El teorema de Belyĭ

José Cuevas Barrientos

Resumen. En este artículo se da un resumen de la versión de Grothendieck del teorema de existencia de Riemann que dice que «todo recubrimiento topológico entre las analitificaciones de esquemas algebraicos sobre $\mathbb{C}$ viene de un morfismo étale» y se aplica para probar el teorema de Belyĭ de que una curva proyectiva y suave sobre $\mathbb{C}$ está definida sobre $\mathbb{Q}^{\text{alg}}$ si y sólo si posee un morfismo hacia $\mathbb{P}^1$ que se ramifica en tres puntos.

1. El teorema de existencia de Riemann

Recordemos primero las dos siguientes nociones paralelas:

Definición 1.1: Un ***recubrimiento (topológico)*** es una función continua y sobreyectiva $f\colon X \to Y$ tal que todo punto $y \in Y$ posee un entorno abierto $y \in U$ tal que $f^{-1}[U] = \coprod_j V_j \subseteq X$, donde $f|_{V_j}\colon V_j \to U$ es un homeomorfismo.

Definición 1.2: Sean X, Y un par de esquemas algebraicos sobre un cuerpo k. Un ***morfismo étale*** $f\colon X \to Y$ es un morfismo plano y sobreyectivo tal que para cada $y \in Y$, la fibra $X_y := X \times_k \operatorname{Spec} \Bbbk(y)$ tiene dimensión 0 (o equivalentemente, es un esquema artiniano).

No es al principio tan claro el cómo estas ideas se relacionan, pero para Grothendieck, el segundo es el análogo algebraico del primero y trataremos de formalizar esa idea aquí. Para poder lograrlo, primero necesitaremos de una forma de pasar de esquemas a espacios con una topología más fina que la de Zariski.

1.1. El funtor de analitificación.

En esta sección asumiremos que el lector conoce las nociones de «espacio (localmente) anillado» y «$\mathscr{O}_X$-módulo coherente» al nivel de, e.g., Hartshorne **[2],** §§II.1 y II.5.

Definición 1.3: Sea k un espacio métrico (i.e., dotado de un valor absoluto) completo. Dado un abierto $U \subseteq k^n$, una función $f\colon U \to k$ se dice

Fecha: 28 de marzo de 2025.

analítica si para cada punto $\boldsymbol{a} = (a_1, \ldots, a_n) \in U$ hay un $\epsilon > 0$ tal que

$$f(\boldsymbol{x} + \boldsymbol{a}) = f(\boldsymbol{a}) + \sum_{\alpha} c_\alpha \boldsymbol{x}^\alpha, \qquad \|\boldsymbol{x}\| < \epsilon; \tag{1}$$

donde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ es un multiíndice y $\boldsymbol{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. En particular, suponemos que estas series formales de potencias *convergen*: es decir, dada la expansión (1), existen reales $r_1, \ldots, r_n, M > 0$ tales que

$$\forall \alpha \qquad |c_\alpha| r_1^{\alpha_1} \cdots r_n^{\alpha_n} \leq M.$$

Al espacio dotado de la topología producto k^n le asociamos el haz de anillos $\mathscr{O}_{\text{an}}$ que a cada abierto $U \subseteq k^n$ le asigna el conjunto $\mathscr{O}_{\text{an}}(U) = \text{Hom}_{\mathsf{An}}(U, k)$ de funciones analíticas $U \to k$. Con ello, obtenemos el espacio anillado $\mathbb{A}_k^{n,\text{an}}$.

Observación 1.3.1: El espacio $\mathbb{A}_k^{n,\text{an}}$ es localmente anillado: sea $\boldsymbol{a} \in \mathbb{A}_k^{n,\text{an}}$ un punto, el anillo local en $\boldsymbol{a}$ es isomorfo al anillo de series formales convergentes $k\langle\langle x_1, \ldots, x_n \rangle\rangle$ (también $k\{x_1, \ldots, x_n\}$). Es claro que el ideal $(x_1, \ldots, x_n)$ es maximal y es un ejercicio ver que es el único, o dicho de otro modo, hay que ver que una serie convergente tal que $f(\mathbf{0}) \neq 0$ tiene inversa *convergente*.

Más aún el cuerpo de restos es k mismo y $k\langle\langle x_1, \ldots, x_n \rangle\rangle$ es noetheriano.

Definición 1.4: Un ***espacio analítico*** sobre un cuerpo métrico completo k es un espacio localmente anillado $(X, \mathscr{O}_X)$ tal que cada punto $x \in X$ posee un entorno $x \in U$, tal que el subespacio $(U, \mathscr{O}_X|_U)$ es isomorfo a un subespacio anillado *de presentación finita* de $\mathbb{A}_k^{n,\text{an}}$.

Un ***morfismo*** entre espacios analíticos es un morfismo de espacios localmente anillados $(f, f^\sharp) \colon (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ tal que para cada abierto $V \subseteq Y$, el homomorfismo $f^\sharp(V) \colon \mathscr{O}_Y(V) \to \mathscr{O}_X(f^{-1}[V])$ es de k-álgebras. Con esto se define la categoría An_k de espacios analíticos sobre k.

Note que no exigimos que nuestros espacios analíticos sean ni de Hausdorff, ni que satisfagan el segundo axioma de numerabilidad.

Ejemplo. Sea $F(x) := \sum_{n=0}^{\infty} c_n x^n \in k\langle\langle x \rangle\rangle$ una serie convergente en toda la recta afín. Esto induce una función continua $f \colon \mathbb{A}_k^{1,\text{an}} \to \mathbb{A}_k^{1,\text{an}}$ y, dado un abierto $U \subseteq k$, induce el homomorfismo

$$f^\sharp(U) \colon \mathscr{O}_{\mathbb{A}^{1,\text{an}}}(U) \longrightarrow \mathscr{O}_{\mathbb{A}^{1,\text{an}}}(F^{-1}[U]), \qquad g \longmapsto F \circ g.$$

Es claro que $f^\sharp$ es un homomorfismo de k-álgebras y que es funtorial en U, de modo que $(f, f^\sharp)$ es un morfismo de espacios analíticos. Naturalmente, toda función analítica en más variables satisface lo mismo.

Ahora hacemos un resumen de resultados dados en **[SGA I],** Exposé XII.

Teorema 1.5 (1.1): Sea X un esquema algebraico sobre el cuerpo de números complejos $\mathbb{C}$. Considere el siguiente funtor:

$$\text{ⱡ}X^{\text{an}}\colon \mathsf{An}_{\mathbb{C}}^{\text{op}} \longrightarrow \mathsf{Set}, \qquad \mathcal{Y} \longmapsto \text{Hom}_{\mathbb{C}}(\mathcal{Y}, X),$$

donde $\text{Hom}_{\mathbb{C}}$ denota los morfismos de espacios anillados en $\mathbb{C}$-álgebras.

El funtor $\text{ⱡ}X^{\text{an}}$ es representable por (un espacio analítico) X^{an}, llamado la ***analitificación*** de X. Además:

1. El espacio subyacente a X^{an} está en biyección natural con los puntos racionales $X(\mathbb{C})$.
2. El morfismo canónico $\varphi\colon X^{\text{an}} \to X$ es local y, para cada punto $x \in X^{\text{an}} = X(\mathbb{C})$, induce un isomorfismo en las compleciones

$$\widehat{\varphi}_x^\sharp\colon \widehat{\mathscr{O}}_{X,\varphi(x)} \xrightarrow{\sim} \widehat{\mathscr{O}}_{X^{\text{an}},x}.$$

Proposición 1.6 (3.1 y 3.2): Sean X, Y un par de esquemas algebraicos sobre $\mathbb{C}$. Un morfismo $f\colon X \to Y$ es:

plano,	un isomorfismo,	sobreyectivo,
étale,	un encaje abierto,	propio y/o
suave,	un encaje cerrado,	finito

syss $f^{\text{an}}\colon X^{\text{an}} \to Y^{\text{an}}$ lo es.

1.2. Esquemas propios.

Teorema 1.7 (4.4): Supongamos que X es un esquema propio sobre $\mathbb{C}$. Entonces el funtor $\mathscr{F} \mapsto \varphi^*\mathscr{F} =: \mathscr{F}^{\text{an}}$ es una equivalencia entre la categoría de $\mathscr{O}_X$-módulos coherentes y la categoría de $\mathscr{O}_{X^{\text{an}}}$-módulos coherentes.

De esto se deducen dos corolarios de gran interés:

Corolario 1.7.1 (4.5): El funtor de analitificación $X \mapsto X^{\text{an}}$ restringido a los $\mathbb{C}$-esquemas propios es plenamente fiel.

Dicho de otro modo, si X, Y son esquemas propios sobre $\mathbb{C}$ y $F\colon X^{\text{an}} \to Y^{\text{an}}$ es una función analítica, entonces existe un morfismo $f\colon X \to Y$ de $\mathbb{C}$-esquemas tal que $F = f^{\text{an}}$.

Demostración: Darse un morfismo de esquemas (resp. de espacios analíticos) $X \to Y$ es lo mismo que darse un subesquema (resp. subespacio analítico) cerrado de $X \times Y$ correspondiente al gráfico del morfismo, lo cual equivale a darse un haz de ideales coherente de $\mathscr{O}_{X\times Y}$. □

Corolario 1.7.2 (4.6): Sea X un $\mathbb{C}$-esquema propio. El funtor que a todo X-esquema (étale) finito Y le asocia Y^{an} establece una equivalencia con los espacios analíticos (étale) finitos sobre X^{an}.

DEMOSTRACIÓN: Darse un morfismo finito $Y \to X$ de esquemas (resp. de espacios analíticos) equivale a darse una $\mathscr{O}_X$-álgebra coherente. □

Finalmente, un resultado muy importante (cfr. Thm. 5.1):

Teorema 1.8 – *Teorema de existencia de Riemann*: Sea X un esquema algebraico sobre $\mathbb{C}$. El funtor de analitificación establece una equivalencia entre recubrimientos étale finitos de X y recubrimientos étale finitos de X^{an}.

👀 Es importante notar que ahora no le exigimos a X que sea propio, de lo contrario se deduciría del corolario anterior.

2. El teorema de Belyĭ

Lema 2.1 (de Belyĭ): Sea $g\colon X \to Y$ un morfismo entre curvas íntegras suaves sobre un cuerpo numérico K. Sea $S \subseteq X(\mathbb{Q}^{\mathrm{alg}})$ un conjunto finito de puntos geométricos, entonces hay un K-morfismo racional no constante $h\colon Y \to \mathbb{P}^1_K$ tal que la composición $f := g \circ h\colon X \to \mathbb{P}^1_K$ es no ramificada fuera de $f^{-1}[\{0,1,\infty\}]$ y tal que $f[S] \subseteq \{0,1,\infty\}$.

DEMOSTRACIÓN: Sea $Y \to \mathbb{P}^1_K$ un K-morfismo no constante cualquiera (uno viene dado por el teorema de normalización de Noether) y digamos que su lugar de ramificación son los puntos geométricos $T \subseteq \mathbb{P}^1(\mathbb{Q}^{\mathrm{alg}})$. Vamos a ver que podemos suponer que $T \subseteq \mathbb{P}^1(\mathbb{Q})$ por inducción sobre el máximo grado de un punto de T. Si $\alpha \in T$ es algebraico sobre $\mathbb{Q}$ con polinomio minimal $p(t) \in \mathbb{Q}[t]$ y de grado maximal d entre los puntos de T, entonces $p\colon \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ determina un $\mathbb{Q}$-morfismo que se ramifica en las raíces T' de $p'(t)$, los cuales son números de grado $d-1$; así el lugar de ramas de la composición es $p[T] \cup p[T']$ que tiene menos puntos de grado $< d$. Así procediendo inductivamente, nos reducimos al caso de $K = \mathbb{Q}$ y $T \subseteq \mathbb{P}^1(\mathbb{Q})$.

Reordenando, digamos que $\lambda_1 < \lambda_2 < \cdots < \lambda_n \leq \infty$ son los puntos de T. Tras componer con $z \mapsto Nz$ podemos suponer que todos los λ_j's son enteros y componiendo con $z \mapsto z+1$ y $z \mapsto 1/z$, también suponer que $\lambda_n \neq \infty$. Luego, sea

$$V := \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \cdots & \lambda_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \cdots & \lambda_n^{n-1} \end{vmatrix} = \prod_{i<j} (\lambda_i - \lambda_j)$$

el determinante de la matriz de Vandermonde, y sean

$$y_j := \prod_{\ell \neq j} (\lambda_j - \lambda_\ell)^{-1}, \qquad a_j := V y_j \in \mathbb{Z}.$$

Con estos definimos $G(t) := \prod_{j=1}^n (t - \lambda_j)^{a_j} \in \mathbb{Q}[t]$ el cual determina el $\mathbb{Q}$-endomorfismo de $\mathbb{P}^1$.

Note que $G[\{\lambda_1,\dots,\lambda_n,\infty\}] = \{0,\infty,G(\infty)\}$. Para ver en qué puntos se ramifica G basta ver los polos de

$$(\log G(t))' = \frac{G'(t)}{G(t)} = \sum_{j=1}^{n} \frac{a_j}{t-\lambda_j} = \frac{V}{\prod_{j=1}^{n}(t-\lambda_j)};$$

esta igualdad equivale a $\sum_{j=1}^{n} y_j \prod_{\ell\neq j}(x-\lambda_\ell) - 1 = 0$ lo que se deduce de que el polinomio tenga grado $\leq n-1$ y n raíces.

Así G se ramifica en $\{\lambda_1,\dots,\lambda_n,\infty\}$. Por último, faltaría ver que $G(\infty) = 1$, esto equivale a ver que

$$\sum_{j=1}^{n} a_j = 0.$$

Lo cual se deduce de que $a_j = Vy_j = (-1)^j V(\lambda_1,\dots,\lambda_{j-1},\lambda_{j+1},\dots,\lambda_n)$ y de la fórmula del determinante mirando los cofactores de la última fila de la matriz no inversible:

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \cdots & \lambda_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{vmatrix}. \qquad \square$$

Teorema 2.2 – *Teorema de Belyĭ, 1979*: Sea C una curva (algebraica) íntegra, proyectiva y suave sobre $\mathbb{C}$. Son equivalentes:

1. Existe una curva C' sobre $\mathbb{Q}^{\mathrm{alg}}$ tal que C es $\mathbb{C}$-isomorfa al cambio de base $C'_{\mathbb{C}}$.
2. Existe una función racional no constante $f\colon C \to \mathbb{P}^1(\mathbb{C})$ ramificada a lo más en tres puntos. Más aún, poscomponiendo con una transformación de Möbius, podemos suponer que su locus de ramificación está contenido en $\{0,1,\infty\}$.
3. Existe un subgrupo de índice finito de $\Gamma(2)$ tal que $\Gamma \setminus \mathfrak{H}$ es biholomorfa a $U(\mathbb{C})$, donde $U \subseteq C$ es un abierto de Zariski denso.

Demostración: $2 \implies 1$. Supongamos que el lugar de ramificación está contenido en $S = \{0,1,\infty\}$. Así, $C \smallsetminus f^{-1}[S] \to \mathbb{P}^1(\mathbb{C}) \smallsetminus S$ es un recubrimiento étale y, por el teorema de existencia de Riemann viene de un morfismo étale de $\mathbb{C}$-esquemas. Ahora bien, como $\mathbb{P}^1 \smallsetminus S$ está definido sobre $\mathbb{Q}$, vemos que un morfismo étale sobre $\mathbb{C}$ debe venir de uno sobre $\mathbb{Q}^{\mathrm{alg}}$ (cfr. [**SGA I,** pág. 266], Cor. X.1.8) y, por el principio de extensión finita, este morfismo viene definido sobre una extensión finita de $\mathbb{Q}$.

$1 \implies 2$. Basta emplear el lema de Belyĭ con $f = g$ e $Y = \mathbb{P}^1_K$, para poscomponerlo y obtener un morfismo que se ramifica solo en $\{0,1,\infty\}$.

$2 \iff 3$. Sea $f\colon C \to \mathbb{P}^1_{\mathbb{C}}$ un morfismo no constante que se ramifica en $S := \{0,1,\infty\}$, de modo que la restricción $U := C \smallsetminus f^{-1}[S] \to \mathbb{P}^1_{\mathbb{C}} \smallsetminus S$ es un recubrimiento (étale) finito. Como la superficie de Riemann $\mathbb{P}^1(\mathbb{C}) \smallsetminus S$

tiene género 2 (¿por qué?), entonces su recubrimiento universal es $\pi\colon \mathfrak{H} \to \mathbb{P}^1(\mathbb{C}) \smallsetminus S$ (por el teorema de uniformización; cfr. Girondo y González-Diez [**1,** pág. 82], Th. 2.1).

Así obtenemos una factorización por un recubrimiento $\mathfrak{H} \twoheadrightarrow U(\mathbb{C})$ y, como $\pi_1^{\text{top}}(\mathbb{P}^1(\mathbb{C}) \smallsetminus S) = \Gamma(2)$ (cfr. [**1,** pág. 126], Th. 2.34), vemos que hay un subgrupo de índice finito $\Gamma \leq \Gamma(2)$ tal que $U(\mathbb{C}) \cong \Gamma \setminus \mathfrak{H}$. □

Notas históricas

El teorema de existencia de Riemann original dice que toda superficie de Riemann compacta es la analitificación de una curva proyectiva y suave sobre $\mathbb{C}$ (vid. apéndice B de [**2**]). Esta versión, en cambio, fue hecha principalmente por Grothendieck con la colaboración de Michèle Raynaud (esposa de Michel Raynaud) y publicada en el **[SGA I].** Hay gran inspiración en el teorema de Serre [**7**] y, de hecho, puede considerarse una forma de «principio GAGA».

El teorema de Belyĭ fue probado por el soviético en [**4**] (1979) y más tarde también dio otra prueba en [**5**]**.** A tal punto éste impresionó a Grothendieck que cuenta (cfr. [**6,** pág. 17]):

> (...) ¿Será que toda curva algebraica proyectiva suave definida sobre un cuerpo númerico se produzca como una «curva modular», parametrizada por curvas elípticas con una rigidificación apropiada? Tal suposición resultaba tan descabellada que me sentía casi avergonzado de siquiera ponerla a prueba. Efectivamente, tras consultarlo con Deligne él también la encontraba descabellada, mas no pudo sacar ningún contraejemplo de la manga. Menos de un año después, en el Congreso Internacional de Helsinki, el matemático soviético Belyĭ anunció precisamente este resultado, con una demostración de una simpleza desconcertante contenidas en unas minúsculas diez páginas de una carta de Deligne – ¡jamás, sin lugar a dudas, un resultado tan profundo y desconcertante fue probado en tan pocas líneas![1]

Referencias recomendadas son los libros de Girondo y González-Diez [**1**] con un enfoque más analítico, y el libro de Szamuely [**3**] con un enfoque más algebraico.

Referencias

1. Girondo, E. y González-Diez, G. *Introduction to Compact Riemann Surfaces and Dessins d'Enfants* (Cambridge University Press, 2012).

[1](...) Serait-il vrai que toute courbe algébrique projective et lisse définie sur un corps de nombres interviendrait comme une «courbe modulaire» possible pour paramétriser les courbes elliptiques munies d'une rigidification convenable ? Une telle supposition avait l'air à tel point dingue que j'étais presque gêné de la soumettre aux compétences en la matière. Deligne consulté trouvait la supposition dingue en effet, mais sans avoir un contre-exemple dans ses manches. Moins d'un an après, au Congres International de Helsinki, le mathematicien soviétique Bielyi annonce justement ce résultat, avec une demonstration d'une simplicité déconcertante tenant en deux petites pages d'une lettre de Deligne – jamais sans doute un résultat profond et déroutant ne fut démontré en si peu de lignes !

SGA I. Grothendieck, A. y Raynaud, M. *Séminaire de Géométrie Algébrique du Bois Marie (SGA).* I: *Revêtements étales et groupe fondamental* arXiv: `math/0206203 [math.AG]` (Springer-Verlag, 1960).

2. Hartshorne, R. *Algebraic Geometry Graduate Texts in Mathematics* **52** (Springer-Verlag New York, 1977).
3. Szamuely, T. *Galois groups and fundamental groups* (Cambridge University Press, 2009).

Documentos históricos

4. Белый Г. В. О расширениях Галуа максимального кругового поля. *Изв. АН СССР. Сер. матем.* **43,** 267-276 (1979). Belyi, G. V. On Galois extensions of a maximal cyclotomic field. *Math. USSR-Izv.* **14,** 247-256. doi:`10.1070/IM1980v014n02ABEH001096` (1980).
5. Белый Г. В. Новое доказательство теоремы о трех точках. *Матем. сб.* **193,** 21-24. doi:`10.4213/sm633` (2002).
6. Grothendieck, A. *Esquisse d'un Programme* en *Geometric Galois Actions. Around Grothendieck's* Esquisse d'un Programme (eds. Schneps, L. y Lochak, P.) **1** (Cambridge University Press, 1984), 5-48.
7. Serre, J.-P. Géométrie algébrique et géométrie analytique. *Ann. Inst. Fourier (Grenoble)* **6,** 1-42. doi:`10.5802/aif.59` (1956).