BUNTES - Belyi's Theorem

María Ines de Frutos Fernandez
Mar 16, 2018

Thm 3.1 [Belyi]: Let S be a compact Riemann surface.
The following are equivalent:
① S is defined over $\overline{\mathbb{Q}}$
② S admits a morphism $f: S \to \mathbb{P}^1$ with at most 3 branching values.

Remark: To say S is defined over $\overline{\mathbb{Q}}$ is in fact to say it is defined over a number field K.

Dfn: A meromorphic function with less than 4 branching values is a Belyi function.

Remarks: ① For a Belyi function, we will assume branching values $\subseteq \{0, 1, \infty\}$.
② If $S \neq \mathbb{P}^1$, then $f: S \to \mathbb{P}^1$ has at least 3 branching values.

Dfn: Fix $m, n \in \mathbb{Z}_{>0}$, $\lambda = \frac{m}{m+n}$.
Define

$$P_\lambda(x) = P_{m,n}(x) = \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n,$$

the Belyi polynomials.

Prop 3.3: $P_\lambda : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ satisfies

① P_λ ramifies exactly at $x = 0, 1, \lambda, \infty$

② $P_\lambda(0) = P_\lambda(1) = 0, \quad P_\lambda(\lambda) = 1, \quad P_\lambda(\infty) = \infty.$

Ex: $S_\lambda : \; y^2 = x(x-1)(x-\lambda) \quad$ with $\lambda = \frac{m}{m+n}$

From ex 1.32, $\quad x : S_\lambda \longrightarrow \mathbb{P}^1$

$(x, y) \longmapsto x$

$\infty \longmapsto \infty \quad$ ramifies over $0, 1, \lambda, \infty$

Then $f = P_\lambda \circ x : S_\lambda \longrightarrow \mathbb{P}^1$ ramifies exactly at $(0,0), (1,0), (\lambda, 0)$, and ∞, with branching values $0, 0, 1, \infty$.

$\Rightarrow f$ is a Belyi function.

§3.1. Proof of ① ⇒ ② in Belyi's thm

Note: It's enough to show that there exists $f : S \longrightarrow \mathbb{P}^1$ ramified over $\{0, 1, \infty, \lambda_1, \dots, \lambda_n\} \subseteq \mathbb{Q} \cup \{\infty\}$.

Since given this, we can repeatedly compose with Belyi polynomials to obtain $S \longrightarrow \mathbb{P}^1$ ramified over $\{0, 1, \infty\}$.

Write $S = S_F$, for $F(X, Y) = p_0(X) Y^n + \dots + p_n(X) \in \overline{\mathbb{Q}}[X, Y]$.

Let $B_0 = \{\mu_1, \dots, \mu_s\}$ be the set of branching values of $x : S_F \longrightarrow \mathbb{P}^1$.

Thm 1.86: Each μ_i is ∞, a root of $p_0(X)$, or the x-coordinate of a common root of F, F_y.

$\Rightarrow B_0 \subseteq \overline{\mathbb{Q}} \cup \{\infty\}$ (Lemma 1.84)

If $B_0 \subseteq \mathbb{Q} \cup \{\infty\}$, we are done.

Otherwise, let $m_1(T) \in \mathbb{Q}[T]$ be the minimal polynomial of $\{\mu_1, \dots, \mu_s\}$.
Let $\{\beta_1, \dots, \beta_d\}$ be the roots of $m_1'(T)$ and $p(T)$ their minimal polynomial.

Note: • $\deg P(T) < \deg m_1'(T)$

• Let $\mathrm{Branch}(f) = \{\text{branching values of } f\}$
Then
$$\mathrm{Branch}(g \circ f) = \mathrm{Branch}(g) \cup g(\mathrm{Branch}(f))$$

Thus $\mathrm{Branch}(m_1 \circ x) = m_1(\{\text{roots of } m_1'\}) \cup \{0, \infty\} =: B_1$

If $B_1 \subseteq \mathbb{Q} \cup \{\infty\}$, done.

Otherwise, let $m_2(T)$ be the minpoly $/\mathbb{Q}$ of $\{m_1(\beta_1), \dots, m_1(\beta_d)\}$.
$B_2 = \mathrm{Branch}(m_2 \circ m_1 \circ x)$.

Fact: $\deg m_2(T) < \deg m_1(T)$

So the degree of the minimal polynomial is lowering (strictly) each time. Repeat inductively until

$$B_k \subseteq \mathbb{Q} \cup \{\infty\}.$$

Then we are done, and we have ① $\Longrightarrow$ ②, as required. $\square$

---

§3.2. Algebraic characterisation of morphisms

<u>Prop 3.5</u>: Defining a morphism $f: S_F \longrightarrow S_G$ is equivalent to giving a pair of rational functions

$$f = (R_1, R_2), \qquad R_i = P_i / Q_i, \qquad P_i, Q_i \in \mathbb{C}[X, Y]$$
$$Q_i \notin (F)$$

such that

$$Q_1^{\deg_X G} Q_2^{\deg_Y G} G(R_1, R_2) = HF \quad \text{for some } H \in \mathbb{C}[X, Y].$$

If you have an isomorphism $f = (R_1, R_2)$, there exists an inverse morphism $h: S_G \longrightarrow S_F$. This is also described by a pair of polynomials, and the fact that these are mutually inverse can be expressed via some polynomial relations.

<u>Remark 3.10</u>:

$$\begin{tikzcd} S_F \arrow[r, "f"] \arrow[dr] & S_G \arrow[d, "h"] \\ & S_D \end{tikzcd}$$

The fact that the diagram commutes can be expressed by polynomial identities.

§3.3. Galois action

Let $\mathrm{Gal}(\mathbb{C}) = \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$.

Dfn: For $\sigma \in \mathrm{Gal}(\mathbb{C})$, $a \in \mathbb{C}$, denote $a^\sigma := \sigma(a)$.

① If $P = \sum a_{ij} x^i y^j \in \mathbb{C}[x,y]$, set
$$P^\sigma = \sum a_{ij}^\sigma x^i y^j \in \mathbb{C}[x,y].$$

If $R = \frac{P}{Q}$, set $R^\sigma = \frac{P^\sigma}{Q^\sigma}$.

② If $S = S_F$, $S^\sigma = S_{F^\sigma}$.

③ If $\Psi = (R_1, R_2) : S_F \longrightarrow S_G$ is a morphism, set
$$\Psi^\sigma = (R_1^\sigma, R_2^\sigma) : S_{F^\sigma} \longrightarrow S_{G^\sigma}.$$

④ For an equivalence class $(S, f) = (S_F, R(x,y))$ of ramified cover of $\mathbb{P}^1$, set
$$(S,f)^\sigma =: (S^\sigma, f^\sigma) = (S_{F^\sigma}, R^\sigma(x,y)).$$

Exercise: Verify this Galois action is well-defined (Lemma 3.12).

Recall: S_F is constructed from a noncompact Riemann surface $S_F^\times \subseteq \mathbb{C}^2$ by adding finitely many points. (Thm 1.86).

If $P = (a,b) \in S_F^\times$, then $P^\sigma = (a^\sigma, b^\sigma)$.

What about the other points?

Need to use valuations.

§3.4. Points and Valuations

Dfn 3.14: Let $\mathcal{M}$ be a function field.

A (discrete) valuation of $\mathcal{M}$ is $\nu : \mathcal{M}^\times \longrightarrow \mathbb{Z}$ s.t.

1. $\nu(\varphi\psi) = \nu(\varphi) + \nu(\psi)$
2. $\nu(\varphi \pm \psi) \geq \min\{\nu(\varphi), \nu(\psi)\}$
3. $\nu(\varphi) = 0$ if $\varphi \in \mathbb{C}^\times$
4. ν is nontrivial (i.e. $\exists \varphi$ s.t. $\nu(\varphi) \neq 0$)

Set $\nu(0) = \infty$.

Facts: • $A_\nu = \{\varphi \in \mathcal{M} \mid \nu(\varphi) \geq 0\} \subseteq \mathcal{M}$ is a local ring with maximal ideal $m_\nu = \{\varphi \in \mathcal{M} \mid \nu(\varphi) > 0\} = (\psi)$ for some ψ, a uniformiser.

• If $\nu(\psi) = 1$, ν is normalised.

Prop 3.15: Every point $P \in S$ (S a compact Riemann surface) defines a valuation on $\mathcal{M}(S)$ by $\nu_P(\varphi) = \mathrm{ord}_P(\varphi)$.

Pf: Easy exercise. $\square$

Thm 3.23: For any compact Riemann surface S,

$$\begin{aligned} S &\longrightarrow \{\text{normalised valuations on } \mathcal{M}(S)\} \\ P &\longmapsto \nu_P = \mathrm{ord}_P \end{aligned}$$

is a bijection.

Pf (sketch): First prove it for $S = \mathbb{P}^1$.

Injectivity: follows from the fact that meromorphic functions separate points.

Surjectivity: study behavior of valuations in finite extensions of fields and use a nonconstant morphism $f: S \longrightarrow \mathbb{P}^1$ to reduce to the case $S = \mathbb{P}^1$. $\square$

§ 3.4.1. Galois action on points

Dfn: ① Given a valuation ν on $\mathcal{M}(S)$, define a valuation ν^σ on $\mathcal{M}(S^\sigma)$ by $\nu^\sigma = \nu \circ \sigma^{-1}$.
(i.e. $\nu^\sigma(\varphi^\sigma) = \nu(\varphi)$ for all $\varphi \in \mathcal{M}(S)$).

② For $P \in S$ define $P^\sigma \in S^\sigma$ to be the unique point in S^σ such that $\nu_{P^\sigma} = (\nu_P)^\sigma$.

Prop 3.25: ① For $\sigma \in Gal(\mathbb{C}/\mathbb{Q})$, $P \longmapsto P^\sigma$ is a bijection $S \longrightarrow S^\sigma$

② On $P \in S_F^\times$, this agrees with the previous definition of P^σ

③ $a^\sigma = a \quad \forall\, a \in \mathbb{Q} \cup \{\infty\}$

Pf (sketch): ① $\mathbb{G} \longmapsto \mathbb{G}^{\sigma^{-1}}$

② Follows as in proof of 3.23.

③ Obvious for $a \in \mathbb{Q}$.

For ∞, $(\nu_\infty)^\sigma(x-a) = \nu_\infty(x - a^{\sigma^{-1}}) = 1$

$= \nu_\infty(x-a)$

for all $a \in \mathbb{C}$

$\Rightarrow (\nu_\infty)^\sigma = \nu_\infty \Rightarrow \infty^\sigma = \infty$, by 3.23. $\square$

§3.5. Elementary invariants of the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$

Remark: The bijection $S \longleftrightarrow S^\sigma$ is not holomorphic.
In general, S and S^σ are not isomorphic.

Thm 3-28: The action of $\mathrm{Gal}(\mathbb{C})$ on pairs (S, f) satisfies:

① $\deg(f^\sigma) = \deg(f)$

② $(f(P))^\sigma = f^\sigma(P^\sigma)$

③ $\mathrm{ord}_{P^\sigma}(f^\sigma) = \mathrm{ord}_P f$

④ $a \in \hat{\mathbb{C}}$ is a branching value of f
$\iff a^\sigma$ is a branching value of f^σ.

⑤ $\mathrm{genus}(S) = \mathrm{genus}(S^\sigma)$, ie. they are homeomorphic

⑥ $\mathrm{Aut}(S, f) \longrightarrow \mathrm{Aut}(S^\sigma, f^\sigma)$ is a group isomorphism
$h \longmapsto h^\sigma$

⑦ The monodromy group $\mathrm{Mon}(f)$ of (S, f) is isomorphic to $\mathrm{Mon}(f^\sigma)$ of (S^σ, f^σ)

§3-6. A criterion for definability over $\overline{\mathbb{Q}}$

Criterion 3.29: Let S be a compact Riemann surface.
The following are equivalent:

① S is defined over $\overline{\mathbb{Q}}$

② $\{S^\sigma\}_{\sigma \in \mathrm{Gal}(\mathbb{C})}$ contains only finitely many isomorphism classes of Riemann surfaces.

pf: ① $\Rightarrow$ ②: $S = S_F$, $F \in K[X, Y]$, $K/\mathbb{Q}$ a number field

Then $\#\{F^\sigma\}_{\sigma \in Gal(\mathbb{C})} \leq [K:\mathbb{Q}]$.

② $\Rightarrow$ ①: Section 3.7. □

§3.6.1. Proof of ② $\Rightarrow$ ① of Belyi's Thm

Suppose $f: S \longrightarrow \mathbb{P}^1$ is a morphism of degree d with branching values $\{0, 1, \infty\}$.

By Thm 3.28, $\forall \sigma \in Gal(\mathbb{C})$, $f^\sigma : S^\sigma \longrightarrow \mathbb{P}^1$ is a morphism of deg d with branching values $\{\sigma(0), \sigma(1), \sigma(\infty)\} = \{0, 1, \infty\}$.

So $\{f^\sigma\}_{\sigma \in Gal(\mathbb{C})}$ gives rise to only finitely many monodromy homomorphisms

$$M_{f^\sigma} : \pi_1(\underbrace{\mathbb{P}^1 \setminus \{0, 1, \infty\}}_{\text{free on two generators}}) \longrightarrow \Sigma_d$$

Thm 2.61 $\Rightarrow$ $\{S^\sigma\}_{\sigma \in Gal(\mathbb{C})}$ contains only finitely many equivalence classes

Criterion 3.29 $\Rightarrow$ S is defined over $\overline{\mathbb{Q}}$.

§3.8. The field of definition of Belyi functions

Prop 3.34: Belyi functions are defined over $\overline{\mathbb{Q}}$.

Pf: Use methods of 3.7. □