Notes on Belyi's Theorem

Taylor Dupuy

Abstract

The following note is based on a conversation I had with Zach Scherr.

Theorem 1. *Let $C/\mathbf{C}$ be a projective curve. There exists a map $\varphi : C \to \mathbf{P}^1$ ramified above at most three points if and only if C is defined over $\bar{\mathbf{Q}}$.*

Recall that for every point $Q \in \mathbf{P}(\mathbf{C})$ we have $\deg(\varphi) = \sum_{P \mapsto Q} e_f(P)$, and that P is a branch point of f if $e_f(P) > 1$. We say that Q is a branch value if $f(P) = Q$ where P is a branch point. The set of all branch values of a morphism f will be denoted $\mathrm{Br}(f)$. If $f : \mathbf{P}^1 \to \mathbf{P}^1$ is just a given by $f \in \mathbf{C}[x]$ then away from infinity the branch points are defined by $f(x) - a$ having a zero of multiplicity bigger than one.

Remark 1. The statement that if a curve only has these branch values then it is defined over $\bar{\mathbf{Q}}$ was actually proved first and the converse, that every curve over $\bar{\mathbf{Q}}$ has this property was actually proved later. This is interesting because it appears the harder theorem came first.

In this note we prove that every projective curve $C/\bar{\mathbf{Q}}$ admits a map to $\mathbf{P}^1$ which is ramified at $\{0, 1, \infty\}$. The proof goes in three steps.

Step 1 Pick an arbitrary morphism to $C \to \mathbf{P}^1$.

Step 2 Arrange so that the branch values are in $\mathbf{P}^1(\mathbf{Q})$; this is done by composing with a maps so that branch values of the previous map to zero under the next map.

Step 3 Arrange so that the critical values are in $\{0, 1, \infty\}$

Step 1: pick $\varphi_1 : C \to \mathbf{P}^1$ any morphism. The problem may be that $|\mathrm{Br}(f_1)| > 3$.

Step 2: We will now send $\mathrm{Br}(\varphi_1)$ to $\mathbf{P}^1(\mathbf{Q})$ via an inductive procedure. Set $S_0 := \mathrm{Br}(\varphi_1) \setminus \{\infty\}$ and let $S_0' =$ set of galois conjugates of S_0.

We construct the polynomial so that $\alpha \in S_0$ maps to zero under this map:

$$f_0 := \prod_{\alpha \in S_0'} (x - \alpha) \in \mathbf{Q}[x].$$

Set $S_1 =$ critical values of $f_0 \subset \mathbf{A}^1(\mathbf{C}) \subset \mathbf{P}^1(\mathbf{C})$.

Since S_1 is galois stable that map f_0 is galois-equivariant: $\forall \gamma \in S_0, \forall \sigma \in G_{\mathbf{Q}}$:

$$f_0'(\gamma) = 0 \text{ and } f_0(\gamma) = \beta \implies f_0'(\sigma(\gamma)) = 0 \text{ and } f_0(\sigma(\gamma)) = \sigma(\beta)$$

We repeat this process inductively defining $S_i = \mathrm{Br}(f_{i-1})$ for $i \geq 2$ and letting

$$f_i := \prod_{\alpha \in S_i} (x - \alpha) \in \mathbf{Q}[x].$$

Claim 1. *' Now define*

$$\varphi_{2,k} = f_k \circ f_{k-1} \circ \cdots \circ f_1 \circ f_0 \in \mathbf{Q}[x].$$

1. *The number of critical values of $\varphi_{2,k+1} \circ \varphi_1$ less than or equal to the number of critical values of $\varphi_{2,k} \circ \varphi_1$.*

2. *The number of rational critical values of $\varphi_{2,k+1} \circ \varphi_1$ is strictly bigger than the number of rational critical values of $\varphi_{2,k} \circ \varphi_1$*

Proof. Let $(f_0 \circ \varphi_1)'(\gamma) = 0$ then $f_0'(\varphi_1(\gamma))\varphi_1'(\gamma) = 0$. If $\varphi_1'(\gamma) = 0$ then $f_0(\varphi_1(\gamma)) = 0$. Suppose $f_0'(\varphi_1(\gamma)) = 0$. The number of such roots is strictly one less than $\#S_0$ since $f_0'(x)$ has degree $\#S_0 - 1$. So $f_0 \circ \varphi_1$ has less than or equal to the number of branch values as φ_1 and at least one more rational branch value.

Now the inductive step. Define $\varphi_{1,i} = f_{i-1} \circ \cdots \circ f_0 \circ \varphi_1$. Suppose that $(f_i \circ \varphi_{1,i})'(\gamma)) = 0$. Then $f_i'(\varphi_{1,i}(\gamma) = 0$ or $\varphi_{1,i}'(\gamma) = 0$. If $\varphi_{1,i}'(\gamma) = 0$ then $f_i(\varphi_{1,i}(\gamma)) = 0$ by definition of f_i. This shows that all previous critical values map to zero. If $f_i'(\varphi_{1,i}(\gamma)) = 0$ then $\varphi_{1,i}(\gamma)$ is a critical point of f_i and there are less than or equal to $\#S_i - 1$ of these.

So if $\deg(\varphi_1) = d$ the process will terminate in at most d steps. Let φ_2 be the map where this terminates. And consider the map $\varphi_2 \circ \varphi_1 : C \to \mathbf{P}^1$. The critical values of $\varphi_2 \circ \varphi_1 \subset \mathbf{P}^1(\mathbf{Q})$. (Note that we can actually can assume the branch values are in $\mathbf{P}^1(\mathbf{Z})$ by clearing the denominators in our f_i's.)

□

Last Step: take these points to $\{0, 1, \infty\}$ and φ_3 with critical values $\{0, 1, \infty\}$

Claim 2. *Let $n_i \in \mathbf{Z}$ be the critical values of $\varphi_2 \circ \varphi_1$. If $\varphi_2 = \varphi_{2,k}$ then the rational function*

$$g := \prod_{i=1}^{k} (x - n_i)^{c_i}$$

has the property that the branch values of $g \circ \varphi_2 \circ \varphi_1$ are a subset of $\{0, 1, \infty\}$ for some suitable choice of $c_i \in \mathbf{Z}$.

Proof. If $g'/g = 0$ then the formula

$$\frac{g'}{g} = \sum_{i=1}^{n} c_i(x - n_i)$$

We choose the c_i so that

$$\frac{g'}{g} = \frac{A}{(x - n_1)(x - n_2) \cdots (x - n_k)}.$$

Choosing $c_j = \prod_{i \neq j}^{k} (n_j - n_i)$ makes this work. It turns out that $g' = A \prod_i (x - n_i)^{c_i - 1}$ and hence g has no finite critical points except maybe at one of the n_i. But $g(n_i) = 0$ or ∞ Maybe ∞ is a critical point and we have

$$g(\infty) = 0, 1 \text{ or } \infty.$$

□