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

El Problema Inverso de Galois a través del Teorema de Existencia de Riemann

Tesina Licenciatura en Matemática

SEBASTIÁN PÉREZ GARBAYO
2020

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

Índice general

Agradecimientos

Quiero agradecer a la profesora Michela Artebani por guiar esta tesina; por todas sus correcciones, por todos sus comentarios, y por el trabajo que significa hacer lo anterior en un año como el presente.

Agradezco a los profesores del Departamento de Matemática, quienes siempre han estado disponibles a la discusión y a la enseñanza.

Quiero agradecer a mi familia por el incondicional apoyo y cariño que han demostrado a lo largo de estos años.

Agradezco también a mis compañeros (y más aún, amigos) de carrera, con quienes siempre hay espacio tanto como para jugar un juego de mesa como para discutir, a veces hasta altas horas de la madrugada, un problema matemático.

Muchísimas gracias a mis amigos, los cuales han demostrado un nivel de paciencia y comprensión más allá de mi entendimiento.

Agradezco a Chomksy, Drakax, Eggward, Juanito, Kael y Ren por su devoción constante a la aventura. Que Tymora siempre guíe sus caminos.

Muchísimas gracias a Alejandra, quien ha sido gran amiga y mentora en un camino profundo y pedregoso. Espero que el futuro nos vuelva a reunir, con más experiencias e historias que compartir.

Quisiera manifestar mi más sincera y eterna gratitud a Camila, quien siempre ha depositado absoluta confianza en la completitud de este proceso. Esta tesina (y muchísimo más) no hubiera sido posible sin su invaluable presencia y su constante preocupación.

Dedico esta tesina a todos y cada uno de aquellos que han hecho mi estadía en este planeta un poco menos desagradable.

Introducción

La Teoría de Galois, introducida en [1] por el mítico matemático del siglo 19 Évariste Galois, fue un hito en el álgebra de la época; mostrando una conexión entre la teoría de campos y la teoría de grupos motivada por el problema de encontrar una fórmula por radicales para resolver la ecuación general de quinto grado. Galois mostró la imposibilidad de su existencia a través del hoy conocido como Teorema de Correspondencia de Galois (ver 1.5.22), que en esencia muestra que la información de una extensión de campos L/K puede ser codificada en un grupo asociado: el grupo de Galois $\mathrm{Gal}(L/K)$.

Bajo esta lógica, uno puede realizarse la pregunta inversa: ¿es todo grupo finito el grupo de Galois de alguna extensión de campos? Si no fijamos el campo base, la respuesta es afirmativa y bastante sencilla. En efecto, si fijamos cualquier campo k y un grupo finito G y definimos $K = k(g : g \in G)$ (agregando todos los elementos de G como elementos trascendentales sobre k), el grupo G actúa naturalmente como grupo de automorfismos de K. Por el Teorema 1.5.24, $\mathrm{Gal}(K/K^G)$ es isomorfo a G, donde K^G es el campo fijo de G.

Sin embargo, si fijamos el campo base la pregunta es tremendamente complicada y de hecho un problema abierto hoy en día, conocido como el Problema Inverso de Galois. Este fue considerado sistemáticamente por primera vez por David Hilbert en [4]; donde, por medio del Teorema de Irreducibilidad de Hilbert, muestra que existen infinitas extensiones de $\mathbb{Q}$ con grupo de Galois isomorfo a S_n y A_n. El problema sobre $\mathbb{Q}$, usualmente conocido como el Problema Inverso de Galois clásico, ha sido fuente de profundo estudio por varias décadas y testigo de importantes resultados; entre los cuales se destaca la realización de todos los grupos resolubles por Igor Shafarevich en [5] y la realización del Monster Group y otros grupos esporádicos por John Thompson en [6] por medio del método de rigidez (ver, por ejemplo, [7] o [9]).

El problema más general también ha sido, por supuesto, fuente de estudio; y una de las áreas más clásicas al respecto es el problema sobre $\mathbb{C}(x)$, el campo de funciones racionales sobre los números complejos. En este contexto, las principales herramientas son las desarrolladas originalmente por Bernhard Riemann en su tesis doctoral [2] y su posterior artículo [3]. En estas, Riemann desarrolla el concepto de superficie de Riemann y muestra el hoy conocido como Teorema de Existencia de Riemann, que asegura la

existencia de "suficientes" funciones meromorfas en una superficie de Riemann compacta. Este Teorema puede ser convertido a una condición de existencia de espacios cubrientes ramificados finitos de Galois de $\mathbb{P}^1_{\mathbb{C}}$, que a su vez son, en algún sentido, equivalentes a las extensiones de campos finitas de Galois de $\mathbb{C}(x)$. Esta equivalencia es clásicamente desarrollada a través de la teoría de espacios de Hilbert y de la cohomología (ver, por ejemplo, [8] o [9]); y permite mostrar que todo grupo finito es realizable como grupo de Galois sobre $\mathbb{C}(x)$. Esto revela una profunda conexión entre el análisis, la teoría de grupos y la topología algebraica.

En el capítulo 1 fijamos notaciones básicas y presentamos los preliminares de análisis, topología, superficies de Riemann, topología algebraica y teoría de Galois que son necesarios para comprender la demostración del Teorema de Existencia de Riemann (Teorema 2.1.16), que demostramos en completitud en la sección 2.1. Dedicamos la sección 2.2 al estudio de los cubrimientos ramificados de $\mathbb{P}^1_{\mathbb{C}}$, culminando con una versión topológica del Teorema de Existencia de Riemann (Teorema 2.2.13). La sección 2.3 trata las extensiones de campos de $k(x)$ y luego especializa propiedades de estos al caso $k = \mathbb{C}$. A continuación, la sección 2.4 trata la conexión entre espacios cubrientes y extensiones de campos, y utilizamos su equivalencia para mostrar una versión algebraica del Teorema de Existencia Riemann (Teorema 2.4.12), del cuál sigue la realización de los grupos finitos sobre $\mathbb{C}(x)$. Finalmente, el capítulo 3 contiene una pequeña introducción a la aplicación de los resultados que hemos obtenido en el capítulo 2 al estudio del Problema Inverso de Galois Clásico, comenzando por el Método de Rigidez en la sección 3.1 y terminando por el Teorema de Irreducibilidad de Hilbert en la seccion 3.2. Este capítulo tiene la meta principal de tentar al lector a continuar leyendo sobre el tema, por lo que omitimos algunos detalles en la presentación para simplificarla y los reemplazamos por referencias completas a los resultados.

1 Preliminares

1.1. Espacios de Hilbert

Definición 1.1.1. Un espacio vectorial normado $(X, |\cdot|)$ se dice **de Banach** si este es completo con respecto a la métrica inducida por su norma.

Teorema 1.1.2. [11, Teorema 11.1] *Sean X, Y espacios de Banach. Si $f : X \to Y$ es una función lineal, continua y biyectiva, entonces f^{-1} es lineal y continua.*

Definición 1.1.3. Un espacio vectorial equipado de un producto interno $\langle , \rangle$ se dice **de Hilbert** si es completo con respecto a la métrica inducida por el producto interno. (equivalentemente, si es de Banach con respecto a la norma inducida por el producto interno).

Definición 1.1.4. Sea $D \subseteq \mathbb{C}$ abierto. El espacio vectorial $L^2(D)$ es el cociente del espacio de todas las funciones holomorfas $f : D \to \mathbb{C}$ que cumplen $|f|^2 := \int_D |f|^2 < \infty$ bajo la relación de equivalencia $f \sim g$ cuando $|f - g| = 0$; equipado con el producto interno $\langle f, g \rangle = \int_D f\bar{g}$.

Proposición 1.1.5. [9, Proposición 6.14] *$L^2(D)$ es un espacio de Hilbert.*

1.2. Topología y Medida

Definición 1.2.1. Un subconjunto S de un espacio topológico es **relativamente compacto** si su clausura es compacta.

Teorema 1.2.2. [10, Teorema 7.26] *Sea $V \subseteq \mathbb{R}^n$ abierto, $f : \mathbb{R}^n \to [0, \infty]$ una función medible y $T : V \to \mathbb{R}^n$ una función diferenciable e inyectiva. Se tiene:*

$$\int_{T(V)} f = \int_V (f \circ T)|J_T|,$$

donde J_T es el jacobiano de T.

Proposición 1.2.3. [16, Lema 2.13] *La función*

$$f(x) = \begin{cases} e^{-\frac{1}{x}} & \text{para } x > 0 \\ 0 & \text{para } x \leq 0 \end{cases}$$

es una función diferenciable $\mathbb{R} \to \mathbb{R}$ *que es 0 si y sólo si* $x \leq 0$.

Corolario 1.2.4. [16, Lemas 2.14 y 2.15] *Sean* r, R *dos números reales con* $0 < r < R$. *La función*

$$\chi(x) = \frac{f(R - |x|)}{f(R - |x|) + f(|x| - r)}$$

es una función diferenciable $\mathbb{R}^n \to \mathbb{R}$ *que es* 0 *si* $|x| > R$ *y* 1 *si* $|x| < r$.

Teorema 1.2.5. [14, Teorema 1.6.23] *Si* X *es un espacio topológico segundo contable, entonces* X *es compacto si y sólo si* X *es secuencialmente compacto.*

Definición 1.2.6. Sean Y una superficie suave, I un conjunto finito y $\{X_i\}_{i\in I}$ una familia de abiertos con $Y = \bigcup_{i\in I} X_i$. Una **partición de la unidad** $(\chi_i)_{i\in I}$ **asociada a** $\{X_i\}_{i\in I}$ es una colección de funciones $\chi_i : Y \to \mathbb{R}$ diferenciables y no negativas que cumplen que cada χ_i se anula en un abierto $\tilde{X}_i$ con $Y = \tilde{X}_i \cup X_i$, y que $\sum_{i\in I} \chi_i = 1$.

1.3. Análisis Complejo y Superficies de Riemann

Denotaremos por $D(a, r) := \{z \in \mathbb{C} : |z - a| < r\}$ al disco centrado en a de radio r. Además, durante esta sección, denotaremos por $\Omega \subseteq \mathbb{C}$ a un subconjunto abierto del plano complejo.

Lema 1.3.1. [9, Lema 6.12] *Sea* $D = D(a, r)$, *y* $f \in L^2(D)$ *con expansión de Taylor* $f(z) = \sum_{n=0}^{\infty} c_n(z-a)^n$. *Si* f *se extiende a una función holomorfa en* $D(a, r')$ *con* $r' > r$, *se tiene*

$$|f|_D^2 = \sum_{n=0}^{\infty} |c_n|^2 \pi r^{2n+2}(n+1)^{-1}.$$

Definición 1.3.2. Sea $f : \Omega \to \mathbb{C}$ una función. La **derivada conjugada** de f, cuando esta existe, es la función

$$\frac{\partial f}{\partial \bar{z}} = \frac{1}{2}\left(\frac{\partial f}{\partial x} + i\frac{\partial f}{\partial y}\right).$$

Proposición 1.3.3. [10, Teorema 11.2] *Sea* $f : \Omega \to \mathbb{C}$ *diferenciable en* U. *Entonces,* f *es holomorfa en* U *si y sólo si* $\frac{\partial f}{\partial \bar{z}} = 0$.

Teorema 1.3.4. [13, Teorema 4.3.1.7] *Sea $a \in \Omega$, con $\Omega \subseteq \mathbb{C}$ abierto, y $f : \Omega \setminus \{a\} \to \mathbb{C}$ holomorfa. Entonces, existe g holomorfa en Ω con $f(z) = g(z)$ en $\Omega \setminus \{a\}$ si y sólo si $(z-a)f(z) \xrightarrow{z \to a} 0$.*

Corolario 1.3.5. *Sean $Q \subseteq \Omega$ finito, con $\Omega \subseteq \mathbb{C}$ abierto, y $f : \Omega \to \mathbb{C}$ una función continua en Ω y holomorfa en $\Omega \setminus Q$. Entonces, f es holomorfa en Ω.*

Teorema 1.3.6. [18, Teorema 3.11] *Sea $F(z, w) : \mathbb{C}^2 \to \mathbb{C}$ una función holomorfa en ambas variables en una vecindad de (z_0, w_0) que cumple que $F(z_0, w_0) = 0$ y*

$$\frac{\partial F}{\partial w}(z_0, w_0) \neq 0.$$

Entonces, existen vecindades U, V de z_0 y w_0 respectivamente de modo que la ecuación $F(z, w) = 0$ tiene una única solución $w = w(z)$ en V para cualquier $z \in U$. Además, la función $w = w(z)$ es holomorfa en U y $w(z_0) = w_0$.

Corolario 1.3.7. *Sea $F(z, w) \in \mathbb{C}[z, w]$ de grado $n \geq 1$ en w, y $c_0 \in \mathbb{C}$ de modo que $F(c_0, w) \in \mathbb{C}[w]$ es separable de grado n. Entonces, existen funciones holomorfas $\psi_1, ..., \psi_n$ en una vecindad abierta U de c_0 de modo que para cada $c \in U$ el polinomio $F(c, w)$ tiene n raíces distintas $\psi_1(c), ..., \psi_n(c)$.*

Demostración. Por la separabilidad de $F(c_0, w)$, $\frac{\partial F}{\partial w}(c_0, \gamma_i) \neq 0$ para cada raíz γ_i de $F(c_0, w)$. Por lo tanto, por el Teorema 1.3.6, existe una función holomorfa ψ_i definida alrededor de c_0 con $\psi(c_0) = \gamma_i$ de modo que $F(c, d) = 0$ si y sólo si $d = \psi_i(c)$ para una vecindad suficientemente pequeña de (c_0, γ_i). Las funciones ψ_i son las funciones que queremos. □

Lema 1.3.8. *Sea $\varphi : D(0, 1) \to \mathbb{C}$ una función diferenciable con soporte compacto. Entonces, existe una función diferenciable ψ en $D(0, 1)$ con*

$$\frac{\partial \psi}{\partial \bar{z}} = \varphi.$$

Demostración. Podemos extender φ a una función diferenciable en $\mathbb{C}$ que es 0 fuera de $D(0, 1)$. Así ψ está dada por

$$\psi(z) = -\frac{1}{\pi} \int_0^{2\pi} \int_0^2 \varphi(z + re^{i\theta}) e^{-i\theta} dr d\theta$$

y es rutina chequear que ψ cumple lo que queremos (se puede encontrar un desarrollo completo en [25, Lema 1.2]). □

Corolario 1.3.9. *Para cada función diferenciable $\varphi : D(0,1) \to \mathbb{C}$ existe una función ψ diferenciable y acotada en $D(0,r)$ para $0 < r < 1$, con*

$$\frac{\partial \psi}{\partial \bar{z}} = \varphi.$$

Demostración. Sea $D(0,r')$ otro disco alrededor de cero, con $D(0,r) \subsetneq D(0,r') \subsetneq D(0,1)$. Por la Proposición 1.2.3 existe una función χ diferenciable que es idénticamente 1 en $D(0,r)$ y 0 fuera de $D(0,r')$. Así, la función $\varphi' = \varphi\chi$ cumple con las hipótesis del Lema 1.3.8, y por tanto existe ψ con $\frac{\partial \psi}{\partial \bar{z}} = \varphi'$. La función ψ es acotada en $D(0,r)$ y su restricción a $D(0,r)$ cumple lo que queremos. □

Definición 1.3.10. Una **superficie de Riemann** Y es un espacio topológico de Hausdorff segundo contable que admite un cubrimiento abierto $\{W_\alpha\}$ de modo que cada W_α admite un homeomorfismo $z_\alpha : W_\alpha \to V_\alpha \subseteq \mathbb{C}$, donde V_α es abierto; y tal que $z_\alpha \circ z_\beta^{-1}$ es holomorfa en $V_\alpha \cap V_\beta$ para cada α, β con $V_\alpha \cap V_\beta \neq \emptyset$. Los pares (W_α, z_α) se llaman **cartas** de Y, y el conjunto de todas las cartas se llama un **atlas** de Y.

Definición 1.3.11. Sean X, Y superficies de Riemann con atlas $\{(W_\alpha, z_\alpha)\}$, $\{(W_\beta, z_\beta)\}$ respectivamente. Una función $f : X \to Y$ es **holomorfa** si $z_\beta \circ f \circ z_\alpha^{-1}$ es holomorfa en su dominio de definición para cada α, β.

Definición 1.3.12. Sea X una superficie de Riemann. Una función **meromorfa** en X es una función $X \to \mathbb{P}^1_{\mathbb{C}}$ holomorfa que no es idénticamente ∞. Denotamos por $\mathcal{M}(X)$ el campo de todas las funciones meromorfas en X.

Proposición 1.3.13. [9, Ejemplo 5.3] *Si z es la función identidad en $\mathbb{P}^1_{\mathbb{C}}$, $\mathcal{M}(\mathbb{P}^1_{\mathbb{C}}) = \mathbb{C}(z)$, el campo de funciones racionales en z.*

Definición 1.3.14. El **grupo de automorfismos** de una superficie de Riemann X, denotado $\mathrm{Aut}(X)$, es el grupo de todas las funciones $f : X \to X$ que son biyectivas, holomorfas y con inversa holomorfa.

Lema 1.3.15. [9, Lema 5.5] *Sea $D \subseteq \mathbb{C}$ abierto y conexo, $p_0 \in D$ y $D_0 = D \setminus \{p_0\}$. Vemos $\mathcal{M}(D)$ como subcampo de $\mathcal{M}(D_0)$ (vía restricción). Así, $\mathcal{M}(D)$ es algebraicamente cerrado en $\mathcal{M}(D_0)$.*

Proposición 1.3.16. [12, Definición 1.27] *Sea $f : X \to Y$ una función holomorfa no constante entre superficies de Riemann. Para cada $p \in X$, existe una carta local centrada en p de forma que f se expresa en la forma $z \mapsto z^{k_p}$ en estas coordenadas. Este número entero k_p es invariante bajo cambio de cartas (sólo depende de p).*

Definición 1.3.17. Sea $f : X \to Y$ una función holomorfa no constante entre superficies de Riemann. El número entero k_p de la Proposición 1.3.16 se denomina **índice de ramificación de f en p.**

Proposición 1.3.18. [12, Proposición 4.8] *Sea $f : X \to Y$ una función holomorfa no constante entre superficies de Riemann compactas. El número*

$$d(f) := \sum_{p \in f^{-1}(y)} k_p$$

*no depende de $y \in Y$ y se llama el **grado** de f.*

Definición 1.3.19. Sea X una superficie de Riemann compacta.

1. Una **triangulación** de X es una descomposición de X en subconjuntos cerrados, cada uno homeomorfo a un triángulo, de modo que cualquier par de triángulos son disjuntos, se intersectan en un único vértice o se intersectan en un único lado.

2. Dada una triangulación de X con V vértices, E aristas y T triángulos, el **número de Euler** de X con respecto a esta triangulación es $\chi(X) = V - E + T$.

Teorema 1.3.20. [26, Teorema 1] *Toda superficie de Riemann compacta admite una triangulación.*

Proposición 1.3.21. [12, Proposición 4.15] *El número de Euler de una superficie de Riemann compacta no depende de la triangulación escogida.*

Definición 1.3.22. El **género** de una superficie de Riemann compacta X es el número

$$g(X) = \frac{2 - \chi(X)}{2}.$$

Intuitivamente, el género de X es la cantidad de agujeros que tiene; en el sentido en el que una esfera no tiene ninguno, un toro tiene exactamente uno, etcétera.

Teorema 1.3.23. [12, Teorema 4.16] *Sea $f : X \to Y$ una función holomorfa no constante entre superficies de Riemann compactas. Se tiene:*

$$2g(X) - 2 = d(2g(Y) - 2) + \sum_{p \in X} (k_p - 1),$$

donde d es el grado de f.

1.4. Topología Algebraica

Definición 1.4.1. Sea X un espacio topológico e $I = [0,1] \subseteq \mathbb{R}$. Una función continua $f : I \to X$ es un **camino**. Además, f es un **camino cerrado en** $p \in X$ o un **lazo en** $p \in X$ si $f(0) = f(1) = p$.

Definición 1.4.2. Sea X un espacio topológico. Fijado $p \in X$, dos lazos $f : I \to X$, $g : I \to X$ en p se dicen **homotópicos** si existe una función $H : I \times I \to X$ continua con $H(0,t) = f(t)$, $H(1,t) = g(t)$ y $H(t,0) = p = H(t,1)$ para cada t en I.

Lema 1.4.3. [17, Lema 51.1] *La homotopía de lazos es una relación de equivalencia.*

Definición 1.4.4. Sea X un espacio topológico. El **grupo fundamental** de X en p, $\pi_1(X,p)$, es el grupo de clases de homotopía de lazos basados en p

$$[\gamma] = \{\eta : \eta \text{ es un lazo en } p \text{ homotópico a } \gamma\}$$

con la operación $[\alpha] \cdot [\beta] = [\alpha \cdot \beta]$ y

$$(\alpha \cdot \beta)(t) = \begin{cases} \alpha(2t) & \text{para } 0 \leq t \leq \frac{1}{2} \\ \beta(2t-1) & \text{para } \frac{1}{2} \leq t \leq 1 \end{cases}.$$

Proposición 1.4.5. [13, Sección 8.1.6] *Si $\mathbb{D} = \{z \in \mathbb{C} : 0 < |z| < 1\}$ y $p \in \mathbb{D}$, entonces $\pi_1(\mathbb{D},p) \simeq \mathbb{Z}$. Además, $\pi_1(\mathbb{D},p)$ está generado por la clase del lazo $\gamma(t) = r\exp(2\pi i t)$, con $0 < r < 1$.*

Definición 1.4.6. Sean X, Y espacios topológicos. Una función $f : X \to Y$ continua es un **espacio cubriente** (o un **cubrimiento**) si para cada $y \in Y$ existe una vecindad abierta V de y tal que $f^{-1}(V)$ es unión de abiertos disjuntos U_α, y $f|_{U_\alpha} : U_\alpha \to V$ es un homeomorfismo para cada α. Los abiertos V se llaman **abiertos fundamentales** del espacio cubriente.

Definición 1.4.7. Sea $f : X \to Y$ un espacio cubriente:

(a) Una **fibra** de f es un conjunto $f^{-1}(p)$, con $p \in Y$.

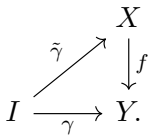
(b) El **grado** de f es la cardinalidad de cualquier fibra $f^{-1}(p)$.

Observación 1.4.8. Si Y es conexo y tiene al menos una fibra finita, entonces todas las fibras tienen la misma cardinalidad. Esto es porque, alrededor de cada $p \in Y$, la función

$$Y \to \mathbb{Z}, \quad p \mapsto |f^{-1}(p)|$$

es localmente constante por la definición de espacio cubriente. Por tanto, el grado está bien definido.

Definición 1.4.9. Sea $f : X \to Y$ un espacio cubriente, y $\gamma : I \to Y$ un camino. Un **levantamiento** de γ es una función $\tilde{\gamma} : I \to X$ que hace conmutar el siguiente diagrama:



Lema 1.4.10. [17, Lema 54.1] *Sean $f : X \to Y$ un espacio cubriente, $x \in X$ e $y \in Y$ con $f(x) = y$. Entonces, todo camino $\gamma : I \to Y$ con $\gamma(0) = y$ tiene un único levantamiento $\tilde{\gamma}$ con $\tilde{\gamma}(0) = x$. Además, caminos homotópicos tienen levantamientos homotópicos.*

Corolario 1.4.11. [9, Corolario 4.13] *Sea $f : X \to Y$ un cubrimiento y Y conexo por caminos. Sea X_1 una componente conexa de X. Entonces, f se restringe a un cubrimiento $X_1 \to Y$. Si $f^{-1}(p) \subseteq X_1$ para algún $p \in Y$, entonces $X = X_1$ es conexo por caminos.*

Lema 1.4.12. [12, Lema 4.4] *Sea $f : X \to Y$ un espacio cubriente de grado finito con Y conexo por caminos y $p \in Y$. El grupo fundamental $\pi_1(Y, p)$ actúa sobre $f^{-1}(p)$ de la siguiente forma: $[\gamma]$ envía a_0 a a_1 donde a_1 es el punto final del único levantamiento de $[\gamma]$ con punto inicial a_0 (que existe y es único por el Lema 1.4.10). Esta acción es transitiva si y sólo si X es conexo por caminos. Denotamos esta acción por $b \mapsto b^{[\gamma]}$.*

Corolario 1.4.13. [9, Corolario 4.14] *Sean $f_i : X_i \to Y$ cubrimientos para $i = 1, 2$; con X_i conexo por caminos. Sea $b_i \in X_i$ con $f_1(b_1) = f_2(b_2) =: p$. Supongamos que para cada $[\gamma] \in \pi_1(Y, p)$ tenemos $b_1^{[\gamma]} = b_1$ si y sólo si $b_2^{[\gamma]} = b_2$. Entonces, existe un homeomorfismo $\alpha : X_1 \to X_2$ con $f_2 \circ \alpha = f_1$ y $\alpha(b_1) = b_2$.*

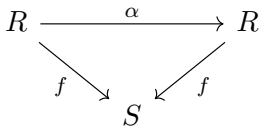
Definición 1.4.14.

(a) Dos espacios cubrientes $f : X \to Y$ y $\tilde{f} : X' \to Y$ se dicen **equivalentes** si existe un homeomorfismo $\alpha : X \to X'$ con $\tilde{f}\alpha = f$.

(b) Un **automorfismo** del cubrimiento $f : X \to Y$ es un homeomorfismo $\alpha : X \to X$ con $f \circ \alpha = f$. Estos automorfismos forman un grupo denotado por $\mathrm{Deck}(f)$.

(c) Dado $f : X \to Y$ espacio cubriente y $p \in Y$, el conjunto $f^{-1}(p)$ es una **fibra** de Y.

Es claro que el grupo $\mathrm{Deck}(f)$ actúa sobre cada fibra. Un automorfismo de R se puede ver como un homeomeorfismo que hace conmutar el diagrama:



Lema 1.4.15. *Sea $f : X \to Y$ un espacio cubriente:*

(a) Sean $p, q \in Y$ y γ un camino en Y con punto inicial p y punto final q. Para cada $b \in f^{-1}(p)$, b^γ denotará el punto final del levantamiento $\tilde{\gamma}$ de γ con punto inicial b. Entonces, $b \mapsto b^\gamma$ es una biyección entre $f^{-1}(p)$ y $f^{-1}(q)$. Además, esta biyección conmuta con la acción de $\mathrm{Deck}(f)$.

(b) La acción de $\mathrm{Deck}(f)$ *en $f^{-1}(p)$ conmuta con la de $\pi_1(Y, p)$.*

(c) Sea $\alpha \in \mathrm{Deck}(f)$. Si X es conexo por caminos y α fija un punto $b \in X$ entonces $\alpha = id$.

(d) Si X es conexo por caminos y $G \leq \mathrm{Deck}(f)$ actúa transitivamente en alguna fibra, entonces $G = \mathrm{Deck}(f)$.

Demostración.

(a) La función $f^{-1}(q) \to f^{-1}(p)$, $b \to b^{\gamma^{-1}}$ es inversa de $b \mapsto b^\gamma$, donde $\gamma^{-1}(t)$ es el camino $\gamma(1-t)$. Además, notemos que para un camino γ entre p y q con levantamiento $\tilde{\gamma}$ y un $\alpha \in \mathrm{Deck}(f)$, $\alpha \circ \tilde{\gamma}$ es el único levantamiento de γ con punto inicial $\alpha(p)$ (es único por el Lema 1.4.10).

(b) Es (a) con $p = q$, notando que la elección de un camino dentro de su clase de homotopía es irrelevante (también por el Lema 1.4.10).

(c) Sea $b' \in X$ y γ' un camino en X de b a b'. Sea $\gamma = f \circ \gamma'$ un camino en Y de $f(b)$ a $f(b')$. Así, γ' es el levantamiento de γ con punto inicial b'. Si $\alpha(b) = b$ tenemos $\alpha(b') = \alpha(b^\gamma) = \alpha(b)^\gamma = b^\gamma = b'$ y por tanto $\alpha = id$.

(d) Sea $b \in f^{-1}(p)$. Para cada $\alpha \in \mathrm{Deck}(f)$, existe $\beta \in G$ con $\beta(\alpha(b)) = b$. Luego, $\beta\alpha = id$ por (c), así que $\alpha \in G$. □

Observación 1.4.16. Notamos que si $\mathrm{Deck}(f)$ actúa transitivamente en una fibra, actúa transitivamente en todas. Además, si X, Y son superficies de Riemann compactas y f es holomorfa, el grado de f como espacio cubriente coincide con el grado de f como función holomorfa.

1.5. Teoría de Galois

Lema 1.5.1. [22, Lema 1.2.2] *Sea A un dominio de factorización única, y K su campo de fracciones. Si $f \in A[x]$ es irreducible, entonces $f \in K[x]$ también.*

Definición 1.5.2.

1. Una **extensión de campos** es una inclusión de campos $\varphi : K \to L$, que denotamos por L/K.
2. El **grado** $[L : K]$ de una extensión L/K es la dimensión de L visto como espacio K-vectorial.
3. Una extensión de campos L/K es **finita** si $[L : K] < \infty$.

Definición 1.5.3. Sea L/K una extensión de campos.

- El **polinomio minimal** (si existe) de $\alpha \in L$ sobre K es el único polinomio mónico irreducible en $K[x]$ que se anula en α. En este caso, α se dice **algebraico** sobre K. Si este polinomio no existe, α se dice **trascendental** sobre K.
- L/K es **algebraica** si cada $\alpha \in L$ es algebraico sobre K.
- Un conjunto $\{t_1, ..., t_n\}$ de elementos de L se dice **algebraicamente independiente sobre** K si no existe un polinomio no constante $P \in K[x_1, ..., x_n]$ de modo que $P(t_1, ..., t_n) = 0$.
- L/K se dice **puramente trascendental** si existe $S \subseteq L$ algebraicamente independiente sobre K de modo que $K(S) = L$.

Lema 1.5.4. *Sea α algebraico sobre un campo K. Sea $f(y) = \sum_{i=0}^{n} a_i y^i$ un polinomio sobre K de grado $n > 0$ con $f(\alpha) = 0$. Entonces*

$$g(y) = y^n + \sum_{i=0}^{n-1} a_i a_n^{n-i-1} y^i \in K[y]$$

es un polinomio mónico de grado n con $g(a_n\alpha) = 0$. Claramente $K(\alpha) = K(a_n\alpha)$.

Demostración. Evidente. □

Definición 1.5.5. Una extensión de campos L/K es **normal** si cada polinomio irreducible $f(x) \in K[x]$ que tiene una raíz en L tiene todas sus raíces en L.

Definición 1.5.6. Sea K un campo, $f(x) \in K[x]$. Un **campo de descomposición** para f es un campo $L \supseteq K$ que contiene todas las raíces de f y es minimal con esta propiedad.

Teorema 1.5.7. [19, Teorema 3.1.4] *Sean K un campo, $f \in K[x]$ con $\deg(f) > 0$. Entonces, existe una extensión L/K de modo que f tiene todas sus raíces en L.*

Corolario 1.5.8. *Sea K un campo, $f(x) \in K[x]$. Si $\alpha_1, ..., \alpha_n$ son todas las raíces de f en algún campo $L \supseteq K$, entonces $K(\alpha_1, ..., \alpha_n)$ es un campo de descomposición para f.*

Teorema 1.5.9. [19, Teorema 5.2.4] *Sean $K \subseteq L$ dos campos. Entonces, L es campo de descomposición de algún polinomio $f \in K[x]$ si y sólo si L/K es finita y normal.*

Teorema 1.5.10. [19, Corolario 5.1.7] *Sea K un campo. Si L_1, L_2 son dos campos de descomposición de $f \in K[x]$, existe un isomorfismo $L_1 \simeq L_2$ que es la identidad en K.*

Definición 1.5.11. Sea K un campo. Un polinomio $f \in K[x]$ es **separable** si no es constante y todas sus raíces son distintas en algún campo de descomposición. Además, si L/K es una extensión de campos algebraica,

- $\alpha \in L$ es separable si su polinomio minimal sobre K lo es.
- L/K es separable si cada $\alpha \in L$ lo es.

Definición 1.5.12. Sea K un campo, $f \in K[x]$ mónico, L un campo de descomposición para f y $u_1, ..., u_n$ las raíces de f en L. El **discriminante** $D(f)$ de f es el número

$$D(f) = \prod_{i<j} (u_i - u_j)^2.$$

Proposición 1.5.13. [19, Teorema 5.3.2] *Sea K un campo, $f \in K[x]$ mónico y no constante. Son equivalentes:*

1. *f es separable.*
2. *$D(f) \neq 0$.*

Teorema 1.5.14. [19, Teorema 5.4.1] *Sea L/K una extensión finita y separable de un campo K. Entonces existe $\gamma \in L$, separable sobre K, tal que $L = K(\gamma)$.*

Teorema 1.5.15. [19, Teorema 5.3.5] *Toda extensión algebraica de un campo de característica 0 es separable.*

Corolario 1.5.16. *Sea L/K una extensión finita de un campo K de característica 0. Entonces, existe $\gamma \in L$ tal que $L = K(\gamma)$.*

Definición 1.5.17. Sea L/K una extensión de campos. El **Grupo de Galois** de L sobre K es el grupo con la composición:

$$\mathrm{Gal}(L/K) = \{f \in \mathrm{Aut}(L) : f(k) = k \text{ para todo } k \in K\}.$$

Definición 1.5.18. Una extensión L/K es **de Galois** si es normal y separable.

Teorema 1.5.19. [19, Teorema 7.1.5] *Sea L/K una extensión de campos finita. Se tiene:*

(a) $|\mathrm{Gal}(L/K)| \leq [L : K]$.

(b) L/K es de Galois si y sólo si $|\mathrm{Gal}(L/K)| = [L : K]$.

Definición 1.5.20. Sea L un campo y sea $H \leq \mathrm{Aut}(L)$. El **campo fijo** de H es el campo $K^H = \{k \in L : f(k) = k \text{ para todo } f \in H\}$.

Lema 1.5.21. *Sea L un campo y $f(x, y) \in L[x, y]$ separable como polinomio en y sobre $L(x)$. Entonces, el polinomio especializado $f(b, y) \in L[y]$ es separable para todo salvo finitos $b \in L$.*

Demostración. Por el Lema 1.5.4 podemos suponer que f es mónico como polinomio en y. Su discriminante es $D(x) \in L[x]$, no nulo porque f es separable (en y) (por la Proposición 1.5.13). Para cada $b \in L$, $f(b, y)$ tiene discriminante $D(b)$; y luego $f(b, y)$ es separable para todo $b \in L$ distinto de las raíces de $D(x)$. □

Teorema 1.5.22. [15, Teorema 14.1.5] *(de Correspondencia de Galois) Sea L/K una extensión de Galois finita y $G = \mathrm{Gal}(L/K)$. La función*

$$H \mapsto L^H$$

es una biyección entre los subgrupos de G y los campos intermedios $K \subseteq F \subseteq L$, y su función inversa es

$$F \mapsto \mathrm{Gal}(L/F).$$

Teorema 1.5.23. [15, Teorema 14.4.6] *Sea G un grupo de orden n de automorfismos de un campo K. Entonces, $[K : K^G] = n$*

Corolario 1.5.24. [15, Corolario 14.4.7] *Sea G un grupo finito de automorfismos de un campo K. Entonces K/K^G es una extensión de Galois con grupo de Galois G.*

Demostración. Cada elemento de G es un automorfismo de K, y por definición fijan K^G. Por tanto, $G \leq \mathrm{Gal}(K/K^G)$. Por el Teorema 1.5.19, $|\mathrm{Gal}(K/K^G)| \leq [K : K^G]$. Además, $[K : K^G] = |G| \leq |\mathrm{Gal}(K/K^G)|$ por el Teorema anterior. De estos, sigue que $|\mathrm{Gal}(K/K^G)| = [K : K^G]$ y que $\mathrm{Gal}(K/K^G) = G$. Concluimos, una vez más el Teorema 1.5.19, que K/K^G es de Galois. □

Definición 1.5.25. Sean L/K, L/F dos extensiones de campos. El **compositum** de K y F es el más chico subcampo de L que contiene K y F.

El Teorema 1.5.22 nos hace preguntarnos si, fijado un campo K y un grupo finito G, ¿existirá una extensión de Galois L/K con grupo de Galois $\mathrm{Gal}(L/K) \simeq G$? Este es el Problema Inverso de Galois; que motiva la siguiente Definición:

Definición 1.5.26. Sea K un campo. Un grupo finito G se dice **realizable sobre** K si existe una extensión de campos L/K finita y de Galois de modo que $G \cong \mathrm{Gal}(L/K)$.

En este documento, estudiaremos principalmente el problema inverso de Galois en el caso $K = \mathbb{C}(x)$.

2 El Teorema de Existencia de Riemann

A lo largo de este capítulo, estudiaremos los grupos realizables sobre $\mathbb{C}(x)$ a través del Teorema de Existencia de Riemann; y mostraremos que, de hecho, todo grupo finito es realizable sobre $\mathbb{C}(x)$.

2.1. Espacios de Hilbert sobre Superficies de Riemann

A lo largo de esta sección, Y será una superficie de Riemann, I un conjunto finito, y $\{(W_i, z_i)\}_{i\in I}$ serán cartas coordenadas en Y (no necesariamente el atlas completo).

Definición 2.1.1. Dado un conjunto abierto $E \subseteq W_i$, definimos el conjunto $L^2(E, z_i)$ como el espacio de todas las funciones holomorfas $f : E \to \mathbb{C}$ con $f \circ z_i^{-1} \in L^2(z_i(E))$.

Si equipamos $L^2(E, z_i)$ con el producto interno $\langle f, g\rangle = \langle f \circ z_i^{-1}, g \circ z_i^{-1}\rangle$ (como en la Definición 1.1.4), es claro que tenemos un espacio de Hilbert isomorfo a $L^2(z_i(E))$ (por la Proposición 1.1.5).

Lema 2.1.2. *Sea E un conjunto abierto y relativamente compacto en $W_i \cap W_j$. Entonces, existe $k > 0$ tal que para cada función holomorfa $E \to \mathbb{C}$ se tiene:*

$$|f \circ z_i^{-1}|_{z_i(E)} \leq k|f \circ z_j^{-1}|_{z_j(E)}.$$

Por lo tanto, $L^2(E, z_i)$ y $L^2(E, z_j)$ coinciden como espacios topológicos, y los denotaremos por $L^2(E)$.

Demostración. Sea $D_i = z_i(E)$, y $D_j = z_j(E)$. Por el Teorema 1.2.2, se tiene:

$$|f \circ z_i^{-1}|^2_{D_i} = \int_{D_i} |f \circ z_i^{-1}|^2 = \int_{D_j} |f \circ z_j^{-1}|^2 |J|,$$

donde J es el jacobiano de $z_i \circ z_j^{-1}$. Como $|J|$ es continuo en $z_j(W_i \cap W_j)$, es acotado en $z_j(E) = D_j$. Eligiendo $k > 0$ con $|J| \leq k^2$ en D_j, sigue el Lema. □

Definición 2.1.3. Sea $\mathcal{U} = (U_i)_{i\in I}$ una familia de abiertos $U_i \subseteq W_i$ de modo que cada U_i es relativamente compacto en W_i. Definimos los espacios de Hilbert

$$C^0(\mathcal{U}) = \bigoplus_{i\in I} L^2(U_i) \qquad \text{y} \qquad C^1(\mathcal{U}) = \bigoplus_{(i,j)\in I^2} L^2(U_i \cap U_j)$$

y denotamos los elementos de $C^0(\mathcal{U})$ y $C^1(\mathcal{U})$ como uplas $(f_i)_{i\in I}$ y $(f_{ij})_{i,j\in I}$ respectivamente.

Esto nos permitirá definir un espacio de Hilbert sobre "toda la superficie Y", y nos servirá más adelante para realizar un proceso de pegado de funciones definidas sólo sobre una carta.

Definición 2.1.4. Fijamos índices $i, j, k \in I$ y consideramos la función

$$\begin{aligned} \varphi_{i,j,k} : C^1(\mathcal{U}) &\to L^2(U_i \cap U_j \cap U_k) \\ (f_{\nu\mu}) &\mapsto (f_{ij} - f_{ik} - f_{kj}) \big|_{U_i\cap U_j\cap U_k}, \end{aligned}$$

que es lineal y continua por ser composición de proyecciones y restricciones. El subespacio $Z^1(\mathcal{U}) \subseteq C^1(\mathcal{U})$ es la intersección de los núcleos $\operatorname{Ker}(\varphi_{i,j,k})$ al variar de $i, j, k \in I$, y sus elementos se llaman **cociclos**. Estos son exactamente las uplas $(f_{\nu\mu})$ con $f_{ij} = f_{ik} + f_{kj}$ para todo $i, j, k \in I$; esta relación se llama la **relación del cociclo**.

Definición 2.1.5. La función

$$\begin{aligned} \partial : C^0(\mathcal{U}) &\to Z^1(\mathcal{U}) \\ (g_\mu) &\mapsto (f_{ij}) = \big((g_j - g_i) \big|_{U_i\cap U_j}\big) \end{aligned}$$

se llama la **función de cofrontera** y está bien definida porque los f_{ij} cumplen la relación del cociclo.

Proposición 2.1.6. *La función ∂ es lineal y continua.*

Demostración. La linealidad es clara. Para la continuidad, notemos que la función

$$\begin{aligned} C^0(\mathcal{U}) &\to L^2(U_i \cap U_j) \\ (g_i) &\mapsto (g_j - g_i) \big|_{U_i\cap U_j} \end{aligned}$$

es continua; no es más que composición de proyecciones. Así, la función inducida $C^0(\mathcal{U}) \to C^1(\mathcal{U})$ lo es y por tanto también su restricción a $Z^1(\mathcal{U})$, que es ∂. □

Proposición 2.1.7. *Supongamos que $D(0,1) = \bigcup_{i\in I} X_i$, con X_i abiertos, que existe una partición de la unidad $(\chi_i)_{i\in I}$ asociada a $\{X_i\}_{i\in I}$ y que para cada $i, j \in I$ existen funciones holomorfas f_{ij} en $X_i \cap X_j$ que satisfacen la relación del cociclo. Denotamos $X_i' = X_i \cap D(0, r)$, para algún radio $0 < r < 1$. Si cada f_{ij} está en $L^2(X_i' \cap X_j')$, entonces existen funciones $g_i \in L^2(X_i')$ con $f_{ij} = g_i - g_j$ en $X_i' \cap X_j'$ para cada $i, j \in I$.*

Demostración. Extendemos por 0 cada f_{ik} a una función en $D(0,1)$. Luego, la función $\chi_k f_{ik}$ es diferenciable en X_i: en efecto, con la notación de la Definición 1.2.6, X_i es la unión de los abiertos $(X_i \cap \tilde{X_k})$ y $(X_i \cap X_k)$; y $\chi_k f_{ik}$ es diferenciable en ambos. Así, $\psi_i = \sum_{k\in I} \chi_k f_{ik}$ es una función diferenciable en X_i, y $\int_{X_i'} |\psi_i|^2 < \infty$. En $X_i \cap X_j$, se tiene:

$$\psi_i - \psi_j = \sum_{k\in I} \chi_k (f_{ik} - f_{jk}) = \sum_{k\in I} \chi_k f_{ij} = f_{ij} \sum_{k\in I} \chi_k = f_{ij}.$$

Ahora, como f_{ij} es holomorfa en $X_i \cap X_j$, $\partial f_{ij}/\partial \bar{z} = 0$ (por la Proposición 1.3.3), se tiene que $\partial\psi_i/\partial\bar{z} = \partial\psi_j/\partial\bar{z}$ en $X_i \cap X_j$. Así, podemos definir una función φ en todo $D(0,1)$ con $\varphi = \partial\psi_i/\partial\bar{z}$. Por el Corolario 1.3.9, existe una función diferenciable y acotada ψ en algún disco $D(0,r)$ (para algún radio $r < 1$) con $\varphi = \partial\psi/\partial\bar{z}$ en $D(0,r)$.
Como ψ_i es de cuadrado integrable, también lo será $g_i := \psi_i - \psi$. Además, $\partial g_i/\partial\bar{z} = \partial\psi_i/\partial\bar{z} - \partial\psi/\partial\bar{z} = 0$ en X_i', y por tanto g_i es holomorfa en X_i'. Finalmente,

$$g_i - g_j = \psi_i - \psi_j = f_{ij} \text{ en } X_i' \cap X_j',$$

que es lo que queríamos. □

Observación 2.1.8. Supongamos que Y es una superficie de Riemann compacta. Fijamos $a_0 \in Y$, y tomamos una carta (W_α, z_α) para cada $\alpha \in Y$. Podemos asumir que $a_0 \notin W_\alpha$ para $\alpha \neq a_0$ porque Y es Hausdorff. Por la compacidad de Y, sólo necesitamos finitas cartas para cubrir todo; así que las denotamos por (W_i, z_i) con $i \in I = \{0, ..., s\}$, donde $W_0 := W_{a_0}$. También podemos suponer que $z_i(W_i) = D(0,1)$. De aquí, notamos que existe $0 < r < 1$ tal que los $U_i = \{a \in W_i : |z_i(a)| < r\}$ siguen cubriendo Y. En efecto, Y es la unión de los abiertos $Y_n = \bigcup_{i\in I}\{a \in W_i : |z_i(a)| < 1 - \frac{1}{n}\}$. Como Y es compacto, $Y = Y_N$ para algún N.

Ponemos $\mathcal{U} = (U_i)_{i\in I}$ como en la Observación 2.1.8. Con esta notación, queremos probar:

Teorema 2.1.9. *El cokernel de $\partial : C^0(\mathcal{U}) \to Z^1(\mathcal{U})$ tiene dimensión finita.*

Seguiremos con esta notación por el resto de la sección. Necesitaremos algunos resultados extra para mostrar esto.

Observación 2.1.10. Notemos que podemos elegir r' de modo que $r < r' < 1$, y denotar $V_i = \{a \in W_i : |z_i(a)| < r'\}$. Así, U_i, V_i y W_i son abiertos de Y con $U_i \subseteq V_i \subseteq W_i$ y $Y = \bigcup_{i\in I} U_i$. Además, cada U_i es relativamente compacto en V_i; y asimismo V_i lo es en W_i. Ponemos $\mathcal{V} = (V_i)_{i\in I}$. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} C^1(\mathcal{V}) & \longrightarrow & L^2(V_i \cap V_j \cap V_k) \\ \downarrow & & \downarrow \\ C^1(\mathcal{U}) & \longrightarrow & L^2(U_i \cap U_j \cap U_k), \end{array}$$

donde las flechas horizontales son las funciones $\varphi_{i,j,k}$ de la Definición 2.1.4 y las flechas verticales son restricciones. La linealidad y continuidad de estas funciones induce una función lineal y continua

$$\begin{aligned} Z^1(\mathcal{V}) &\to Z^1(\mathcal{U}) \\ (g_{ij}) &\mapsto (g_{ij}\,|_{U_i\cap U_j}), \end{aligned}$$

que denotaremos por $\theta \mapsto \theta|_{\mathcal{U}}$ y que estudiaremos a continuación.

Lema 2.1.11. *Existe una partición de la unidad en Y asociada a $\mathcal{U} = \{U_i\}_{i\in I}$.*

Demostración. Como en la Observación 2.1.8, podemos elegir $0 < r'' < r$ de modo que los $U_i'' = \{a \in U_i : |z_i(a)| < r''\}$ sigan cubriendo Y. Si ponemos $C_i := Y \setminus \bar{U_i}''$, C_i es abierto y $C_i \cup U_i = Y$. Por la Proposición 1.2.3, existen funciones χ_i' diferenciables en U_i que se anulan exactamente en $U_i \setminus \bar{U_i''}$; y por tanto se pueden extender por 0 a una función diferenciable en Y. Como los U_i'' cubren Y, $\chi = \sum_{i\in I} \chi_i$ es estrictamente positiva, y luego $\chi_i = \frac{\chi_i'}{\chi}$ son una partición de la unidad asociada a U_i. □

Proposición 2.1.12. *Para cada $\xi \in Z^1(\mathcal{U})$ existen $\theta \in Z^1(\mathcal{V})$ y η en $C^0(\mathcal{U})$ con*

$$\xi = \theta|_{\mathcal{U}} + \partial\eta.$$

Demostración. Sea $\xi = (f_{ij}) \in Z^1(\mathcal{U})$. Para un $\alpha \in I$ fijo, $\{U_i \cap W_\alpha\}$ es una cubierta abierta de W_α y existe una partición de la unidad asociada a ella (la restricción a W_α de la partición del Lema 2.1.11). Como $z_\alpha(W_\alpha) = D(0,1)$ y $z_\alpha(V_\alpha) = D(0,r)$ (para algún $0 < r < 1$), la Proposición 2.1.7 nos garantiza que existen $g_{\alpha i}$ en $L^2(U_i \cap V_\alpha, z_\alpha)$ con

$$f_{ij} = g_{\alpha i} - g_{\alpha j}$$

en $U_i \cap U_j \cap V_\alpha$. Si hacemos variar α, tenemos que en $U_i \cap U_j \cap V_\alpha \cap V_\beta$:

$$g_{\alpha i} - g_{\alpha j} = f_{ij} = g_{\beta i} - g_{\beta j},$$

y por tanto $g_{\alpha i} - g_{\beta i} = g_{\alpha j} - g_{\beta j}$. Esto muestra que esta expresión no depende de i, j; y por tanto existe $F_{\alpha\beta}$ holomorfa en $V_\alpha \cap V_\beta$ con

$$F_{\alpha\beta} = g_{\alpha i} - g_{\beta i}$$

en $U_i \cap V_\alpha \cap V_\beta$. Como $g_{\alpha i}, g_{\beta i}$ son de cuadrado integrable en $U_i \cap V_\alpha \cap V_\beta$, también lo será $F_{\alpha\beta}$; y luego $F_{\alpha\beta} \in L^2(V_\alpha \cap V_\beta)$ (porque podemos cubrir $V_\alpha \cap V_\beta$ con los finitos $U_i \cap V_\alpha \cap V_\beta$). Es más, de la Definición de $F_{\alpha\beta}$, estas satisfacen la relación del cociclo, así que $(F_{\alpha\beta}) = \theta \in Z^1(\mathcal{V})$.

Ahora; denotamos $h_\alpha := g_{\alpha\alpha} \in L^2(U_\alpha \cap V\alpha) = L^2(U_\alpha)$, y $\eta = (h_\alpha) \in C^0(\mathcal{U})$. De la Definición de f_{ij} y $F_{\alpha\beta}$, tenemos que

$$f_{\alpha\beta} = g_{\beta\alpha} - g_{\beta\beta} \text{ y } F_{\alpha\beta} = g_{\beta\alpha} - g_{\alpha\alpha} \text{ en } U_\alpha \cap U_\beta$$

y por lo tanto, en $U_\alpha \cap U_\beta$

$$F_{\alpha\beta} - f_{\alpha\beta} = g_{\beta\beta} - g_{\alpha\alpha} = h_\beta - h_\alpha,$$

es decir, que $\theta|_{\mathcal{U}} - \xi = \partial\eta$. □

Denotaremos por $|\cdot|_{\mathcal{U}}$ la norma en $Z^1(\mathcal{U})$ y en $C^0(\mathcal{U})$; y por $|\cdot|_{\mathcal{V}}$ la norma en $Z^1(\mathcal{V})$ y en $C^0(\mathcal{V})$. Además, cuando hagamos referencia a la norma en $Z^1(\mathcal{U})$ de la imagen por restricción de un elemento φ, escribiremos $|\varphi|_{\mathcal{U}}$ en vez de $|\varphi\,|_{\mathcal{U}}\,|_{\mathcal{U}}$ para simplificar la notación.

Corolario 2.1.13. *Existe $C > 0$ con la siguiente propiedad: Para cada $\xi \in Z^1(\mathcal{U})$ existen $\theta \in Z^1(\mathcal{V})$ y η en $C^0(\mathcal{U})$ con $\xi = \theta|_{\mathcal{U}} + \partial\eta$ y*

$$\text{máx}(|\theta|_{\mathcal{V}}, |\eta|_{\mathcal{U}}) \leq C|\xi|_{\mathcal{U}}.$$

Demostración. Sea $H_0 = Z^1(\mathcal{V}) \oplus C^0(\mathcal{U})$. La función

$$\begin{aligned} \pi_0 : H_0 &\to Z^1(\mathcal{U}) \\ (\theta, \eta) &\mapsto \theta|_{\mathcal{U}} + \partial\eta \end{aligned}$$

es lineal y continua por la Observación 2.1.10 y la Proposición 2.1.6. Además, es sobreyectiva por la Proposición 2.1.12. Si ponemos $H = (\text{Ker}(\pi_0))^\perp$, la restricción de π_0 a H es una biyección lineal continua. Por el Teorema 1.1.2, π_0^{-1} es continua, y por tanto existe $C > 0$ con $|\pi_0^{-1}(\xi)| \leq C|\xi|_{\mathcal{U}}$ para todo $\xi \in Z^1(U)$. Finalmente, poniendo $\pi_0^{-1}(\xi) = (\theta, \eta)$, se tiene que $|\pi_0^{-1}(\xi)| = \sqrt{|\theta|_{\mathcal{V}}^2 + |\eta|_{\mathcal{U}}^2} \geq \text{máx}(|\theta|_{\mathcal{V}}, |\eta|_{\mathcal{U}})$. □

Lema 2.1.14. *Sean D, D' abiertos y A compacto con $D' \subseteq A \subseteq D \subseteq \mathbb{C}$. Para cada $\varepsilon > 0$, existe un subespacio cerrado $M \subseteq L^2(D)$ de codimensión finita de modo que $|f|_{D'} \leq \varepsilon|f|_D$ para toda $f \in M$.*

Demostración. Elegimos $r' > 0$ de modo que $D(a, r') \subseteq D$ para todo $a \in A$. Sea $0 < r < r'$. Como A es compacto, existen $a_1, ..., a_s \in A$ de modo que $A \subseteq \bigcup_{j=1}^s D(a_j, \frac{r}{2})$. Dado $\varepsilon > 0$, elegimos $m \in \mathbb{N}$ con $s2^{-2m-2} \leq \varepsilon^2$. Sea M el conjunto de todas las $f \in L^2(D)$ que tienen un cero de orden al menos m en cada a_j. Entonces, M es la intersección de los núcleos de las funciones lineales continuas $L^2(D) \to \mathbb{C}$, $f \to \partial^\mu f(a_j)$, donde $\partial^\mu f$ es la derivada μ-ésima de f, al variar de $\mu = 0, ..., m-1$ y $j = 1, ..., s$. Cada uno de estos núcleos es un subespacio cerrado de $L^2(D)$ y, por el primer Teorema de isomorfismo, de

codimensión ≤ 1. Así, M también es cerrado y de codimensión finita. Por el Lema 1.3.1, para $f \in M$ se tiene:

$$|f|^2_{D(a_j,r)} = \sum_{n=m}^{\infty} d_{nj} r^{2n+2} \quad \text{y} \quad |f|^2_{D(a_j,r/2)} = \sum_{n=m}^{\infty} d_{nj} r^{2n+2} 2^{-2n-2}$$

para algunos coeficientes reales no negativos d_{nj}. Así,

$$|f|^2_{D(a_j,r/2)} \leq 2^{-2m-2} |f|^2_{D(a_j,r)} \leq 2^{-2m-2} |f|^2_D.$$

Además, como $D' \subseteq A \subseteq \bigcup_{j=1}^{s} D(a_j, r/2)$, tenemos que

$$|f|^2_{D'} \leq \sum_{j=1}^{s} |f|^2_{D(a_j,r/2)} \leq s 2^{-2m-2} |f|^2_D \leq \varepsilon |f|^2_D.$$

□

Ahora, estamos en condiciones de mostrar lo que queríamos.

Demostración del Teorema 2.1.9. Sea C la constante del Corolario 2.1.13, y ponemos $\varepsilon = (2C)^{-1}$. Como U_i es relativamente compacto en V_j para cada i, j, lo es también $U_i \cap U_j$ en $V_i \cap V_j$ para cada i, j. Luego, por el Lema 2.1.14, existe un subespacio cerrado M_{ij} de $L^2(V_i \cap V_j, z_i)$ de codimensión finita de modo que para cada $g \in M_{ij}$ se tiene $|g \circ z_i^{-1}|_{z_i(U_i \cap U_j)} \leq \varepsilon |g \circ z_i^{-1}|_{z_i(V_i \cap V_j)}$. Sea M' la suma directa de todos los subespacios M_{ij}, que es un subespacio cerrado de $C^1(\mathcal{V})$ de codimensión finita; y $M = M' \cap Z^1(\mathcal{V})$, que también es un subespacio cerrado de $Z^1(\mathcal{V})$ de codimensión finita. Así, para cada $\nu = (g_{ij}) \in M$ se tiene

$$\begin{aligned} |\nu|_{\mathcal{U}} &= \sqrt{\sum_{i,j \in I} |g_{ij} \circ z_i^{-1}|^2_{z_i(U_i \cap U_j)}} \\ &\leq \sqrt{\sum_{i,j \in I} \varepsilon^2 |g_{ij} \circ z_i^{-1}|^2_{z_i(V_i \cap V_j)}} \\ &\leq \varepsilon |\nu|_{\mathcal{V}}. \end{aligned}$$

Ponemos $F = M^{\perp}$. Definimos $\pi_M : Z^1(\mathcal{V}) \to M$ y $\pi_F : Z^1(\mathcal{V}) \to F$ las proyecciones asociadas a cada subespacio. Ahora, fijamos $\xi \in Z^1(\mathcal{U})$. Construimos sucesiones (ξ_n), (φ_n), (η_n) como sigue: Definimos $\xi_1 = \xi$. Dado ξ_n, lo escribimos en la forma $\xi_n = \theta_n|_{\mathcal{U}} + \partial\eta_n$ como en el Corolario 2.1.13. Esto define η_n y $\varphi_n = \pi_F(\theta_n)$. Además, definimos $\xi_{n+1} = \pi_M(\theta_n)|_{\mathcal{U}}$. Estas sucesiones satisfacen

$$\xi_n = \xi_{n+1} + \varphi_n|_{\mathcal{U}} + \partial\eta_n. \tag{2.1.1}$$

También por el Corolario 2.1.13, máx$(|\theta_n|_{\mathcal{V}}, |\eta_n|_{\mathcal{U}}) \leq C|\xi_n|_{\mathcal{U}}$. Así,

$$\begin{aligned} |\xi_{n+1}|_{\mathcal{U}} &\leq \left|\pi_M(\theta_n)\right|_{\mathcal{U}} \\ &\leq \varepsilon|\pi_M(\theta_n)|_{\mathcal{V}} \\ &\leq \varepsilon|\theta_n|_{\mathcal{V}} \\ &\leq C\varepsilon|\xi_n|_{\mathcal{U}} \\ &= \frac{1}{2}|\xi_n|_{\mathcal{U}}, \end{aligned}$$

y por lo tanto $|\xi_n| \leq 2^{-n+1}c_1$, con $c_1 = |\xi|_{\mathcal{U}}$. Por lo tanto, máx$(|\theta_n|_{\mathcal{V}}, |\eta_n|_{\mathcal{U}}) \leq 2^{-n+1}Cc_1$, y también $|\varphi_n|_{\mathcal{V}} \leq 2^{-n+1}Cc_1$. Sumando en la ecuación 2.1.1 para $n = 1, ..., N$, tenemos que

$$\xi_1 = \xi_{N+1} + \left(\sum_{n=1}^{N} \varphi_n\,|_{\mathcal{U}}\right) + \partial\left(\sum_{n=1}^{N} \eta_n\right).$$

De las cotas que hemos conseguido en la parte anterior, estas sumas parciales forman series de Cauchy, y por lo tanto convergen a $\varphi \in F$ y $\eta \in C^0(\mathcal{U})$ respectivamente. Además, como $\lim \xi_{N+1} = 0$, tenemos que

$$\xi = \varphi|_{\mathcal{U}} + \partial\eta.$$

Como ξ era arbitrario y φ está en el espacio F que es finito dimensional, tenemos lo que queríamos. □

Este Teorema nos permitirá "pegar" funciones que son localmente meromorfas en cada una de las cartas de Y; pero no necesariamente en toda la superficie.

Corolario 2.1.15. *Sea Y una superficie de Riemann compacta y $a_0 \in Y$. Existe una función meromorfa en Y que tiene un polo en a_0 y es holomorfa en $Y \setminus \{a_0\}$.*

Demostración. Sea (W_0, z) una carta de Y con $a_0 \in W_0$ y $z(a_0) = 0$. Para $\nu \in \mathbb{N}$, definimos $\xi_\nu = (f_{ij}^{(\nu)})$ de modo que $f_{ij}^{(\nu)} = 0$ cuando $i, j \neq 0$, $f_{00}^{(\nu)}$=0 y

$$f_{0j}^{(\nu)} = -f_{j0}^{(\nu)} = z^{-\nu} \text{ en } U_0 \cap U_j.$$

La función $z^{-\nu}$ está bien definida en $W_0 \cap W_j$ porque z_0 es biyectiva y $a_0 \notin W_j$ para $j \neq 0$. Además, es continua, y por tanto es acotada en $U_0 \cap U_j$ (que es relativamente compacto). Así, cada f_{ij} es de cuadrado integrable en $U_i \cap U_j$. Además, las funciones f_{ij} satisfacen la relación del cociclo, por lo que hemos definido $\xi_\nu \in Z^1(\mathcal{U})$ para cada $\nu \in \mathbb{N}$. Por el Teorema 2.1.9, ξ_ν son linealmente dependientes modulo la imagen de ∂. Así, existen $c_1, ..., c_n \in \mathbb{C}$, no todos cero, con

$$\sum_{\nu=1}^{n} c_\nu \xi_\nu = \partial\eta, \text{ para algún } \eta \in C^0(\mathcal{U}).$$

Escribimos $\eta = (h_i)_{i\in I}$. Definimos la función $f : Y \setminus \{a_0\} \to \mathbb{C}$ por

$$f(u) = \begin{cases} h_j(u) & \text{para } u \in U_j, j \neq 0 \\ h_0(u) + \sum_{\nu=1}^{n} c_\nu z^{-\nu} & \text{para } u \in U_0. \end{cases}$$

Observamos que f está bien definida puesto que en $U_i \cap U_j$ se tiene:

$$h_j - h_i = \partial\eta = \sum_{\nu=1}^{n} c_\nu f_{ij}^{(\nu)} = \begin{cases} 0 & \text{para } i, j \neq 0 \\ \sum_{\nu=1}^{n} c_\nu z^{-\nu} & \text{para } i = 0, j \neq 0, \end{cases}$$

y por tanto $f(u)$ vale lo mismo al pensarlo como elemento de U_i como de U_j. La función f es claramente holomorfa fuera de a_0, y tiene un polo en a_0 porque los c_ν no son todos cero. □

Teorema 2.1.16. *(de Existencia de Riemann: Versión Analítica) Sea Y una superficie de Riemann compacta. Para cualesquiera $a_1, ..., a_n$ puntos distintos en Y y números complejos $c_1, ..., c_n$ existe una función meromorfa en Y con $f(a_i) = c_i$ para cada i.*

Demostración. Sean $a_1, ..., a_n$ puntos distintos de Y, y $c_1, ..., c_n \in \mathbb{C}$. Por el Corolario 2.1.15, existe una función meromorfa $f^{(i)}$ en Y que tiene un polo en a_i y es holomorfa en $Y \setminus \{a_i\}$ para cada $i = 1, ..., n$. Definimos funciones meromorfas

$$g^{(ij)} = \frac{f^{(i)} - f^{(i)}(a_j)}{f^{(i)} - f^{(i)}(a_j) + d_{ij}}$$

para $i, j = 1, ..., n$ e $i \neq j$; con d_{ij} constantes de modo que el denominador de $g^{(ij)}(a_k)$ no se anule para ningún $k = 1, ..., n$. Notemos que $g^{(ij)}(a_i) = 1$ y $g^{(ij)}(a_j) = 0$. Así, las funciones

$$h^{(i)} = \prod_{j\neq i} g^{(ij)}$$

satisfacen $h^{(i)}(a_k) = \delta_{ik}$. Así, $f = \sum_{i=1}^{n} c_i h^{(i)}$ cumple que $f(a_i) = c_i$. □

2.2. Espacios Cubrientes de Galois

El objetivo de esta sección será estudiar los cubrimientos ramificados de $\mathbb{P}^1_{\mathbb{C}}$; estos objetos serán útiles para traducir el Teorema de Existencia de Riemann en una forma algebraica que utilizaremos durante las próximas secciones.

Definición 2.2.1. Un espacio cubriente $f : R \to S$ es **de Galois** si R (y por tanto S) es conexo por caminos y $\mathrm{Deck}(f)$ actúa transitivamente en las fibras de S. Es **finito** si su grado lo es.

Proposición 2.2.2. *Sea $f : R \to S$ un cubrimiento de Galois, y sea $H = \mathrm{Deck}(f)$.*

(a) El grado n de f es igual al orden de H. Además, para cada U contenido en algún abierto fundamental de S el conjunto $f^{-1}(U)$ tiene n componentes, que son permutados transitivamente por H.

(b) Sean $b \in R$, $p = f(b)$. Existe un homomorfismo sobreyectivo

$$\Phi_b : \pi_1(S, p) \to H = \mathrm{Deck}(f)$$

de modo que $\Phi_b[\gamma]$ envía $b^{[\gamma]}$ en b.

Demostración. Fijado $b \in R$, consideremos la función $\theta_b : H \to f^{-1}(p)$, $\alpha \mapsto \alpha(b)$. Esta función es inyectiva por el Lema 1.4.15, y es sobreyectiva porque f es de Galois. Luego, $|H| = n$. Como cada componente de $f^{-1}(U)$ tiene exactamente un elemento de $f^{-1}(p)$, sigue (a).
Por el Lema 1.4.12, la función $\Psi_b : \pi_1(S, p) \to f^{-1}(p)$, $[\gamma] \mapsto b^{[\gamma]}$ es sobreyectiva. Luego, $\Phi'_b := \theta_b^{-1} \circ \Psi_b$ es una sobreyección $\pi_1(S, p) \to H$. Este no es necesariamente un homomorfismo, pero $\Phi_b : [\gamma] \mapsto \Phi'_b([\gamma])^{-1}$ lo es. Este cumple claramente con las propiedades que queremos. □

Observación 2.2.3. Es natural pensar también en el espacio S como el cociente (topológico) R/H; identificando cada punto $x \in R$ con toda su fibra $f^{-1}(f(x))$ (que podemos siempre realizar como cociente por el grupo de automorfismos por la transitividad de su acción en las fibras). Así, tenemos el diagrama conmutativo:

$$\begin{array}{ccc} & R & \\ {\scriptstyle f}\swarrow & & \searrow{\scriptstyle \pi} \\ S & \xrightarrow[\simeq]{} & R/H, \end{array}$$

donde π es la aplicación cociente. De esta forma, podemos preguntarnos qué grupos H se pueden realizar como grupos de automorfismos de espacios cubrientes de Galois $f : R \to S$. Responderemos esta pregunta para el caso particular de $S = \mathbb{P}^1_{\mathbb{C}} \setminus P$, donde P es un subconjunto finito de $\mathbb{P}^1_{\mathbb{C}}$, en el Teorema 2.2.13 hacia el final de esta sección.

Durante el resto de la sección, P será un subconjunto finito de $\mathbb{P}^1_{\mathbb{C}}$ y $\mathbb{D}(r) = \{z \in \mathbb{C} : 0 < |z| < r\} = D(0, r) \setminus \{0\}$ denota el disco pinchado de radio r en $\mathbb{C}$.

Lema 2.2.4. *La función $f_e : \mathbb{D}(r^{1/e}) \to \mathbb{D}(r)$, $x \mapsto x^e$ es un cubrimiento de Galois de grado e, para cada $e \in \mathbb{N}$. Además, $\mathrm{Deck}(f_e) \simeq C_e$.*

Demostración. f_e es claramente un cubrimiento. Además, las funciones $z \to \zeta_i z$, donde ζ_i es una raíz e-ésima de la unidad, forman un subgrupo de $\mathrm{Deck}(f_e)$ que actúa transitivamente en cada fibra. Concluimos que $\mathrm{Deck}(f_e) \simeq C_e$ por el Lema 1.4.15. □

Proposición 2.2.5. *Sea $f : E \to \mathbb{D}(r)$ un cubrimiento de grado finito e, con E conexo por caminos. Entonces:*

(a) f es equivalente a $f_e : \mathbb{D}(r^{1/e}) \to \mathbb{D}(r)$, $z \mapsto z^e$; y por tanto existe un homeomorfismo $\varphi : E \to \mathbb{D}(r^{1/e})$ con $\varphi(u)^e = f(u)$ para todo $u \in E$. Abreviamos esto con $\varphi^e = f$. Además, φ es único módulo multiplicar por una raíz e-ésima de la unidad ζ.

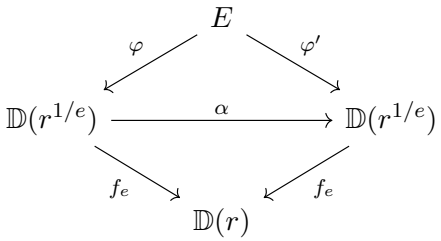
*(b) El grupo $\mathrm{Deck}(f) \simeq C_e$ tiene un único elemento σ con la siguiente propiedad: para cada homeomorfismo $\varphi : E \to \mathbb{D}(r^{1/e})$ con $\varphi^e = f$ se tiene $\varphi \circ \sigma^{-1} = \zeta_e \varphi$, donde $\zeta_e = \exp(\frac{2\pi i}{e})$. El automorfismo σ genera $\mathrm{Deck}(f)$ y se llama el **generador distinguido**.*

(c) Sea $u \in E$ y $p = f(u)$. Sea σ como en (b). Entonces $\gamma(t) = p\exp(2\pi i t)$ es un camino cerrado en $\mathbb{D}(r)$ que pasa por p y el levantamiento de γ via f con punto inicial $\sigma(u)$ tiene punto final u.

(d) Sean $0 < \hat{r} < r$, $\hat{E} := f^{-1}(\mathbb{D})(\hat{r})$ y $\hat{f} = f|_{\hat{E}}$. Entonces $\hat{E}$ es conexo por caminos y $\hat{E} \to \mathbb{D}(\hat{r})$ es un cubrimiento de grado e. El generador distinguido de $\mathrm{Deck}(f)$ se restringe al generador distinguido de $\mathrm{Deck}(\hat{f})$.

Demostración.

(a) Sean $u \in E$ y $p = f(u)$. El grupo fundamental $\Gamma := \pi_1(\mathbb{D}(r), p)$ actúa transitivamente en $f^{-1}(p)$ por el Lema 1.4.12. Como $f^{-1}(p)$ tiene cardinalidad e, el estabilizador Γ_u es un subgrupo de Γ de índice e. Aplicando esto a f_e, tenemos que el estabilizador $\Gamma'_{u'}$ de cualquier $u' \in f_e^{-1}(p)$ tiene índice e en Γ. Como $\Gamma \simeq \mathbb{Z}$ (por la Proposición 1.4.5), sigue que $\Gamma_u = \Gamma'_{u'}$. Así, existe φ por el Lema 1.4.13. La segunda parte sigue del hecho que si φ' cumple estas condiciones entonces $\alpha := \varphi'\varphi^{-1} \in \mathrm{Deck}(f_e)$, y luego es de la forma $z \mapsto \zeta z$ (por la demostración del Lema 2.2.4).

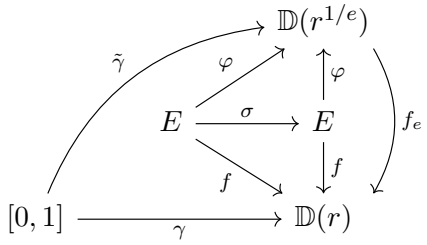


(b) Es fácil ver que $g \mapsto \varphi \circ g \circ \varphi^{-1}$ es un isomorfismo de $\mathrm{Deck}(f) \to \mathrm{Deck}(f_e)$. Además, es independiente de la elección de φ:

$$\varphi' \circ g \circ \varphi'^{-1} = \alpha \circ (\varphi \circ g \circ \varphi^{-1}) \circ \alpha^{-1} = \varphi \circ g \circ \varphi^{-1}$$

porque $\mathrm{Deck}(f_e)$ es abeliano. Por el Lema 2.2.4, multiplicar por ζ_e^{-1} es un generador de $\mathrm{Deck}(f_e)$. Si llamamos σ a la imagen inversa de este generador por el isomorfismo anterior, entonces $\sigma = \varphi^{-1}\zeta_e^{-1}\varphi$; de donde sigue la segunda parte.

(c) Sea $u' = \varphi(\sigma(u)) \in f_e^{-1}(p)$. Definimos el camino $\tilde{\gamma}$ en $\mathbb{D}(r^{1/e})$ por $\tilde{\gamma}(t) = u' \exp(\frac{2\pi i t}{e})$. Así, $f_e \circ \tilde{\gamma}$ es el camino γ de arriba, ya que $f_e(u') = (\varphi(\sigma(u)))^e = f(\sigma(u)) = f(u) = p$. Por lo tanto, $\tilde{\gamma}$ es el levantamiento de γ por f_e con punto inicial u'. Aplicando φ^{-1}, $\varphi^{-1} \circ \tilde{\gamma}$ es el levantamiento de γ vía f con punto inicial $\sigma(u)$. Su punto final es $\varphi^{-1} \circ \tilde{\gamma}(1) = \varphi^{-1}(u'\zeta_e) = \varphi^{-1}(\zeta_e \varphi(\sigma(u))) = u$, por (b).



(d) Sigue de (a).

□

Esto nos permite clasificar los cubrimientos finitos del disco pinchado: son exactamente aquellos de la forma $z \mapsto z^e$.

Proposición 2.2.6. *Sea $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ un cubrimiento de Galois finito, y $p \in P$.*

*(a) Sea $D = D(p, r)$ un disco alrededor de p que no contiene otros elementos de P; de modo que $D^* = D \setminus \{p\}$ esté contenido en $\mathbb{P}^1_{\mathbb{C}} \setminus P$. Sea $\kappa_p : D^* \to \mathbb{D}(r)$ el homeomorfismo $z \mapsto z - p$ si $p \neq \infty$ y $z \mapsto 1/z$ si $p = \infty$. Entonces, para cada componente conexa E de $f^{-1}(D^*)$ la función $f_E = \kappa_p \circ f|_E : E \to \mathbb{D}(r)$ es un cubrimiento finito. Llamamos a E una **componente circular** de nivel r en p.*

(b) Sea $0 < \hat{r} < r$. Hay una correspondencia biyectiva entre las componentes circulares E de nivel r y las componentes circulares $\hat{E}$ de nivel $\hat{r}$ dada por inclusión. Además, si $\hat{E} \subseteq E$, $f_{\hat{E}} = f_E|_{\hat{E}}$ y $\hat{E} = f_E^{-1}(\mathbb{D}(\hat{r}))$.

*(c) El grupo $H := \mathrm{Deck}(f)$ permuta las componentes E de $f^{-1}(D^*)$ transitivamente. Sea H_E el estabilizador de E en H. Restringiendo la acción de H_E a E tenemos un ismomorfismo $H_E \to \mathrm{Deck}(f_E)$, así que H_E es cíclico. Sea $h_E \in H_E$ el elemento correspondiente al generador distinguido de $\mathrm{Deck}(f_E)$. Llamamos a h_E el **generador disntiguido** de H_E.*

(d) Sea $h \in H$ y $E' = h(E)$. Entonces $hh_Eh^{-1} = h_{E'}$, y por tanto los h_E forman una clase de conjugación C_p de H. La clase C_p depende sólo de p, pero no de la

elección de D. Sea e el orden común de los elementos de C_p. El grado del cubrimiento $f_E : E \to \mathbb{D}(r)$ es e para cualquier componente E de $f^{-1}(D^*)$. En particular, $C_p = 1$ si y sólo si f_E es un homeomorfismo.

(e) Sea $p^* \in D^*$ y $\bar{p} = \kappa_p(p^*)$. Sea $\lambda(t) = \kappa_p^{-1}(\bar{p}\exp(2\pi i t))$ un camino cerrado en D^* que pasa por p^*. Sea $b \in R$, $q_0 = f(b)$ y δ un camino en $\mathbb{P}^1_{\mathbb{C}} \setminus P$ uniendo q_0 y p^*. Entonces, $\gamma = \delta^{-1}\lambda\delta$ es un camino cerrado en $\mathbb{P}^1_{\mathbb{C}} \setminus P$ que pasa por q_0 y la función $\Phi_b : \pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus P, q_0) \to H$ de la Proposición 2.2.2 envía $[\gamma]$ a un elemento de C_p.

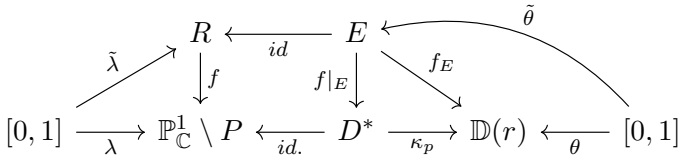
Demostración.

(a) El cubrimiento f se restringe a un cubrimiento $f^{-1}(D^*) \to D^*$. Componiéndolo con el homeomorfismo κ_p, obtenemos un cubrimiento $f^{-1}(D^*) \to \mathbb{D}(r)$. Este se restringe a un cubrimiento $E \to \mathbb{D}(r)$.

(b) Sea $X := f^{-1}(D(p, \hat{r}) \setminus \{p\})$. El espacio $\tilde{E} := f_E^{-1}(\mathbb{D}(r)) = E \cap X$ es conexo por caminos por la Proposición 2.2.5 (d). Es abierto y cerrado en X, así que es una componente conexa de X. Por tanto, es una componente circular de nivel $\hat{r}$ contenida en E. Recíprocamente, consideremos $\hat{E} \subseteq E$ una componente circular de nivel $\hat{r}$ sobre p. Entonces, claramente $f|_{\hat{E}} = f_E|_{\hat{E}}$, así que $\hat{E} \subseteq \tilde{E}$; y por tanto $\hat{E} = \tilde{E}$ porque ambos son componentes conexas.

(c) El grupo H actúa en $f^{-1}(D^*)$, y por tanto permuta las componentes E de $f^{-1}(D^*)$. Sea H_E el estabilizador de E. Si $h \in H$ envía un punto de E a E' entonces $h(E) = E'$ (porque las componentes son disjuntas dos a dos). En particular, si h envía un punto de E a E entonces $h \in H_E$.
Para $p^* \in D^*$, el conjunto $F_E = f^{-1}(p^*) \cap E$ es una fibra de f_E. Como H actúa transitivamente en $f^{-1}(p^*)$, dos puntos de F_E pueden ser llevados al otro por algún elemento de $h \in H$. Por lo tanto, $h \in H_E$ y luego H_E actúa transitivamente en F_E. Por restricción, tenemos un homomorfismo $H_E \to \mathrm{Deck}(f_E)$; inyectivo por el Lema 1.4.15 (si α fija todo E, en particular fija un punto; así que es la identidad). Su imagen es un subgrupo de $\mathrm{Deck}(f_E)$ que actúa transitivamente en la fibra F_E, y por tanto es todo $\mathrm{Deck}(f_E)$ (también por el Lema 1.4.15). Así, tenemos un isomorfismo $H_E \simeq \mathrm{Deck}(f_E)$. Como H actúa transitivamente en $f^{-1}(p^*)$ (y $f^{-1}(p^*)$ intersecta cada E) entonces H permuta las componentes E transitivamente.

(e) El levantamiento $\tilde{\delta}$ de δ por f con punto inicial b tiene punto final b^* en algún componente E de $f^{-1}(D^*)$. Sea $\tilde{\lambda}$ el levantamiento de λ por f con punto inicial $h_E(b^*)$. Entonces, si $\theta = \bar{p}\exp(2\pi i t)$, $\lambda = \kappa_p^{-1} \circ \theta$; y por unicidad de los levantamientos, $\tilde{\lambda}$ es igual al levantamiento $\tilde{\theta}$ de θ por f con punto inicial $h_E(b^*)$. Una vez más por unicidad de los levantamientos, este es igual al levantamiento de θ por f_E. Concluimos por la Proposición 2.2.5 (c) que el punto final de $\tilde{\lambda}$ es b^*.



El camino $h_E \circ \tilde{\delta}$ es el levantamiento de δ con punto inicial $h_E(b)$. Así, $\tilde{\delta}^{-1}\tilde{\lambda}(h_E \circ \tilde{\delta})$ es el levantamiento de γ con punto inicial $h_E(b)$. Claramente, tiene punto final b, así que $\Phi_b([\gamma]) = h_E \in C_p$.

(d) Continuamos con la notación anterior. Sea $h \in H$. Entonces $h \circ \tilde{\lambda}$ es el levantamiento de λ por f con punto inicial $h(h_E(b^*)) \in h(E) = E'$. El camino $h \circ \tilde{\lambda}$ tiene punto final $h(b^*)$. Como en (e), notamos que h'_E lleva el punto final de $h \circ \tilde{\lambda}$ a su punto inicial. Por tanto, $h_{E'}(h(b^*)) = h(h_E(b^*))$; y por tanto $h_E^{-1}h^{-1}h_{E'}h$ fija b^* y luego es la identidad (por el Lema 1.4.15). En la situación de (b), con $\hat{E} \subseteq E$, tenemos $h_{\hat{E}} = h_E$ por la Proposición 2.2.5 (d). Luego, la clase C_p no depende del radio r de D. La igualdad $e = \deg(f_E)$ sigue de la Proposición 2.2.5 (b), y el resto de (a).

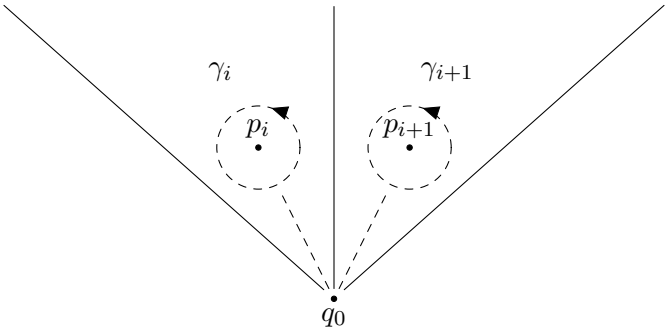
□

Estudiaremos un poco más estas componentes circulares en la sección 2.4. Ahora, queremos estudiar los caminos en el plano complejo pinchado $\mathbb{C} \setminus \{p_1, ..., p_n\}$. Diremos que el camino $\exp(2\pi it)$ recorre el círculo en sentido antihorario, y $\exp(-2\pi it)$ en sentido horario.

Lema 2.2.7. *Sean $\{X_j\}_{j\in I}$ subconjuntos abiertos de un espacio topológico X de modo que $X = \bigcup_{j\in I} X_j$. Entonces, cada camino δ en X es homotópico al producto de finitos caminos δ_ν con δ_ν un camino en algún X_j.*

Demostración. Evidente (ver, por ejemplo, [9, Lema 4.26]). □

Fijamos ahora un poco de notación. Sean $p_1, ..., p_n \in \mathbb{C}$ puntos distintos, y $X = \mathbb{C} \setminus \{p_1, ..., p_n\}$. Elegimos un punto $q_0 \in X$ de modo que el segmento de q_0 a p_i no contenga otros p_j. Escribimos $p_i = q_0 + \rho_i \exp(i\nu_i)$, con $\rho_i \in \mathbb{R}^+$ y $\nu_i \in [0, 2\pi]$. Reetiquetamos los p_i de modo que $\nu_1 > \nu_2 > ... > \nu_n$. Elegimos $M_1, ..., M_n$ rayos en $\mathbb{C}$ con punto inicial q_0 de modo que cada componente conexa de $\mathbb{C} \setminus \{M_1, ..., M_n\}$ contiene exactamente un p_i. Llamamos X_i a la componete conexa que contiene p_i, y D_i a un disco alrededor de p_i cuya clausura está contenida en X_i. γ_i será un camino con inicio en q_0 viajando en línea recta hacia p_i hasta alcanzar la frontera de D_i, luego viajará una vez en sentido antihorario por esta frontera y luego volverá a q_0 por el segmento de p_i a q_0.



Teorema 2.2.8. *Con esta notación, se tiene que:*

(a) Los caminos $\gamma_1, ..., \gamma_n$ son caminos cerrados en X con inicio en q_0 y sus clases generan $\pi_1(X, q_0)$.

(b) Sea G un grupo con generadores $g_1, ..., g_n$. Existe un cubrimiento de Galois $f : R \to X$, un isomorfismo $\theta : \mathrm{Deck}(f) \to G$ y un punto $b \in f^{-1}(q_0)$ de modo que la composición de θ con la sobreyección $\Phi_b : \pi_1(X, q_0) \to \mathrm{Deck}(f)$ de la Proposición 2.2.2 envía $[\gamma_i]$ a g_i. Si identificamos G con $\mathrm{Deck}(f)$ vía θ y G es finito, entonces $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus \{p_1, ..., p_n, \infty\}$ es un cubrimiento de Galois finito y las clases asociadas $C_i := C_p$ y C_∞ cumplen

$$g_i \in C_i \quad y \quad (g_1 \cdots g_n)^{-1} \in C_\infty.$$

Demostración.

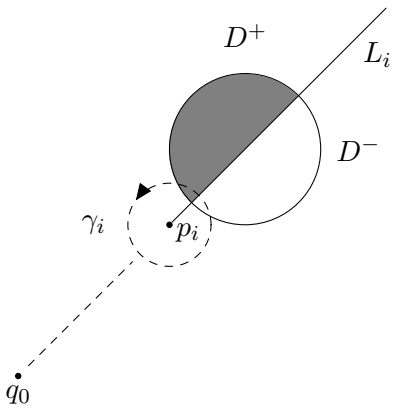
(a) Agrandamos cada X_i a $X_i' = \{a \in \mathbb{C} : d(a, X_i) < \varepsilon\}$ de modo que $X_i' \cap D_j = \emptyset$ para $i \neq j$. Así los X_i' forman una cubierta abierta de $\mathbb{C}$, y por lo tanto $X_i' \setminus \{p_i\}$ forman una cubierta abierta de X. Sea γ un camino cerrado en X con inicio q_0. Por el Lema 2.2.7, podemos escribir $\gamma \simeq \delta_s \cdots \delta_1$, donde cada δ_ν es un camino en algún $T_\nu := X_{i_\nu}' \setminus \{p_{i_\nu}\}$. Sea κ_ν el camino que une q_0 y el punto inicial de δ_ν en línea recta (como este punto está en T_ν y $T_{\nu-1}$, κ_ν es un camino en $T_\nu \cap T_{\nu-1}$); y κ_{s+1} el camino constante q_0. Ponemos $\omega_\nu = \kappa_{\nu+1}^{-1} \delta_\nu \kappa_\nu$. Luego, ω_ν es un camino cerrado en T_ν que pasa por q_0 y γ es homotópico en X al producto de los ω_ν. Ahora, notemos que el espacio T_ν es homeomorfo a $\mathbb{D}(1)$, y por tanto su grupo fundamental es isomorfo a $\mathbb{Z}$ y generado por γ_{i_ν} (por la Proposición 1.4.5). Así, ω_ν es homotópico a una potencia de γ_{i_ν} y luego γ es homotópico a un producto de potencias de γ_i.

(b) Sea L_i el rayo en la línea de q_0 a p_i; con punto inicial en p_i y de modo que $q_0 \notin L_i$. Sea $Q = X \setminus (L_1 \cup ... \cup L_n)$. Como conjunto, definimos $R = X \times G$. Ahora definiremos una topología en R especificando una base de vecindades para cada punto de R. Fijemos $(q, g) \in R$. Si $q \in Q$, la base consistirá de todos los $B \times \{g\}$, donde B es un disco abierto centrado en q contenido en Q. Si $q \in L_i$, entonces la base consistirá de

todos los

$$\hat{D}_g = (D^- \times \{g\}) \cup (D^+ \times \{gg_i^{-1}\}),$$

donde D es un disco abierto alrededor de q que no intersecta ningún q_0p_j con $j \neq i$ y que no contenga p_i. Además, D^+ es la mitad abierta de D en el lado "positivo" de L_i; y D^- la mitad semicerrada en el lado "negativo" de D (como en la figura).



Claramente, para cualquier par de vecindades de (q, g); se tiene que una debe estar contenida en la otra. Por tanto, esta base de vecindades define una topología en R.
Afirmación 1: La función $f : R \to X$, $(q, g) \mapsto q$ es un cubrimiento.
Demostración. En la notación anterior, tenemos $f^{-1}(B) = \bigcup_{g\in G} B\times\{g\}$ y $f^{-1}(D) = \bigcup_{g\in G} \hat{D}_g$. Claramente, cada $B \times \{g\}$ es homeomorfo a B; y cada $\hat{D}_g$ es homeomorfo a D.
Afirmación 2: Para cada $h \in G$, la función $\alpha_h : R \to R$, $(q, g) \mapsto (q, hg)$ es un automorfismo de f. Además, se tiene $\alpha_{hh'} = \alpha_h \circ \alpha_{h'}$.
Demostración. La segunda parte es evidente e implica que α_h es biyectiva, con inversa $\alpha_{h^{-1}}$. Además, α_h permuta las vecindades que definen la topología en R. En efecto, $\alpha_h(B\times\{g\}) = B\times\{hg\}$ y $\alpha_h(\hat{D}_g) = \hat{D}_{hg}$. Así, α_h es un homeomorfismo. Concluimos porque $f \circ \alpha_h = f$.
Afirmación 3: $f : R \to X$ es un cubrimiento de Galois, y $G \to \mathrm{Deck}(f)$, $g \mapsto \alpha_g$ es un isomorfismo.
Demostración. Primero, mostramos que R es conexo por caminos. Cada uno de sus subconjuntos $Q \times \{g\}$ es homeomorfo a Q y por tanto conexo por caminos. Sea C la componente conexa de R que contiene a $Q \times \{1\}$. Sea D un disco alrededor de $q \in L_i$ como en el enunciado. Entonces, existe un camino en $\hat{D}_1$ que une $Q \times \{1\}$ a $Q\times\{g_i^{-1}\}$; y por tanto C contiene $Q\times\{g_i^{-1}\}$. Como $\alpha_{g_i^{-1}}$ envía $Q\times\{1\}$ en $Q\times\{g_i^{-1}\}$, C es invariante para todo α_{g_i}; y luego para todo α_g (porque g_i generan G). Por tanto, C contiene todos los $Q \times \{g\}$. Así, C es denso en R. Como las componentes conexas son cerradas, $C = R$ y luego R es conexo por caminos. Ahora, por la afirmación 2, el grupo $\{\alpha_g : g \in G\}$ es un subgrupo de $\mathrm{Deck}(f)$. Este actúa transitivamente en cada fibra $f^{-1}(q)$; por tanto f es un cubrimiento de Galois y $\mathrm{Deck}(f) = \{\alpha_g : g \in G\}$.

(Por el Lema 1.4.15)
Afirmación 4: El levantamiento de γ_i con punto inicial $b = (q_0, 1)$ tiene punto final (q_0, g_i^{-1}).
Demostración. El camino γ_i se intersecta con L_i en exactamente un punto en el tiempo t_i. Definimos:

$$\tilde{\gamma_i}(t) = \begin{cases} (\gamma_i(t), 1) & \text{para } t \leq t_i \\ (\gamma_i(t), g_i^{-1}) & \text{para } t > t_i \end{cases}.$$

Observemos que $\tilde{\gamma_i}$ es continua por la Definición de la topología en R. Luego, $\tilde{\gamma_i}$ es el levantamiento de γ_i con punto inicial $(q_0, 1)$.
Desde ahora en adelante, identificaremos G con $\mathrm{Deck}(f)$ por el isomorfismo $g \mapsto \alpha_g$.
Afirmación 5: Se tiene que $\Phi_b([\gamma_i]) = g_i$. Así, g_i está en la clase C_i de $G = \mathrm{Deck}(f)$ asociada a p_i.
Demostración. Por la Definición de Φ_b, el automorfismo $\Phi_b([\gamma_i])$ de f envía el punto final (q_0, g_i^{-1}) de $\tilde{\gamma_i}$ a su punto inicial $b = (q_0, 1)$. Así, $\Phi_b([\gamma_i]) = g_i$. El camino γ_i tiene las propiedades del camino γ de la Proposición 2.2.6 (e), para $p = p_i$. Luego, $\Phi_b([\gamma_i]) \in C_{p_i} = C_i$.
Afirmación 6: Sea $\rho > 0$ suficientemente grande de modo que q_0 y todos los p_i están en el círculo K_0 alrededor de 0 de radio ρ. Entonces, el camino $\gamma_\infty = \gamma_1 \cdots \gamma_n$ es homotópico en X a un camino γ' que va de q_0 en una línea recta hasta alcanzar K_0, luego gira una vez en sentido antihorario por su frontera y vuelve en línea recta a q_0.
Demostración. Sea D un disco abierto alrededor de q_0 conteniendo todos los p_i. Sea $X_i^* := X_i \cap D$ (un segmento de D). γ_i es homotópico en X a un camino γ_i^* que comienza y termina en q_0 y recorre una vez la frontera de X_i^* en sentido antihorario. Así, γ_∞ es homotópico a $\gamma_1^* \dots \gamma_n^*$; que a su vez es homotópico a un camino γ^* que va en línea recta de q_0 a la frontera de D, recorre una vez esta frontera en sentido antihorario y vuelve a q_0 por la misma línea. Terminamos porque γ^* es homotópico a γ'.
Afirmación 7: $(g_1 \dots g_n)^{-1} \in C_\infty$.
Demostración. Sea γ' como en la afirmación 6. El camino $\gamma := (\gamma')^{-1}$ tiene las propiedades de 2.2.6 (e), para $p = \infty$. Luego, $\Phi_b([(\gamma')^{-1}]) \in C_\infty$. Por otro lado, $\Phi_b([(\gamma')^{-1}]) = \Phi_b([(\gamma_\infty]) = g_1 \dots g_n$ por las afirmaciones 5 y 6.

□

El resultado siguiente se obtiene usualmente como aplicación del Teorema de Seifert-Van Kampen en el marco de la topología algebraica (ver, por ejemplo, [20, Capítulo 4] o [17, Capítulo 11]). Sin embargo, la teoría que hemos desarrollado hasta ahora nos permite concluir de forma alternativa en este caso en particular.

Corolario 2.2.9. *En la notación del Teorema, el grupo fundamental* $\pi_1(X, q_0)$ *de* $X = \mathbb{C} \setminus \{p_1, \dots, p_n\}$ *está generado libremente por* $\gamma_1, \dots, \gamma_n$. *Además, para cualesquiera* $(n+1)$

puntos $p_1, ..., p_{n+1}$ distintos en S^2, el grupo fundamental de $S^2 \setminus \{p_1, ..., p_{n+1}\}$ es libre de rango n.

Demostración. La segunda afirmación es directa de la primera porque S^2 es homeomorfa a $\mathbb{C}\setminus\{p_{n+1}\}$. Para la primera afirmación, sea G el grupo libre en $g_1, ..., g_n$. Por el Teorema 2.2.8 (b), existe un homomorfismo $\pi_1(X, q_0) \to G$ enviando $[\gamma_i]$ a g_i. Como G es libre, existe un homomorfismo $G \to \pi_1(X, q_0)$ enviando g_i a $[\gamma_i]$. Estos homomorfismos son inversos uno del otro. □

Definición 2.2.10. Consideremos las triplas $(G, P, \mathbf{C})$, donde G es un grupo finito, P es un subconjunto finito de $\mathbb{P}^1_{\mathbb{C}}$ y $\mathbf{C} = (C_p)_{p\in P}$ es una familia de clases de conjugación no triviales de G. Decimos que dos triplas $(G, P, \mathbf{C})$ y $(G', P', \mathbf{C}')$ son equivalentes si $P = P'$ y existe un isomorfismo $G \to G'$ que envía C_p a C'_p para cada $p \in P$. Esta es una relación de equivalencia; por lo que denotamos la clase de $(G, P, \mathbf{C})$ por $\mathcal{T} = [G, P, \mathbf{C}]$. Un **tipo de ramificación** es una clase del tipo $\mathcal{T}$.

Definición 2.2.11. Sea $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ un cubrimiento de Galois finito. Sea $H = \mathrm{Deck}(f)$, y para cada $p \in P$ sea C_p la clase de conjugación asociada a p de H (de la Proposición 2.2.6). Sea $P' = \{p \in P : C_p \neq 1\}$. Definimos el **tipo de ramificación** de f como la clase de la tripla $(H, P', (C_p)_{p\in P'})$.

Observación 2.2.12. El tipo de ramificación se comporta "bien" bajo cambios de coordenadas. Sea $g : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ un homeomorfismo de la forma $z \mapsto z-p_0$, $\infty \mapsto \infty$ o bien de la forma $z \mapsto 1/z$, $0 \mapsto \infty$, $\infty \mapsto 0$. En la notación de la Definición, $\tilde{f} := g \circ f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ es otro cubrimiento de Galois finito, con $\mathrm{Deck}(\tilde{f}) = H$. Además, $\tilde{f}$ es de tipo de ramificación $[H, g(P'), (C_{g^{-1}(q)})_{q\in g(P')}]$. En efecto, sea $p \in P$ y γ un camino como en la Proposición 2.2.6 (e) (girando una vez alrededor de p en sentido antihorario). Entonces $\tilde{\gamma} := g \circ \gamma$ es un camino girando una vez alrededor de $g(p)$ en sentido antihorario, porque g preserva la orientación. Sea $b \in f^{-1}(q_0)$, donde q_0 es el punto inicial de γ. El levantamiento de $\tilde{\gamma}$ vía $\tilde{f}$ es igual al levantamiento de γ vía f, ambos con punto inicial b. El (único) elemento de H que envía el punto final de este levantamiento a b está en la clase de $H = \mathrm{Deck}(f)$ asociada con p, y también en la clase de $H = \mathrm{Deck}(\tilde{f})$ asociada con $g(p)$ (por la Proposición 2.2.6 (e)).

Con esto, estamos listos para probar el Teorema central de la sección.

Teorema 2.2.13. *(de Existencia de Riemann: Versión Topológica) Sea $T = [G, P, (K_p)_{p\in P}]$ un tipo de ramificación. Sea $r = |P|$, y denotamos por $p_1, ..., p_r$ los elementos de P. Entonces, existe un cubrimiento de Galois finito de $\mathbb{P}^1_{\mathbb{C}} \setminus P$ de tipo de ramificación T si y sólo si existen generadores $g_1, ..., g_r$ de G con $g_1 \cdots g_r = 1$ y $g_i \in K_{p_i}$.*

Demostración. Por la Observación 2.2.12, podemos aplicar un cambio de coordenadas para que $\infty = p_r \in P$.
Primero, supongamos que G tiene generadores $g_1, ..., g_r$ como en el Teorema. Por el Teorema 2.2.8 (b), tomando $n = r - 1$, existe un cubrimiento de Galois finito $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ y una identificación de $\mathrm{Deck}(f)$ con G de modo que $g_i \in C_{p_i}$ de $\mathrm{Deck}(f)$ asociada con p_i, para cada $i = 1, ..., n$. Además, $g_r = (g_1 \cdots g_n)^{-1} \in C_\infty = C_{p_r}$. Por tanto, $C_p = K_p$ para todo $p \in P$; y luego f tiene tipo T.
Recíprocamente, supongamos que $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ es un cubrimiento finito de Galois de tipo T. Entonces, tenemos $G = \mathrm{Deck}(f)$ y $K_p = C_p$, la clase asociada a cada $p \in P$. Sea $X = \mathbb{P}^1_{\mathbb{C}} \setminus P$, y $n = r - 1$. Elegimos $q_0 \in X$ y caminos $\gamma_1, ..., \gamma_n$ como en el Teorema 2.2.8. Ponemos $\gamma_r = (\gamma_1 \cdots \gamma_{r-1})^{-1}$. Fijamos $b \in f^{-1}(q_0)$, y consideramos el homomorfismo sobreyectivo $\Phi_b : \pi_1(X, q_0) \to G$ de la Proposición 2.2.2. Como en la demostración del Teorema 2.2.8, tenemos que $g_i := \Phi_b([\gamma_i]) \in C_{p_i}$ para cada $i = 1, ..., r$. Estos elementos generan G por el Teorema 2.2.8 (a), y claramente $g_1 \dots g_r = 1$. □

2.3. Extensiones de Campos de Funciones

En esta sección, estudiaremos las extensiones de campos finitas de $k(x)$.

Definición 2.3.1. Sea k un campo y sea Λ el conjunto de todas las sucesiones $(a_i)_{i\in\mathbb{Z}}$ de elementos $a_i \in k$ para las cuales existe un $N \in \mathbb{Z}$ tal que $a_i = 0$ para $i < N$. Definimos la suma en Λ por $(a_i) + (b_i) = (a_i + b_i)$ y el producto por $(a_i)(b_j) = (c_n)$, donde $c_n = \sum_{i+j=n} a_i b_j$. Es rutina chequear que Λ es un campo con estas operaciones (donde 0 es la sucesión (a_i) con $a_i = 0$ para todo i y 1 es la sucesión (b_i) con $b_0 = 1$, $b_i = 0$ para todo $i \neq 0$); lo denotaremos por $k((t))$ y lo llamaremos el **campo de series formales de Laurent sobre** k.

Observación 2.3.2. Quizá la única parte algo confusa de mostrar que Λ es efectivamente un campo es ver la existencia de los inversos. En este caso, para un elemento $(a_i)_{i\in\mathbb{Z}}$ con $a_i = 0$ para $i < N$, tomamos la sucesión $(b_i)_{i\in\mathbb{Z}}$ con $b_i = 0$ para $i < -N$; $b_{-N} = a_N^{-1}$; y luego resolvemos inductivamente las ecuaciones

$$\sum_{i+j=n} a_i b_j = 0$$

para n desde $-N$ en adelante. Así, (b_i) es inverso de (a_i).

Observación 2.3.3. Claramente, podemos ver k como un subcampo de $k((t))$ a través de la inclusión $a \mapsto (a_i)$ con $a_0 = a$, $a_i = 0$ para $i \neq 0$. Además, si llamamos t a la sucesión (a_i) con $a_1 = 1$, $a_i = 0$ para $i \neq 1$; tenemos un isomorfismo entre el anillo $k[t]$

y el subanillo de $k((t))$ generado por k y t:

$$\sum_{i=0}^{M} a_i t^i = (a_i),$$

donde $a_i = 0$ si $i < 0$ o $i > M$. En general, usaremos la notación $\sum_{i=N}^{\infty} a_i t^i$ para referirnos a la sucesión análoga con $a_i = 0$ si $i < N$.

Definición 2.3.4. El subanillo de $k((t))$ que consiste de todas las sumas $\sum_{i=0}^{\infty} a_i t^i$ se llama el **anillo de series formales de potencia sobre** k, y se denota por $k[[t]]$.

Claramente, $k((t))$ es el campo de fracciones de $k[[t]]$, lo que justifica la notación. En particular, $k((t))$ contiene $k(t)$.

Definición 2.3.5. Es fácil chequear que la función $\sigma : k[[t]] \to k$ que envía $\sum_{i=0}^{\infty} a_i t^i$ a su término constante a_0 es un homomorfismo de anillos (es la "evaluación en $t = 0$"). Si $F(y)$ es un polinomio en $k[[t]][y]$, denotamos por $F_0(y)$ al polinomio obtenido al aplicar σ a los coeficientes de F.

Lema 2.3.6. *Sea F un polinomio mónico en $k[[t]][y]$. Supongamos que $F_0 \in k[y]$ se factoriza como $F_0 = gh$ para $g, h \in k[y]$ mónicos y coprimos. Entonces, $F = GH$ con G, H mónicos en $k[[t]][y]$ con $G_0 = g$, $H_0 = h$.*

Demostración. Extendiendo la notación de la Observación 2.3.3, escribimos

$$F = \sum_{i=0}^{\infty} F_i t^i$$

con $F_i \in k[y]$. Ponemos $m := \deg(F) = \deg(F_0)$. Entonces $\deg(F_i) < m$ para $i > 0$. Sean $r = \deg(g)$, $s = \deg(h)$. Queremos encontrar

$$G = \sum_{i=0}^{\infty} G_i t^i \quad \text{y} \quad H = \sum_{i=0}^{\infty} H_i t^i$$

con $G_0 = g$, $H_0 = h$ y $G_i, H_i \in k[y]$ de grados $< r$, $< s$ respectivamente; y con $F = GH$. La condición $F = GH$ es equivalente al sistema de ecuaciones

$$F_n = \sum_{i+j=n} G_i H_j$$

para $n \in \mathbb{N}$. Resolvemos estas ecuaciones de manera inductiva: Para $n = 0$, tenemos la hipótesis $F_0 = gh = G_0 H_0$. Ahora, para $n > 0$, supongamos que ya hemos encontrado

G_i, H_j para todos los $i, j < n$ con $i + j = \nu$ para $\nu < n$. La n-ésima ecuación se puede escribir como

$$G_0 H_n + H_0 G_n = U_n \tag{2.3.1}$$

donde $U_n = F_n - \sum_{i=1}^{n-1} G_i H_{n-i}$ tiene grado menor a m. Para completar la inducción, basta mostrar que el sistema 2.3.1 tiene solución para $G_n, H_n \in k[y]$ de grado $< r$, $< s$ respectivamente. Como G_0, H_0 son coprimos en $k[y]$, existen $P, Q \in k[y]$ con $G_0 P + H_0 Q = U_n$. Por el algoritmo de división, podemos escribir $P = H_0 S + R$ para $S, R \in k[y]$ con $\deg(R) < s$. Si ponemos $H_n = R$ y $G_n = Q + G_0 S$, se satisface el sistema 2.3.1 y $\deg(H_n) < s$ por construcción. Además, como $H_0 G_n = U_n - G_0 H_n$, $\deg(H_0 G_n) < m$, así que $\deg(G_n) < r$. □

Corolario 2.3.7. *Sea k un campo algebraicamente cerrado de característica 0, y $F \in k[[t]][y]$ un polinomio mónico de grado $n \geq 2$. Supongamos que el coeficiente de y^{n-1} en F_0 es 0 y que $F_0(y) \neq y^n$. Entonces, $F = GH$ con $G, H \in k[[t]][y]$ mónicos y no constantes.*

Demostración. Como k es algebraicamente cerrado, $F_0 \in k[y]$ se factoriza como producto de factores lineales mónicos. Si estos factores no son todos iguales, entonces $F_0 = gh$ para g, h no constantes y coprimos en $k[y]$. Luego, el resultado sigue del Lema. Si $F_0 = (y-a)^n$, entonces el coeficiente de y^{n-1} es $-na$; y por tanto $a = 0$ (porque k tiene característica 0). Pero entonces $F_0 = y^n$, contradicción. □

Definición 2.3.8.

(a) Para cada entero positivo e, $\mathbb{Z}e^{-1}$ será el conjunto de todos los números racionales de la forma i/e, con $i \in \mathbb{Z}$. $\mathbb{Z}e^{-1}$ es un grupo aditivo, isomorfo a $\mathbb{Z}$ por la función $i \mapsto i/e$. Este contiene $\mathbb{Z}$ como subgrupo de índice e.

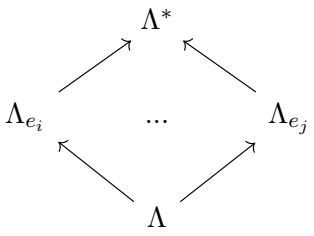
(b) Definimos Λ_e como el conjunto de todas las sucesiones $(a_j)_{j \in \mathbb{Z}e^{-1}}$ de elementos $a_j \in k$ para las cuales existe un $N < 0$ tal que $a_j = 0$ para $j < N$. Si definimos la suma y el producto como en la Definición 2.3.1, Λ_e es un campo isomorfo a $\Lambda = k((t))$ a través de la función $(a_j)_{j \in \mathbb{Z}e^{-1}} \mapsto (b_i)_{i \in \mathbb{Z}}$ donde $b_i = a_{i/e}$. Bajo este isomorfismo, el elemento t de Λ corresponde al elemento $\tau = (a_j)$ en Λ_e con $a_{1/e} = 1$ y $a_j = 0$ para $j \neq 1/e$.

Identificamos Λ con el subcampo de Λ_e que consiste de todas las sucesiones $(a_j)_{j \in \mathbb{Z}e^{-1}}$ con $a_j = 0$ si $j \notin \mathbb{Z}$. Así, $\tau^e = t$. En la notación simbólica de la Observación 2.3.3, escribimos el elemento general (a_j) de Λ_e como

$$\sum_{j \in \mathbb{Z}e^{-1}} a_j t^j = \sum_{i \in \mathbb{Z}} a_{i/e} \tau^i = \sum_{i \in \mathbb{Z}} b_i \tau^i$$

identificando Λ_e con $k((t^{1/e})) = k((\tau))$.

Observación 2.3.9. Esta definición recuerda un poco a la definición del campo de series de Puiseux sobre k, con la diferencia que los campos Λ_e admiten sólo exponentes con denominador e para t; mientras que el campo de series de Puiseux admite todo tipo de exponentes racionales para t. Se puede mostrar que, si k es algebraicamente cerrado y de característica 0, el campo de series de Puiseux es la clausura algebraica de Λ. Por tanto, tenemos un diagrama de extensiones de campos:



donde Λ^* es el campo de series de Puiseux sobre k y e_i, e_j son números naturales. Desde aquí, es interesante preguntar qué puede pasar con las extensiones de campos intermedias a Λ^*/Λ, por ejemplo. No consideraremos esta línea de estudio, pero se puede leer más sobre ella, por ejemplo, en [24].

Lema 2.3.10. *Sea $e \in \mathbb{Z}$ positivo, y supongamos que k contiene una raíz primitiva e-ésima de la unidad ζ_e. Entonces, Λ_e es de Galois sobre Λ de grado e. El grupo de Galois de la extensión es cíclico, generado por $\omega : \sum_{i\in\mathbb{Z}} b_i\tau^i \mapsto \sum_{i\in\mathbb{Z}}(b_i\zeta_e^i)\tau^i$. Además, $\Lambda_e = \Lambda(\tau)$ con $\tau^e = t$.*

Demostración. Es rutina chequear que ω es un automorfismo de Λ_e. Su campo fijo consiste de los $\sum_{i\in\mathbb{Z}} b_i\tau^i$ con $b_i = 0$ a menos que $\zeta_e^i = 1$; es decir, a menos que e divida i. Por tanto, el campo fijo de ω es Λ. Sigue del Teorema 1.5.24 que Λ_e/Λ es de Galois y tiene grupo de Galois $\langle\omega\rangle$. Además, es claro que ω tiene orden e; y luego $[\Lambda_e : \Lambda] = |\operatorname{Gal}(\Lambda_e/\Lambda)| = e$. Tenemos que ω envía τ a $\zeta_e\tau$, así que ω^μ envía τ a $\zeta_e^\mu\tau$. De aquí, sigue que ningún elemento no trivial de $\operatorname{Gal}(\Lambda_e/\Lambda)$ fija τ. De las inclusiones $\Lambda \subseteq \Lambda(\tau) \subseteq \Lambda_e$, tenemos que $\operatorname{Gal}(\Lambda_e/\Lambda(\tau)) \leq \operatorname{Gal}(\Lambda_e/\Lambda)$. Como ningún elemento no trivial de $\operatorname{Gal}(\Lambda_e/\Lambda)$ fija τ, entonces $\operatorname{Gal}(\Lambda_e/\Lambda(\tau)) = \{\mathrm{id}\}$; y por tanto $[\Lambda_e : \Lambda(\tau)] = 1$. Concluimos entonces que $\Lambda_e = \Lambda(\tau)$. □

Lema 2.3.11. *Si k es un campo algebraicamente cerrado de característica 0 y $F \in k[[t]][y]$ es un polinomio mónico no constante, entonces F tiene una raíz en algún Λ_e.*

Demostración. Supongamos que F es de grado minimal y para el que falla el Lema. Evidentemente, $n = \deg(F) \geq 2$. Escribimos $F(y) = y^n + \lambda_{n-1}y^{n-1} + ... + \lambda_0$, con

$\lambda_\nu \in k[[t]]$. Entonces, el polinomio

$$\tilde{F}(y) = F\left(y - \frac{\lambda_{n-1}}{n}\right)$$

tiene coeficiente cero en y^{n-1}. Reemplazamos F por $\tilde{F}$ para asegurar esto. Si además $F_0(y) \neq y^n$, entonces F se factoriza como en el Corolario 2.3.7; lo que contradice la hipótesis sobre la minimalidad de F. Esto implica que $F_0 = y^n$, y por tanto todos los λ_ν tienen término libre cero.
Notemos que existe algún ν entre 0 y $n-2$ con $\lambda_\nu \neq 0$ (si no, $F = y^n$ tiene raíz 0). Consideraremos sólo estos λ_ν por el resto de la demostración. Sea m_ν la menor potencia de t que aparece con coeficiente no cero en λ_ν:

$$\lambda_\nu = at^{m_\nu} + \text{ términos de mayor orden}$$

con $a \in k$ no cero. Sea u el mínimo de los números $m_\nu/(n-\nu)$. Como u es un racional positivo, ponemos $u = d/e$, con d, e enteros positivos. Ahora, veremos Λ incrustado en $\Lambda_e = k((\tau))$ como arriba. Consideramos el polinomio

$$F^*(y) = \tau^{-dn}F(\tau^d y) = y^n + \sum_{\nu=0}^{n-2} \lambda_\nu \tau^{d(\nu-n)} y^\nu \in \Lambda_e[y].$$

El coeficiente de y^ν de este polinomio (si no es cero) es una serie de Laurent en τ de la forma

$$\begin{aligned}\lambda_\nu \tau^{d(\nu-n)} &= at^{m_\nu}\tau^{d(\nu-n)} + \text{ términos de mayor orden} \\ &= a\tau^{E_\nu} + \text{ términos de mayor orden}\end{aligned}$$

donde

$$E_\nu = e(n-\nu)\left(\frac{m_\nu}{n-\nu} - u\right) \geq 0$$

y $E_\nu = 0$ para al menos un ν. Por lo tanto, cada coeficiente de F^* es una serie de potencia en τ, y para al menos un ν esta serie de potencias tiene término constante no cero. Por lo tanto, F^* satisface las condiciones del Corolario 2.3.7 con t reemplazada por τ. Luego, $F^* = GH$ con factores en $k[[\tau]]$ como en este resultado. Así H tiene grado estrictamente menor a n, y luego tiene raíz en algún $\Lambda_e(\tau^{1/e'})$ por la minimalidad de n. Luego, F^* tiene raíz en $\Lambda_e(\tau^{1/e'}) = (\Lambda_e)_{e'}$, y por lo tanto F también. □

Teorema 2.3.12. *Si k es un campo algebraicamente cerrado de característica 0, y Δ es una extensión de Λ de grado e, entonces $\Delta = \Lambda(\delta)$ con $\delta^e = t$.*

Demostración. Por el Teorema 1.5.16, podemos poner $\Delta = \Lambda(\theta)$. Sea $F \in \Lambda[y]$ un polinomio irreducible con raíz θ. Por el Lema 1.5.4 podemos asumir que F es mónico. Así, por el Lema 2.3.11, F tiene una raíz θ' en algún $\Lambda_{e'}$. Por tanto, podemos asumir que

$\Delta \subseteq \Lambda_{e'}$. Como $\mathrm{Gal}(\Lambda_{e'}/\Lambda)$ es cíclico de orden e' (por el Lema 2.3.10), para cada divisor e de e' hay un único campo intermedio a Λ y $\Lambda_{e'}$ de grado e sobre Λ (por el Teorema 1.5.22). Luego $\Delta = \Lambda_e = \Lambda(t^{1/e})$, por el Lema 2.3.10. □

Definición 2.3.13. Un **sistema compatible de raíces primitivas n-ésimas de la unidad** es una sucesión $(\zeta_n)_{n\geq 1}$ de raíces primitivas n-ésimas de la unidad de modo que si $n = n'n''$ entonces $\zeta_n^{n''} = \zeta_{n'}$.

Observación 2.3.14. En $\mathbb{C}$, la elección canónica es $\zeta_n = \exp(2\pi i/n)$.

Por el resto de la sección, k será un campo algebraicamente cerrado de característica 0, y (ζ_n) será un sistema compatible de raíces primitivas n-ésimas de la unidad.

Definición 2.3.15. Sea $\Lambda = k((t))$, y Δ/Λ una extensión de Galois finita de grado e. Por el Teorema 2.3.12, $\Delta = \Lambda(\delta)$ con $\delta^e = t$. Luego, existe un único $\omega \in \mathrm{Gal}(\Delta/\Lambda)$ con $\omega(\delta) = \zeta_e\delta$. Llamamos a ω el **generador distinguido** de $\mathrm{Gal}(\Delta/\Lambda)$.

Observación 2.3.16. Notemos que para cada $\delta' \in \Lambda$ con $(\delta')^{e'} = t$ para algún $e' \geq 1$ se tiene $\omega(\delta') = \zeta_{e'}\delta'$. Como e/e' es un entero, basta mostrar el resultado para $\delta^{e/e'}$ (todos los otros δ' difieren de él por una raíz e'-ésima de la unidad). En efecto, $\omega(\delta') = \zeta_e^{e/e'}\delta' = \zeta_{e'}\delta'$ por la compatibilidad de ζ_n. En particular, si $\Lambda \subseteq \Delta' \subseteq \Delta$ entonces $\omega|_{\Delta'}$ es el generador distinguido de $\mathrm{Gal}(\Delta'/\Lambda)$.

Definición 2.3.17. Escribiremos $\mathbb{P}^1_k = k \cup \{\infty\}$, con $\infty \notin k$. Además, para cada $p \in \mathbb{P}^1_k$ definimos el isomorfismo $\nu_p : k(x) \to k(t)$ como la identidad en k y $x \mapsto t + p$ si $p \neq \infty$; o bien $x \mapsto 1/t$ si $p = \infty$.

A esta notación se le puede dar un significado más profundo a través de la teoría de espacios proyectivos; pero para nosotros será simplemente una notación formal. Por supuesto, esta noción encaja (sin pensar en la estructura topológica) con la del espacio proyectivo $\mathbb{P}^1_k$ (se puede leer sobre esta teoría, por ejemplo, en [21, Capítulo 4]). Extendemos cada $\alpha \in \mathrm{Aut}(k)$ a $\mathbb{P}^1_k$ por $\alpha(\infty) = \infty$.

Proposición 2.3.18. *Sea $L/k(x)$ una extensión de Galois finita, y sean $G = \mathrm{Gal}(L/k(x))$, $p \in \mathbb{P}^1_k$.*

(a) Podemos extender $\nu_p : k(x) \to k(t)$ a un isomorfismo $\nu : L \to L_\nu$, donde L_ν es un subcampo de alguna extensión de Galois finita Δ/Λ, de modo que $\mathrm{Gal}(\Delta/\Lambda)$ deja L_ν invariante. Definimos $g_\nu \in G$ como

$$g_\nu = \nu^{-1} \circ \omega \circ \nu$$

donde ω es el generador distinguido de $G(\Delta/\Lambda)$. Si Δ' es otra extensión de Galois finita de Λ, con subcampo $L_{\nu'}$ y $\nu' : L \to L_{\nu'}$ extendiendo ν_p, entonces g_ν y $g_{\nu'}$ pertenecen a la misma clase de conjugación de G. Esta clase de conjugación depende sólo de p, así que la llamamos la ***clase de conjugación asociada a*** *p de G.*

(b) Sea e el orden común de los elementos de C_p. Este número $e = e_{L,p}$ se llama la ***ramificación*** *de L en p. Tiene la siguiente propiedad: Sea γ un elemento primitivo de la extensión $L/k(x)$ (que existe por el Corolario 1.5.16). Entonces γ satisface un polinomio irreducible $F(y) \in k(x)[y]$. Sea $\nu_p F \in k(x)[y]$ el polinomio obtenido al aplicar ν_p a los coeficientes de F. Luego todos los factores irreducibles H de $\nu_p F$ en $\Lambda[y]$ tienen grado e. Además, podemos tomar $\Delta = \Lambda_e$ en (a).*

(c) Podemos elegir γ en (b) de modo que $F(y) = F(x, y) \in k[x, y]$ es mónico en y. Luego el discriminante $D(x)$ de $F(y)$ sobre $k(x)$ es distinto de cero en $k[x]$. Además, si $p \in k$ y $D(p) \neq 0$, entonces $e_{L,p} = 1$.

(d) Si $L'/k(x)$ es una extensión de Galois finita con $L' \subseteq L$, entonces el homomorfismo de restricción de G en $G' = \mathrm{Gal}(L'/k(x))$ envía C_p a la clase C'_p de G' asociada a p.

Demostración.

(a) En las notaciones de (b), notamos que el campo $\Delta = \Lambda[y]/(H)$ contiene una raíz γ' de H. Luego, podemos extender ν_p a un isomorfismo ν de $L = k(x)(\gamma)$ a $L_\nu = k(t)(\gamma') \subseteq \Delta$. Como $\mathrm{Gal}(\Delta/\Lambda)$ permuta las raíces de $\nu_p F$ y L_ν está generado sobre $k(t)$ por estas raíces, L_ν queda invariante.
Para la segunda parte, podemos asumir que Δ y Δ' son subcampos de alguna extensión de Galois finita Δ_0 de Λ. Como L_ν y $L_{\nu'}$ son subcampos de Δ_0 y están ambos generados sobre $k(t)$ por las raíces de $\nu_p F$, $L_\nu = L_{\nu'}$. Denotamos $h = \nu^{-1}\nu' \in G$. Como el generador distinguido ω_0 de $\mathrm{Gal}(\Delta_0/\Lambda)$ se restringe al generador distinguido de $\mathrm{Gal}(\Delta/\Lambda)$ (y similarmente para Δ') se tiene que

$$g'_\nu = \nu'^{-1}\omega_0\nu' = h^{-1}\nu^{-1}\omega_0\nu h = h^{-1}g_\nu h$$

porque $\nu h = \nu'$ y $h^{-1}\nu^{-1} = \nu'^{-1}$ por Definición.

(b) Notemos que el grado $[\Delta : \Lambda]$ es igual al orden de ω, y por la forma de g_ν este a su vez es igual al orden de g_ν. Por Definición, el orden de g_ν es $e_{L,p}$, así que $\deg(H) = [\Delta : \Lambda] = e_{L,p}$. Concluimos porque por el Teorema 2.3.12 tenemos un isomorfismo entre las extensiones Δ/Λ y Λ_e/Λ.

(c) Por el Lema 1.5.4 podemos asumir que F es mónico en y en $k[x, y]$. Lo pensamos como polinomio en $k(x)[y]$. Su discriminante $D(x) \in k[x]$ es distinto de cero porque F es irreducible y por tanto separable (porque la característica de k es 0, usando la Proposición 1.5.13 y el Teorema 1.5.15). Notemos que para cada $b \in k$, $F(b, y)$ tiene discriminante $D(b)$; y por tanto $F(p, y)$ es separable cada vez que $D(p) \neq 0$ (por el

mismo razonamiento que en la demostración del Lema 1.5.21).
Tenemos que $\nu_p F(y) = F(t+p, y)$. Por tanto $\nu_p F$ es un polinomio mónico en y con coeficientes en $k[t]$. Además, $(\nu_p F)_0(y) = F(p, y)$. Como $F(p, y)$ es separable, el Lema 2.3.6 nos dice que $\nu_p F$ se factoriza como producto de factores lineales en $\Lambda[y]$. Luego, $e_{L,p} = \deg(H) = 1$.

(d) $\tilde{\nu} = \nu|_{L'}$ es un isomorfismo de L' a $\tilde{\nu}(L') \subseteq \Delta$ que extiende ν_p. Luego $g_{\tilde{\nu}} = \tilde{\nu}^{-1}\omega\tilde{\nu} = \nu^{-1}\omega\nu|_{L'} = (g_\nu)_{L'}$

□

Definición 2.3.19. Sea $L/k(x)$ una extensión de Galois finita y $p \in \mathbb{P}^1_k$. Decimos que p es un **punto branch** de $L/k(x)$ si $e_{L,p} > 1$ (o, equivalentemente, si la clase C_p de $\mathrm{Gal}(L/k(x))$ es no trivial).

Sigue de (c) en la Proposición 2.3.18 que el número de puntos branch es finito. Por tanto, hemos definido dos invariantes de una extensión de Galois finita $L/k(x)$: el conjunto de puntos branch $P \subseteq \mathbb{P}^1_{\mathbb{C}}$ y las clases de conjugación C_p. Esto motiva la siguiente Definición:

Definición 2.3.20. Sea $L/k(x)$ una extensión de Galois finita. El **tipo de ramificación** de $L/k(x)$ es el tipo $T = [\mathrm{Gal}(L/k(x)), P, (C_p)_{p\in P}]$, donde P es el conjunto de puntos branch de $L/k(x)$ y C_p es la clase de conjugación asociada a p en $\mathrm{Gal}(L/k(x))$.

2.4. Conexión entre Extensiones y Cubrimientos

A continuación, desarrollaremos la interacción entre extensiones finitas de campos de $\mathbb{C}(x)$ y cubrimientos ramificados de $\mathbb{P}^1_{\mathbb{C}}$. Durante esta sección, P es un subconjunto finito de $\mathbb{P}^1_{\mathbb{C}}$, $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ es un cubrimiento de Galois finito y $H = \mathrm{Deck}(f)$.

Definición 2.4.1. Decimos que $r > 0$ es **suficientemente pequeño** si $D(p, r) \cap P = \{p\}$ para todo $p \in P$. Ahora fijemos $p \in P$. Definimos una relación en el conjunto de componentes circulares de p de nivel suficientemente pequeño: $E \equiv E'$ si $E \subseteq E'$ o $E' \subseteq E$. Por la Proposición 2.2.6 (b), esto es una relación de equivalencia. Estas clases de equivalencia se llaman los **puntos ideales** de R sobre p.

Observación 2.4.2. Fijemos un r suficientemente pequeño. Por la Proposición 2.2.6 (b), cada punto ideal de p está representada por exactamente una componente circular de nivel r sobre p. Por tanto, el número de puntos ideales sobre p es igual al número de componentes E de $f^{-1}(D^*)$. Como $\mathrm{Deck}(f)$ permuta estos componentes transitivamente, el número de puntos ideales sobre p es $\leq |\mathrm{Deck}(f)| = \deg(f)$.

Queremos pensar intuitivamente en los puntos ideales como los centros faltantes de los componentes E. Ahora, pondremos estos centros.

Proposición 2.4.3. *Sea $\bar{R}$ la unión disjunta de R y todos sus puntos ideales sobre $p \in P$. Decimos que $V \subseteq \bar{R}$ es abierto si $V \cap R$ es abierto en R y por cada punto ideal $\pi \in V$ existe un $E \in \pi$ con $E \subseteq V$. Esto vuelve a $\bar{R}$ un espacio de Hausdorff compacto y conexo por caminos. El cubrimiento f se extiende a una sobreyección continua $\bar{f} : \bar{R} \to \mathbb{P}^1_{\mathbb{C}}$ con $\bar{f}(\pi) = p$ para cada punto ideal sobre p. Además, cada $\alpha \in \mathrm{Deck}(f)$ se extiende de manera única a un homeomorfismo $\bar{\alpha} : \bar{R} \to \bar{R}$ con $\bar{f} \circ \bar{\alpha} = \bar{f}$.*

Demostración. Es claro que la topología inducida en $\bar{R}$ coincide con la topología original en R y que $\bar{f}$ es sobreyectiva. Sea $p \in P$ y $\pi_1, ..., \pi_m$ los puntos ideales sobre p. Para cada $j = 1, ..., m$ y r suficientemente pequeño hay exactamente un $E_j \in \pi_j$ de nivel r y

$$\bar{f}^{-1}(D(p,r)) = \bigcup_{j=1}^{m} E_j \cup \{\pi_j\}. \tag{2.4.1}$$

De aquí sigue que $\bar{f}$ es continua, ya que f lo es y por tanto basta que exista un disco $D(p,r)$ alrededor de cada $p \in P$ de modo que $\bar{f}^{-1}(D(r,p))$ sea abierto.
Tomemos $\alpha \in \mathrm{Deck}(f)$. Para cada $p \in P$, α permuta los componentes E_j. Definimos $\bar{\alpha}(\pi_j) = \pi_k$ si $\alpha(E_j) = E_k$. Esto extiende α a una biyección $\bar{\alpha} : \bar{R} \to \bar{R}$ con $\bar{f} \circ \bar{\alpha} = \bar{f}$. $\bar{\alpha}$ es un homeomorfismo porque α lo es y porque $\bar{\alpha}$ permuta las vecindades $E_j \cup \{\pi_j\}$. Es único porque R es denso en $\bar{R}$.
Vemos que $\bar{R}$ es Hausdorff. Si dos puntos tienen imagen distinta por $\bar{f}$, podemos separarlos con dos vecindades $\bar{f}^{-1}(U)$ diferentes porque f es un espacio cubriente. Como R ya es Hausdorff, basta ver qué pasa para los puntos π, π' sobre el mismo $p \in P$. Estos los podemos separar por los abiertos $E \cup \{\pi\}$, $E' \cup \{\pi'\}$ con $E \in \pi$ y $E' \in \pi'$.
Como R es conexo por caminos y denso en $\bar{R}$, $\bar{R}$ lo es. Para terminar, basta probar que $\bar{R}$ es compacto. En primer lugar, notamos que $\bar{R}$ tiene una base numerable: tomamos todos los componentes $f^{-1}(U)$, donde U es un abierto fundamental para f de la forma $U = D(a,r)$, con $a \in \mathbb{Q} \cup \{\infty\}$ y $r \in \mathbb{Q}$. Además, tomamos todos los conjuntos $E \cup \{\pi\}$, con π un punto ideal y $E \in \pi$ de nivel $r \in \mathbb{Q}$ suficientemente pequeño. Cada abierto de $\bar{R}$ es una unión de estos conjuntos. Así, por el Teorema 1.2.5, basta ver que X es secuencialmente compacto. Sea (a_n) una sucesión en $\bar{R}$. Entonces, $\bar{f}(a_n)$ forma una sucesión en el espacio compacto $\mathbb{P}^1_{\mathbb{C}}$; y por tanto tiene una subsucesión $\bar{f}(a_{n_k})$ convergente a $p \in \mathbb{P}^1_{\mathbb{C}}$. Si $p \in P$, sean $\pi_1, ..., \pi_m$ los puntos ideales sobre p. Afirmamos que uno de los π_j es un punto límite de (a_{n_k}). Supongamos que no. Entonces cada π_j tiene una vecindad $E_j \cup \{\pi_j\}$ con $E_j \in \pi_j$ que no contiene ningún a_n. Podemos asumir que los E_j son todos del mismo nivel r. Por lo tanto, vale la ecuación 2.4.1 y por tanto $D(p,r)$ no contiene ningún $\bar{f}(a_{n_k})$; una contradicción. Asimismo, si $p \notin P$ procedemos de manera similar; usando abiertos fundamentales de f alrededor de p. □

Lema 2.4.4. *Consideramos abiertos $U \subseteq \mathbb{P}^1_{\mathbb{C}} \setminus P$ contenidos en algún abierto fundamental de f que satisfacen $\{0,\infty\} \not\subset U$. Para cada componente V de $f^{-1}(U)$, la función f se restringe a un homeomorfismo $V \to U$ (por Definición). Sea $\varphi = f|_V$ si $\infty \notin U$, y $\varphi = 1/(f|_V)$ si $\infty \in U$. Entonces (V,φ) son cartas de R; y R es una superficie de Riemann con ellas con la propiedad que $f : R \to \mathbb{P}^1_{\mathbb{C}}$ es holomorfa. Además, cada $\alpha \in H$ se vuelve una función holomorfa $\alpha : R \to R$.*

Demostración. Si (V_1,φ_1) y (V_2,φ_2) son cartas como arriba, entonces $\varphi_1\varphi_2^{-1}$ es la identidad o $1/z$; en cualquier caso biholomorfa. Como claramente cubren R, R es una superficie de Riemann con ellas. En coordenadas locales, f es la identidad o $1/z$; y cada $\alpha \in H$ es también la identidad o $1/z$. Por tanto, ambas son holomorfas. □

Observación 2.4.5. Sea $\bar{f} : \bar{R} \to \mathbb{P}^1_{\mathbb{C}}$ la extensión de f que construimos en la Proposición 2.4.3. Desde ahora, sólo escribiremos $f = \bar{f}$. Sea π un punto ideal de R y ponemos $p = f(\pi)$. Para cada $E \in \pi$ de nivel r, consideramos el cubrimiento $f_E = \kappa_p \circ f|_E : E \to \mathbb{D}(r)$ de grado finito e de la Proposición 2.2.6. Por la Proposición 2.2.5, existe un homeomorfismo $\varphi : E \to \mathbb{D}(r^{1/e})$ con $\varphi^e = f_E$. Este se extiende a un homeomorfismo

$$\varphi_\pi : V_\pi = E \cup \{\pi\} \to D(0, r^{1/e}) = \mathbb{D}(r^{1/e}) \cup \{0\}$$

que envía π a 0 (es un homeomorfismo porque las vecindades $\hat{E} \cup \{\pi\}$ se corresponden con los discos $D(0,\hat{r}^{1/e})$ por la parte (b) de la Proposición 2.2.6).

Lema 2.4.6. *Las cartas del Lema 2.4.4 y de la Observación 2.4.5 le dan estructura de superficie de Riemann compacta a $\bar{R}$ de modo que $f : \bar{R} \to \mathbb{P}^1_{\mathbb{C}}$ es holomorfa, Además, cada $\alpha \in H$ se extiende de manera única a un homeomorfismo holomorfo $\bar{\alpha} : \bar{R} \to \bar{R}$ con $f \circ \bar{\alpha} = f$.*

Demostración. Primero, mostramos que una carta (V_π,φ_π) es compatible con las cartas (V,φ) del otro tipo. En las notaciones de la Observación 2.4.5, tenemos que $\varphi_\pi^e = f_E = \kappa_p \circ f$ en $V \cap V_\pi$, donde $p = f(\pi)$. Por tanto $\varphi\varphi_\pi^{-1}$ es la función $z \mapsto \kappa_p^{-1}(z^e)$ o la función $z \mapsto 1/\kappa_p^{-1}(z^e)$; y en cualquier caso es biholomorfa. Ahora, supongamos que (V_π,φ_π) y $(V'_{\pi'},\varphi'_{\pi'})$ son de la misma forma. Podemos asumir que $\pi = \pi'$ (si no, la intersección de V_π y $V'_{\pi'}$ está cubierta por cartas del otro tipo); y luego podemos suponer que $V_\pi \subseteq V'_{\pi'}$ por la Proposición 2.2.6(b). Ponemos $V_\pi = E \cup \{\pi\}$, con $E \in \pi$ de nivel r. Luego $\varphi'_\pi\varphi_\pi^{-1}$ es multiplicar por una raíz ζ de la unidad (por la Proposición 2.2.5(a)). Como $z \mapsto \zeta z$ es biholomorfa, las cartas son compatibles. De esto, $\bar{R}$ es una superficie de Riemann compacta.
Mostramos ahora que f es holomorfa. Alrededor de cada punto ideal π que no está sobre ∞, la representación de f en cartas es $f \circ \varphi_\pi^{-1} = \kappa_p^{-1}(z^e)$, que es holomorfa. Asímismo, si π está sobre ∞ la representación de f en cartas será $1/(\kappa_p^{-1}(z^e))$; también holomorfa. Así, f es holomorfa en los puntos ideales, y por el Lema 2.4.4 es holomorfa en todo $\bar{R}$.
Finalmente, sabemos que $\alpha \in H$ se extiende únicamente a un homeomorfismo $\bar{\alpha} : \bar{R} \to \bar{R}$

con $f \circ \bar{\alpha} = f$ (por la Proposición 2.4.3). También sabemos del Lema 2.4.4 que α es holomorfa en R. Consideremos una carta (V_π, φ_π), y notemos que $(\bar{\alpha}(V_\pi), \varphi_\pi \circ \bar{\alpha}^{-1})$ es otra carta de $\bar{R}$. En estas coordenadas locales, $\bar{\alpha}$ es la función $z \mapsto \zeta z$ (como más arriba); y luego α es holomorfa. □

Observación 2.4.7. Claramente, los homeomorfismos $\bar{\alpha}$ con $\alpha \in H$ forman un grupo con la composición isomorfo a H bajo la función $\alpha \mapsto \bar{\alpha}$, así que desde ahora escribimos $\alpha = \bar{\alpha}$. Esto identifica H con un grupo de automorfmismos de $\bar{R}$ como superficie de Riemann. Este grupo actúa transitivamente en cada fibra $f^{-1}(p)$; para $p \notin P$ no es más que el hecho que f es Galois, para $p \in P$ es la Proposición 2.2.6(c) (los puntos ideales de f sobre p son los componentes E de f^{-1} de D^* como en la Proposición).

Lema 2.4.8. *Supongamos que $g \in \mathcal{M}(\bar{R})$ satisface $g \circ \alpha = g$ para todo $\alpha \in H$. Luego, $g = g' \circ f$ para algún $g' \in \mathcal{M}(\mathbb{P}^1_{\mathbb{C}})$.*

Demostración. Como H actúa transitivamente en cada fibra $f^{-1}(p)$, sigue que g toma el mismo valor en cada punto de la fibra. Definimos $g'(p)$ como este valor. Si $U \subseteq \mathbb{P}^1_{\mathbb{C}} \setminus (P \cup \{\infty\})$ está contenido en un abierto fundamental de f y V es una componente de $f^{-1}(U)$, entonces en U tenemos que $g' = g \circ (f|_V)^{-1}$. Como $f|_V : V \to U$ es una carta de R, g' es meromorfa en U. Haciendo variar U vemos que g' es meromorfa en $\mathbb{P}^1_{\mathbb{C}} \setminus (P \cup \{\infty\})$. Además, g' es continua en cada $p \in \mathbb{P}^1_{\mathbb{C}}$, ya que localmente se puede escribir en la forma $g' = g \circ (f)^{-1}$ para cada punto de $\bar{R}$ (y luego es composición de funciones continuas). Por tanto, g' es meromorfa en cada punto $p \in \mathbb{P}^1_{\mathbb{C}}$ por el Corolario 1.3.5. Así, $g' \in \mathcal{M}(\mathbb{P}^1_{\mathbb{C}})$. □

Teorema 2.4.9. *Sea $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ un cubrimiento de Galois finito. Sea $f : \bar{R} \to \mathbb{P}^1_{\mathbb{C}}$ su extensión a una función holomorfa en la superficie de Riemann compacta $\bar{R}$ (en la notación del Lema 2.4.6). Vemos $H = \mathrm{Deck}(f)$ como grupo de isomorfismos de $\bar{R}$ (como en la Observación 2.4.7). Sea $\mathcal{M} = \mathcal{M}(\bar{R})$ el campo de funciones meromorfas en $\bar{R}$, y $\mathbb{C}(f)$ el subcampo de $\mathcal{M}$ generado por f y las funciones constantes $\mathbb{C}$-valuadas. Entonces, para cada $\alpha \in H$, la función*

$$\begin{aligned} \iota_\alpha : \mathcal{M} &\to \mathcal{M} \\ g &\mapsto g \circ \alpha^{-1} \end{aligned}$$

es un automorfismo de $\mathcal{M}$. La extensión $\mathcal{M}/\mathbb{C}(f)$ es de Galois, y la función

$$\begin{aligned} \iota : H &\to \mathrm{Gal}(\mathcal{M}/\mathbb{C}(f)) \\ \alpha &\mapsto \iota_\alpha \end{aligned}$$

es un isomorfismo.

Demostración. Para g in $\mathcal{M}$, $g \circ \alpha^{-1}$ está en $\mathcal{M}$ porque α es un isomorfismo de $\bar{R}$ (y por tanto es biholomorfa). Así, ι_α está bien definida. Es, además, claramente inyectiva y sobreyectiva ($g \circ \alpha \mapsto g$). Luego, ι_α es un automorfismo de $\mathcal{M}$ que fija $\mathbb{C}(f)$ (fija f por el Lema 2.4.6). También es claro que $\iota_{\alpha\beta} = \iota_\alpha \iota_\beta$. Por lo tanto, $\alpha \mapsto \iota_\alpha$ es un homomorfismo de grupos de H a $G \leq \mathrm{Gal}(\mathcal{M}/\mathbb{C}(f))$. El campo fijo de G consiste de los $g \in \mathcal{M}$ con $g \circ \alpha = g$ para todo $\alpha \in H$. Por tanto, por el Lema 2.4.8, $g = g' \circ f$ con $g' \in \mathcal{M}(\mathbb{P}^1_{\mathbb{C}})$. Como $\mathcal{M}(\mathbb{P}^1_{\mathbb{C}}) = \mathbb{C}(z)$ (por el Lema 1.3.13), sigue que $g \in \mathbb{C}(f)$. Hemos probado que el campo fijo de G en $\mathcal{M}$ es $\mathbb{C}(f)$. Por tanto, por el Teorema 1.5.24, $\mathcal{M}/\mathbb{C}(f)$ es de Galois con grupo de Galois G. Sólo falta mostrar que ι es inyectiva, así que sea $\alpha \in H$ con $\iota_\alpha = id$. Sea $a \in \bar{R}$, y $p = f(a)$. Por el Teorema 2.1.16, existe una función $g \in \mathcal{M}$ que toma valores distintos dos a dos en $f^{-1}(p)$. Como $b := \alpha(a) \in f^{-1}(p)$ y $g(b) = \iota_\alpha(g)(b) = (g(\alpha^{-1}(b)) = g(a)$, sigue que $a = b$. Así, $\alpha(a) = a$ y luego $\alpha = id$ por el Lema 1.4.15, que es lo que queríamos. □

Teorema 2.4.10. *Usamos las mismas notaciones que en el Teorema 2.4.9. Para cada $p \in P$, sea C_p^{top} la clase de conjugación de $H = \mathrm{Deck}(f)$ asociada con p en la Proposición 2.2.6. Para cada $p \in \mathbb{P}^1_{\mathbb{C}}$, sea C_p^{alg} la clase de conjugación de $G = \mathrm{Gal}(\mathcal{M}/\mathbb{C}(f))$ asociada con p en la Proposición 2.3.18, para $x = f$. Entonces, $C_p^{alg} = 1$ si $p \notin P$. Además, para cada $p \in P$, el isomorfismo $\iota : H \to G$ envía C_p^{top} a C_p^{alg}. Por tanto, $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ y $\mathcal{M}/\mathbb{C}(f)$ tienen el mismo tipo de ramificación.*

Demostración. Sea $\Lambda = \mathbb{C}((t))$ el campo de series formales de Laurent sobre $\mathbb{C}$ (como en la Definición 2.3.1).
Caso 1: $p \in \mathbb{P}^1_{\mathbb{C}} \setminus P$.
Sea $v \in f^{-1}(p)$. Hay una carta (V, φ) (como en el Lema 2.4.6) con $v \in V$. Si $p \neq \infty$, podemos asumir que $\infty \notin \varphi(V)$ y $\varphi = f|_V$. Si $p = \infty$, tenemos $\varphi = 1/(f|_V)$. Cada $g \in \mathcal{M}$ tiene una expansión en serie de Laurent alrededor de v de la forma

$$g = \sum_{i=N}^{\infty} a_i(\varphi - \varphi(v))^i$$

en esta carta coordenada. Enviando g a $\sum_{i=N}^{\infty} a_i t^i$ tenemos un homomorfismo de campos

$$\nu : \mathcal{M} \to \Lambda.$$

Este homomorfismo es claramente distinto de 0, así que es inyectivo. Queremos computar $\nu(f)$. Si $p \neq \infty$, entonces $f = \varphi = p + (\varphi - \varphi(v))$ en V, así que $\nu(f) = p + t$. Si $p = \infty$, entonces $f = 1/\varphi = 1/(\varphi - \varphi(v))$ en V, asi que $\nu(f) = t^{-1}$. De esta forma, $\nu : \mathcal{M} \to \Lambda$ extiende la función $\nu_p : \mathbb{C}(f) \to \mathbb{C}(t)$ de la Proposición 2.3.18 para $x = f$. Luego, el subcampo asociado L_ν en esta proposición es simplemente Λ (contenido en la extensión Λ/Λ) y por tanto generador distinguido ω de la extensión asociada es la identidad. Luego, el índice de ramificación en p de $\mathcal{M}/\mathbb{C}(f)$ es 1 y por tanto $C_p^{alg} = 1$.
Caso 2: $p \in P$.

Sea $\pi \in f^{-1}(p)$ un punto ideal. Sea (V_π, φ_π) una carta coordenada alrededor de π como en la Observación 2.4.5. En particular, $V_\pi = E \cup \{\pi\}$ y $\varphi_\pi^e = \kappa_p \circ f$ en V_π. Cada $g \in \mathcal{M}$ tiene una expansión en serie de Laurent alrededor de π de la forma

$$g = \sum_{i=N}^{\infty} b_i \varphi_\pi^i$$

y llevando g a $\sum_{i=N}^{\infty} b_i \tau^i$ tenemos una inclusión

$$\nu : \mathcal{M} \to \Lambda_e = \mathbb{C}((\tau))$$

con la notación de 2.3.8. Aquí, queremos pensar en $\Lambda = \mathbb{C}((t))$ como subcampo de $\Lambda_e = \mathbb{C}((\tau))$, con $t = \tau^e$. Como arriba, ν extiende $\nu_p : \mathbb{C}(f) \to \Lambda$. En efecto, de $\varphi_\pi^e = \kappa_p \circ f$ tenemos que $f = \kappa_p^{-1} \circ \varphi_\pi^e = p + \varphi_\pi^e$ si $p \neq \infty$ y $f = 1/\varphi_\pi^e$ si $p = \infty$. Así, $\nu(f) = p + \tau^e = p + t$ en el primer caso y $\nu(f) = \tau^{-e} = t^{-1}$ en el segundo. Sea ω el generador distinguido de $\mathrm{Gal}(\Lambda_e/\Lambda)$ (como en la Definición 2.3.15). Por la Definición de la clase C_p^{alg} (en la Proposición 2.3.18), contiene el elemento

$$\nu^{-1} \circ \omega \circ \nu.$$

Por la Definición de la clase C_p^{top} (en la Proposición 2.2.6), contiene el generador distinguido h_E del estabilizador de E en H. Por lo tanto, el Teorema sigue de mostrar que

$$\iota(h_E) = \nu^{-1} \circ \omega \circ \nu.$$

En efecto, por Definición, h_E fija E (y por tanto V_π) e induce el generador distinguido del cubrimiento $f_E = \kappa_p \circ f : E \to \mathbb{D}(r)$. Como $\varphi_\pi^e = f_E$ en E, $\varphi_\pi \circ h_E^{-1} = \zeta_e \varphi_\pi$ (en E) por la Proposición 2.2.5(b). Para $g \in \mathcal{M}$ como arriba, tenemos que

$$\iota(h_E)(g) = g \circ h_E^{-1} = \sum_{i=N}^{\infty} b_i (\varphi_\pi \circ h_E^{-1})^i = \sum_{i=N}^{\infty} b_i (\zeta_e \varphi_\pi)^i = \sum_{i=N}^{\infty} (b_i \zeta_e^i) \varphi_\pi^i$$

en una vecindad de π. Por el Lema 2.3.10, ω envía $\sum_{i=N}^{\infty} b_i \tau^i$ a $\sum_{i=N}^{\infty} (b_i \zeta_e^i) \tau^i$, así que

$$(\nu^{-1} \circ \omega \circ \nu)(g) = (\nu^{-1} \circ \omega) \left(\sum_{i=N}^{\infty} b_i \tau^i \right) = \nu^{-1} \left(\sum_{i=N}^{\infty} (b_i \zeta_e^i) \tau^i \right) = \iota(h_E)(g)$$

que es lo que queríamos. □

Teorema 2.4.11. *Sea $L/\mathbb{C}(x)$ una extensión de Galois finita. Entonces, existe un subconjunto finito P de $\mathbb{P}^1_{\mathbb{C}}$ y un cubrimiento de Galois finito $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ de modo que existe un isomorfismo $\mathbb{C}$-lineal $L \to \mathcal{M}(\bar{R})$ enviando x a f; donde identificamos f con su extensión a $\bar{R}$.*

Demostración. Fijemos $F(x,y) \in \mathbb{C}[x,y]$ irreducible como polinomio en y sobre $\mathbb{C}(x)$ de modo que L es campo de descomposición de F sobre $\mathbb{C}(x)$ (a priori, $F(x,y)$ será un elemento de $\mathbb{C}(x)[y]$. Sin embargo, podemos considerar el polinomio $F'(x,y) = H(x)F(x,y)$, donde H es el denominador común de los coeficientes de F. Este nuevo polinomio F' sí es un elemento de $\mathbb{C}[x,y]$, es aún irreducible como polinomio en y y L seguirá siendo su campo de descomposición sobre $\mathbb{C}(x)$). Sea n el grado (en y) de F. Por el Lema 1.5.21, sólo hay finitos $p \in \mathbb{C}$ para los cuales $F(p,y)$ tiene menos de n raíces distintas. Sea P el conjunto de estos p, además de ∞. Sea R' el conjunto de todos los $(u, v_1, ..., v_n) \in \mathbb{C}^{n+1}$ con $u \in \mathbb{P}^1_{\mathbb{C}} \setminus P$, $F(u, v_i) = 0$ para cada i y $v_1, ..., v_n$ distintos dos a dos (v_1,...,v_n son exactamente las raíces de $F(u,y)$). Pensamos en R' como espacio topológico con la topología inducida por $\mathbb{C}^{n+1}$.

Afirmación 1: $f' : R' \to \mathbb{P}^1_{\mathbb{C}} \setminus P$, $(u, v_1, ..., v_n) \mapsto u$ es un cubrimiento. El grupo simétrico S_n actúa naturalmente como $\mathrm{Deck}(f')$ (permutando los v_i).

Demostración. Para cada $u_0 \in \mathbb{P}^1_{\mathbb{C}} \setminus P$ existen funciones holomorfas $\psi_1, ..., \psi_n$ definidas en una vecindad U de u_0 de modo que $\psi_1(u), ..., \psi_n(u)$ son exactamente las raíces de $F(u,y) \in \mathbb{C}[y]$ para cada $u \in U$ (por el Colorario 1.3.7). Para cada $\sigma \in S_n$, denotamos

$$V_\sigma = \{(u, \psi_{\sigma(1)}(u), ..., \psi_{\sigma(n)}(u)) : u \in U\}$$

así, $(f')^{-1}(U)$ es la unión disjunta de los V_σ. La función

$$U \to V_\sigma, \quad u \mapsto (u, \psi_{\sigma(1)}(u), ..., \psi_{\sigma(n)}(u))$$

es la inversa de $f'|_{V_\sigma}$, así que $f'|_{V_\sigma}$ es un homeomorfismo. Por tanto, f' es un cubrimiento.

Afirmación 2: Sea R una componente conexa de R'. Entonces, la restricción de f' a R es un cubrimiento de Galois finito $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$.

Demostración. $f = f'|_R$ es un cubrimiento por el Lema 1.4.11. Sea $u \in \mathbb{P}^1_{\mathbb{C}} \setminus P$ y $v, v' \in f^{-1}(u)$. Por la afirmación 1, existe $\alpha \in \mathrm{Deck}(f')$ enviando v a v'; y por lo tanto α envía R a sí mismo (porque R es una componente conexa de R' que contiene v y v'). Lo mismo es cierto para α^{-1}, así que α se restringe a un automorfismo de f. Así, como $\mathrm{Deck}(f)$ actúa transitivamente en $f^{-1}(u)$, f es de Galois. Además, es finito porque $\deg(f) \leq \deg(f') = n!$.

Afirmación 3: Para cada i, la función $g_i : R \to \mathbb{C}$, $(u, v_1, ..., v_n) \mapsto v_i$ se extiende a una función meromorfa $\bar{g}_i : \bar{R} \to \mathbb{P}^1_{\mathbb{C}}$ que satisface la ecuación $F(f, \bar{g}_i) = 0$.

Demostración. Cada punto de R tiene una vecindad de la forma V_σ, y la función $f|_{V_\sigma}$ es una carta en R (con la estructura definida en el Lema 2.4.4). En estas cartas locales, g_i está representada por la función holomorfa $\psi_{\sigma(i)}$; así que g_i es holomorfa en R. Miramos $\mathcal{M}(\bar{R})$ como subcampo de $\mathcal{M}(R)$ (vía restricción). Así, $\mathcal{M}(\bar{R})$ es algebraicamente cerrado en $\mathcal{M}(R)$: en efecto, si $h \in \mathcal{M}(R)$ es algebraico sobre $\mathcal{M}(\bar{R})$ entonces h es meromorfa en cada uno de los finitos puntos de $\bar{R} \setminus R$ por el Lema 1.3.15. Para cada $v = (u, v_1, ..., v_n) \in R$ tenemos que $F(u, v_i) = 0$, y por tanto $F(f(v), \bar{g}_i(v)) = 0$ para todo $v \in R$. Luego f y $\bar{g}_i$, vistos como elementos de $\mathcal{M}(R)$, satisfacen la ecuación $F(f, \bar{g}_i) = 0$. Como $f \in \mathcal{M}(\bar{R})$ y $\mathcal{M}(\bar{R})$ es algebraicamente cerrado en $\mathcal{M}(R)$, sigue que $\bar{g}_i \in \mathcal{M}(\bar{R})$.

Afirmación 4: Las funciones $g_1, ..., g_n$ generan $\mathcal{M}(\bar{R})$ sobre $\mathbb{C}(f)$

Demostración. Por el Teorema 2.4.9, cada elemento de $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(f))$ es de la forma

ι_α, $\alpha \in \mathrm{Deck}(f)$. Por tanto, basta probar que si ι_α fija $g_1, ..., g_n$ entonces $\alpha = id$ (de este modo, tendríamos que $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(f)(g_1, ..., g_n)) = 1$, así que $\mathcal{M}(\bar{R}) = \mathbb{C}(f)(g_1, ..., g_n)$ porque la extensión es de Galois). En efecto, en este caso, para todo $v \in R$ tenemos que $g_i(v) = g_i(\alpha^{-1}(v))$. Como también $f(v) = f(\alpha^{-1}(v))$, sigue que $v = \alpha^{-1}(v)$ (porque entonces α^{-1} no mueve u ni v_i en v). Así, $\alpha = id$.
Para concluir; como los g_i satisfacen el polinomio irreducible $F(f, y)$ sobre $\mathbb{C}(f)$, sigue de la afirmación 4 que $\mathcal{M}(\bar{R})$ es el campo de descomposición de F sobre $\mathbb{C}(f)$. Así, por el Teorema 1.5.10, $L \simeq \mathcal{M}(\bar{R})$; y de la construcción es claro que $x \mapsto f$. □

Ahora estamos preparados para mostrar la conexión que buscamos.

Teorema 2.4.12. *(de Existencia de Riemann: Versión Algebraica) Sea $T = [G, P, (C_p)_{p\in P}]$ un tipo de ramificación, sea $r = |P|$ y etiquetamos P por $p_1, ..., p_r$. Entonces, existe una extensión de Galois finita de $\mathbb{C}(x)$ de tipo T si y sólo si existen generadores $g_1, ..., g_r$ de G con $g_1 \cdots g_r = 1$ y $g_i \in C_{p_i}$*

Demostración. Supongamos que existen los generadores $g_1, ..., g_r$ con estas propiedades. Por el Teorema 2.2.13, existe un cubrimiento de Galois finito $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ de tipo T. Por el Teorema 2.4.10, la extension de Galois $\mathcal{M}/\mathbb{C}(f)$ asociada tiene el mismo tipo de ramificación. Recíprocamente, sea $L/\mathbb{C}(x)$ una extensión de Galois finita. Por el Teorema 2.4.11, podemos asociar a esta extensión un cubrimiento de Galois finito $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$. Por el Teorema 2.4.10, los puntos branch $p_1, ..., p_r$ de L son exactamente los elementos de P con $C_p^{top} \neq 1$. Así, por el Teorema 2.2.13, el grupo $\mathrm{Deck}(f)$ tiene generadores $h_1, ..., h_r$ con $h_1 \cdots h_r = 1$ y $h_i \in C_{p_i}^{top}$ para cada i. Así, las imágenes de $h_1, ..., h_r$ bajo el isomorfismo ι del Teorema 2.4.10 son generadores de $\mathrm{Gal}(\mathcal{M}(\bar{R})/\mathbb{C}(f))$ con las propiedades análogas. Esto prueba el Teorema porque $L \simeq \mathcal{M}(\bar{R})$ (por el Teorema 2.4.11). □

Corolario 2.4.13. *Todo grupo finito es realizable sobre $\mathbb{C}(x)$.*

Ejemplo 2.4.14. Como ejemplo, realizaremos la familia de grupos diedrales D_n como grupos de Galois sobre $\mathbb{C}(x)$. D_n está generado por dos elementos: una rotación r de orden n y una simetría s. Por la demostración del Teorema 2.2.8, podemos tomar $X = \mathbb{C}\setminus\{0, 1\}$ y el cubrimiento

$$f : R = X \times G \to \mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}, \quad (x, g) \mapsto x,$$

con clases de conjugación $r \in C_0$, $s \in C_1$, $(rs)^{-1} \in C_\infty$. Notemos que este cubrimiento tiene grado $2n = |D_n|$. Ahora, pensamos en la extensión de f a una superficie de Riemann compacta $f : \overline{R} \to \mathbb{P}^1_{\mathbb{C}}$ (como en la Proposición 2.4.3). Alrededor de los puntos en $f^{-1}(0)$, la Proposición 2.2.6 (c) nos dice que f se comporta como un cubrimiento de grado n; porque n es el orden común de los elementos de C_0. Así, el índice de ramificación de

f en un punto en $f^{-1}(0)$ es n. Razonamos análogamente sobre 1 e ∞ para ver que el índice de ramificación en las preimágenes de estos puntos es 2. Además, como el grado de f como función holomorfa entre superficies de Riemann es $2n$, tenemos que

$$\sum_{p\in\overline{R}}(k_p-1)=\sum_{p\in f^{-1}(\{0,1,\infty\})}(k_p-1)=4n-2.$$

Por tanto, por el Teorema 1.3.23, tenemos que:

$$2g(\overline{R})-2=d(2g(\mathbb{P}^1_{\mathbb{C}})-2)+\sum_{p\in\overline{R}}(k_p-1)=-2d+\sum_{p\in\overline{R}}(k_p-1)$$

y luego,

$$2g(\overline{R})-2=-4n+4n-2$$

lo que implica que $g(\overline{R})=0$. Por tanto, cada grupo diedral D_n se puede realizar como grupo de automorfismos de $\mathbb{P}^1_{\mathbb{C}}$ de manera que el cociente por su acción sea una vez más $\mathbb{P}^1_{\mathbb{C}}$, de manera similar a como lo hicimos en la Observación 2.2.3. Con esto en mente, y en este caso en particular, podemos encontrar un ejemplo específico de función holomorfa $g:\mathbb{P}^1_{\mathbb{C}}\to\mathbb{P}^1_{\mathbb{C}}$ que realice D_n. En primer lugar, notemos que las funciones

$$f_r: z\to\zeta_n z$$
$$f_s: z\to\frac{1}{z}$$

generan un grupo de automorfismos de $\mathbb{P}^1_{\mathbb{C}}$ isomorfo a D_n (para esto basta ver que $f_sf_rf_s=f_s^{n-1}$). Así, g será una función racional (ya que sabemos que $\mathcal{M}(\mathbb{P}^1_{\mathbb{C}})=\mathbb{C}(z)$) que queda invariante por f_r y f_s (en el sentido que $g=g\circ f_i$) y cuyo grado como función holomorfa sea $2n=|D_n|$. Claramente $z\mapsto z^n$ es invariante por f_r. Sin embargo, no es tan obvio qué función racional es invariante por f_s, por lo que introducimos el cambio de coordenadas

$$w(z)=\frac{z-1}{z+1}$$

que tiene la propiedad $w(1/z)=-w(z)$ (hemos encontrado este cambio de coordenadas enviando los puntos fijos de f_s a los puntos fijos de $w\mapsto w^2$; una transformación de orden 2 mucho más simple de estudiar). Así, $w(z)^2$ es invariante por f_s. Por tanto, una función racional invariante por tanto f_r como f_s es $g(z)=w(z^n)^2$, es decir,

$$g(z)=\frac{(z^n-1)^2}{(z^n+1)^2}$$

que es una función holomorfa $\mathbb{P}^1_{\mathbb{C}}\to\mathbb{P}^1_{\mathbb{C}}$ de grado $2n$. Por tanto, la función g realiza D_n como grupo de automorfismos de $\mathbb{P}^1_{\mathbb{C}}$. Así, por el Teorema 2.4.9, la extensión

$$\mathcal{M}(\mathbb{P}^1_{\mathbb{C}})/\mathbb{C}(g)=\mathbb{C}(z)/\mathbb{C}(g)$$

es de Galois con grupo de Galois D_n, y luego el Teorema 2.4.11 nos da la identificación que queríamos.

Observación 2.4.15. Como en este caso $\overline{R}$ resultó tener género 0, encontrar una función que realizara el grupo D_n fue más sencillo de lo usual. No es tan obvio cómo se podría hacer esto en el caso más general; y de hecho no hay mucha literatura al respecto de construcciones en el marco del Teorema de Existencia de Riemann, o de versiones 'efectivas' del mismo. Para una referencia al respecto de algunos trabajos en este sentido, se puede ver [28] o [29].

Ejemplo 2.4.16. También como ejemplo, realizamos la familia de grupos simétricos S_n. Por [35, Teorema 2.5], $\{g_1, g_2\}$ con $g_1 = (12)$ y $g_2 = (12...n)$ es un conjunto de generadores para S_n. Así, por el mismo argumento que en 2.4.14, tenemos un cubrimiento $f : \overline{R} \to \mathbb{P}^1_{\mathbb{C}}$ de grado $n! = |S_n|$ y con ramificación 2 en los puntos de $f^{-1}(0)$, n en los puntos de $f^{-1}(1)$ y $n-1$ en los puntos de $f^{-1}(\infty)$ (porque g_1 tiene orden 2, g_2 tiene orden n y $(g_1g_2)^{-1}$ tiene orden $n-1$) y sin ramificación fuera de estos. Así, el Teorema 1.3.23 nos dice que

$$2g(\overline{R}) - 2 = -2n! + \left(\frac{n!}{2} + \frac{n!}{n}(n-1) + \frac{n!}{n-1}(n-2)\right)$$

y luego

$$g(\overline{R}) = 1 + \frac{1}{4}(n^2 - 5n + 2)(n-2)!$$

que es una función creciente de n. Esto muestra que S_n se realiza, con nuestro método, en superficies de género 0 para S_3 y S_4 y con superficies de mayor género para valores mayores de n (por ejemplo, S_5 se realiza en género 4, S_6 en género 49 y S_{10} en género 524161. No es necesario decir que ese número crece bastante rápido).

Ejemplo 2.4.17. Finalmente, realizamos la familia de grupos alternos A_n, con $n \geq 4$. Separamos este en dos casos:

1. n **impar.** Por [35, Teorema 3.5], $\{g_1, g_2\}$ con $g_1 = (123)$ y $g_2 = (12...n)$ es un conjunto de generadores para A_n. Una vez más por el mismo argumento de 2.4.14, existe un cubrimiento $f : \overline{R} \to \mathbb{P}^1_{\mathbb{C}}$ de grado $n!/2 = |A_n|$ con ramificación 3 en los puntos de $f^{-1}(0)$, n en los puntos de $f^{-1}(1)$ y n en los puntos de $f^{-1}(\infty)$ (porque g_1 tiene orden 2, g_2 tiene orden n y $(g_1g_2)^{-1}$ tiene orden n) y sin ramificación fuera de estos. Por el Teorema 1.3.23, tenemos que

$$2g(\overline{R}) - 2 = -n! + \left(2\frac{n!}{6} + \frac{n!}{2n}(n-1) + \frac{n!}{2n}(n-1)\right)$$

y luego

$$g(\overline{R}) = 1 + \frac{1}{6}(n-3)(n-1)!$$

donde de nuevo tenemos una función creciente de n. Este método realiza A_5 en género 9; y una vez más crece muy rápido: realiza A_{11} en género 4838401.

2. n **par.** Por [35, Teorema 3.5], $\{g_1, g_2\}$ con $g_1 = (123)$ y $g_2 = (23...n)$ es un conjunto de generadores para A_n. Una vez más por el mismo argumento de 2.4.14, existe un cubrimiento $f : \overline{R} \to \mathbb{P}^1_{\mathbb{C}}$ de grado $n!/2 = |A_n|$ con ramificación 3 en los puntos de $f^{-1}(0)$, $n-1$ en los puntos de $f^{-1}(1)$ y $n-2$ en los puntos de $f^{-1}(\infty)$ (porque g_1 tiene orden 2, g_2 tiene orden $n-1$ y $(g_1g_2)^{-1}$ tiene orden $n-2$) y sin ramificación fuera de estos. Por el Teorema 1.3.23, tenemos que

$$2g(\overline{R}) - 2 = -n! + \left(2\frac{n!}{6} + \frac{n!}{2(n-1)}(n-2) + \frac{n!}{2(n-2)}(n-3)\right)$$

y luego

$$g(\overline{R}) = 1 + n!\frac{(n^2 - 5n + 5)}{4(n-2)(n-1)}$$

donde de nuevo tenemos una función creciente de n. Este método realiza A_4 en género 2; y una vez más crece muy rápido: realiza A_{10} en género 693001.

Observación 2.4.18. Una función Magma que puede calcular el género de la superficie de Riemann obtenida por este método es la siguiente:

```
genus:=function(G);
L:=Setseq(Generators(G));
S:=L cat [&*L];
return (2-2*Order(G)+&+[Order(G)*(Order(g)-1)/Order(g) : g in S])/2;
end function;
```

donde G es un grupo finito. Esto ocupa generadores para G calculados por Magma, por lo que algunos resultados de este programa difieren de los que hemos obtenido hacia arriba. Por ejemplo, Magma realiza A_4 sobre una superficie de género 3; lo que muestra que diferentes elecciones de generadores cambian la superficie que obtenemos.

Observación 2.4.19. Se puede mostrar, de hecho, que los subgrupos finitos de $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}})$ son necesariamente isomorfos a C_n, D_n, A_4, A_5 o S_4 (ver [27, Lema 3.1]).

Cerramos la sección detallando un poco más la equivalencia entre cubrimientos y extensiones que hemos evidenciado.

Lema 2.4.20. *Sean $s, n \in \mathbb{N}$. Existe un grupo finito $H = H_{n,s}$ con generadores $h_1, ..., h_s$ que satisface:*

(a) Para cualquier grupo G de orden $\leq n$ y $g_1, ..., g_s \in G$, existe un homomorfismo $H \to G$ enviando h_i a g_i.

(b) La intersección de todos los subgrupos normales de H de índice $\leq n$ es trivial.

(c) Si $h'_1, ..., h'_s$ son generadores de un grupo H' que satisface (b) entonces existe un homomorfismo sobreyectivo $H \to H'$, $h_i \mapsto h'_i$.

(d) Si $h'_1, ..., h'_s$ son generadores de H existe un automorfismo de H enviando h_i a h'_i.

Demostración. Sea $\mathcal{F}_s$ el grupo libre en s generadores. Notemos que $\mathcal{F}_s$ tiene finitos subgrupos normales de índice $\leq n$ ya que cada uno es el núcleo de un homomorfismo $\phi : \mathcal{F}_s \to G$, con G de orden $\leq n$ (por el primer Teorema de isomorfismo). Construimos $H_{n,s}$ como el cociente de $\mathcal{F}_s$ por la intersección de todos estos subgrupos normales. Este grupo es finito por lo anterior y el segundo Teorema de isomorfismo. Además;

- cumple (b): sea K el subgrupo de $\mathcal{F}_s$ tal que $H_{n,s} = \mathcal{F}_s/K$. Sea G/K un subgrupo normal de $H_{n,s}$ de índice $\leq n$. Se tiene:

$$H_{n,s} \Big/ \left(G/K\right) \simeq \left(\mathcal{F}_s/K\right) \Big/ \left(G/K\right) \simeq \mathcal{F}_s/G$$

  por el tercer teorema de isomorfismo. Luego, G también tiene índice $\leq n$ en $\mathcal{F}_s$. Por tanto, como la intersección $\bigcap G/K$ de todos los subgrupos de índice $\leq$ de $H_{n,s}$ contiene K,

$$H_{n,s} \Big/ \bigcap G/K \simeq \mathcal{F}_s \Big/ \bigcap G \simeq H_{n,s}$$

  y luego $\bigcap G/K = 1$,

- cumple (c): tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathcal{F}_s & \xrightarrow{\varphi} & H' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\psi} & \\ H & & \end{array}$$

  donde $\varphi(f_i) = h'_i$ y $\pi(f_i) = h_i$. Estas funciones inducen un homomorfismo sobreyectivo ψ si $K \subseteq \mathrm{Ker}(\varphi)$, así que sea $x \in K$. La función φ es sobreyectiva, así que $\varphi(x)$ está en todos los subgrupos de índice $\leq n$ de H'; cuya intersección es trivial por hipótesis. Sigue que $x \in \mathrm{Ker}(\varphi)$;

- cumple (a) por el mismo argumento de (c), notando que la intersección de los subgrupos normales de índice $\leq n$ de G es trivial porque 1 es uno de estos subgrupos;

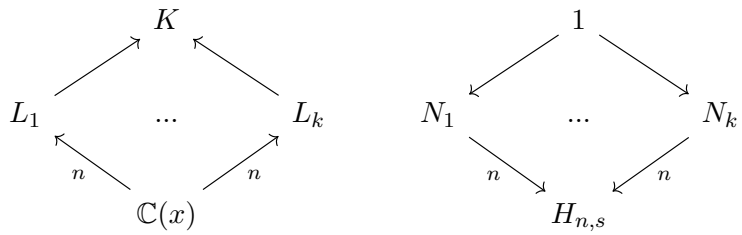
- cumple (d) porque existe un endomorfismo sobreyectivo enviando h_i en h'_i por (c).

□

Corolario 2.4.21. *Sean $P \subseteq \mathbb{P}^1_{\mathbb{C}}$ finito y $s = |P| - 1$. Para cada $n \geq 2$, consideremos el compositum $K_n(P)$ de todas las extensiones finitas de Galois de $\mathbb{C}(x)$ de grado $\leq n$ con puntos branch contenidos en P (dentro de alguna clausura algebraica de $\mathbb{C}(x)$).*

Entonces, $K_n(P)/\mathbb{C}(x)$ *es una extensión finita de Galois con* $\mathrm{Gal}(K_n(P)/\mathbb{C}(x)) \simeq H_{n,s}$ *y con puntos branch en* P*. Recíprocamente, si* $K/\mathbb{C}(x)$ *es una extensión finita de Galois con* $\mathrm{Gal}(K/\mathbb{C}(x)) \simeq H_{n,s}$ *y puntos branch contenidos en* P*, entonces* $K = K_n(P)$*.*

Demostración. Por el Teorema 2.4.12, existe una extensión finita de Galois $K/\mathbb{C}(x)$ con grupo de Galois isomorfo a $H_{n,s}$ y puntos branch en P (aplicando el Teorema a $h_1, ..., h_{s+1} \in H_{n,s}$, donde $h_{s+1} = (h_1 \cdots h_s)^{-1}$). La condición (b) del Lema 2.4.20 implica que K es el compositum de las extensiones finitas de Galois $L_i/\mathbb{C}(x)$ de grado $\leq n$ contenidas en K; ya que, por el Teorema 1.5.22, tenemos la siguiente situación:



donde cada N_i es el subgrupo normal de $H_{n,s}$ asociado al subcampo L_i. Como la intersección de estos es trivial, el subgrupo asociado al compositum de $L_1, ..., L_k$ es trivial, y por tanto la extensión $K/L_1 \cdots L_k$ es de grado 1. Cada una de estas extensiones tiene sus puntos branch en P, ya que un elemento de $\mathrm{Gal}(K/\mathbb{C}(x))$ es trivial si y solo si es trivial en cada L, y por tanto la clase C_p se "restringe" por la Proposición 2.3.18.
Ahora, sea $L/\mathbb{C}(x)$ cualquier extensión finita de Galois de grado $\leq n$ con puntos branch contenidos en P, y sea K' el compositum de L y K. Así, K' también tiene puntos branch contenidos en P, y luego por el Teorema 2.4.12 el grupo $H' = \mathrm{Gal}(K'/\mathbb{C}(x))$ puede ser generado por s elementos. Como K es compositum de extensiones de grado $\leq n$, K' también lo será; así que la intersección de todos los subgrupos normales de H' de índice $\leq n$ es trivial (por el Teorema 1.5.22 y el mismo argumento de arriba). Así, sigue del Lema 2.4.20(c) que $|H'| \leq |H_{n,s}|$. De aquí, $K' = K$, y por tanto $L \subseteq K$. Sigue que $K = K_n(P)$, porque todas las extensiones que cumplen las mismas condiciones de $L/\mathbb{C}(x)$ están contenidas en K; y K es compositum de todas ellas. □

Proposición 2.4.22. *Sea* G *un grupo finito, y* $P \subseteq \mathbb{P}^1$ *finito. El número* $\lambda(G, P)$ *de extensiones finitas de Galois de* $\mathbb{C}(x)$ *con grupo de Galois isomorfo a* G *y puntos branch contenidos en* P *es finito e igual al número de órbitas de* $\mathrm{Aut}(G)$ *en el conjunto de sistemas generadores de* G *de largo* $s = |P| - 1$*.*

Demostración. Por el Corolario 2.4.21 y el Teorema 1.5.22, $\lambda(G, P)$ es igual al número de subgrupos normales N de $H_{n,s}$ con $H_{n,s}/N \simeq G$, con $n = |G|$ y $s = |P| - 1$. Este N es el núcleo de un homomorfismo sobreyectivo $\psi : H_{n,s} \to G$ determinado por las imágenes $g_1, ..., g_s$ de $h_1, ..., h_s$. $g_1, ..., g_s$ generan G, y cualquier sistema de generadores

está asociado a algún ψ por la Definición de $H_{n,s}$. Dos elecciones de ψ, ψ' tienen el mismo núcleo si y sólo si existe un automorfismo de G enviando g_i a los g_i' correspondientes. Para los sistemas de generadores, esto significa que $(g_1', ..., g_n') = \alpha \cdot (g_1, ..., g_n)$, donde α actúa componente a componente en n-uplas de elementos del grupo. Por lo tanto, λ es igual al número de órbitas de $\mathrm{Aut}(G)$ en sistemas generadores de G de largo s. □

Teorema 2.4.23. *Sea G un grupo finito, $P \subseteq \mathbb{P}^1_{\mathbb{C}}$ finito, y $q \in \mathbb{P}^1_{\mathbb{C}} \setminus P$. Hay una correspondencia biyectiva entre los siguientes objetos:*

(a) Las clases de $\mathbb{C}(x)$-isomorfismo de extensiones de Galois $L/\mathbb{C}(x)$ con grupo de Galois isomorfo a G y puntos branch contenidos en P.

(b) Las clases de equivalencia de cubrimientos de Galois $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ con grupo de automorfismos isomorfo a G.

(c) Las clases de equivalencia de cubrimientos ramificados $\overline{f} : \overline{R} \to \mathbb{P}^1_{\mathbb{C}}$, con $\overline{R}$ una superficie de Riemann compacta y conexa, con conjunto de puntos branch contenido en P y que tienen un subgrupo $H \leq \mathrm{Aut}(\overline{R})$ isomorfo a G y de modo que cada $h \in H$ cumple que $f \circ h = f$ y además es transitivo en cada fibra $f^{-1}(p)$; bajo la relación de equivalencia $\overline{f_1} : \overline{R}_1 \to \mathbb{P}^1_{\mathbb{C}} \sim \overline{f_2} : \overline{R}_2 \to \mathbb{P}^1_{\mathbb{C}}$ si y solo si existe una función biholomorfa $\alpha : \overline{R}_1 \to \overline{R}_2$ con $\overline{f_2} \circ \alpha = \overline{f_1}$.

(d) Los subgrupos normales del grupo fundamental $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus P, q)$ con cociente isomorfo a G.

La correspondencia entre (a) y (b) está dada asociando f con las extensiones $L/\mathbb{C}(x)$ para las cuales existe un isomorfismo $\mathbb{C}$-lineal $L \to \mathcal{M}(\bar{R})$ que envía x a f (donde $\bar{R}$ está construido como en la Proposición 2.4.3); mientras que la correspondencia entre (b) y (d) está dada asociando f con el kernel de la sobreyección $\Phi_b : \pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus P, q) \to \mathrm{Deck}(f)$ de la Proposición 2.2.2, para cualquier $b \in f^{-1}(q)$; y la correspondencia entre (b) y (c) está dada asociando f a su extensión $\overline{f}$ de la Proposición 2.4.3.

Demostración. Comenzamos con la correspondencia entre (b) y (d). Notemos que el núcleo de Φ_b no depende de b. En efecto, para otro $b' \in f^{-1}(q)$; si denotamos por σ el elemento de $\mathrm{Deck}(f)$ tal que $\sigma(b) = b'$ y $\Psi \in \mathrm{Inn}(\mathrm{Deck}(f))$ con $\Psi(\alpha) = \sigma \circ \alpha \circ \sigma^{-1}$, se tiene que $\Phi_{b'} = \Psi \circ \Phi_b$. Es claro que cubrimientos equivalentes tendrán asociado el mismo subgrupo normal. Recíprocamente, dos cubrimientos asociados al mismo subgrupo normal son equivalentes por el Lema 1.4.13. Así, basta ver que cada subgrupo normal N de $\Gamma = \pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus P, q)$ con $\Gamma/N \simeq G$ es de la forma $\mathrm{Ker}(\Phi_b)$ para algún espacio cubriente f. Si $\infty \in P$, esto sigue del Teorema 2.2.8 tomando $g_1, ..., g_n$ como las imágenes de $\gamma_1, ..., \gamma_n$ en G a través de la proyección π. El caso general sigue de un cambio de coordenadas.
Queremos contar el número de elementos en (b) y (d), digamos λ. Sea $n = |P| - 1$. Por el Corolario 2.2.9, Γ es libre de rango n, con generadores $\gamma_1, ..., \gamma_n$. Así, existe una correspondencia entre los homomorfismos sobreyectivos $\varphi : \Gamma \to G$ y los sistemas de

generadores $g_1, ..., g_n$ de G de largo n, dada por $g_i = \varphi(\gamma_i)$. Dos de estos homomorfismos tienen el mismo núcleo si y sólo si $\varphi' = \alpha\varphi$ para algún $\alpha \in \mathrm{Aut}(G)$. Por lo tanto, λ es igual al número de órbitas de $\mathrm{Aut}(G)$ en sistemas generadores de G de largo n (al igual que en la Proposición 2.4.22).
Ahora, mostramos la correspondencia entre (a) y (b). Por el Teorema 2.4.11, cada espacio cubriente f tiene asociada una extensión $L/\mathbb{C}(x)$. Claramente, espacios cubrientes equivalentes tienen asociada la misma extensión módulo $\mathbb{C}(x)$-isomorfismo. Por tanto hemos definido una función entre los objetos en (b) a los objetos en (a), que es sobreyectiva por el Teorema 2.4.11. Basta entonces probar que (a) tiene exactamente λ elementos, y que λ es finito. Esto sigue de la Proposición 2.4.22.
Finalmente, mostramos la correspondencia entre (b) y (c). Por la Proposición 2.4.3 y el Lema 2.4.6; cada espacio cubriente f se asocia con su extensión $\overline{f}$ a una superficie de Riemann compacta y conexa que cumple la condición del subgrupo. El mismo argumento en estos resultados que muestra que un elemento de $\mathrm{Deck}(f)$ se extiende a una función holomorfa $\overline{R} \to \overline{R}$ muestra que si tenemos dos espacios cubrientes $f_i : R_i \to \mathbb{P}^1_{\mathbb{C}} \setminus P$ y un homeomorfismo $\beta : R_1 \to R_2$ que cumple que $f_1 = f_2 \circ \beta$; este se extiende a una función holomorfa y biyectiva $\overline{\beta} : \overline{R}_1 \to \overline{R}_2$. Como lo mismo es cierto para β^{-1}, hemos definido una función entre los objetos en (b) a los objetos en (c). Esta función tiene inversa: a cada cubrimiento ramificado $\overline{f} : \overline{R} \to \mathbb{P}^1_{\mathbb{C}}$ de este tipo podemos quitarle su conjunto de puntos branch $P' \subseteq P$ y su preimagen $\overline{f}^{-1}(P')$ para obtener una función $f : \overline{R} \setminus \overline{f}^{-1}(P') \to \mathbb{P}^1_{\mathbb{C}} \setminus P'$. Notemos que f es un cubrimiento de Galois por la condición de transitividad de H y porque $\overline{R}$ es conexo (y por tanto todas las fibras tendrán la misma cardinalidad). Esto muestra la correspondencia. □

Observación 2.4.24. El Teorema 2.4.23 tiene una versión más general si quitamos la hipótesis de ser de Galois en todas partes. Más específicamente, se puede mostrar que existe una correspondencia entre los siguientes objetos:

(a) Las clases de $\mathbb{C}(x)$-isomorfismo de extensiones $L/\mathbb{C}(x)$ con puntos branch contenidos en P.

(b) Las clases de equivalencia de cubrimientos $f : R \to \mathbb{P}^1_{\mathbb{C}} \setminus P$.

(c) Las clases de equivalencia de cubrimientos ramificados $\overline{f} : \overline{R} \to \mathbb{P}^1_{\mathbb{C}}$, con $\overline{R}$ compacta y conexa y puntos branch en P.

(d) Las clases de conjugación de subgrupos del grupo fundamental $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus P, q)$.

Este resultado es una combinación de los encontrados, por ejemplo, en [23, Teoremas 2.3.4, 3.2.7 y 3.3.7] en el caso específico de $\mathbb{P}^1_{\mathbb{C}}$ como imagen para los cubrimientos. Estos Teoremas están de hecho enunciados de manera aún más general, pero estas formulaciones requieren lenguaje extra que está fuera del alcance de este trabajo.

3 Hacia el Problema Inverso de Galois Clásico

Un posible estudio del Problema Inverso de Galois clásico se beneficia mucho del acercamiento que acabamos de hacer hasta aquí. Comenzamos con una primera Definición:

Definición 3.0.1. Sea G un grupo finito, K un campo. Una **realización** de G sobre K es una extensión de campos L/K con $\mathrm{Gal}(L/K) \simeq G$.

Estas realizaciones pueden ser sujetas a un proceso de descenso. En efecto, si G es un grupo y $x_1, ..., x_m$ son elementos trascendentales sobre $\mathbb{Q}$, podemos encontrar extensiones de campos de modo que se tenga la siguiente evolución:

$$\begin{array}{c} \text{Realización de } G \text{ sobre } \mathbb{C}(x) \\ \downarrow \\ \text{Realización de } G \text{ sobre } \mathbb{Q}(x_1, ..., x_m) \\ \downarrow \\ \text{Realización de } G \text{ sobre } \mathbb{Q}. \end{array}$$

La primera flecha es definitivamente la más complicada: no sabemos si todos los grupos realizables sobre $\mathbb{C}(x)$ lo son sobre $\mathbb{Q}(x_1, ..., x_m)$. Sin embargo, con una condición (bastante fuerte de hecho) impuesta sobre el grupo G, es posible obtener un resultado que nos permite descender: la existencia de una n-upla **rígida** de clases de conjugación de G. Hablamos un poco de esta condición y del método que le da nombre en la sección 3.1.
La segunda flecha es muchísimo más simple: una vez que tenemos demostrado el **Teorema de Irreducibilidad de Hilbert**, obtenemos como consecuencia bastante directa de él que todo grupo realizable sobre $\mathbb{Q}(x_1, ..., x_m)$ lo es también sobre $\mathbb{Q}$. Hablaremos un poco de este resultado en la sección 3.2.

3.1. El Método de Rigidez

Como pretendemos realizar grupos sobre $\mathbb{Q}(x_1, ..., x_m)$, comenzamos con una primera Definición. Durante esta sección, L, k y K serán siempre campos.

Definición 3.1.1. Sea G un grupo finito. Decimos que G **ocurre regularmente** sobre K si existe algún entero $m > 0$ y alguna extensión de Galois $L/K(x_1, ..., x_m)$, donde $x_1, ..., x_m$ son elementos trascendentales sobre K, de modo que K es algebraicamente cerrado en L y $\mathrm{Gal}(L/K(x_1, ..., x_m)) \simeq G$

Un obstáculo importante en nuestro descenso es el hecho de que pueden existir múltiples extensiones no isomorfas con el mismo tipo de ramificación (las hemos contado, de hecho, en la demostración del Teorema 2.4.23). Esto motiva la Definición de rigidez.

Definición 3.1.2. Sea $(C_1, ..., C_r)$ una r-upla de clases de conjugación de un grupo G. Decimos que es **débilmente rígida** en G si

(a) existen generadores $g_1, ..., g_r$ de G con $g_1 \cdots g_r = 1$ y $g_i \in C_i$, y

(b) si $g_1', ..., g_r'$ es otro sistema de generadores de G con las mismas propiedades, entonces existe un único automorfismo γ de G con $\gamma(g_i) = g_i'$.

Además, decimos que es **rígida** si cumple (a) y en (b) el automorfismo γ es un automorfismo interno.

Observación 3.1.3. La unicidad en el caso rígido es equivalente a la condición de que el centro $Z(G)$ sea trivial. En efecto, si g, h son dos elementos de G con $gg_ig^{-1} = g_i' = hg_ih^{-1}$ para cada i, entonces $h^{-1}gg_i = g_ih^{-1}g$; es decir, que $h^{-1}g$ conmuta con cada generador g_i y luego $h^{-1}g \in Z(G)$; por lo que si $Z(G)$ es trivial entonces $h = g$. Por otra parte, si $Z(G)$ no es trivial entonces cualquier elemento no trivial $z \in Z(G)$ es tal que $gzg_i(gz)^{-1} = gg_ig^{-1} = g_i'$, en contradicción con la unicidad.

Definición 3.1.4. Un tipo $T = [G, P, \mathbf{C}]$ es **rígido** (**débilmente rígido**) si los elementos de P se pueden etiquetar como $p_1, ..., p_r$ de modo que las clases $C_i = C_{p_i}$ forman una r-upla rígida (débilmente rígida) en G.

Se puede probar que si $(C_1, ..., C_r)$ es (débilmente) rígida sigue siéndolo después de una permutación de los C_i, así que la elección de estas etiquetas no importa.

Teorema 3.1.5. [32, Teorema 4.4.8] *Para cada tipo débilmente rígido T existe una única extensión finita de Galois de $\mathbb{C}(x)$ de tipo T (salvo isomorfismo).*

Idea de la Demostración. La existencia viene del Teorema 2.4.12. Para la unicidad, consideramos dos extensiones $L_1/\mathbb{C}(x)$ y $L_2/\mathbb{C}(x)$ del mismo tipo dentro de alguna extensión finitamente generada $L/\mathbb{C}(x)$, y el homomorfismo por restricción

$$\rho_j : G = \mathrm{Gal}(L/\mathbb{C}(x)) \to G_j = \mathrm{Gal}(L_j/\mathbb{C}(x)).$$

Por una parte, el Teorema 2.4.12 induce generadores $\rho_j(g_1), ..., \rho_j(g_r)$ de G_j con las propiedades del Teorema; mientras que el hecho de que L_1 y L_2 tengan el mismo tipo significa que existe un isomorfismo $\varepsilon : G_2 \to G_1$ enviando $C_p^{(2)}$ a $C_p^{(1)}$ para todo $p \in P$. Por tanto el conjunto de generadores $\{\varepsilon(\rho_2(g_k))\}_{k=1}^r$ satisface las mismas condiciones que el conjunto $\{\rho_1(g_k)\}_{k=1}^r$. La rigidez implica que existe un automorfismo δ de G_1 enviando $\varepsilon(\rho_2(g_k))$ a $\rho_1(g_k)$ para cada k. Por tanto $\gamma = \delta \circ \varepsilon$ es un isomorfismo de G_2 en G_1 que envía $\rho_2(g_k)$ en $\rho_1(g_k)$, así que $\rho_1 = \gamma \circ \rho_2$. Sigue que $L_1 = L^{\mathrm{Ker}(\rho_1)} = L^{\mathrm{Ker}(\rho_2)} = L_2$. □

Observación 3.1.6. Es claro que las extensiones abelianas (es decir, aquellas con grupo de Galois abeliano) de $\mathbb{C}(x)$ tienen tipo débilmente rígido, y por el Teorema 3.1.5 están únicamente determinadas por él. Esto las hace mucho más fáciles de manejar que aquellas no abelianas, y por tanto no es sorprendente que sean tan usadas, por ejemplo, en Teoría de Números. El detalle que sí es sorprendente es que la clase de extensiones únicamente determinadas por su tipo contiene muchas extensiones con grupos de Galois simple y no abeliano.

La principal pregunta de este acercamiento es la siguiente: dada una extensión $L/K(x)$ finita y de Galois y un subcampo $k \subseteq K$, ¿existe algún subcampo $L_k \subseteq L$ de modo que $\mathrm{Gal}(L_k/k(x)) \simeq \mathrm{Gal}(L/K(x))$? Esto motiva la siguiente Definición:

Definición 3.1.7. Dado un subcampo $k \subseteq K$, la extensión de Galois $L/K(x)$ está **definida** sobre k si existe un subcampo $L_k \subseteq L$ de modo que $L_k/k(x)$ es de Galois, k es algebraicamente cerrado en L_k y $[L_k : k(x)] = [L : K(x)]$.

Esto es suficiente por el siguiente Lema:

Lema 3.1.8. [32, Lema 5.1.3] *Si $L/K(x)$ está definida sobre k, entonces*

$$\mathrm{Gal}(L/K(x)) \simeq \mathrm{Gal}(L_k/k(x))$$

a través del homomorfismo de restricción a L_k.

Idea de la Demostración. Primero notamos que un elemento primitivo de la extensión $L_k/k(x)$ es también primitivo para $L/K(x)$, y por tanto cualquier elemento de $\mathrm{Gal}(L/K(x))$ deja L_k invariante. El resultado sigue porque el homomorfismo de restricción es inyectivo entre grupos del mismo orden. □

Lema 3.1.9. [32, Lema 5.1.6] *Si $L/K(x)$ está definida sobre k y k es algebraicamente cerrado, entonces $L/K(x)$ y $L_k/k(x)$ tienen el mismo tipo.*

Idea de la Demostración. Básicamente la demostración de la Proposición 2.3.18, haciendo uso de la extensión de ν_p natural. La igualdad de tipos se tiene por la restricción análoga de la parte (d). □

Definición 3.1.10. Sea $\alpha \in \mathrm{Aut}(k)$. Extendemos α a un automorfismo de $k(x)$ fijando x. Consideramos dos extensiones finitas y de Galois $L/k(x)$ y $L'/k(x)$. Un isomorfismo $\lambda : L \to L'$ que cumple que $\lambda|_{k(x)} = \alpha$ es un **α-isomorfismo**.

Observación 3.1.11. Cada α-isomorfismo λ induce un isomorfismo de grupos

$$\lambda^* : \mathrm{Gal}(L/k(x)) \to \mathrm{Gal}(L'/k(x)), \quad \sigma \mapsto \lambda\sigma\lambda^{-1}.$$

Lema 3.1.12. [32, Lema 5.1.9] *Sean $K = \overline{k}$ y $L/K(x)$ una extensión de Galois finita con grupo de Galois G de modo que $Z(G) = 1$. Si para cada $\alpha \in \mathrm{Gal}(K/k)$ existe un α-isomorfismo $\lambda : L \to L$ con $\lambda^* = id$, entonces $L/K(x)$ está definida sobre k.*

Idea de la Demostración. La extensión $L/K(x)$ está definida en una extensión finitamente generada k_1 de k (agregando las raíces del polinomio mínimo de un elemento primitivo de $L/K(x)$). Ponemos $L_1 = L_{k_1}$. Consideremos $\alpha_1 \in \mathrm{Gal}(k_1/k)$ y lo extendemos a $\alpha \in \mathrm{Gal}(K/k)$; que por hipótesis tiene un α-isomorfismo λ con $\lambda^* = id$. El campo intermedio L_1 es único con la propiedad de ser Galois sobre $k_1(x)$ y de que k_1 es algebraicamente cerrado en L_1 (aquí ocupamos el hecho de que el centro del grupo de Galois es trivial), así que $\lambda(L_1) = L_1$. La restricción $\lambda|_{L_1} = \lambda_1$ resulta ser un α_1-isomorfismo; lo que luego de un cálculo implica que $G_1 := \mathrm{Gal}(L_1/k(x))$ es el producto directo de $H := \mathrm{Gal}(L_1/k_1(x))$ y el centralizador C de G_1 en H. Si tomamos L_k como el campo fijo de C en L_1, $\mathrm{Gal}(L_k/k(x)) \simeq H/C \simeq G_1 \simeq G$. Finalmente, k es algebraicamente cerrado en L_k porque k_1 lo es en L_1, $L_k \cap k_1(x) = k(x)$ y $L_k \subseteq L_1$. □

Definición 3.1.13.

1. Una clase de conjugación C de un grupo G es **racional** si $C^m = C$ para todo entero $m < |G|$ con $\mathrm{mcd}(m, |G|) = 1$.

2. Un tipo $T = [G, P, \mathbf{C}]$ es **k-racional** si $P \subseteq \overline{k} \cup \{\infty\}$ y para cada $p \in P$ y $\alpha \in \mathrm{Gal}(\overline{k}/k)$,

   a) $\alpha(p) \in P$, y

   b) $C_{\alpha(p)} = C_p^m$, donde m es el entero tal que $\alpha^{-1}(\zeta_n) = \zeta_n^m$, ζ_n es una raíz n-ésima de la unidad en $\overline{k}$ y $n = |G|$.

Además, si $k = \mathbb{Q}$ decimos que T es simplemente **racional**.

Observación 3.1.14. Un tipo $T = [G, P, \mathbf{C}]$ es k-racional si $P \subseteq k \cup \{\infty\}$ y cada clase $C \in \mathbf{C}$ es racional.

El siguiente será nuestro principal teorema de descenso.

Teorema 3.1.15. [32, Teorema 5.2.2] *Sean $K = \overline{k}$ y $L/K(x)$ una extensión finita y de Galois. Si el tipo T de la extensión es rígido y k-racional, entonces $L/K(x)$ está definida sobre k.*

Idea de la Demostración. La rigidez de T implica que $G = \mathrm{Gal}(L/K(x))$ tiene centro trivial. Dado $\alpha \in \mathrm{Gal}(K/k)$, lo extendemos a $K(x)[y]$ fijando x, y. El automorfismo α induce un α-isomorfismo

$$\lambda : L = K(x)[y]/(F) \to L' = K(x)[y]/(\alpha F),$$

donde F es un polinomio irreducible en $K(x)[y]$. Sea $G' = \mathrm{Gal}(L'/K(x))$. Se puede mostrar que la rigidez de T, la k-racionalidad de T y la trivialidad de $Z(G)$ implican que λ^* envía las clases de conjugación destacadas C_q de G a las clases destacadas C'_q de G'; por tanto $L/K(x)$ y $L'/K(x)$ tienen el mismo tipo de ramificación. Por el Lema 3.1.5, existe un $K(x)$-isomorfismo $\mu : L' \to L$. Definimos $\Psi = \mu \circ \lambda : L \to L$. Un cálculo muestra que Ψ^* fija todas las clases de conjugación, así que Ψ^* debe ser un automorfismo interno (el automorfismo que fija las clases de conjugación es único por la rigidez de T). Sea $g \in G$ tal que $\Psi^*(h) = ghg^{-1}$. Otro cálculo muestra que $\Phi = g^{-1}\Psi$ es un α-isomorfismo con $\Phi^* = id$, así que $L/K(x)$ está definida sobre k por el Lema 3.1.12. □

Teorema 3.1.16. [32, Teorema 5.2.3] *Si $T = [G, P, \mathbf{C}]$ es un tipo rígido y k-racional, con $k \subseteq \mathbb{C}$; entonces existe una única extensión de Galois finita $L/\mathbb{C}(x)$ de este tipo. Esta extensión está definida sobre una extensión puramente trascendental $k(t_1, ..., t_n)$ de k y G ocurre regularmente sobre k.*

Idea de la Demostración. $L/\mathbb{C}(x)$ existe por el Teorema 2.4.12 y es única por el Teorema 3.1.5. Por el mismo argumento que en la demostración del Lema 3.1.12, $L/\mathbb{C}(x)$ está definida en una extensión $k_1 = k(t_1, ..., t_r)$ de k. Si tomamos algunos $t_1, ..., t_s$ de estos generadores de modo que sean maximales con respecto a ser algebraicamente independientes, entonces k_1/k_0 con $k_0 = k(t_1, ..., t_s)$ es finita y k_0/k es puramente trascendental. Sea $K = \overline{k_1}$. Por un argumento similar al de la demostración del Lema 3.1.8, $L/\mathbb{C}(x)$ está definida sobre K, y por el Lema 3.1.9 $L/\mathbb{C}(x)$ y L_K/K tienen el mismo tipo. T es k-racional, así que por restricción también es k_0-racional. Esto implica que el tipo de L_K/K es k_0-racional, así que L_K/K está definida sobre k_0 por el Teorema 3.1.15. Así, L_{k_0} es tal que

$$\mathrm{Gal}(L/\mathbb{C}(x)) \simeq \mathrm{Gal}(L_K/K(x)) \simeq \mathrm{Gal}(L_{k_0}/k_0(x)) = \mathrm{Gal}(L_{k_0}/k(t_1, ..., t_s, x)).$$

Concluimos porque k es algebraicamente cerrado en k_0 y este a su vez lo es en L_{k_0} por Definición, así que k lo es en L_{k_0}. □

Corolario 3.1.17. *Si G es un grupo que tiene una r-upla rígida de clases de conjugación $(C_1, ..., C_r)$, con C_i racionales, entonces G ocurre regularmente sobre $\mathbb{Q}$.*

Idea de la Demostración. Directo del Teorema 3.1.16, usando la Observación 3.1.14. □

Esto es, por supuesto, lo que queríamos lograr.

Observación 3.1.18. En su celebrado artículo [6], John Thompson encontró una 3-upla rígida de clases de conjugación racionales (C_1, C_2, C_3) del Monster Group M; donde el orden común de los elementos de C_1, C_2 y C_3 es $2, 3$ y 29, respectivamente. Este resultado, junto al Corolario 3.1.17 y la Sección a continuación, mostrarán que este grupo es realizable sobre $\mathbb{Q}$.

3.2. El Teorema de Irreducibilidad de Hilbert

Una vez que hemos realizado los grupos sobre $\mathbb{Q}(x_1, ..., x_r)$, nos embarcamos en su realización sobre $\mathbb{Q}$. Nuestra Definición más importante para estos propósitos es la siguiente:

Definición 3.2.1. Un campo K se dice **hilbertiano** si para cada polinomio irreducible $f \in K[x, y]$ existen infinitos $b \in K$ de modo que $f_b(y) := f(b, y)$ es irreducible en $K[y]$.

Esta Definición será importante porque ser hilbertiano es suficiente para que un campo permita realizar este proceso de descenso. Para mostrar esto, requeriremos algunos lemas previos. Durante esta sección, L y K serán siempre campos de característica 0; y utilizaremos la expresión "casi todos" para referirnos a todos salvo finitos elementos de algún conjunto.

Teorema 3.2.2. [33, Teorema 1] *Sea $L/K(x)$ una extensión finita de Galois, α un elemento primitivo para la extensión y $f \in K[x][y]$ su polinomio mínimo. Para casi todo $b \in K$, si $f_b(y)$ es irreducible en $K[y]$, entonces L'/K es una extensión de Galois, donde $L' = K[y]/(f_b(y))$. Además,* $\mathrm{Gal}(L/K(x)) \simeq \mathrm{Gal}(L'/K)$.

Idea de la Demostración. Fijado $b \in K$, definimos el homomorfismo $\omega_b : K[x] \to K$, $p(x) \mapsto p(b)$. Se puede probar que, si $\omega_b(f(y)) = f_b(y)$ es irreducible, entonces L' es campo de descomposición de $\omega_b(f)$ sobre K si y sólo si $\omega_b(D(f)) \neq 0$, donde $D(f)$ es el discriminante del polinomio f. Así, en este caso L'/K es de Galois. Sean $\alpha_1, ..., \alpha_r$ las raíces de f (que generan L). El homomorfismo ω_b induce un isomorfismo entre $\mathrm{Gal}(L/K(x))$

y $\mathrm{Gal}(L'/K)$, definido por $\sigma_i \mapsto \sigma_i'$, donde σ_i es el único automorfismo de $\mathrm{Gal}(L/K(x))$ que envía α_1 a α_i y σ_i' es el único automorfismo de $\mathrm{Gal}(L'/K)$ que envía $\omega_b(\alpha_1)$ a $\omega_b(\alpha_i)$. Por tanto, el teorema es válido para todo $b \in K$ excepto las raíces de $h(x) = \omega_x(D(f))$, que son finitas porque este es un polinomio en una variable. □

Lema 3.2.3. [33, Teorema 2] *Sea K hilbertiano y $f \in K[x_1, ..., x_n]$ irreducible. Entonces, existen infinitos $b \in K$ de modo que $f(b, x_2, ..., x_n)$ es irreducible en $K[x_2, ..., x_n]$.*

Idea de la Demostración. Sea d un entero mayor que el grado de f en todas las variables $x_2, ..., x_n$. Definimos el homomorfismo de anillos

$$\begin{aligned} S_d : K[x_1, ..., x_n] &\to K[x, y] \\ f(x_1, ..., x_n) &\mapsto f(x, y, y^d, y^{d^2}, ..., y^{d^{n-2}}). \end{aligned}$$

que es biyectivo entre los conjuntos V_d de polinomios de grado menor a d en cada variable $x_2, ..., x_n$ y W_d de polinomios de grado menor a d^{n-1} en y. A través de este homomorfismo, agruparemos todos los factores de grado 0 en y de $S_d(f)$ en un polinomio $g(x)$, es decir,

$$S_d(f) = g(x) \prod_{i \in I} g_i(x, y)$$

donde cada g_i es de grado positivo en y e irreducible. Como K es hilbertiano, para casi todo $b \in K$ cada uno de los $g_i(b, y)$ es irreducible. Consideraremos el conjunto de estos b, con la condición extra $g(b) \neq 0$. Supongamos que $f_b = f(b, x_2, ..., x_n)$ es reducible, es decir, $f_b = hh' \in K[x_1, ..., x_n]$. Como $S_d(h)S_d(h') = g(b) \prod_{i \in I} g_i(b, y)$, podemos particionar I en $\{A, B\}$ de modo que $S_d(h) = u \prod_{i \in A} g_i(b, y)$ y $S_d(h') = u' \prod_{i \in B} g_i(b, y)$, con $uu' = g(b)$. Escribimos $H = \prod_{i \in A} g_i(b, y)$ y $H' = \prod_{i \in B} g_i(b, y)$, de modo que

$$uHu'H' = g(b)HH' = S_d(f).$$

Como tanto H como H' están en W_d, existen únicos $\tilde{h}, \tilde{h}'$ tal que $S_d(\tilde{h}) = H$ y $S_d(\tilde{h}') = H'$. Así (luego de un cálculo sencillo), encontramos que $\tilde{h}_b \tilde{h}_b' = g(b)^{-1} f_b$ y que $\tilde{h}\tilde{h}' \notin V_d$. De aquí, notamos que b debe ser raíz de los coeficientes de cada monomio de $\tilde{h}\tilde{h}'$ como polinomio en $F[x_2, ..., x_n][x_1]$ donde alguna variable $x_2, ..., x_n$ tiene grado mayor a $d-1$, ya que $\tilde{h}\tilde{h}' \notin V_d$ pero $f \in V_d$. Sin embargo, sólo hay finitos de estos coeficientes, porque sólo pueden haber finitas factorizaciones gHH' de $S_d(f)$. Por tanto, si tomamos b fuera de este conjunto, tenemos una contradicción, y por tanto f_b es irreducible. Así, f_b es irreducible para casi todo $b \in K$. □

Teorema 3.2.4. [33, Teorema 3] *Toda extensión finitamente generada y puramente trascendental de un campo hilbertiano es hilbertiana.*

Idea de la Demostración. Sea $L = K(x_1, ..., x_n)/K$ esta extensión. Sea $f \in L[x, y]$ un polinomio irreducible. Elegimos $g \in K[x_1, ..., x_n]$ de modo que $gf \in K[x_1, ..., x_n, x, y]$.

Por el Teorema 3.2.3, existirán infinitos $b \in K$ de modo que $(gf)_b = (gf)(x_1, ..., x_n, b, y)$ es irreducible en $K[x_1, ..., x_n, y]$. Por el Lema 1.5.1, $(gf)_b$ será irreducible en $L[y]$. Como $(gf)_b = g_b f_b$ y $g_b = g$ es una unidad en $L[y]$, f_b es irreducible en $L[y]$. □

Observación 3.2.5. De hecho, se puede probar que toda extensión finitamente generada de un campo hilbertiano es hilbertiana. Esto sigue del Teorema anterior y de mostrar que toda extensión finita lo es; lo que no es muy complicado de probar (en [33, Teorema 3] se muestra este resultado en completitud). Esto, junto al Teorema de Irreducibilidad de Hilbert, implicará que todo campo de números es hilbertiano; otro resultado muy útil para la Teoría de Números.

Teorema 3.2.6. [33, Teorema 4] *Si K es hilbertiano y $L/K(x_1, ..., x_n)$ es finita y de Galois, entonces existe L' de modo que L'/K es finita y de Galois y* $\mathrm{Gal}(L/K(x_1, ..., x_n)) \simeq \mathrm{Gal}(L'/K)$.

Idea de la Demostración. Por inducción en n utilizando el Teorema 3.2.2 y el Teorema 3.2.4. □

De este modo, lo único que nos queda para terminar es el siguiente Teorema:

Teorema 3.2.7. *(Teorema de Irreducibilidad de Hilbert) $\mathbb{Q}$ es hilbertiano.*

Este Teorema fue presentado por primera vez por David Hilbert en [4]. Las demostraciones modernas de este resultado son bastante elementales, si bien un poco involucradas. Una de ellas se encuentra, por ejemplo, en [34, Teorema 7]. Así, todo grupo realizable sobre $\mathbb{Q}(x_1, ..., x_n)$ lo es sobre $\mathbb{Q}$, que es lo que queríamos.

Observación 3.2.8. A través de este método, se han realizado exitosamente, por ejemplo, las familias de grupos simétricos S_n y alternos A_n (por David Hilbert, en [4]), todos los grupos espóradicos a excepción del grupo de Mathieu M_{23} (por John Thompson en [6] y Bernd Matzat en [30]) y los grupos proyectivos especiales lineales $\mathrm{PSL}_2(q)$ para $q \not\equiv \pm 1 \mod 24$ (por Kuang-yen Shih en [31]).

Ejemplo 3.2.9. Como ejemplo, realizamos la familia de grupos simétricos S_n con $n \geq 3$ sobre $\mathbb{Q}$. Sabemos por el Corolario 3.1.17 y los Teoremas 3.2.6 y 3.2.7 que nos basta encontrar una r-upla rígida de clases de conjugación $(C_1, ..., C_r)$ de S_n con C_i racionales. Consideramos la tripla $(C^{(2)}, C^{(n)}, C^{(n-1)})$, donde $C^{(i)}$ es la clase de conjugación de $i-$ciclos de S_n. Estas clases contienen elementos $\tau = (12)$, $\sigma = (12...n)$ y $(\tau\sigma)^{-1}$ con producto 1 que generan S_n. Además, como el centro $Z(S_n)$ es trivial, la condición de unicidad de 3.1.2 (b) está satisfecha. Luego, la tripla que hemos encontrado es rígida.
Ahora, mostramos que todas las clases $C^{(i)}$ son racionales. Sean $(a_1, ..., a_i)$ un i-ciclo y $l < n!$ un entero con $\mathrm{mcd}(l, n!) = 1$. Como $(a_1, ..., a_i)^l$ solo mueve i elementos, su

descomposición en ciclos disjuntos sólo contiene ciclos de largo $\leq i$. Además el orden m de $(a_1, ..., a_i)^l$ es tal que

$$1 = ((a_1, ..., a_i)^l)^m = (a_1, ..., a_i)^{lm}$$

y por tanto el orden i de $(a_1, ..., a_i)$ divide a lm. Como l es coprimo con $n!$, lo es con i; así que i divide a m. Concluimos que $(a_1, ..., a_i)^l$ es un i-ciclo, y por tanto ${C^{(i)}}^l \subseteq C^{(i)}$. Recíprocamente, como $\text{mcd}(l, n!) = 1$, existen enteros a, b tal que $al + bn! = 1$ por el Lema de Bézout. Así,

$$(a_1, ..., a_i) = ((a_1, ..., a_i)^a)^l,$$

de donde $(a_1, ..., a_i)$ está en ${C^{(i)}}^l$ porque, por el mismo argumento anterior, $(a_1, ..., a_i)^a$ es un ciclo de largo i (usando que también $\text{mcd}(a, n!) = 1$). Luego, $C^{(i)} \subseteq {C^{(i)}}^l$. Así, $C^{(i)} = {C^{(i)}}^l$; es decir, es racional. Por tanto, la tripla que hemos encontrado deriva en una realización de S_n como grupo de Galois sobre $\mathbb{Q}$.

Referencias

[1] Évariste Galois, *Mémoire sur les conditions de résolubilité des équations par radicaux*, Journal de Liouville (1846), 417–433. Recuperado de *Oeuvres mathematiques*, publicado por Jacques Gabay, 1989. ↑4

[2] Bernhard Riemann, *Grundlagen für eine allgemeine Theorie der Funktionen einer veränderlichen complexen Größe*, Inauguraldissertation, University of Göttingen (1851). ↑4

[3] Bernhard Riemann, *Theorie der Abel'schen Functionen*, Journal für die Reine und Angewandte Mathematik. **54** (1857), 115–155. ↑4

[4] David Hilbert, *Über die Irreducibilität ganzer rationaler Funktionen mit ganzzahligen Koefficienten*, Journal für die Reine und Angewandte Mathematik. **110** (1892), 104–129. ↑4, 64

[5] I. R. Šafarevič, *The imbedding problem for splitting extensions*, Doklady Akademii Nauk SSSR **120** (1958), 1217–1219. ↑4

[6] John G. Thompson, *Some finite groups which appear as* $\mathrm{Gal}(L/K)$*, where* $K \subseteq \mathbb{Q}(\mu_n)$, Journal of Algebra **89** (1984), no. 2, 437–499. ↑4, 62, 64

[7] Gunter Malle, B.H. Matzat, *Inverse Galois theory*, 1st ed., Springer monographs in mathematics, Springer, 2002. ↑4

[8] Otto Forster, *Riemannsche Flächen*, 1st ed., Heidelberger Taschenbücher 184, Springer-Verlag Berlin Heidelberg, 1977. ↑5

[9] Helmut Volklein, *Groups as Galois Groups: An Introduction*, 1st ed., Cambridge Studies in Advanced Mathematics, Cambridge University Press, 2008. ↑4, 5, 6, 7, 9, 12, 30

[10] Walter Rudin, *Real and complex analysis*, 3rd ed., MGH, 1986. ↑6, 7

[11] Balmohan Vishnu Limaye, *Functional analysis*, 3rd ed, New age international, 2013. ↑6

[12] Rick Miranda, *Algebraic curves and Riemann surfaces*, Graduate studies in mathematics 5, American Mathematical Society, 1995. ↑9, 10, 12

[13] Ahlfors L., *Complex analysis*, 2nd ed., MGH, 1966. ↑8, 11

[14] R. Beattie, H.- P. Butzmann, *Convergence Structures and Applications to Functional Analysis*, 1st ed., Springer Netherlands, 2002. ↑7

[15] Michael Artin, *Algebra*, United States ed, Prentice Hall, 1991. ↑16

[16] John M. Lee, *Introduction to Smooth Manifolds*, version 3.0 draft, Graduate Texts in Mathematics 218, Springer New York, 2003. ↑7

[17] James Munkres, *Topology*, 2nd ed, Prentice Hall, Inc, 2000. ↑11, 12, 33

[18] A. I. Markushevich, *Theory of Functions of a Complex Variable, Volume 2*, Chelsea Publishing, 1960. ↑8

[19] David A. Cox, *Galois Theory*, Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts, Wiley, 2004. ↑15, 16

[20] William S. Massey, *Algebraic topology, an introduction*, 4th corrected printing, Graduate texts in mathematics 56, Springer-Verlag, 1977. ↑33

[21] Marcel Berger, M. Cole, S. Levy, *Geometry 1*, Corrected, Universitext, Springer, 1987. ↑40

[22] Antonio Laface, *Teoría de Galois*, Notas de Curso, Universidad de Concepción, 2018. ↑14

[23] Tamás Szamuely, *Galois Groups and Fundamental Groups*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2009. ↑56

[24] Jean-Pierre Serre, *Local Fields*, Graduate Texts in Math., vol. 67, Springer, 1980. ↑38

[25] Jairo A. Charris, Guillermo Rodriguez-Blanco, *Sobre el Teorema Integral de Cauchy*, Boletín de Matemáticas **1** (1994), 1–8. ↑8

[26] P.H. Doyle, D.A. Moran, *A short proof that compact 2-manifolds can be triangulated*, Inventiones Mathematicae **5** (1968), 160–162. ↑10

[27] Bonnie Huggins, *Fields of moduli of hyperelliptic curves*, Mathematical Research Letters **14** (2007), no. 2, 249–262. ↑52

[28] É. I. Zverovich, *An algebraic method for constructing the basic functionals of a Riemann surface given in the form of a finite covering of a sphere*, Akademiya Nauk SSSR. Sibirskoe Otdelenie. Sibirskiĭ Matematicheskiĭ Zhurnal **28** (1987), no. 6, 32–43, 217. ↑51

[29] Yuri F. Bilu, Marco Strambi, *Quantitative Riemann existence theorem over a number field*, Acta Arithmetica **145** (2010), no. 4, 319–339. ↑51

[30] B. Heinrich Matzat, *Rationality criteria for Galois extensions*, in Galois groups over **Q** (Berkeley, CA, 1987), 1989, pp. 361–383. ↑64

[31] Kuang-yen Shih, *On the construction of Galois extensions of function fields and number fields*, Mathematische Annalen **207** (1974), 99–120. ↑64

[32] Amin Saied, *The Inverse Galois Problem: The Rigidity Method*, Tesis en el Departmento de Matemáticas, Imperial College London, available at https://aminsaied.files.wordpress.com/2012/04/the-inverse-galios-problem-the-rigidity-method.pdf (2011). ↑58, 59, 60, 61

[33] Logan Chariker, *The Inverse Galois Problem, Hilbertian Fields, and Hilbert's Irreducibility Theorem*, University of Chicago VIGRE REU, available at https://math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Chariker.pdf (2007). ↑62, 63, 64

[34] Rodney Coleman, Laurent Zwald, *Hilbertian fields and Hilbert's irreducibility theorem*, preprint at HAL, available at https://hal.archives-ouvertes.fr/hal-01883575 (2018). ↑64

[35] Keith Conrad, *Generating Sets*, Expository Paper at kconrad.math.uconn.edu (2018). ↑51, 52