closed derived group $\overline{G}^{(j)}$ of G as the closure in the Krull topology of $[\overline{G}^{(j-1)},\overline{G}^{(j-1)}]$ for any $j\in\mathbb{N}$.

Let us provide an alternate definition of the closed derived group. A pro-algebraic subgroup G of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$ is a projective limit $\varprojlim_{k\in\mathbb{N}} G_k$ of algebraic groups and hence it makes sense to consider the projective limit $\varprojlim_{k\in\mathbb{N}} G_k^{(1)}$ of the derived groups. Such group is indeed the closed derived group of G.

Proposition 4.2. *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Then $\overline{G}^{(j)}$ is a pro-algebraic group for any $j\in\mathbb{N}\cup\{0\}$. More precisely $\{\varphi_k:\varphi\in\overline{G}^{(j)}\}$ is the algebraic matrix group $G_k^{(j)}$ for all $j\in\mathbb{N}\cup\{0\}$ and $k\in\mathbb{N}$ and we have $\overline{G}^{(j)}=\varprojlim G_k^{(j)}$ for any $j\in\mathbb{N}\cup\{0\}$.*

Proof. The derived group of a linear algebraic group is algebraic (cf. [3, 2.3, p. 58]). As a consequence $G_k^{(j)}$ is algebraic for all $j\in\mathbb{N}\cup\{0\}$ and $k\in\mathbb{N}$.

We define $\tilde{G}^{(j)}=\{\varphi\in\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0):\varphi_k\in G_k^{(j)}\text{ for all }k\in\mathbb{N}\}$. Since $\pi_{l,k}(G_l)=G_k$, we obtain $\pi_{l,k}(G_l^{(j)})=G_k^{(j)}$ for all $l\geq k\geq 1$ and $j\geq 0$. The group $\tilde{G}^{(j)}$ is pro-algebraic for any $j\geq 0$ by Lemma 3.23.

The remainder of the proof is devoted to show $\overline{G}^{(j)}=\tilde{G}^{(j)}$ for any $j\geq 0$. It suffices to prove the result for $j=1$. The inclusion $\overline{G}^{(1)}\subset\tilde{G}^{(1)}$ is clear.

Let $\varphi\in\tilde{G}^{(1)}$. Fix $k\in\mathbb{N}$. Then φ_k is a product of commutators of elements of G_k. Since $\varprojlim_{j\in\mathbb{N}} G_j\to G_k$ is surjective by Corollary 3.25, we obtain that there exists $\eta(k)\in(\overline{G}^z)^{(1)}$ such that $(\eta(k))_k=\varphi_k$. Therefore φ is the limit in the Krull topology of the sequence $(\eta(k))_{k\geq 1}$. We are done since the Krull closure of $(\overline{G}^z)^{(1)}$ is equal to $\overline{G}^{(1)}$ by definition. □

The next lemma provides the analogue of the derived series for pro-algebraic groups.

Lemma 4.3. *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n,0)$. Then $\overline{G}^{(j)}$ is the closure in the Krull topology of the j-derived group of $\overline{G}^{(0)}$ for any $j\in\mathbb{N}$. Moreover, the series $\ldots\triangleleft\overline{G}^{(m)}\triangleleft\ldots\triangleleft\overline{G}^{(1)}\triangleleft\overline{G}^{(0)}$ is normal.*

Proof. Since the derived series of a group is normal and $\overline{G}^{(j)}=\varprojlim G_k^{(j)}$ by Proposition 4.2, the series $\ldots\triangleleft\overline{G}^{(m)}\triangleleft\ldots\triangleleft\overline{G}^{(1)}\triangleleft\overline{G}^{(0)}$ is normal. Analogously as in Proposition 4.2 we can show that $\overline{G}^{(j)}$ is contained in the closure of $(\overline{G}^z)^{(j)}$ in the Krull topology. Since $(\overline{G}^z)^{(j)}\subset\overline{G}^{(j)}$, we deduce that $\overline{G}^{(j)}$ is the closure of $(\overline{G}^z)^{(j)}$ in the Krull topology. □

Remark 4.4. The previous results justify the definition of $\overline{G}^{(j)}$. On the one hand $\overline{G}^{(j)} = \{Id\}$ is equivalent to $G^{(j)} = \{Id\}$ by Lemmas 3.36 and 4.3. On the other hand the group $\overline{G}^{(j)}$ is more compatible with the pro-algebraic nature of $\overline{G}^z$ than $(\overline{G}^z)^{(j)}$ by Proposition 4.2.

Let G be a pro-algebraic subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Suppose that G is connected, i.e. $G = \overline{G}^z_0$. We want to obtain the Lie algebras of the closed derived groups of G. In order to complete this task we introduce some definitions for Lie algebras of formal vector fields.

Definition 4.5. The derived Lie algebra $\mathfrak{g}^{(1)}$ (or $[\mathfrak{g}, \mathfrak{g}]$) of a complex Lie algebra $\mathfrak{g}$ is the complex Lie algebra generated by the Lie brackets of elements of $\mathfrak{g}$. The derived series of $\mathfrak{g}$ is defined by setting $\mathfrak{g}^{(0)} := \mathfrak{g}$ and $\mathfrak{g}^{(j)} := [\mathfrak{g}^{(j-1)}, \mathfrak{g}^{(j-1)}]$ for $j > 0$.

Let us introduce the closed derived series of a Lie algebra.

Definition 4.6 ([13])**.** Let $\mathfrak{g}$ be a Lie subalgebra of $\hat{\mathfrak{X}}(\mathbb{C}^n, 0)$. We denote by $\overline{\mathfrak{g}}^{(0)}$ the closure of $\mathfrak{g}$ in the Krull topology. We define the j-closed derived Lie algebra $\overline{\mathfrak{g}}^{(j)}$ of $\mathfrak{g}$ as the closure in the Krull topology of $[\overline{\mathfrak{g}}^{(j-1)}, \overline{\mathfrak{g}}^{(j-1)}]$ for any $j \in \mathbb{N}$.

In next proposition we describe the closed derives series of a Lie algebra $\mathfrak{g}$ of a pro-algebraic group G in terms of the closed derived series of G. Moreover we interprete the closed derived series of $\mathfrak{g}$ as a "projective limit" of derived series.

Proposition 4.7. *Let G be a subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ such that $\overline{G}^z = \overline{G}^z_0$. Let $\mathfrak{g}$ be the Lie algebra of $\overline{G}^z$. Then $\overline{\mathfrak{g}}^{(j)}$ is the Lie algebra of $\overline{G}^{(j)}$ and $\overline{G}^{(j)}$ coincides with its connected component of Id for any $j \in \mathbb{N}$. Moreover we have $\overline{\mathfrak{g}}^{(j)} = \varprojlim_{k\in\mathbb{N}} \mathfrak{g}_k^{(j)}$ for any $j \in \mathbb{N} \cup \{0\}$, where $\mathfrak{g}_k$ is the Lie algebra of G_k for any $k \in \mathbb{N}$.*

Proof. Since we work in characteristic 0 and G_k is a connected algebraic group by definition of $\overline{G}^z_0$, we have that $\mathfrak{g}_k^{(j)}$ is the Lie algebra of the connected algebraic group $G_k^{(j)}$ for every $j \in \mathbb{N}$ [3, Proposition 7.8, p. 108].

The Lie algebra

$$\tilde{\mathfrak{g}}^{(j)} := \{X \in \hat{\mathfrak{X}}(\mathbb{C}^n, 0) : X_k \in \mathfrak{g}_k^{(j)} \text{ for all } k \in \mathbb{N}\}$$

is the Lie algebra of $\overline{G}^{(j)}$ since

$$\overline{G}^{(j)} = \{\varphi \in \widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0) : \varphi_k \in G_k^{(j)} \text{ for all } k \in \mathbb{N}\}$$

by Proposition 4.2. It suffices to prove $\overline{\mathfrak{g}}^{(j)} = \tilde{\mathfrak{g}}^{(j)}$ for every $j \in \mathbb{N} \cup \{0\}$. The property $\overline{\mathfrak{g}}^{(j)} \subset \tilde{\mathfrak{g}}^{(j)}$ is obvious for every $j \in \mathbb{N} \cup \{0\}$. Let us show the other inclusions.

Consider the homomorphism $(d\pi_{k+1,k})_{Id} : \mathfrak{g}_{k+1} \to \mathfrak{g}_k$ defined in the proof of Proposition 3.41. Since $(d\pi_{k+1,k})_{Id}(\mathfrak{g}_{k+1}) = \mathfrak{g}_k$ for every $k \in \mathbb{N}$, the natural projection $\varprojlim \mathfrak{g}_l \to \mathfrak{g}_k$ is surjective for any $k \in \mathbb{N}$. Analogously as in the proof of Proposition 4.2 given any $X \in \tilde{\mathfrak{g}}^{(j)}$ and $k \in \mathbb{N}$ there exists $X(k) \in \mathfrak{g}^{(j)}$ such that $X(k)_k = X_k$. Hence X is the limit of the sequence $(X(k))_{k\in\mathbb{N}}$ and by definition X belongs to $\overline{\mathfrak{g}}^{(j)}$. We obtain $\tilde{\mathfrak{g}}^{(j)} \subset \overline{\mathfrak{g}}^{(j)}$ and then $\tilde{\mathfrak{g}}^{(j)} = \overline{\mathfrak{g}}^{(j)}$ for any $j \geq 0$. □

Given a connected Lie group G with Lie algebra $\mathfrak{g}$, the Lie algebra of $G^{(1)}$ is the derived Lie algebra $\mathfrak{g}^{(1)}$. Proposition 4.7 is an analogue of such result adapted to the context of connected pro-algebraic groups.

The next lemma is the analogue of Lemma 4.3 for Lie algebras.

Lemma 4.8. *Let G be a solvable subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Let $\mathfrak{g}$ be the Lie algebra of $\overline{G}^z$. Then $\overline{\mathfrak{g}}^{(j)}$ is the closure in the Krull topology of $\mathfrak{g}^{(j)}$ for any $j \in \mathbb{N}$. Moreover we have $\varphi_*\overline{\mathfrak{g}}^{(j)} = \overline{\mathfrak{g}}^{(j)}$ for all $\varphi \in \overline{G}^z$ and $j \in \mathbb{N}$. The series*

$$\ldots \lhd \overline{\mathfrak{g}}^{(m)} \lhd \ldots \lhd \overline{\mathfrak{g}}^{(1)} \lhd \overline{\mathfrak{g}}^{(0)} = \mathfrak{g}$$

is normal.

Proof. Since $\varprojlim \mathfrak{g}_l \to \mathfrak{g}_j$ is surjective for any $j \in \mathbb{N}$, $\overline{\mathfrak{g}}^{(j)}$ is contained in the closure in the Krull topology of $\mathfrak{g}^{(j)}$ for any $j \in \mathbb{N}$. Since $\mathfrak{g}^{(j)} \subset \overline{\mathfrak{g}}^{(j)}$ and $\overline{\mathfrak{g}}^{(j)}$ is closed in the Krull topology, we deduce that $\overline{\mathfrak{g}}^{(j)}$ is the closure of $\mathfrak{g}^{(j)}$ in the Krull topology for any $j \geq 0$.

The property $\varphi_*\mathfrak{g} = \mathfrak{g}$ for any $\varphi \in \overline{G}^z$ is a consequence of $\mathfrak{g}$ being the Lie algebra of $\overline{G}^z$. Since the Lie subalgebras of the derived series of $\mathfrak{g}$ are characteristic, we obtain $\varphi_*\mathfrak{g}^{(j)} = \mathfrak{g}^{(j)}$ for all $\varphi \in \overline{G}^z$ and $j \geq 0$. We get $\varphi_*\overline{\mathfrak{g}}^{(j)} = \overline{\mathfrak{g}}^{(j)}$ for all $\varphi \in \overline{G}^z$ and $j \geq 0$ by taking the Krull closures.

Since $\overline{\mathfrak{g}}^{(j)} = \varprojlim_{k\in\mathbb{N}} \mathfrak{g}_k^{(j)}$ for any $j \geq 0$ and the derived series are normal, the series

$$\ldots \lhd \overline{\mathfrak{g}}^{(m)} \lhd \ldots \lhd \overline{\mathfrak{g}}^{(1)} \lhd \overline{\mathfrak{g}}^{(0)} = \mathfrak{g}$$

is normal. □

The next proposition establishes that the derived length of a connected subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ and its Lie algebra coincide.

Proposition 4.9. *Let G be a solvable subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ such that $\overline{G}^z = \overline{G}_0^z$. Then the derived lengths of G and $\mathfrak{g}$ coincide.*

Proof. Fix $j \geq 0$. We have $G^{(j)} = \{Id\}$ if and only if $(\overline{G}^{(0)})^{(j)}$ by Lemma 3.36. Since the closure of $(\overline{G}^{(0)})^{(j)}$ in the Krull topology is equal to $\overline{G}^{(j)}$ by Lemma 4.3, we obtain $G^{(j)} = \{Id\}$ if and only if $\overline{G}^{(j)} = \{Id\}$. The Lie algebra of $\overline{G}^{(j)}$ is equal to $\overline{\mathfrak{g}}^{(j)}$ by Proposition 4.7; moreover $\exp(\overline{\mathfrak{g}}^{(j)})$ generates $\overline{G}^{(j)}$ since this group coincides with is connected component of Id (Proposition 4.7) and Proposition 3.41. Clearly $\overline{G}^{(j)} = \{Id\}$ if and only if $\overline{\mathfrak{g}}^{(j)} = 0$. Moreover $\mathfrak{g}^{(j)} = 0$ if and only if $\overline{\mathfrak{g}}^{(j)} = 0$ since $\overline{\mathfrak{g}}^{(j)} = 0$ is the closure in the Krull topology of $\mathfrak{g}^{(j)}$ by Lemma 4.8. We deduce $G^{(j)} = \{Id\}$ if and only $\mathfrak{g}^{(j)} = 0$ for any $j \geq 0$. □

This text is intended to be elementary and we will not provide the details of the calculations of sharp upper bounds of the derived length of solvable subgroups of $\mathrm{Diff}\,(\mathbb{C}^n, 0)$. Anyway the previous ideas can be used to show the following results.

Theorem 4.10 ([13])**.** *Let G be a solvable subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ such that $\overline{G}_0^z = \overline{G}^z$. Then $\ell(G) \leq 2n$. Moreover there exists a subgroup H of $\mathrm{Diff}\,(\mathbb{C}^n, 0)$ such that $\overline{H}_0^z = \overline{H}^z$ and $\ell(H) = 2n$.*

Theorem 4.11 ([13])**.** *Let G be a unipotent solvable subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Then we have $\ell(G) \leq 2n - 1$. Moreover there exists a unipotent subgroup H of $\mathrm{Diff}\,(\mathbb{C}^n, 0)$ such that $\ell(H) = 2n - 1$.*

The next theorem is classical. As a generalization we can calculate sharpest upper bounds of the derived length of solvable subgroups of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ for $n \leq 5$.

Theorem 4.12 (cf. [11], [9, Theorem 6.10, p. 85])**.** *Let G be a solvable subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}, 0)$. Then $\ell(G) \leq 2$. Moreover there exists a subgroup H of $\mathrm{Diff}\,(\mathbb{C}, 0)$ such that $\ell(H) = 2$.*

Theorem 4.13 ([21])**.** *Fix $2 \leq n \leq 5$. Let G be a solvable subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$. Then $\ell(G) \leq 2n+1$. Moreover there exists a subgroup H of $\mathrm{Diff}\,(\mathbb{C}^n, 0)$ such that $\ell(H) = 2n+1$.*

5 Pro-algebraic groups in dimension 1

The theory of pro-algebraic groups is powerful but so far we exhibited just a few examples of pro-algebraic groups. The situation is very simple in dimension 1 where pro-algebraic groups can be characterized. We classify all pro-algebraic subgroups of $\widehat{\mathrm{Diff}}\,(\mathbb{C}, 0)$ in this section.

We denote by T_d the centralizer of μz in $\widehat{\mathrm{Diff}}\,(\mathbb{C},0)$ where μ is a primitive d-root of the unit. An element ϕ of T_d is of the form

$$\phi(z) = \lambda z + \sum_{k=1}^{\infty} \lambda_k z^{kd+1}$$

where $\lambda \in \mathbb{C}^*$ and $\lambda_k \in \mathbb{C}$ for any $k \geq 2$.

Definition 5.1. Consider a formal vector field $X = \sum_{j=p}^{\infty} a_{j+1} z^{j+1} \frac{\partial}{\partial z} \in \hat{\mathfrak{X}}(\mathbb{C},0)$ such that $a_{p+1} \neq 0$. We define $\mathrm{ord}(X) = p$.

Remark 5.2. Given $X, Y \in \hat{\mathfrak{X}}(\mathbb{C},0)$ we have

$$\mathrm{ord}[X,Y] = \mathrm{ord}(X) + \mathrm{ord}(Y)$$

if $\mathrm{ord}(X) \neq \mathrm{ord}(Y)$.

Theorem 5.3. *Let G be a pro-algebraic subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C},0)$. Then up to a formal conjugacy G is of one of the forms:*

- $G = \{\lambda z : \lambda \in H\}$ *where H is an algebraic subgroup of $\mathbb{C}^*$.*
- $G = \left\{(\lambda^k z) \circ \exp\left(t \frac{z^{p+1}}{1+\lambda z^p} \frac{\partial}{\partial z}\right) : k \in \mathbb{Z}, t \in \mathbb{C}\right\}$ *where $p \geq 1$, $\lambda^p = 1$ and $\lambda \in \mathbb{C}$.*
- $G = \left\{(\lambda z) \circ \exp\left(t z^{p+1} \frac{\partial}{\partial z}\right) : \lambda \in H, t \in \mathbb{C}\right\}$ *where $p \geq 1$ and H is an algebraic subgroup of $\mathbb{C}^*$.*
- $G \subset T_d$ *for some $d \geq 1$, there exists $k_0 \geq 0$ such that $\{\phi_{k_0 d} : \phi \in G\}$ is algebraic and $G = \{\phi \in T_d : \phi_{k_0 d} \in G_{k_0 d}\}$.*

The three first possibilities correspond to solvable pro-algebraic groups. Notice that in the last possibility the subgroup $\{\phi \in T_d : j^{k_0 d}\phi \equiv Id\}$ is contained in G. If $d = 1$ then G contains all the elements of $\widehat{\mathrm{Diff}}\,(\mathbb{C},0)$ whose order of contact with the identity is higher than k_0.

Proof. Since G is pro-algebraic, the group $j^1 G$ is algebraic and then either a finite cyclic group or equal to $\{\lambda z : \lambda \in \mathbb{C}^*\}$. Suppose that G is solvable. The classification of solvable subgroups of $\widehat{\mathrm{Diff}}\,(\mathbb{C},0)$ (cf. [11], [9, section $6B_3$, p. 89]) implies that G is of one of the forms describe in the first three items.

Suppose G is non-solvable. The set G_u is a pro-algebraic group since it is the intersection of the pro-algebraic groups G and $\widehat{\mathrm{Diff}}_1(\mathbb{C},0)$ (Remark 3.27). The Lie algebra $\mathfrak{g}_N$

of G_u consists of formal vector fields with vanishing linear part and is closed in the Krull topology by Corollary 3.43. We denote $K(G) = \{\mathrm{ord}(X) : X \in \mathfrak{g}_N\}$ and $d = \gcd(K(G))$. The formal centralizer of G is a cyclic group of cardinal d by a theorem of Loray [12]. Up to a formal change of coordinates we can suppose that the centralizer of G is equal to $\langle e^{2\pi i/d} z\rangle$ and then $G \subset T_d$. The set $K(G)$ satisfies $k_1 + k_2 \in K(G)$ for all $k_1, k_2 \in K(G)$ such that $k_1 \neq k_2$ by Remark 5.2. Hence it is simple to see that $K(G)$ contains all the natural numbers of the form kd for some $k_0 \in \mathbb{N}$ and any $k \geq k_0$. Since $\mathfrak{g}_N$ is closed in the Krull topology, it contains all formal vector fields of the form $z^{k_0 d+1}\tilde{g}(z^d)\frac{\partial}{\partial z}$. Thus G contains all formal diffeomorphisms of the form $z + z^{k_0 d+1}\tilde{g}(z^d)$. The group $\{\phi_{k_0 d} : \phi \in G\}$ is algebraic by Proposition 3.26. The inclusion $G \subset \{\phi \in T_d : \phi_{k_0 d} \in G_{k_0 d}\}$ is clear. Let us show the reverse inclusion. Given an element $\phi \in T_d$ such that $\phi_{k_0 d} \in G_{k_0 d}$ there exists $\eta \in G$ such that $\eta_{k_0 d} = \phi_{k_0 d}$ since G is pro-algebraic. The formal diffeomorphism $\eta^{-1} \circ \phi$ is of the form $z + z^{k_0 d+1}\tilde{g}(z^d)$ and hence it belongs to G. Since η belongs to G, ϕ belongs to G. □

The pro-algebraic solvable subgroups of $\widehat{\mathrm{Diff}}\,(\mathbb{C}, 0)$ have the finite determination property and their dimension is 0, 1 or 2. On the other hand up to ramification a non-solvable pro-algebraic subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}, 0)$ has finite codimension. More precisely G has finite codimension in T_d for some $d \in \mathbb{N}$.

The derived group of a pro-algebraic subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^n, 0)$ is not necessarily pro-algebraic

We justified that the closed derived series of a pro-algebraic group is the right concept instead of the derived series in section 4. But a priori these series could be the same, making the introduction of the closed derived series redundant. We show in this section that in general the series are different.

The closed derived series and the derived series coincide for any pro-algebraic group if and only if the derived group of a pro-algebraic group is always pro-algebraic. We exhibit in this section an example of a pro-algebraic subgroup G of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^3, 0)$ whose derived group is not pro-algebraic.

Consider

$$X = x\frac{\partial}{\partial y},\ Y = y\frac{\partial}{\partial z} \text{ and } Z = x\frac{\partial}{\partial z}.$$

We have $[X, Y] = Z$, $[X, Z] = 0$ and $[Y, Z] = 0$.

Let us consider sequences $(X_n)_{n\geq 1}$ and $(Y_n)_{n\geq 1}$ of vector fields defined in a neighborhood of 0 in $\mathbb{C}^3$ such that $X_j = P_j X$, $Y_j = Q_j Y$ where $P_j, Q_j \in \mathbb{C}\{x\}$ for any $j \in \mathbb{N}$. Moreover we suppose that the multiplicity of P_j and Q_j at 0 tend to ∞ when $j \to \infty$. We also want to guarantee the independence condition

$$\sum_{1\leq j,k} \lambda_{j,k} P_j Q_k = 0 \implies \lambda_{j,k} = 0 \text{ for all } j,k \geq 0 \tag{9}$$

where the left hand side is a linear combination with complex coefficients. The expression $\sum_{1\leq j,k} \lambda_{j,k} P_j Q_k$ makes sense since $P_j Q_k$ tends to 0 in the Krull topology when $j+k \to \infty$.

Lemma 5.4. *There exists a choice of homogeneous polynomials $(P_j)_{j\geq 1}$ and $(Q_j)_{j\geq 1}$ such that $\lim_{j\to\infty} P_j = 0 = \lim_{j\to\infty} Q_j$ in the Krull topology and $\deg(P_j Q_k) \neq \deg(P_{j'} Q_{k'})$ if $(j,k) \neq (j',k')$. In particular the independence condition (9) holds.*

Proof. We define $P_1 = x$ and $Q_1 = x$. Let us define $P_j = x^{a_j}$ and $Q_j = x^{b_j}$ for certain sequences $(a_j)_{j\geq 1}$ and $(b_j)_{j\geq 1}$ of natural numbers. Suppose that we already defined $P_1, Q_1, \ldots, P_j, Q_j$ for $j \geq 1$. We define

$$a_{j+1} = \max_{1\leq k,l\leq j} \deg(P_k Q_l) \text{ and then } b_{j+1} = \max_{1\leq k\leq j+1,\ 1\leq l\leq j} \deg(P_k Q_l).$$

Notice that $(a_j)_{j\geq 1}$ and $(b_j)_{j\geq 1}$ are strictly increasing.

We claim that $\deg(P_j Q_k) \neq \deg(P_{j'} Q_{k'})$ if $(j,k) \neq (j',k')$. We define

$$c_{j,k} = (\max\{2j-1, 2k\}, \min\{2j-1, 2k\}) \text{ for } j,k \in \mathbb{N}.$$

Notice that $(j,k) \neq (j',k')$ implies $c_{j,k} \neq c_{j',k'}$. Moreover if $c_{j,k} < c_{j',k'}$ in the lexicographical order then we obtain $\deg(P_j Q_k) < \deg(P_{j'} Q_{k'})$ by our choice of $(a_j)_{j\geq 1}$ and $(b_j)_{j\geq 1}$.

The equation $\sum_{1\leq j,k} \lambda_{j,k} P_j Q_k = 0$ implies $\lambda_{j,k} = 0$ for all $j,k \geq 1$ since all monomials $P_j Q_k$ with $j,k \geq 1$ have different degrees. □

Definition 5.5. We denote $\lim^k_{n\to\infty} W_n = W$ if the sequence $(W_n)_{n\geq 1}$ converges to W in the Krull topology.

Consider the sets $\mathfrak{g}, \mathfrak{h} \subset \hat{\mathfrak{X}}_N(\mathbb{C}^3, 0)$ defined by

$$\mathfrak{g} = \{X \in \hat{\mathfrak{X}}_N(\mathbb{C}^3, 0) \text{ of the form } \sum_{j=1}^{\infty} \lambda_j X_j + \sum_{k=1}^{\infty} \mu_k Y_k + \sum_{m,l\geq 1} \gamma_{m,l}[X_m, Y_l]\}$$

and

$$\mathfrak{h} = \{X \in \hat{\mathfrak{X}}_N(\mathbb{C}^3, 0) : X \text{ is of the form } \sum_{m,l\geq 1} \gamma_{m,l}[X_m, Y_l]\}$$

where λ_j, μ_k and $\gamma_{m,l}$ are complex numbers.

Lemma 5.6. *$\mathfrak{g}$ is a step-2 nilpotent complex Lie algebra. Moreover $\mathfrak{h}$ is an ideal of $\mathfrak{g}$ contained in the center of $\mathfrak{g}$ such that $\mathfrak{g}^{(1)} \subset \mathfrak{h}$ and $\mathfrak{h}$ is the closure of $\mathfrak{g}^{(1)}$ in the Krull topology.*

Proof. Let $W_1, W_2 \in \mathfrak{g}$. We have

$$W_n = \sum_{j=1}^{\infty} \lambda_{j,n} X_j + \sum_{k=1}^{\infty} \mu_{k,n} Y_k + \sum_{m,l\geq 1} \gamma_{m,l,n}[X_m, Y_l]$$

for $n \in \{1, 2\}$. The vector field

$$[W_1, W_2] = \sum_{j,k\geq 1} (\lambda_{j,1}\mu_{k,2} - \lambda_{j,2}\mu_{k,1})[X_j, Y_k]$$

belongs to $\mathfrak{g}$. The previous formula implies $[W_3, [W_1, W_2]] = 0$ for all $W_1, W_2, W_3 \in \mathfrak{g}$, the inclusion of $\mathfrak{h}$ in the center of $\mathfrak{g}$ and $\mathfrak{g}^{(1)} \subset \mathfrak{h}$. The Lie algebra $\mathfrak{g}$ is step-2 nilpotent since $\mathfrak{g}^{(1)}$ is contained in the center of $\mathfrak{g}$.

Let us prove that $\mathfrak{h}$ is closed in the Krull topology. It suffices to show that given a sequence

$$W_n = \sum_{m,l\geq 1} \gamma_{m,l,n} P_m(x) Q_l(x) x \frac{\partial}{\partial z}$$

in $\mathfrak{g}$ such that $\lim^k_{n\to\infty} W_n = W$ then the W belongs to $\mathfrak{h}$. Since the degrees of the monomials $P_m(x)Q_l(x)$ are pairwise different, there exists a unique sequence $(\gamma_{m,l})_{m,l\geq 1}$ such that $\sum_{m,l\geq 1} \gamma_{m,l,n} P_m(x)Q_l(x)x$ converges to $\sum_{m,l\geq 1} \gamma_{m,l} P_m(x)Q_l(x)x$ in the Krull topology when $n \to \infty$. The vector field $W = \sum_{m,l\geq 1} \gamma_{m,l} P_m(x)Q_l(x)x\partial/\partial z$ belongs to $\mathfrak{h}$.

Notice that $[X_m, Y_l]$ belongs to $\mathfrak{g}^{(1)}$ for all $m, l \geq 1$. Given an element $\sum_{m,l\geq 1} \gamma_{m,l}[X_m, Y_l]$ of $\mathfrak{h}$ the elements $\sum_{m+l\leq k} \gamma_{m,l}[X_m, Y_l]$ belong to $\mathfrak{g}^{(1)}$ and converge to $\sum \gamma_{m,l}[X_m, Y_l]$ when $k \to \infty$. We deduce that $\mathfrak{h}$ is contained in the closure of $\mathfrak{g}^{(1)}$ in the Krull topology. Since $\mathfrak{g}^{(1)} \subset \mathfrak{h}$ and $\mathfrak{h}$ is closed, $\mathfrak{h}$ is the closure of $\mathfrak{g}^{(1)}$. □

Lemma 5.7. *The complex Lie algebra $\mathfrak{g}$ is closed in the Krull topology.*

Proof. It suffices to show that given a sequence

$$W_n = \sum_{j=1}^{\infty} \lambda_{j,n} P_j(x) x \frac{\partial}{\partial y} + \sum_{k=1}^{\infty} \mu_{k,n} Q_k(x) y \frac{\partial}{\partial z} + \sum_{m,l\geq 1} \gamma_{m,l,n} P_m(x) Q_l(x) x \frac{\partial}{\partial z}$$

in $\mathfrak{g}$ such that $\lim^k_{n\to\infty} W_n = W$ then W belongs to $\mathfrak{g}$. Since $\lim^k_{n\to\infty} W_n(y) = W(y)$ and $(\deg(P_j))_{j\geq 1}$ is strictly increasing, there exists a unique sequence $(\lambda_j)_{j\geq 1}$ such that $\lim^k_{n\to\infty}\sum_{j=1}^{\infty}\lambda_{j,n}P_j(x) = \sum_{j=1}^{\infty}\lambda_j P_j(x)$. We obtain $W(y) = \sum_{j=1}^{\infty}\lambda_j P_j(x)x$. Analogously, by noticing $\lim^k_{n\to\infty}\frac{\partial W_n(z)}{\partial y} = \frac{\partial W(z)}{\partial y}$, we deduce the existence of a unique sequence $(\mu_k)_{k\geq 1}$ such that

$$\lim_{n\to\infty}^{k}\sum_{k=1}^{\infty}\mu_{k,n}Q_k(x)y\frac{\partial}{\partial z} = \sum_{k=1}^{\infty}\mu_k Q_k(x)y\frac{\partial}{\partial z}.$$

The previous discussion implies that the series $\sum_{m,l\geq 1}\gamma_{m,l,n}P_m(x)Q_l(x)x$ converges in the Krull topology when $n\to\infty$. Since $\mathfrak{h}$ is closed in the Krull topology by Lemma 5.6, there exists a unique sequence $(\gamma_{m,l})_{m,l\geq 1}$ such that $\sum_{m,l\geq 1}\gamma_{m,l,n}P_m(x)Q_l(x)x$ converges to $\sum_{m,l\geq 1}\gamma_{m,l}P_m(x)Q_l(x)x$ in the Krull topology when $n\to\infty$. The vector field

$$W = \sum_{j=1}^{\infty}\lambda_j P_j(x)x\frac{\partial}{\partial y} + \sum_{k=1}^{\infty}\mu_k Q_k(x)y\frac{\partial}{\partial z} + \sum_{m,l\geq 1}\gamma_{m,l}P_m(x)Q_l(x)x\frac{\partial}{\partial z}$$

belongs to $\mathfrak{g}$. □

Proposition 5.8. *The set $G := exp(\mathfrak{g})$ is a pro-algebraic unipotent subgroup of $\widehat{\mathrm{Diff}}\,(\mathbb{C}^3, 0)$ consisting of tangent to the identity elements.*

Proof. Every element of $\mathfrak{g}$ has order of contact at least 2 with 0 and then every element of G is tangent to the identity.

Since the Lie algebra $\mathfrak{g}$ is step-2 nilpotent, it can be proved that G is a group by Baker-Campbell-Hausdorff formula. It is very easy to calculate $\exp(W)$ for $W\in\mathfrak{g}$ since $W(x) = 0$, $W^2(y) = 0$ and $W^3(z) = 0$. It can be checked out that G is given by algebraic equations in every space of jets and hence $\{\phi_k : \phi\in G\}$ is an algebraic group for any $k\in\mathbb{N}$. Moreover since $\mathfrak{g}$ is closed in the Krull topology by Lemma 5.7, G is closed in the Krull topology. As a consequence G is pro-algebraic by Proposition 3.26. □

Our goal is proving that $G^{(1)}$ is not a pro-algebraic group. In order to accomplish such a task let us describe $\log(G^{(1)})$.

Proposition 5.9. *The set $\log(G^{(1)})$ is equal to the Lie algebra $\mathfrak{g}^{(1)}$. Moreover $\mathfrak{g}^{(1)}$ coincides with the set of formal vector fields of the form*

$$\log\phi = \sum_{r=1}^{s}[\sum_{j=1}^{\infty}\lambda_{j,r}X_j, \sum_{k=1}^{\infty}\mu_{k,r}Y_k] \tag{10}$$

where $s\geq 0$ and $\lambda_{j,r},\mu_{k,r}\in\mathbb{C}$ for all $j,k\geq 1$ and $1\leq r\leq s$.

Proof. Consider elements

$$\phi_r = \exp\left(\sum_{j=1}^{\infty} \lambda_{j,r} X_j + \sum_{k=1}^{\infty} \mu_{k,r} Y_k + \sum_{m,l\geq 1} \gamma_{m,l,r}[X_m, Y_l]\right)$$

of G for $r \in \{1,2\}$. Since $\mathfrak{g}^{(1)}$ is contained in the center of $\mathfrak{g}$ we obtain

$$\log[\phi_1,\phi_2] = [\sum_{j=1}^{\infty} \lambda_{j,1} X_j, \sum_{k=1}^{\infty} \mu_{k,2} Y_k] - [\sum_{j=1}^{\infty} \lambda_{j,2} X_j, \sum_{k=1}^{\infty} \mu_{k,1} Y_k]. \tag{11}$$

Then every commutator of elements of G is of the form (10). Since $\mathfrak{g}^{(1)}$ is contained in the center of $\mathfrak{g}$, we obtain

$$\log([\phi_1,\psi_1] \circ \ldots \circ [\phi_s,\psi_s]) = \sum_{r=1}^{s} \log([\phi_r,\psi_r]) \tag{12}$$

for all $\phi_1, \psi_1, \ldots, \phi_s, \psi_s \in G$. In particular every element of $\log(G^{(1)})$ is of the form (10).

Every element ϕ of the form (10) with $s = 1$ can be obtained by considering $\lambda_{j,2} = 0$ for all $j \geq 1$ in Equation (11). We get a general element of the form (10) by applying Equation (12). □

The next step is showing that $\mathfrak{g}^{(1)}$ is not closed in the Krull topology.

Proposition 5.10. *The element $\sum_{l=1}^{\infty}[X_l, Y_l]$ belongs to the closure of $\mathfrak{g}^{(1)}$ in the Krull topology but it does not belong to $\mathfrak{g}^{(1)}$.*

Proof. Suppose that we have

$$\sum_{l=1}^{\infty}[X_l, Y_l] = \sum_{r=1}^{s}[\sum_{j=1}^{\infty} \lambda_{j,r} X_j, \sum_{k=1}^{\infty} \mu_{k,r} Y_k]. \tag{13}$$

We denote $A_r = \sum_{j=1}^{\infty} \lambda_{j,r} X_j$ and $B_r = \sum_{k=1}^{\infty} \mu_{k,r} Y_k$.

We can suppose up to multiply A_r and B_r by complex numbers that $\lambda_{1,r} \in \{0,1\}$ for any $1 \leq r \leq s$. The independence condition (9) implies $[X_1, \sum_{\lambda_{1,r}=1} B_r] = [X_1, Y_1]$ and then $\sum_{\lambda_{1,r}=1} B_r = Y_1$. Consider $1 \leq r_0 \leq s$ such that $\lambda_{1,r_0} = 1$. By replacing B_{r_0} with $Y_1 - \sum_{\lambda_{1,r}=1,\ r\neq r_0} B_r$ in Equation (13) we obtain

$$\sum_{l=2}^{\infty}[X_l, Y_l] = \sum_{\lambda_{1,r}=1,\ r\neq r_0} [A_r - A_{r_0}, B_r] + [A_{r_0} - X_1, Y_1] + \sum_{\lambda_{1,r}=0} [A_r, B_r].$$

Hence $\sum_{l=2}^{\infty}[X_l, Y_l]$ is of the form

$$\sum_{l=2}^{\infty}[X_l, Y_l] = [C_1, Y_1] + \sum_{r=2}^{s}[C_r, D_r]$$

where $C_r = \sum_{j=2}^{\infty} \lambda'_{j,r} X_j$ and $D_r = \sum_{k=1}^{\infty} \mu'_{k,r} Y_k$ for all $1 \leq r \leq s$. We define $D_1 = Y_1$. We can suppose $\mu'_{1,r} \in \{0, 1\}$ for any $2 \leq r \leq s$. We get $\sum_{\mu'_{1,r}=1} C_r = 0$ by the independence condition. We obtain

$$\sum_{l=2}^{\infty}[X_l, Y_l] = \sum_{\mu'_{1,r}=1,\ r\geq 2} [C_r, D_r - Y_1] + \sum_{\mu'_{1,r}=0} [C_r, D_r]. \tag{14}$$

All the coefficients of X_1 in C_r vanish for $1 \leq r \leq s$. Moreover the coefficient of Y_1 in $D_r - Y_1$ is 0 if $\mu'_{1,r} = 1$ and $r \geq 2$ whereas the coefficient of Y_1 in D_r vanishes if $\mu'_{1,r} = 0$. The right hand side of Equation (14) has $s - 1$ terms whereas the right hand side of Equation (13) had s terms. By repeating this process a finite number of times we deduce that there exists $l_0 \in \mathbb{N}$ such that $\sum_{l=l_0}^{\infty}[X_l, Y_l] = 0$. This contradicts the independence condition. In particular we deduce that $\sum_{l=1}^{\infty}[X_l, Y_l]$ is not of the form (13) and hence it does not belong to $\mathfrak{g}^{(1)}$.

On the other hand it is clear that $\sum_{l=1}^{j}[X_l, Y_l]$ belongs to $\mathfrak{g}^{(1)}$ for any $j \geq 1$. Since $\sum_{l=1}^{\infty}[X_l, Y_l] = \lim_{j\to\infty}^{k} \sum_{l=1}^{j}[X_l, Y_l]$, the vector field $\sum_{l=1}^{\infty}[X_l, Y_l]$ belongs to the closure of $\mathfrak{g}^{(1)}$ in the Krull topology. □

Proposition 5.11. *The group $G^{(1)}$ is not pro-algebraic.*

Proof. It suffices to show that $G^{(1)}$ is not closed in the Krull topology. We are done since $G^{(1)} = \exp(\mathfrak{g}^{(1)})$ and $\mathfrak{g}^{(1)}$ is not closed in the Krull topology by Proposition 5.10. □

References

[1] I.N. Baker. Non-embeddable functions with a fixpoint of multiplier 1. *Math. Z.*, 99:377–384, 1967.

[2] Gal Binyamini. Finiteness properties of formal Lie group actions. *Transform. Groups*, 20(4):939–952, 2015.

[3] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[4] Leonardo Câmara and Bruno Scardua. Closed orbits and integrability for singularities of complex vector fields in dimension three. *arXiv:1407.4560*, 2014.

[5] Serge Cantat and Dominique Cerveau. Analytic actions of mapping class groups on surfaces. *J. Topol.*, 1(4):910–922, 2008.

[6] Jean Écalle. Théorie itérative: introduction à la théorie des invariants holomorphes. *J. Math. Pures Appl. (9)*, 54:183–258, 1975.

[7] Étienne Ghys. Sur les groupes engendrés par des difféomorphismes proches de l'identité. *Bol. Soc. Brasil. Mat. (N.S.)*, 24(2):137–178, 1993.

[8] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, fourth printing, revised edition, 1995. Graduate Texts in Mathematics, No. 21.

[9] Yulij Ilyashenko and Sergei Yakovenko. *Lectures on analytic differential equations*, volume 86 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[10] L.S.O. Liverpool. Fractional iteration near a fix point of multiplier 1. *J. Lond. Math. Soc., II. Ser.*, 9:599–609, 1975.

[11] Frank Loray. Pseudo-groupe d'une singularité de feuilletage holomorphe en dimension deux. https://hal.archives-ouvertes.fr/hal-00016434, 2006.

[12] Frank Loray. Formal invariants for nonsolvable subgroups of $\mathrm{Diff}^{\omega}(\mathbf{C},0)$. *J. Algebra*, 247(1):95–103, 2002.

[13] Mitchael Martelo and Javier Ribón. Derived length of solvable groups of local diffeomorphisms. *Mathematische Annalen*, 358(3):701–728, 2014.

[14] Jean Martinet and Jean-Pierre Ramis. Classification analytique des équations differentielles non linéaires résonnantes du premier ordre. *Ann. Sci. Ecole Norm. Sup.*, 4(16):571–621, 1983.

[15] Jean-François Mattei and Robert Moussu. Holonomie et intégrales premières. *Ann. Sci. École Norm. Sup. (4)*, 13(4):469–523, 1980.

[16] Emmanuel Paul. Feuilletages holomorphes singuliers à holonomie résoluble. *J. Reine Angew. Math.*, 514:9–70, 1999.

[17] Ricardo Pérez-Marco. Convergence or generic divergence of the Birkhoff normal form. *Ann. of Math. (2)*, 157(2):557–574, 2003.

[18] Julio C. Rebelo and Helena Reis. A note on integrability and finite orbits for subgroups of $\mathrm{Diff}(\mathbb{C}^n, 0)$. *Bulletin Brazilian Math. Soc.*, 46(3):469–490, 2015.

[19] Julio C. Rebelo and Helena Reis. Discrete orbits, recurrence and solvable subgroups of $\mathrm{Diff}(\mathbb{C}^2, 0)$. *The Journal of Geometric Analysis*, pages 1–55, 2016.

[20] Javier Ribón. Recurrent orbits of subgroups of local complex analytic diffeomorphisms. Preprint arXiv:1509.01153.

[21] Javier Ribón. The solvable length of groups of local diffeomorphisms. Preprint http://arxiv.org/pdf/1406.0902v2.pdf.

[22] Javier Ribón. Holomorphic extensions of formal objects. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 3(4):657–680, 2004.

[23] Anna Leah Seigal and Sergei Yakovenko. Local dynamics of intersections: V. I. Arnold's theorem revisited. *Israel J. Math.*, 201(2):813–833, 2014.

[24] Jean-Pierre Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, second edition, 1992. 1964 lectures given at Harvard University.

[25] Igor R. Shafarevich. *Basic algebraic geometry. 2*. Springer, Heidelberg, third edition, 2013. Schemes and complex manifolds, Translated from the 2007 third Russian edition by Miles Reid.

[26] John Stillwell. *Naive Lie theory*. Undergraduate Texts in Mathematics. Springer, New York, 2008.

[27] B. A. F. Wehrfritz. *Infinite linear groups. An account of the group-theoretic properties of infinite groups of matrices*. Springer-Verlag, New York, 1973. Ergebnisse der Matematik und ihrer Grenzgebiete, Band 76.

Participantes

VIII Escuela Doctoral Intercontinental de Matemáticas
PUCP-UVA 2015

Alarcón Cárdenas, Noemi Giovanna Universidad Nacional del Altiplano

Alatorre, Darío Universidad Nacional Autónoma de México (UNAM)

Ardila Ardila, Jonny Universidad Federal de Río de Janeiro

Aredo, María Angélica Universidad Nacional de Piura

Arenas Olivera, Sthefany Lioska Universidad Nacional del Altiplano

Aroca, José Manuel Universidad de Valladolid

Arroyo Cabrera, Angélica María Universidad Autónoma del Caribe

Barra Calla, Yordan Alexis Universidad Nacional del Altiplano

Benavente Ticona, Jorge Alexander Universidad Nacional del Altiplano

Burgos Pinazo, Ada Fiorella Universidad Nacional del Altiplano

Calsin Velasquez, Wilfredo Universidad Nacional del Altiplano

Carrillo Torres, Sergio Alejandro Universidad de Valladolid

Casale, Guy Univesité de Rennes I

Condori, José Luis Universidad Nacional San Cristóbal de Huamanga

Corral, Nuria Universidad de Cantabria

Déserti, Julie Université Paris VII

Díaz Arboleda, Juan Universidad Nacional de Colombia, sede Medellín

Fernández, Percy Pontificia Universidad Católica del Perú

Gollés Paico, Yosbi Jhon Universidad Nacional de Piura

Jurado Cerrón, Liliana Universidad Federal de Río de Janeiro

Kuaquira Huallpa, Federico Universidad San Antonio Abad del Cusco

López, Lorena Universidade Federal de Minas Gerais

López Castillo, Julio Universidad Nacional de Piura

Martínez, Víctor Universidad Federal de Río de Janeiro

Mozo, Jorge Universidad de Valladolid

Paternina, José Universidad del Norte

Peña Vilchez, Andy Raúl Universidad Nacional de Piura

Pineda Escobar, Jesús David Universidad Nacional de Colombia

Pocoy Yauri, Víctor Alberto Universidad Nacional Santiago Antúnez de Mayolo

Ribón, Javier Universidade Federal Fluminense

Rodríguez Sabino, Vladimir Universidad Nacional Santiago Antúnez de Mayolo

Rodríguez Sánchez, Ángela Universidad Nacional de Colombia Sede Bogotá

Ruiz Castrillón, Juan Felipe Universidad Nacional de Colombia sede Medellín

Sacatuma Cruz D. Michael Universidad San Antonio Abad del Cusco

Siles, Mercedes Universidad de Málaga

Ugarte, Francisco Pontificia Universidad Católica del Perú

Venegas Gómez, Henock Universidad del Atlántico

Zamora Inuma, Francisco Miguel Universidad Federal de Río de Janeiro

Se terminó de imprimir en
los talleres gráficos de
Tarea Asociación Gráfica Educativa
Psje. María Auxiliadora 156, Breña
Correo e.: tareagrafica@tareagrafica.com
Teléfono: 332-3229 Fax: 424-1582
Se utilizaron caracteres
NimbusRomNo9L en 8 puntos
para el cuerpo del texto
octubre 2016 Lima - Perú