SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Belyi's Theorem and Belyi Maps on Hurwitz Curves

av

Lina Palm

2020 - No K15

Belyi's Theorem and Belyi Maps on Hurwitz Curves

Lina Palm

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Wushi Goldring

2020

Abstract

Trough Belyi maps we explore branching on maps between curves. Using only the fundamentals of the theory of ramification we can prove Belyi's theorem. In an application of the Riemann-Hurwitz formula we find Belyi maps on Hurwitz curves, in particular we look at a map on the Klein quartic.

Acknowledgements

I would like to express my great appreciation to my supervisor Wushi Goldring for his patient guidance and for providing a wealth of inspiration. I would also like to thank Dan Petersen, who reviewed this thesis, for his helpful suggestions.

Many thanks to Joel Fredin for the many times he has listened to revised and rearranged versions of the proof in chapter 4.

Contents

1 Introduction

The first time I encountered the Riemann sphere I was captivated. I copied the picture from the coursebook: two axes to form the complex plane, a third axis and then a sphere with its center at the origin. I tried it out, drawing lines from arbitrary points in the complex plane trough the point of infinity at $(0, 0, 1)$ and imagining their intersections with the sphere. Around this time I also encountered the Riemann sphere in a different form, as the complex projective line $\mathbb{P}^1$. While $\mathbb{P}^1$ is generally not introduced by the lovely picture of the sphere it is no less intriguing. It leaves the door open to all the bigger projective n-spaces $\mathbb{P}^n$ and the curves within them.

A map from a complex curve to the projective line below is called a Belyi map if it branches at no more than three points

$$\{0, 1, \infty\}.$$

Using some of the special properties of $\mathbb{P}^1$ we can construct Belyi maps and prove Belyi's theorem.

Theorem (Belyi)**.** *Let C be a connected, smooth, projective curve defined over the field of algebraic numbers $\bar{\mathbb{Q}}$. Then there exists a morphism*

$$\phi : C \to \mathbb{P}^1$$

with branch locus

$$B(\phi) \subset \{0, 1, \infty\}.$$

2 A Note on the Logarithmic Derivative

Before diving into the matter of curves this chapter will serve as a refresher on one of the more interesting properties of differentiation. The connection between the derivative of a polynomial and its multiple zeros. This is a property we will make frequent use of later in chapters and one that is highlighted by using an algebraic definition.

Definition 2.1. We define differentiation by the map D on the function field $\bar{\mathbb{Q}}(x)$

$$\begin{aligned} D : \bar{\mathbb{Q}}(x) &\to \bar{\mathbb{Q}}(x) \\ x &\to 1 \end{aligned}$$

satisfying the sum and product rule

$$\begin{aligned} D(f+g) &= D(f) + D(g) \\ D(fg) &= D(f)g + fD(g). \end{aligned}$$

The *derivative* f' of a rational function f in $\bar{\mathbb{Q}}(x)$ is given by

$$f' = D(f).$$

From this definition one can deduce the familiar derivative rules. For instance, the power rule follows directly from the product rule

$$D(x^n) = \underbrace{1 \cdot x^{n-1} + 1 \cdot x^{n-1} + \ldots + 1 \cdot x^{n-1} + 1 \cdot x^{n-1}}_{n \text{ times}} = nx^{n-1}.$$

Similarly, the derivative of 1 and so for any constant c

$$\begin{aligned} D(1 \cdot x) &= D(x) \\ D(1)x + 1 \cdot 1 &= 1 \\ D(1) = 0 &\Rightarrow D(c) = 0. \end{aligned}$$

Of course, the connection to multiple zeros also follows from the sum and product rule. Let f be a polynomial defined over the algebraic numbers. Then α is a root of f with multiplicity n if n is the maximal number for which $(x-\alpha)^n$ divides f. In other words if α is a root of f we can write

$$f(x) = (x-\alpha)g(x)$$

for some polynomial g defined over the algebraic numbers. From the product rule we have that

$$f'(x) = g(x) + (x-\alpha)g'(x),$$

then α is a zero of the derivative f' if and only if it is also a zero of g. If $(x-\alpha)$ divides $g(x)$, then $(x-\alpha)^2$ divides $(x-\alpha)g(x) = f(x)$. It follows that α is a multiple zero of f if and only if it is a zero of both f and its derivative f'.

Even better, if β is a zero of f' then it must be a multiple zero of $f(x) - f(\beta)$. In other words the zeros of the derivative f' are precisely the multiple zeros of the polynomials on the form $f + c$.

Further on we will often want to know total number of multiple zeros a certain polynomial has. One tool to look at this is inspired by the logarithm function $\ln(x)$ and its derivative,

$$\ln(x)' = \frac{1}{x}.$$

Say we have two positive differentiable functions f and g and we want to look at $f^n g^m$, if we were to simply differentiate the derivative would have a lot of zeros with high multiplicity. If we use the logarithm function we have

$$\ln(f^n g^m)' = \frac{nf'f^{n-1}}{f^n} + \frac{mg'g^{m-1}}{g^n} = \frac{nf'}{f} + \frac{mg'}{g}$$

where we differentiate and get rid of some excess multiplicity in one step. To be able to use this where functions are negative as well we define the logarithmic derivative as a function on $\bar{\mathbb{Q}}(x)$

Definition 2.2. The *logarithmic derivative* $L(f)$ of a polynomial f in the polynomial ring $\bar{\mathbb{Q}}(x)$ is given by the map

$$\begin{aligned} L : \bar{\mathbb{Q}}(x) &\to \bar{\mathbb{Q}}(x) \\ f &\to \frac{f'}{f}. \end{aligned}$$

The desired property follows from the product rule

$$L(f^n g^m) = \frac{nf'f^{n-1}g + mfg'g^{m-1}}{f^n g^m} = \frac{nf'}{f} + \frac{mg'}{g}.$$

3 Curves and ramification

First let us tackle some basic notation and definitions. We will be using $\mathbb{P}^n$ to mean the projective n-space. We will also be using $\mathbb{Q}[x]$ and $\bar{\mathbb{Q}}[x]$ for polynomial rings in arbitrarily many variables, that is $\mathbb{Q}[x_0, x_1, \ldots, x_n]$ and $\bar{\mathbb{Q}}[x_0, x_1, \ldots, x_n]$ respectively.

An algebraic curve is a projective variety of dimension 1. Our primary focus will be the curves defined over the algebraic and the rational numbers.

Definition 3.1. Let p be an irreducible homogeneous polynomial in the $(n+1)$-variate polynomial ring over the algebraic numbers $\bar{\mathbb{Q}}$. The *complex curve* C given by p is the zero set

$$C = \{\, \alpha \in \mathbb{P}^n \mid p(\alpha) = 0 \,\}.$$

The *homogeneous ideal of* C is

$$I(C) = \{\, p \in \bar{\mathbb{Q}}[x] \mid p \text{ is homogeneous and } p(\alpha) = 0 \text{ for every } \alpha \in C \,\}$$

and the *coordinate ring of* C is $\bar{\mathbb{Q}}[C]/I(C)$. Similarly the *function field of* C is $\bar{\mathbb{Q}}(x)/I(C)$

We say that C is defined over the rational numbers $\mathbb{Q}$ if there is some homogeneous polynomial in $\mathbb{Q}[x]$ that generates the ideal $I(C)$.

As Belyi's theorem is a result on smooth complex curves we may also want to recall what it means for a curve to be smooth.

Definition 3.2. A curve C defined by a polynomial $p(x_0, x_1, \ldots, x_n)$ is *singular* at a point α if each of the partial derivatives of p is zero at α

$$\frac{\partial p}{\partial x_0}(\alpha) = \frac{\partial p}{\partial x_1}(\alpha) = \cdots = \frac{\partial p}{\partial x_n}(\alpha) = 0.$$

If C is nowhere singular we say that C is a *smooth curve.*

We move on from this short review of definitions and notation regarding curves to look at their maps. Specifically to the ramification and branching of maps between curves.

Definition 3.3. Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves, and let α a point in C_1. The *ramification index of* ϕ *at* α, denoted $e_\phi(\alpha)$, is given by

$$\mathrm{ord}_\alpha(q \circ \phi),$$

where q is a generator of the maximal ideal $M_{\phi\alpha}$ in the coordinate ring of C. We say that ϕ is *unramified at* α if the ramification index is 1; and that ϕ is *unramified* if it is unramified at every point α in C_1.

The concept of ramification is similar to the concept of multiple zeros. One might think of the ramification index of α as the number of times that α appears in the preimage of $\phi\alpha$, or as thickness in the fiber. If we envision the fiber as a bundle of strings tying the points above to their common image, then an element with high ramification is tethered with a rope.

Lemma 3.4 ([Sil09, Ch.2, Prop.2.6])**.** *Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves defined over an algebraically closed field of characteristic 0.*

1. *The sum of ramification above a point β is the degree of the map ϕ. That is, for every β in C_2,*
$$\sum_{\alpha \in \phi^{-1}\beta} e_\phi(\alpha) = \deg(\phi)$$
2. *There are finitely many branch points of ϕ. That is, for all but finitely many β in C_2 the cardinality of the preimage $\phi^{-1}\beta$ is the degree of ϕ,*
$$|\phi^{-1}\beta| = \deg(\phi).$$
3. *Ramification indices are multiplicative. Let $\psi : C_2 \to C_3$ be another non-constant map of smooth curves, then for any point α in C_1 the ramification of the composition $\psi \circ \phi : C_1 \to C_3$ at α is*
$$e_{\psi\circ\phi}(\alpha) = e_\phi(\alpha) e_\psi(\phi\alpha)$$

Continuing with the analogy of ramification to strings and ropes, this lemma tells us that every fiber of a map has the same thickness. So for every rope in a fiber fewer additional strings will fit.

We conclude this section with an example to show how one can find the branching of a rational map on $\mathbb{P}^1$.

Example 3.5. Consider the map
$$\phi : \mathbb{P}^1 \to \mathbb{P}^1$$
$$\phi = x^3(x-1)^2.$$

Since ϕ is defined by a separable polynomial a natural place to start looking for ramification points is in the preimage of 0. The generator of M_0 is x, so for either root of $x^3(x-1)^2$ we have the ramification index
$$e_\phi(\alpha) = \operatorname{ord}_\alpha \left(x^3(x-1)^2\right).$$
That gives us 0 with a ramification index 3, and 1 with a ramification index 2. The sum of the ramification indices is $3 + 2 = 5$, the degree of ϕ in accordance with lemma (3.4).

The only pole of $x^3(x-1)^2$ is infinity, so we would expect it to ramify completely. Taking the generator $1/x$ of M_∞ we have

$$e_\phi(\infty) = \mathrm{ord}_\infty\left(\frac{1}{x^3(x-1)^2}\right),$$

which is indeed 5.

To find any remaining ramification points we note that if β is a point in $\mathbb{P}^1$ distinct from infinity then $x-\beta$ is the generator of M_β. So the ramification index of any α in the preimage of β is simply the order of the zero at α of $x^3(x-1)^2-\beta$. Then any remaining ramification points of ϕ must be a root of the derivative of $x^3(x-1)^2$

$$3x^2(x-1)^2 + 2x^3(x-1) = x^2(x-1)(5x-3).$$

So the final ramification point is $\frac{3}{5}$ with ramification index 2. The set of all ramification points, the *ramification locus*, is

$$\{0, 1, \frac{3}{5}, \infty\}.$$

And the set of all branch points, the *branch locus* denoted $B(\phi)$, is

$$\{0, \frac{108}{3125}, \infty\}.$$

4 Belyi's Theorem

Theorem 4.1 (Belyi's Theorem)**.** *Let C be a connected, smooth, projective curve defined over the field of algebraic numbers $\bar{\mathbb{Q}}$. Then there exists a morphism*

$$\phi : C \to \mathbb{P}^1 \tag{1}$$

with branch locus

$$B(\phi) \subset \{0, 1, \infty\}. \tag{2}$$

A map ϕ that satisfies (1) and (2) is called a Belyi map for C. We will follow the proof of [Gol14]. The idea is to take some arbitrary map $\phi_0 : C \to \mathbb{P}^1$, then use a composition of self-maps of $\mathbb{P}^1$ to reduce the branch locus $B(\phi_0)$ to $\{0, 1, \infty\}$. Only relatively simple tools will be used to construct these maps. Yet we will find that they have the required properties to reduce the branch locus and construct a Belyi map.

4.1 Branching in Map Compositions

In order to reduce the branch locus we will make use of the following lemma:

Lemma 4.2. *Let $\phi : C_1 \to C_2$ and $\psi : C_2 \to C_3$ be two non-constant maps of smooth curves. The branch locus of the composition $\psi \circ \phi$ is*

$$B(\psi \circ \phi) = B(\psi) \cup \psi B(\phi)$$

Proof. This follows immediately from the multiplicativity of ramification indices. Since the ramification index of an element α under $\psi \circ \phi$ is $e_\phi(\alpha)e_\psi(\phi\alpha)$ it ramifies under the composition $\psi \circ \phi$ if and only if α ramifies under ϕ, or $\phi\alpha$ ramifies under ψ. □

In the last chapter we saw that it is quite easy to find ramification and branching for maps over $\mathbb{P}^1$. For other curves it is not necessarily as tidy, as the different local rings might have maximal ideals with other generators than the simple $(x-\alpha)$ and $1/x$ that we saw in the example (3.5). This provides some motivation for our method of using compositions of maps over $\mathbb{P}^1$ to reduce the branch locus by one at a time, rather than try for a construction directly from the curve C. Another reason in favor of this method is the relative abundance of self-maps over $\mathbb{P}^1$, a property we will expand upon in a later chapter.

4.2 The Proof

Theorem 4.3. *Suppose S is a finite subset of $\mathbb{P}^1(\bar{\mathbb{Q}})$. Then there exists a map f_S defined over $\mathbb{Q}$ satisfying the following two conditions,*

1. $B(f_S) \subset \{0, 1, \infty\}$
2. $f_S(S) \subset \{0, 1, \infty\}$.

It is not hard to see that Belyi's theorem follows from (4.3). Take $\phi_0 : C \to \mathbb{P}^1$ to be any map defined over $\mathbb{Q}$, that is ϕ_0 is some arbitrary element of the function field $\mathbb{Q}(C)$. Let S be the branch locus $B(\phi_0)$. If the map f_S satisfies the two conditions of theorem (4.3) then the composition of the two maps will have the branch locus

$$B(f_S \circ \phi_0) = B(f_S) \cup f_S(B(\phi_0)) \subset \{0, 1, \infty\}.$$

Then $f_S \circ \phi_0$ is a Belyi map of C.

Note that if the curve C is defined over the rational numbers $\mathbb{Q}$ we can choose some ϕ_0 from $\mathbb{Q}[C]$. Then the composition $\phi_0 \circ f_S$ will also be defined over $\mathbb{Q}$.

Proof. Since S is finite and every element of S is contained in a finite extension of $\mathbb{Q}$ we can without loss of generality assume that S is Galois stable and contains $\{0, 1, \infty\}$. Then, by induction it suffices to construct a map $h_s : \mathbb{P}^1 \to \mathbb{P}^1$ such that the image of S together with the branch locus of h_S fulfills the following three conditions

1. $h_S(S) \cup B(h_S)$ is Galois stable,
2. $h_S(S) \cup B(h_S)$ contains $\{0, 1, \infty\}$, and
3. the cardinality of $h_S(S) \cup B(h_S)$ is strictly less than that of S.

Let S' be the set $S \setminus \{0, 1, \infty\}$ and let d be the cardinality of S'. We construct a polynomial p that maps each element of S' to zero,

$$p(x) = \prod_{\alpha \in S'} (x - \alpha).$$

It is of degree d, and since S' is Galois stable it has rational coefficients. Our function h_s will be on the form

$$h_s(x) = x^m (x - 1)^n p(x)^k$$

for some integers m, n, and k to be determined. To find $h_S(S) \cup B(h_S)$ we consider the logarithmic derivative

$$\frac{h_S'}{h_S}(x) = \frac{m}{x} + \frac{n}{x-1} + \frac{kp'(x)}{p(x)} = \frac{q(x)}{x(x-1)p(x)}$$

with

$$q(x) = m(x-1)p(x) + nxp(x) + kx(x-1)p'(x).$$

The set of distinct roots of q, $\mathcal{Z}(q)$, contains all ramification points of h_S that are not contained in S. So we can write $h_S(S) \cup B(h_S)$ as $h_S(S) \cup h_S(\mathcal{Z}(q))$. It follows that h_S fulfills the first of our conditions.

1. Both S and $\mathcal{Z}(q)$ are Galois stable, S by assumption and $\mathcal{Z}(q)$ since q is a polynomial with rational coefficients. Then their respective images under the rational function h_S will again be Galois stable, as will the union $h_S(S) \cup h_S(\mathcal{Z}(q))$.

Next we want to determine m, n, and k such that the size of $\mathcal{Z}(q)$ is as small as possible. Write

$$p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$$

and

$$q(x) = b_{d+1}x^{d+1} + b_dx^d + \cdots + b_1x + b_0,$$

the degree of q is at most $d+1$, so we have

$$\begin{cases} b_{d+1} = m + n + dk, \\ b_d = (a_{d-1} - 1)m + a_{d-1}n + ((d-1)a_{d-1} - d)k. \end{cases} \tag{3}$$

Setting $b_{d-1} = b_d = 0$ yields two linear equations in three variables, then we have some solution with not all of m, n, and k zero. If we take m, n, k to be such a solution, then h_S fulfills the remaining two conditions.

2. It follows from $m + n + dk = 0$, the first equation of (3), that under h_S at least one of 0, 1, and S' will have the image 0 and at least one will have the image ∞. The image of ∞ will be 1, the leading coefficient of h_S. Then $\{0, 1, \infty\}$ is contained in $h_S(S)$.

3. We note that k is nonzero, as putting $k = 0$ and solving for m and n results in $m = n = k = 0$. From this and $m + n + dk = 0$ we see that there are three possible cases,

   i. both m and n are also nonzero,

   ii. m is zero and n is nonzero,

iii. m is nonzero and n is zero.

i. If m and n are also nonzero the image of S under h_S is precisely $\{0, 1, \infty\}$. Since $b_{d+1} = b_d = 0$ the degree of q is at most $d-1$, then q has at most $d-1$ distinct roots. So the cardinality of $h_S(S) \cup h_S(\mathcal{Z}(q))$ is at most

$$3 + (d - 1) = d + 2,$$

one less than that of S.

ii. Now consider a solution where m is zero. Then $q(x)$ is divisible by x, so the number of distinct roots of q that are not in S is at most $d-2$. The image of $S \setminus \{0\}$ is precisely $\{0, 1, \infty\}$. Then the cardinality of $h_S(S) \cup h_S(\mathcal{Z}(q))$ is at most

$$|h_S(S \setminus \{0\})| + |h_S(\mathcal{Z}(q) \setminus \{0\})| + |\{h_S(0)\}| = 3 + (d-2) + 1 = d + 2,$$

again one less than the cardinality of S.

iii. The remaining case, a solution where n is zero, is handled by an analogous argument as that of ii.

Then h_S fulfills all three conditions which concludes our proof.

□

5 Hurwitz Curves

In this chapter we will explore a very different way of constructing a Belyi map. Rather than composing maps and reducing the branch locus step by step we will look at the map induced by the quotient of a Hurwitz curve C with its automorphism group $\operatorname{Aut} C$,

$$\Pi : C \to C/\operatorname{Aut} C.$$

Both stating the definition of a Hurwitz curve and showing that the map above is indeed a Belyi map requires some further knowledge on curves than what we have used so far. Specifically we will need to know the genera of curves. One way to give an idea of what the genus of a curve is to say that it is the number of holes in the curve. So for instance the Riemann-sphere $\mathbb{P}^1$ has genus 0, and a doughnut-shaped curve would have genus 1.

5.1 The Riemann-Hurwitz Formula

While a more detailed background on the genus of curves lies beyond the scope of this text, just stating the following theorem is enough to convey some of how fundamental the genus is to the ways curves behave.

Theorem 5.1 (Riemann-Hurwitz Formula, [Sil09, Ch.2 Thm 5.9])**.** *Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves defined over an algebraically closed field of characteristic 0. Let g_1 and g_2 be the respective genera. Then*

$$2g_1 - 2 = (\deg \phi)(2g_2 - 2) + \sum_{\alpha \in C_1} (e_\phi(\alpha) - 1).$$

The formula tells us that the total ramification of a map of curves is controlled by the degree of a map and the genera of the curves. There are quite a few interesting properties of maps of curves that follows directly from this. For one, it is immediately apparent that maps of curves of genus 1 have no ramification at all. And that this in fact is true in general if g_1 is equal to g_2 and greater than 0.

We also see that the genus of C_1 has to be greater or equal to that of C_2. If we understand genus as holes or handles on a curve this means that a rational map can preserve or collapse holes when applied to a curve, but it cannot create any new ones.

Example 5.2. To get an idea of how the formula is used we recall an example from p.8, the map

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1$$
$$\phi = x^3(x-1)^2.$$

The genus of $\mathbb{P}^1$ is 0 and the degree of the map ϕ is 5. When first looking at this map we found four ramification points 0, 1, $\frac{3}{5}$, and ∞ with respective ramification indices 3, 2, 2, and 5. Plugging our result into the Riemann-Hurwitz formula yields

$$\begin{aligned} 2 \cdot 0 - 2 &= 5(2 \cdot 0 - 2) + \sum_{\alpha \in C_1} (e_\phi(\alpha) - 1) \\ -2 &= -10 + (3-1) + (2-1) + (2-1) + (5-1) \\ -2 &= -2. \end{aligned}$$

So we can be certain that we did indeed find all ramification points of ϕ.

Before we move on to the application of the formula on to Hurwitz curves we will state two results from the exercises of [Sil09] to better understand how we might use it.

Proposition 5.3 ([Sil09, Exercise 2.5])**.** *Let C be a smooth curve defined over the algebraic numbers $\bar{Q}$. If the genus of C is 0 then C is isomorphic to $\mathbb{P}^1$.*

In conjunction with Riemann-Hurwitz this shows the great wealth of maps on $\mathbb{P}^1$ compared other smooth curves. It is the only one with self-maps of any degree other than 1.

Finally, a method for calculating the genus of curves will be necessary for later examples.

Proposition 5.4 (Genus-degree formula [Sil09, Exercise 2.7])**.** *Let C be some curve in $\mathbb{P}^2$ given by a homogeneous polynomial of degree d, then the* genus *of C is given by*

$$g = \frac{(d-1)(d-2)}{2}.$$

Both of these results are consequences of the Riemann-Roch theorem.

5.2 Belyi maps of Hurwitz curves

The motivation for this chapter lies in a theorem that places an upper bound on the number of automorphisms of a curve.

Theorem 5.5 (Hurwitz's Automorphisms Theorem)**.** *Let C be a smooth projective curve defined over an algebraically closed field of characteristic 0. If the genus of C is greater than 1 then the automorphism group* $\operatorname{Aut} C$ *is a finite group. Specifically*

$$|\operatorname{Aut} C| \leq 84(g-1)$$

where g is the genus of C.

Naturally, this bound engender curiosity towards curves with maximal automorphism groups. Which is why we introduce the following definition.

Definition 5.6. Let C be a smooth projective curve of genus g, with $g \geq 2$. If

$$|\operatorname{Aut} C| = 84(g-1)$$

we say that C is a *Hurwitz curve*.

We will show that for a Hurwitz curve C the quotient map

$$\Pi : C \to C/\operatorname{Aut} C$$

is a Belyi map. So we claim that

1. $C/\operatorname{Aut} C$ is isomorphic to $\mathbb{P}^1$, and
2. the cardinality of the branch locus $B(\Pi)$ is 3.

We will show this by balancing the Rieamnn-Hurwitz formula, eliminating options that have to much or to little ramification until the only one left is that Π a Belyi map.

The map Π is separable, so the degree is the maximal cardinality of the fiber (see (3.4)). Then the degree of Π is $84(g-1)$. So for the map Π the Riemann-Hurwitz formula yields

$$2(g-1) = 2 \cdot 84(g-1) \cdot (g_2 - 1) + S \tag{4}$$

in which g_2 is the genus of the image $C/\operatorname{Aut} C$ and S is the sum

$$\sum_{\alpha \in C} (e_\Pi(\alpha) - 1).$$

The most a single branch point β can contribute to S is if there is only one point above it that ramifies completely, in which case

$$\sum_{\alpha \in \Pi^{-1}\beta} (e_\Pi(\alpha) - 1) = 84(g-1) - 1.$$

The smallest contribution is if each point above β has ramification index 2, in which case

$$\sum_{\alpha \in \Pi^{-1}\beta} (e_\Pi(\alpha) - 1) = \frac{84(g-1)}{2}(2-1) = 42(g-1).$$

From this we have both an upper and a lower bound on S, let b be the number of branch points of Π,

$$b42(g-1) \leq S \leq b(84(g-1) - 1). \tag{5}$$

Even before going into more detail we can show some important things about the map Π, staring with our first claim.

By (4) we have that $g_2 - 1$ at most 0, as S is positive and $2 \cdot 84(g-1)$ is greater than $2(g-1)$. So the genus of $C/\operatorname{Aut} C$ is at most 1. Suppose g_2 is 1, then the right hand side of (4) is

$$2 \cdot 0 + S.$$

The smallest possible nonzero value of S is $42(g-1)$. We have that

$$0 < 2(g-1) < 42(g-1)$$

so the formula can not be balanced if g_2 is 1. Then the genus of $C/\operatorname{Aut} C$ is zero, so it is isomorphic to $\mathbb{P}^1$.

With the genus determined we can write the right hand side of (4)

$$-2 \cdot 84(g-1) + S. \tag{6}$$

It follows from the upper bound from (5) that (6) is at most

$$-2 \cdot 84(g-1) + b(84(g-1) - 1),$$

which is less than $2(g-1)$ for b less than 3. It also follows that (6) is at least

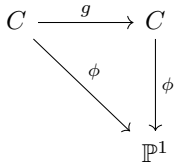
$$-2 \cdot 84(g-1) + b42(g-1)$$

which is greater than $2(g-1)$ for b greater than 4. So the number of branch points is at least 3 and at most 4.

In order to narrow this down further we need to take a closer look at what values S can take on given a certain number of branch points. Given a branch point β in $C/\operatorname{Aut} C$, its contribution to the sum S is

$$\sum_{\alpha \in \Pi^{-1}\beta} (e_\Pi(\alpha) - 1).$$

Action by any element g in the automorphism group commutes with Π



So for a point α in C and a group element g in $C/\operatorname{Aut} C$ we have that $e_\Pi(\alpha)$ must be the same as $e_\Pi(g\alpha)$. Then the ramification index must be the same across the orbit. The orbits of $\operatorname{Aut} C$ are the same as the fibers of the map

$C \to C/\operatorname{Aut} C$. So if e is the ramification index of one point in the fiber of β then every point in the fiber has ramification index e and cardinality of the fiber is

$$|\Pi^{-1}| = \frac{84(g-1)}{e}.$$

Then the contribution of β to S is

$$\sum_{\alpha \in \Pi^{-1}\beta} (e_\Pi(\alpha) - 1) = \frac{84(g-1)}{e}(e-1). \tag{7}$$

A more intuitive approach might be to say that if the fiber is the orbit, then the number of times that an element appears in the fiber will be the same as the cardinality of the stabilizer. So the ramification index $e_\Pi(\alpha)$ is the same as the cardinality of the stabilizer for α. Of course the cardinality of the stabilizer is the same for all elements in the orbit.

With this result in place we can finally eliminate the possibility of 4 branch points. The second smallest contribution a branch point can make to S is if each point above has ramification index 3. In which case its contribution is

$$\frac{84(g-1)}{3}(3-1) = 2 \cdot 28(g-1).$$

Evaluating the right hand side (6) for 4 branch points each contributing the least possible to S, we have

$$-2 \cdot 84(g-1) + 4 \cdot 42(g-1) = 0.$$

Any other valuation with 4 branch points will be at least

$$-2 \cdot 84(g-1) + 3 \cdot 42(g-1) + 2 \cdot 28(g-1) = 14(g-1).$$

As $2(g-1)$ lies between 0 and $14(g-1)$ neither valuation satisfies the formula. Then there are 3 branch points of Π. So Π is a Belyi map, up to some linear fractional transformation.

Example 5.7. Let e_1, e_2, e_3 denote the ramification to each branch point, we obtain the following equation for the sum of ramification

$$\sum_{\alpha \in C_1} (e_\phi(\alpha) - 1) = \frac{84(g-1)}{e_1}(e_1-1) + \frac{84(g-1)}{e_2}(e_2-1) + \frac{84(g-1)}{e_3}(e_3-1).$$

To find a solution that could correspond to a quotient map of a Hurwitz curve we need to solve

$$\begin{aligned} 2(g-1) &= -2 \cdot 84(g-1) + 84(g-1)\left(\frac{e_1-1}{e_1} + \frac{e_2-1}{e_2} + \frac{e_3-1}{e_3}\right) \\ \frac{85}{42} &= \frac{e_1-1}{e_1} + \frac{e_2-1}{e_2} + \frac{e_3-1}{e_3} \end{aligned}$$

with the restriction that each ramification index e_i is greater than 1 and divides $84(g-1)$. What we want to take away from this is that each prime divisor of 42 must divide at least one of the ramification indices. This limits the possible solutions we may think to try out.

Say g is 3. We try the combination with the least possible total ramification, having each prime divisor of 42 occur only once

$$e_1 = 2,\ e_2 = 3,\ e_3 = 7.$$

For these values the Riemann-Hurwitz formula yields

$$\begin{aligned} 2(3-1) &= -2 \cdot 84(3-1) + \frac{84(3-1)}{2} + \frac{2 \cdot 84(3-1)}{3} + \frac{6 \cdot 84(3-1)}{7} \\ 4 &= -4 \cdot 84 + 84 + 4 \cdot 28 + 12 \cdot 12 \\ 4 &= -4 \cdot 84 + 84 + (84+28) + (84+60) \\ 4 &= 4 \end{aligned}$$

so this is a solution. And since any other combination we might try will have more ramification it is the only solution.

One question remains. Does this solution correspond to an actual Hurwitz curve? The answer is yes! There is in fact a Hurwitz curve of genus 3, the Klein quartic defined by the polynomial

$$x^3y + y^3z + z^3x.$$

It has the the automorphism group $PSL(2,7)$, a projective special linear group with 168 elements. Using the genus-degree formula

$$\frac{(4-1)(4-2)}{2} = 3$$

we see that the Klein quartic is indeed of genus 3.

References

[Sil09] Joseph H. Silverman. *Arithmetic of Elliptic Curves (Graduate texts in mathematics ; 106)*. Springer, 2009.

[Gol14] Wushi Goldring. "A new proof of Belyi's Theorem". In: *Journal of Number Theory* 135 (2014), pp. 151–154. DOI: 10.1016/j.jnt.2013.08.017.