The Legacy of Bernhard Riemann
After One Hundred and Fifty Years
ALM 35, pp. 567–594

The Riemann-Hurwitz Formula

Frans Oort*

Abstract

Let $\varphi : S \to T$ be a surjective holomorphic map between compact Riemann surfaces. There is a formula relating the various invariants involved: the genus of S, the genus of T, the degree of φ and the amount of ramification. Riemann used this formula in case T has genus zero. Contemporaries referred to this general formula as "Riemann's theorem". Proofs were given by Zeuthen and Hurwitz. We discuss this formula in its historical context, and in modern generalizations.

2000 Mathematics Subject Classification: 14H30, 14H55, 14H10, 30F99.

Keywords and Phrases: Riemann surfaces, algebraic curves, coverings, ramification, Belyi's theorem.

Contents

*Department of Mathematics, Utrecht University, Princetonplein 5, 3584 CC Utrecht, The Netherlands, Email: f.oort@uu.nl

Introduction

In 1851 and in 1857 Riemann discussed (what we now call) Riemann surfaces and holomorphic maps been them. One of the tools used is a formula which in case

$$\varphi : S \longrightarrow T$$

is a (possibly ramified) cover that relates the invariants degree(φ), genus(S), genus(T) and the ramification indices. As far as I can see Riemann used this in case T has genus zero; see § 7 of [33], *Theorie der Abel'schen Functionen*; here Riemann writes $w - 2n = 2(p-1)$, where n is the degree of a covering $S \to \mathbb{P}^1(\mathbb{C})$, and w the number of simple branch points, and $p = \text{genus}(S)$; see 1.1 below in a more general case. I do not know a proof of this theorem by Riemann. That formula was referred to by his contemporaries as the "Riemann theorem". Proofs and generalizations were given by Zeuthen, Hurwitz, Chasles, Cayley, Brill and others.

We discuss various results in this direction. Where full proofs are easily available we will refer to the existing literature. Also we discuss the case of a ramified cover of algebraic curves in positive characteristic, where a theorem inspired by (RH) was proved by Hasse.

We discuss the Riemann-Hurwitz formula both in the case of Riemann surfaces and of algebraic curves. Algebraic curves over arbitrary ground fields are discussed. We indicate differences between the geometric and the arithmetic approaches in two special cases, see 2.5 end 2.6.

Amongst others we describe a generalization made by Hasse of the Riemann-Hurwitz formula, see 1.10. Curves in characteristic zero that admit a covering to $\mathbb{P}^1$ ramified in at most three points are discussed in the Belyi theorem, 1.8; we show that an analogous result does not hold in positive characteristic, see Section 7.

This paper is meant to indicate the enormous influence the "Riemann theorem" had and still has in mathematics. Basically no new results are contained in this note. This paper recalls basic facts in algebraic geometry, reflecting the influence Riemann's ideas have on our thinking.

Some notation and terminology. The characteristic of the based field is supposed to be zero, with some exceptions, e.g. as in 1.10 and in Section 6. All base field are supposed to be algebraically closed, unless otherwise specified. All Riemann surfaces considered in this note will be compact (non-compact Riemann surfaces are also very interesting, but that would lead us too far) and connected. Algebraic curves will be complete, non-singular and (absolutely) irreducible (see below for more explanation).

We will write k for an algebraically closed field, and K and κ for arbitrary fields. Note that we use the terminology "cover" or "covering" for a holomorphic surjective map between Riemann surfaces, or a (separable, surjective) finite morphism, that can be ramified (whereas in topology a covering usually means that all fibers have the same cardinality). For a covering $\varphi : C \to D$ ramified in P, a point $P \in C$ with $e_P > 1$ is called a *ramification point* and $\varphi(P) \in D$ is called a *branch point*; see 3.2.

A p-group will be a finite group of order a power of a prime number p.

I thank the referee for careful treading and useful suggestions.

1 Results

Riemann surfaces and algebraic curves. We write S and T for Riemann surfaces (for further conditions see Section 2) of genus $g = g_S = \text{genus}(S)$, respectively $g' = g_T = \text{genus}(T)$; we write $\varphi : S \to T$ for a (possibly ramified) covering of degree $n = \deg(\varphi)$. For $\varphi(P) = Q$ we write e_P for the ramification index under φ; note that $e_P > 1$ happens only for a finite number of points on C; hence the number $\delta(\varphi) := \sum_P \, (e_P - 1)$ is finite. We use analogous notation for algebraic curves (for further conditions see Section 2) over a field of *characteristic zero* of genus $g = g_S$ respectively $g' = g_T$ and $n = \deg(\varphi : C \to D)$.

Theorem 1.1 (Riemann-Hurwitz formula, characteristic zero, 1857, 1891)**.**

$$2g - 2 = n{\cdot}(2g' - 2) + \delta(\varphi); \quad \textit{here} \quad \delta(\varphi) = \sum_P \, (e_p - 1). \qquad \text{(RH)}$$

To be discussed in Section 4. For proofs see 4.1, 4.2, 4.3.

Exercise 1.2. Assume (RH) in the case of coverings of $\mathbb{P}^1$, respectively of $\mathbb{P}^1(\mathbb{C})$, and derive the general formula.

Correspondences. Let $S \leftarrow \Gamma \to T$ be a finite-to-finite correspondence with $n = \deg(\Gamma \to S)$ and $n' = \deg(\Gamma \to T)$. Write $\beta = \delta(\Gamma \to S)$ and $\beta' = \delta(\Gamma \to T)$. Analogously for a correspondence $C \leftarrow \Gamma \to D$.

Theorem 1.3 (Zeuthen formula, 1871)**.**

$$\beta + n{\cdot}(2g - 2) = \beta' + n'{\cdot}(2g' - 2). \qquad \text{(Z)}$$

Exercise 1.4. Assume (RH) and give a proof for (Z).
Also: Assume (Z) and give a proof for (RH).

Theorem 1.5 (De Franchis, 1913)**.** *For a Riemann surface of genus $g > 1$, and for an algebraic curve of genus $g > 1$ over an arbitrary field, the number of automorphisms is* finite*.*
See [7]; see [15], Exercise 5.1 in IV.5.

Theorem 1.6 (The Hurwitz bound, 1893)**.** *Let C be an algebraic curve over a field of characteristic* zero *of genus $g > 1$. Then*

$$\#(\text{Aut}(C)) \leq 84(g - 1). \qquad \text{(HB)}$$

See Exercise 4.6.

The valence of a correspondence, see Section 5. We study a curve C over $\mathbb{C}$. Let $\Lambda \subset C \times C$ be a correspondence. Assume that no irreducible component of Λ is contained in any of the vertical or horizontal fibers, and assume that, up to linear equivalence on the surface $C \times C$, there exists $\gamma \in \mathbb{Z}$, called the valence of Λ, such that

$$\Lambda \quad \sim \quad a_1 C_1 + b_2 C_2 - \gamma{\cdot}\Delta,$$

where C_1 is a vertical and C_2 is a horizontal fiber; see [12], pp. 282-287; see [11], 16.1.5. This number γ, if it exists, is called the valence of the correspondence Λ. See Section 5. In this case the degrees n_1 and n_2 of the two projections of Λ on the first, respectively second factor of $C \times C$ are equal to

$$n_1 = a_1 - \gamma, \qquad n_2 = a_1 - \gamma.$$

We say $P \in C(k)$ is a united point, or a coincidence, for Λ if $(P,P) \in \Lambda$.

Theorem 1.7 (Chasles-Cayley-Brill, or the Cayley-Brill formula, 1864, 1866, 1873, 1874)**.** *The number of united points, counted with multiplicities, on an algebraic curve of genus $g =$ genus(C) under Λ equals*

$$n_1 + n_2 + 2\gamma g. \qquad \text{(CB)}$$

`http://en.wikipedia.org/wiki/Chasles-Cayley-Brill_formula`
`http://www.encyclopediaofmath.org/index.php`
`/Chasles-Cayley-Brill_formula`

Theorem 1.8 (Belyi's theorem)**.** *Let C be an algebraic curve over a field K* of characteristic zero. *There exists a surjective morphism $\varphi : C \otimes k \to \mathbb{P}^1_k$ branched in at most three points if and only C can be defined over $\overline{\mathbb{Q}}$.*
See [3], Th. 14 on page 129; see [4], pp. 2188-194; see [12], page 287; see [11], 16.1.5(e). For a proof see [41], pp. 70-73. We use the terminology:
Definition. Supose that C is given over K; we say C "can be defined over κ" if there exists C' over $\kappa \subset K$ such that $C \otimes_K k \cong C' \otimes_\kappa k$. Here k is an algebraically closed field containing K.

Note that an analogue of Belyi's theorem in positive characteristic does not hold, see Section 7.

1.9. Positive characteristic. We consider curves C and D over an algebraically closed field field $k \supset \mathbb{F}_p$ of positive characteristic (see Section 6 for details), and $\varphi : C \to D$ a separable, finite (and hence surjective) morphism. For $P \in C(k)$ we define the ramification index e_p and the different δ_P at P under (this separable, finite morphism) $\varphi : C \to D$; note that $e_P = 1$ implies $\delta_P = 0$ (more generally, if e_P is not divisible by p, then $\delta_P = e_P - 1$); note that if e_P is divisible by p, then $\delta_P \geq e_P$. For a finite separable morphism we have $e_P = 1$ for all but a finite number of points in C; hence $\delta(\varphi) := \sum_P \ \delta_P < \infty$. See Sections 2, 3 and 6 for more details.

Note that $\varphi : C \to D$ is separable if the field inclusion $k(C) \supset k(D)$ is separable, see [15], IV.2; note that a separable morphism can be ramified.

Theorem 1.10 (Riemann-Hurwitz-Hasse formula, 1935).

$$2g-2 = n\cdot(2g'-2)+\delta(\varphi); \qquad \delta(\varphi)=\sum_{P\in C}\delta_P. \qquad \text{(RHH)}$$

See Section 6. For a proof see 4.3.
Remark. This formula also holds in characteristic zero, and in that case it reduces to (RH), with $\delta_P = e_P - 1$ for every $P \in C$.

2 Riemann surfaces and algebraic curves

2.1. Riemann surfaces. A Riemann surface (in this note) will be a compact, connected topological space, locally isomorphic with $D = \{z \in \mathbb{C} \mid \ \mid z \mid < 1\}$, the "unit disk", and where on overlapping charts the transition functions are holomorphic. There are many textbooks on this topic, e.g. see [48].

As a topological space a Riemann surface S is a compact orientable real 2-dimensional manifold $S^{(\text{top})}$. Such topological spaces have been classified: an orientable, real surface X can be obtained by attaching g "handles" to a sphere, where $g \in \mathbb{Z}_{\geq 0}$; in this case we write genus$(X) = g$; any two such surfaces X and Y with genus$(X) = g =$ genus(Y) are isomorphic as real manifolds; see [10], Chapter 17. *This classification defines the number g, the genus of a Riemann surface*:

$$\text{genus}(S) = \text{genus}(S^{(\text{top})}).$$

See 2.4. Warning, and Riemann was very well aware of this: for Riemann surfaces S and T an isomorphism $S^{(\text{top})} \cong T^{(\text{top})}$ of real manifolds, equivalently genus$(S) =$ genus(T), does not imply that S and T are isomorphic as complex manifolds. Riemann studied this phenomenon, and he introduced the word "moduli" in 1857 for the number of essential parameters on which Riemann surfaces of the same genus depend, see [33], page 120. It took us more than a century and many publications before we could precisely pin down this idea in full generality, in the terminology of moduli spaces for algebraic curves. In this note we will not discuss the theory of moduli of algebraic curves.

For $P \in S$ we write $\mathcal{H}_{S,P}$ for the ring of germs of meromorphic functions on S holomorphic at P. This is a local ring, and its maximal ideal $\mathfrak{m}_{S,P}$ is generated by one element, say $z = z_P \in \mathfrak{m}_{S,P}$; this element is unique up to multiplication by a unit in $\mathcal{H}_{S,P}$; such an element is called a *uniformizer* on S at P. After choosing z we have an isomorphism between $\mathcal{H}_{S,P}$ and the subring of all elements of $\mathbb{C}[[z]]$ that are germs of *convergent* holomorphic functions in a neighborhood of P on S.

Let $\varphi : S \to T$ be a surjective, holomorphic map of Riemann surfaces, with $\varphi(P) = Q$. Let $t = z_Q$ be a uniformizer on T at Q and $s = z_P$ a uniformizer on S at P. In this case the pull back of the function t to S satisfies

$$\varphi^*(t) = u\cdot s^e,$$

where $e_P = e \in \mathbb{Z}_{>0}$ and $u \in \mathcal{H}^*_{S,P}$ is a unit. This was studied intensely by Riemann and his contemporaries. It amounts to the fact that locally at P the map φ can given by $x \mapsto x^e$. This number e is called the *ramification index* of φ at p. If $e_p > 1$ we say the map φ is *ramified* at $P \in S$ or we say that the map φ is *branched* at $Q \in T$. The main topic of this note is a formula describing a connection between the integers genus(S), and genus(T) and $\sum_{P \in S}(e_P - 1)$.

At the end of the 19th century the word "monodromy" had two different meanings. On page 90 of [33] we find one meaning: if no ramification appears a function can be extended in a unique way, the function is "einänderig oder monodrom". In that time the "monodromy theorem" meant that prolongation of an analytic function on a simply connected area the function is single-valued. The terminology "monodromy group" or "monodromy substitution" was also used in Riemann's time, see [20], § 3. At present time the the term "monodromy theorem" is used in two ways. One is the 19-th century notion. The other is the fact that eigenvalues of a monodromy substitution are roots of unity; also or more general results in the Grothendieck theory, are referred to by the term "monodromy theorem".

2.2. Algebraic curves. Choose an arbitrary base field κ. An algebraic curve C is an algebraic variety of dimension one defined over κ; we refer to [15], especially Chapters I and IV for the theory. For theory over an algebraically closed field see [38]. In this note we assume C to be absolutely irreducible, i.e. $C \otimes \overline{\kappa}$ is irreducible, non-singular and complete. Let us explain this last condition.

Complete algebraic varieties. For any algebraic variety we have the notion of being complete, as e.g. introduced by Chevalley, [2], Chapter IV. For an algebraic variety (defined over an arbitrary field) we consider the Zariski topology, see [15], I.1; for an algebraic curve C an open set is either the empty set, or C with a finite number of points removed. The notion of a complete variety V is explained in [15], II.4; essentially it means that a morphism $T \supset T\backslash\{x\} \to V$ can be extended to the whole of T, where V is a complete variety, and T is an affine curve, non-singular at $x \in T$. Here are some facts:

- Any closed subvariety of a complete variety is complete.
- Projective space $\mathbb{P}^n_\kappa$ for any $n \in \mathbb{Z}_{\geq 0}$ is an example of a complete variety.
- In particular any projective variety is complete.
- There exist non-singular, complete varieties that cannot be embedded into a projective space, see [15], Appendix B, 3.4.1.
- However, any complete algebraic curve can be embedded into a projective space. In fact any non-singular curve can be embedded into $\mathbb{P}^3_\kappa$ and there exist (many) algebraic curves (irreducible, nonsingular and complete) that cannot be embedded into $\mathbb{P}^2_\kappa$.
- In particular, *for algebraic curves the concepts "complete" and "projective" are equivalent.*

Suppose V is an algebraic variety over $\mathbb{C}$. The set of complex points on V, written as $V(\mathbb{C})$, is naturally endowed with the "complex topology", much finer than the Zariski topology if $\dim(V) > 0$. See [15] I.1 and Appendix B; see [43], Chapters VII. VIII and IX; see [12]. We write $V^{(an)}$ for the complex variety $V(\mathbb{C})$ with the "classical" topology. It can be proved that:

V is complete as an algebraic variety if and only if
$V^{(an)}$ is compact as a complex variety;

see [43], VII.2, Exercise 2.

2.3. Equivalences of categories. Over an arbitrary algebraically closed field k consider the following categories:

(ac) The category of (complete, non-singular, irreducible) algebraic curves over k; as morphisms consider finite (hence surjective) morphisms.

(ff) The category of function fields in one variable over k; as morphisms consider homomorphisms $K \to L$, inducing the identity on k.

These two categories are (anti-)equivalent. This (anti-)equivalence is induced by associating to C its function field $k(C)$. A surjective morphism $C \to D$ induces a k-homomorphism $k(C) \leftarrow k(D)$. Conversely for a function field the set of discrete valuation, trivial on k can be given the structure of an algebraic curve. It is essential to consider complete, non-singular, irreducible curves.

Over $k = \mathbb{C}$ as base field consider the following categories:

(RS) The category of (compact, connected) Riemann surfaces; as morphisms consider finite (hence surjective) holomorphic maps.

(ac) The category of (complete, non-singular, irreducible) algebraic curves over $\mathbb{C}$; as morphisms consider finite (hence surjective) morphisms.

(ff) The category of function field in one variable over $\mathbb{C}$. Morphisms are field homomorphisms inducing the identity on the subfield $\mathbb{C}$.

These three categories are equivalent. One of the ingredients: for an algebraic curve C over $\mathbb{C}$ the set $C^{(an)} := C(\mathbb{C})$ with the "classical topology" is a Riemann surface, and an algebraic morphism induces a holomorphic map. Conversely, every *compact* Riemann surface S is algebraizable, i.e. there exists an algebraic curve C with $C^{(an)} \cong S$, and this curve is unique up to a canonical isomorphism; moreover a holomorphic map between compact Riemann surfaces is a morphism on the algebraizations.

Note that an equivalent statement for non-compact Riemann surfaces is incorrect.

These results, and generalizations to higher dimensions (Lefschetz, Chow) is completely understood, see [39]. For this theory for Riemann surfaces and algebraic curves, see [10], Chapter 20. See [32], Lecture 1.

This means that over $\mathbb{C}$ as base field many results for Riemann surface can be phrased in their equivalent form for the related algebraic curves and conversely.

2.4. Definitions of the genus. We give various possible definitions; that these are equivalent can be proved, but we do not give all relevant references.
(1) Suppose S is a (compact, connected) Riemann surface, or, equivalently, let C be an algebraic curve over $\mathbb{C}$, with $C(\mathbb{C}) = S$ the related Riemann surface. A topological definition of its genus is given in 2.1.

(2) Suppose S as above. Consider a set of circuits on S, such that this surface cut open along these is still connected. The maximum number of such cuts is called the genus. For such considerations see [33], pp. 92-96. It is a nice exercise to show this definition is equivalent to the one given above.

(3) Suppose S as above. Consider a triangulation, say with t_0 vertices, t_1 edges and t_2 triangles. Define g by consideration of the Euler characteristic:

$$2 - 2g = t_0 - t_1 + t_2.$$

On can show the number on the right hand side is independent of the triangulation chosen.

In all topological considerations above we see that the topological surface S of genus $g > 0$ can be constructed by considering a $2g$-gon in $\mathbb{R}^2$, with sides

$$a_1, b_1, a_1^{-1}, b_1^{-1}, \cdots, a_g, b_g, a_g^{-1}, b_g^{-1},$$

and identifying sides with orientation as indicated; see [10], page 239.

(4) Let S be as above, and consider the first homology group $\mathrm{H}_1(S, \mathbb{Z})$. One shows that this is a free $\mathbb{Z}$-module and its rank equals $2g$ in case genus$(S) = g$. This can be used as a definition for genus(S).

(5) Let S and C be as in (1), or let C be a non-singular, complete irreducible algebraic curve over an algebraically closed field k of arbitrary characteristic. Let D be a divisor on S or on C, i.e. a finite sum of points with multiplicities. Define $L(D)$ to be the set of meromorphic (respectively rational) functions such that $(f) - D$ is an effective divisor; here (f) is the divisor of f, the zeros with positives multiplicities, and the poles with negative multiplicities.

Remark. On a curve C and the related compact Riemann surface $C(\mathbb{C})$, the definition of the space $L(D)$ given in two ways amounts to the same.

It is a fact that $L(D)$ is a finite dimensional vector space over k (or, over $k = \mathbb{C}$). The famous theorem by Riemann (starting an important aspect of algebraic geometry) states, *the Riemann inequality*:

$$\dim_k(L(D)) \leq \deg(D) - g + 1 \quad \text{and equality holds for} \quad \deg(D) \geq 2g - 1.$$

We note that Riemann's proof was based on Dirichlet's principle, unproven at that moment; therefore the proof was criticized, see [19], page 119 for a discussion. The exact meaning of the number $\dim_k(L(D)) - (\deg(D) - g + 1)$ was explained by Roch in his PhD-thesis (1862) with Riemann as one of his advisors, see [34]. The smallest integer g satisfying this inequality for every D can be used as definition for genus(S).

(6) Let C be a non-singular, complete irreducible algebraic curve over an algebraically closed field k of arbitrary characteristic. Let ω be a differential on C. We define the divisor (ω) in the following way. At a point P with local uniformizer $t = t_P$ we can write, locally, $\omega = f_P{\cdot}dt_P$; we write $v_P(\omega) := v_P(f_P)$ and $(\omega) := \sum_P\ v_P(\omega){\cdot}P$ (and this divisor is called a canonical divisor). With these notation:

$$\deg((\omega)) = 2g - 2.$$

This can be used as definition of genus(C).

(7) Let C be an algebraic curve over an arbitrary field K (however with $C \otimes k$ being non-singular, complete and irreducible). The sheaf of local rings on C is written as $\mathcal{O}_C$. In sheaf cohomology open can study $\mathrm{H}^1(C, \mathcal{O}_C)$. This is a finite dimensional vector space over K, and

$$\dim_K \left(\mathrm{H}^1(C, \mathcal{O}_C)\right) \quad = \quad g.$$

This can be used as definition of genus(C).

(8) On a Riemann surface, or on a non-singular curve over a field K we consider the sheaf $\Omega = \Omega^1_C$ of regular differentials. These played an influential role in the study of Riemann surfaces from the beginning (e.g. in considerations about Abel integrals). The space of sections $\Gamma(C, \Omega)$ is finite dimensional and we can define

$$\mathrm{genus}(C) = g := \dim_K\left(\Gamma(C, \Omega)\right),$$

sometimes baptized as the geometric genus. The fact that this definition amounts to the same as the one given in (7) is part of the theory of Serre duality, see [40], II.9 and II.10; see [15], III.7 and IV.1.

(9) A non-singular plane curve $C \subset \mathbb{P}^2$ of degree n has genus$(C) = (n-1)(n-2)/2$. An analogous formula holds for singular plane curves, where we can define how much the singularities contribute to the genus. Hence this method can be used to define or compute the genus of any curve, as soon as we have a birational plane model.

For a plane irreducible curve of degree n with d ordinary double points and no other singularities the genus of the normalization equals genus$(C^{\sim}) = (n - 1)(n-2)/2 - d$. One can show that any (complete, nonsingular) algebraic curve over an algebraically closed field can be embedded into $\mathbb{P}^3$, and can be birationally projected onto a plane curve with only ordinary double points as singular points.

All definitions of the genus given above agree. For an algebraic curve C over $\mathbb{C}$ and the related Riemann surface the genus of C and the genus of $C(\mathbb{C})$ are equal (in any of the definitions above).

We did not discuss the Euler characteristic of a non-compact Riemann surface, and we did not discuss the "genus" of a singular curve.

Note that there are many cases of algebraic curves over a field $K \subset \mathbb{C}$, not isomorphic over K as base field, but isomorphic once considered over $\mathbb{C}$. Moreover for an algebraic curve C over K, *usually an analytic parametrization of $C \otimes \mathbb{C}$ gives little arithmetic information about C.* We have seen in history that

Riemann surfaces in particular, and analytic manifolds in general give a lot of information about the geometry of the related algebraic varieties.

However

for arithmetic questions and for number theory only the analytic theory is often not enough;

we give just two (of the many) examples.

2.5. An example: Congruent Numbers. Suppose the base field is $\mathbb{Q}$. For every $N \in \mathbb{Z}_{>0}$ consider the elliptic curve E_N defined over $\mathbb{Q}$ as the zeros (for example over some algebraically closed field containing $\mathbb{Q}$) of:

$$E_N := \mathcal{Z}(-Y^2 + X(X^2 - N^2)),$$

where we consider $E_N \subset \mathbb{P}^2_{\mathbb{Q}}$ defined by the homogeneous equation

$$Y^2 Z = X(X^2 - N^2 Z).$$

The arithmetic of this elliptic curve (for arbitrary N) is hard to understand. These curves play a crucial role in the theory of "congruent numbers": *an integer $N \in \mathbb{Z}_{>0}$ is called a congruent number if there exist*

$$a, b, c \in \mathbb{Q}_{>0}, \quad a^2 + b^2 = c^2, \quad N = ab/2;$$

i.e. if N is the area of a Pythagorean triangle with sides of rational length. This problem, dating from a 10-th century Arabic manuscript (and possibly earlier), is hard: is it *now known whether there exists an effective algorithm that decides for every N whether it is a congruent number*; we can (easily) make a complete (infinite) list of all congruent numbers, but relatively small integers may show up "very late"; we have no bound on N telling you how long you have to wait before you know the decision (if you want an exercise: try to decide whether $N = 13$ is a congruent number, the same for $N = 23$, both easy cases, and the same for $N = 157$, a more difficult problem to do just by hand).

Take a, b, c, N in the formula above. Then

$$x := \frac{c^2}{4}, \quad y := \frac{c \cdot (b^2 - a^2)^2}{4} \quad \text{gives} \quad y^2 = x^3 - N^2 x;$$

we see that the presentation (a, b, c) showing that N is a congruent number determines a rational point x, y on the elliptic curve E_N. One can show that the converse is true for $(x, y) \in E_N(\mathbb{Q})$ with $x > 0$ and $y \neq 0$, and that:

$$\#(E_N(\mathbb{Q})) = \infty \quad \Longleftrightarrow \quad N \quad \text{is a congruent number.}$$

For details, see [27]. As J. Tunnell showed, depending on conjectures and non-trivial results one can "solve" the congruent number problem, see [27], IV.4. This methods gives conjecturally a finite procedure depending on N deciding whether N is a congruent number or not. Using this method one easily shows that $N = 157$ indeed should be a congruent number. P. Monsky proved in 1990 by abstract arguments, and D. Zagier proved by a direct verification that $N = 157$ indeed is a congruent number, see [27], page 5, Figure I.3. This confirms the conjecture by Tunell in this special case.

If N and M are square-free and different then $E_N \not\cong_{\mathbb{Q}} E_M$, and the congruent number problem may have very different answers for N and for M. However

$$(E_N \otimes \mathbb{C}) \cong (E_1 \otimes \mathbb{C}) \cong (E_M \otimes \mathbb{C})\,;$$

Indeed, the substitution $X = N{\cdot}\xi$ and $Y = \sqrt{N^3}{\cdot}\eta$ transforms

$$(E_N \otimes \mathbb{C}) \quad \text{into} \quad (E_1 \otimes \mathbb{C}) = \mathcal{Z}(-\eta^2 + \xi(\xi^2 - 1)).$$

We know every elliptic curve over $\mathbb{C}$ can be parametrized by the Weierstrass $\wp$-function and its derivative; e.g. see [49], Chapter XX. We see that although this parametrization is "the same" for all $E_N \otimes \mathbb{C}$, it does not give enough arithmetic information about the arithmetic of the curves E_N over $\mathbb{Q}$.

2.6. An example: FLT. Consider for any $n \in \mathbb{Z}_{\geq 2}$ the algebraic curve

$$F_n := \mathcal{Z}(X^n + Y^n - Z^n) \subset \mathbb{P}^2_{\mathbb{Q}}.$$

For $n = 2$ the curve F_2 is a rational curve (a curve of genus zero). In fact, for any $t \in \mathbb{Z}$ we obtain

$$t \mapsto [t^2 - 1 : 2t : t^2 + 1] = (\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}) \in \mathcal{Z}(X^2 + Y^2 - 1)(\mathbb{Q}) \subset \mathbb{A}^2(\mathbb{Q});$$

in this way we see that the set of solutions to the equation $X^2 + Y^2 = Z^2$

$$\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + y^2 = z^2\} \quad \text{is an infinite set.}$$

The geometric fact that $\text{genus}(F_2) = 0$ helps us to find a rational parametrization, and hence to find infinitely many solutions (and in fact all solutions) to this diophantine equation.

The famous *Fermat's Last Theorem* reads: for any $n \in \mathbb{Z}_{\geq 3}$

$$(x,y,z) \in (\mathbb{Z}_{\geq 0})^3, \quad x^n + y^n = z^n \quad \Longrightarrow \quad xyz = 0,$$

i.e. there exist no non-trivial solutions to the Fermat equation for any $n \geq 3$. Why can't we find a rational parametrization in this case? The Fermat curve F_n is a non-singular plane curve of degree n and we therefore know that $\text{genus}(F_n) = (n-1)(n-2)/2$; hence $n \in \mathbb{Z}_{\geq 3}$ implies $\text{genus}(F_n) > 0$ and hence *there does not exist a rational parametrization* of F_n. We are tempted to use an analytic parametrization: since Weierstrass and Poincaré we know this exists for every $F_n(\mathbb{C})$; however, suppose we a non-constant holomorphic (or meromorphic) map

$$\psi : \mathbb{C} \quad \longrightarrow \quad F_n(\mathbb{C})$$

is given.

$$\text{How we can we decide what } \psi(\mathbb{C}) \cap \{(x,y,z) \in \mathbb{Z}^3 \mid x^n + y^n = z^n\} \text{ is?}$$

We have seen in history that determining rational values of transcendental functions is difficult. In the case of FLT no proof has been given along these lines.

In 1983 Faltings proved a conjecture by Mordell, 1922: *any curve of genus at least two defined over a number field has only a finite number of rational points* (geometry does give a partial answer); see [8]. In particular this shows that for

$$n \in \mathbb{Z}_{>3}, \text{ hence genus}(F_n) = (n-1)(n-2)/2 \geq 2,$$

we have $\#(F_n(\mathbb{Q})) < \infty$. This is a geometric explanation why the case $n = 2$ and $n > 3$ are drastically different for FLT. However the geometry does not prove the full strength of FLT. For example the curves defined by $X^5 + Y^5 = Z^5$ and $X^5 + Y^5 = 33{\cdot}Z^5$ have different sets of non-trivial solutions over $\mathbb{Q}$, though these two curves are isomorphic over $\mathbb{C}$.

FLT was proved by Andrew Wiles in 1995. G. Frey suggested in 1985 to consider for any possible non-trivial solution $x^n + y^n = z^n$ in non-zero integers, the elliptic curve $E_{x,y,z}$ defined by $U^2 = V(V - x^n)(V + y^n)$; this curve has weird arithmetic properties (contradicting conjectures and experimental feelings about such curves): such a curve should not exist for solutions to F_p for $p \geq 5$ (and FLT would follow). In fact a rational parametrization of this curve $E_{x,y,z}$ by a modular curve (the Shimura-Taniyama-Weil conjecture, proved by Wiles in this case) leads to a proof that an elliptic curve with such arithmetic properties does not exist; hence the hypothetical solution (x,y,z) tot he Fermat problem does not exist. We see, finally, we did not us any parametrization of F_n, but via $E_{x,y,z}$ and a parametrization by a modular curve, a key tot this big secret was found. Along these lines after three and a half century FLT was proved to be correct. For references, for the history and for many details see [5].

Conclusion. We have seen that compact Riemann surfaces and complete non-singular algebraic curves over $\mathbb{C}$ "are the same".

Geometric information about $C(\mathbb{C})$ gives some arithmetic information about a curve C defined over a field $K \subset \mathbb{C}$.

Curves C and D defined over a field $K \subset \mathbb{C}$, though isomorphic as curves considered over $\mathbb{C}$, or giving isomorphic Riemann surfaces $C(\mathbb{C})$ and $D(\mathbb{C})$, may have very different arithmetic properties as curves over K.

2.7. Resolution of singularities. For a variety V over a field K (say V is complete, but possibly singular), one tries to find a morphism $V' \to V$, that is an isomorphism on a dense Zariski open sets

$$V' \supset U' \xrightarrow{\sim} U \subset V$$

and such that V' is regular (= non-singuar) and complete. If this is the case we say resolution of singularities holds for V. Over $K = \mathbb{C}$ this was a long time an outstanding open problem, finally solved by Hironaka [18]; also see [17] for references and discussions. Over fields of positive characteristic this problem in its general form is still unsolved.

One can weaken the problem by requiring $U' \to U$ to be finite and surjective; in this case the morphism $V' \to V$ is called an *alteration.* A. J. de Jong proved in [22] that for any (complete) V over any field there exists an alteration $V' \to V$ with V' complete and nonsingular. This theorem has many applications (in cases where resolution of singularities is still not known).

We say an algebraic variety is *normal* if all local rings are integrally closed. There exist normal surface that are singular. Every normal algebraic curve over a perfect field is non-singular (more generally: the singular set of a normal variety has codimension at least two). Hence the problem of resolution of singularities (over an arbitrary perfect base field) for algebraic curves is solved by the normalization process.

Extending morphisms. Let V be a normal variety, and let $\psi : V \cdots \to \mathbb{P}^n$ be a rational map to a projective space. Then there exists a closed set $T \subset V$ such that every irreducible component of T has codimension at least two in V, and there exists a morphism

$$\psi' : V \setminus T \longrightarrow \mathbb{P}^n$$

realizing ψ, see [43], II.3.1, Theorem 3 and II.5.1, Theorem 3. In particular:

for a non-singular algebraic curve $V = C$ any $\psi' : U \to \mathbb{P}^n$
can be extended tot a morphism $C \to \mathbb{P}^n$.

See [43], II.3, Corollary 1 of Th. 3; see [15], Proposition I.6.8. *We will use this below by just giving a morphism on a dense open subset of a non-singular curve.* For an algebraic curve the concepts "normal" and "non-singular" are these same. Hence, in particular, for non-singular algebraic curves C and D over a field K the following are equivalent:

- The curves C and D are isomorphic.
- There is an isomorphism $C \supset U \xrightarrow{\sim} U' \subset D$ for non-empty open sets $U \subset C$ and $U' \subset D$.
- There is a K-isomorphism $K(C) \quad \cong_K \quad K(D)$.

See [15], I.6.12.

In several of the statements above, conditions imposed earlier, are necessary. Singular curves having isomorphic function fields need not be isomorphic; non-singular algebraic surfaces having isomorphic function fields need not be isomorphic.

Let C be an algebraic curve over a field κ. Let $P \in C(\kappa)$. Suppose the local ring $\mathcal{O}_{C,P}$ is a normal local ring (i.e. C is non-singular at P). In this case the maximal ideal $\mathfrak{m}_{C,P}$ is generated by one element, i.e. there exists

$$s = s_P \in \mathfrak{m}_{C,P} \quad \text{such that} \quad \mathfrak{m}_{C,P} = \mathcal{O}_{C,P} \cdot s,$$

just as we saw in the case of Riemann surfaces. Such an element $s = s_P$ will be called a *uniformizer* on C at P; compare with 2.1.

In this case we obtain an isomorphism

$$\kappa[[s]] \quad \xrightarrow{\sim} \quad (\mathcal{O}_{C,P})^{/P};$$

this last ring is the *completion* of the local ring $\mathcal{O}_{C,P}$, i.e.

$$(\mathcal{O}_{C,P})^{/P} = \text{proj.lim.}_i \ \ \mathcal{O}_{C,P}/\mathfrak{m}^i_{C,P}.$$

Note the analogy with the theory of Riemann surfaces, where $\mathcal{H}_{S,P} \subset \mathbb{C}[[z]]$ is the ring of convergent power series.

For a complex analytic analogue for the extension property but now in the case of mappings of Riemann surfaces, see [10], Proposition 19.9.

2.8. The Lefschetz principle. Note that studying algebraic curves over an algebraically closed field k of characteristic zero "amounts to the same" as studying algebraic curves over $\mathbb{C}$. More generally, loosely speaking, true (geometric) statements in algebraic geometry over $\mathbb{C}$ are also true for algebraic varieties over an algebraically closed field $k \supset \mathbb{Q}$. See [36], see [13], Exp. XII, XIII. The essential argument is given by the fact that an algebraic variety over k is defined over a field $k' \subset k$ of finite type over $\mathbb{Q}$. After choosing an embedding $k' \subset \mathbb{C}$ we can start making comparisons. One of the examples: topology computes the (arithmetic) fundamental group of an algebraic curve over $k = \overline{k}$, see [13], Exp. XIII, Cor. 2.12.

3 Ramification

3.1. We consider a surjective holomorphic map $\varphi : S \to T$ of Riemann surfaces, or a surjective morphism $\varphi : C \to D$ of algebraic curves over some field k. For $P \in S$, or for $P \in C(k)$ we write $\varphi(P) = Q$. We write $s = t_P$ for a uniformizer at P and $t = t_Q$ for as uniformizer at Q. There exists $e = e_P \in \mathbb{Z}_{>0}$ such that

$$\varphi^*(t) = u{\cdot}s^e;$$

here u is a unit at P, i.e. $u \in \mathcal{H}^*_{S,P}$ in the case of Riemann surfaces, respectively $u \in \mathcal{O}^*_{C,P}$ in the case of algebraic curves.

In the case of Riemann surfaces a ramification of index e implies that φ locally at $P \mapsto Q$ can be given by $s^e \leftarrow\!\shortmid t$, a ramified map on a unit circle. In the case of algebraic curves over κ the homomorphism $\mathcal{O}_{C,P} \leftarrow \mathcal{O}_{D,Q}$ induces $\kappa[[s]] \leftarrow \kappa[[t]]$, which can be given by a change of parameters, if necessary, by $s^e \leftarrow\!\shortmid t$.

3.2. Definition. We say that φ is *ramified at* P if $e_P > 1$; if so, we say that P is in the *ramification locus* of φ and we say Q is in the *branch locus* of φ.

4 The Riemann formula, the Hurwitz theorem

In consideration below we use freely the various definitions of the genus (and one can argue at various places what the definition is, and what the proved results are for the various concepts introduced).

4.1. A topological proof of (RH). By the equivalence 2.3 we see proving (RH) for compact Riemann surfaces amounts to the same as proving (RH) for complete, non-singular irreducible algebraic curves over $k = \mathbb{C}$ under the equivalence $S = C(\mathbb{C})$; here we use that in this case genus(S) = genus(C). Note indeed that the definition of e_P for $\varphi(P) = Q$ give the same in both cases.

Hurwitz in his paper [20] on page 338 states the result (RH) for a (ramified) covering $F \to \Phi$; on pp. 375/376 of that paper Hurwitz gives a proof by writing these Riemann surfaces in question as a union of simply connected areas, where the branch points and the ramification points are on the boundaries, and by explicitly connecting the Euler characteristics of F, of Φ and the number W, properly defined, in our notation $W = \sum_P \, (e_P - 1)$.

Here is the argument. Let $\varphi : S \to T$ be a surjective, finite morphism of degree n of Riemann surfaces. Chose a triangulation of T such that every branch point of φ is a vertex in this triangulation. Write

$m_0, \;\; m_1, \;\; m_2$ for the number of vertices, edges, respectively triangles

in this triangulation of T. Pull back by φ this triangulation to S, and write $m'_0, \;\; m'_1, \;\; m'_2$ for the number of vertices, edges, respectively triangles on S. We know:

$$2 - 2g_T = m_0 - m_1 + m_2, \quad \text{and} \quad 2 - 2g_S = m'_0 - m'_1 + m'_2.$$

We note that $m'_1 = n{\cdot}m_1$ and $m'_2 = n{\cdot}m_2$. Above a branch point Q the number of points on S equals

$$\#(\varphi^{-1}(Q)) = n - \sum_{\varphi(P)=Q} \, (e_P - 1); \quad \text{hence} \quad m'_0 = n{\cdot}m_0 - \sum_{P \in S} \, (e_P - 1).$$

From these equalities (RH) follows.

Remark. In papers by Riemann devoted to this topic we find the formula (RH) as a tool, but I do not see a proof. Moreover Riemann considers covers of a rational curve, and I do not know whether Riemann was aware of the formula (RH) in case of a cover $S \to T$ of an arbitrary Riemann surface T. In the paper [20] we find a proof for (RH) in the general situation of Riemann surfaces. In a paper by Zeuthen [51] we find (Z), which implies (RH). Hence I think a good terminology is either “the Riemann-Hurwitz formula”, or “the Riemann formula and the Hurwitz theorem”, but also the “Riemann-Zeuthen-Hurwitz formula”, or the “Zeuthen-Hurwitz theorem” can be used.

Remark. In a footnote on page 150 of [51] the author refers to his paper in the Comptes Rendus de l'Académie des Sciences, Vol. 52 (1861), page 742. However on that page in that volume there is no paper by Zeuthen (note that Zeuthen passed his Masters degree in 1862). Also Zeuthen refers to a proof of "Riemann's theorem" by E. Bertini. For a description of Zeuthen's work on enumerative geometry, see Kleiman, [24].

4.2. An analytic proof of (RH). In [12], pp. 216-219 we find a proof of (RH) for Riemann surfaces, using the Gauss-Bonnet formula and topological considerations. As we indicated in the previous subsection this also proves (RH) for complete, non-singular irreducible algebraic curves over $k = \mathbb{C}$.

4.3. An algebraic proof of (RH) **and of** (RHH). We remind the rear that (RHH) stands for the Riemann-Hurwitz-Hasse formula, v laid for algebraic curves in arbitrary characteristic. We consider algebraic curves and a separable surjective morphism $\varphi : C \to D$ defined over an algebraically closed field k. Ramification, the ramification index e_P and the different δ_P at a point $P \in C(k)$ are defined as in Section 3 and in 6.1. Details can be found in [15], IV.2. For a curve X one defines a canonical divisor K_X. In our situation one can prove:

$$K_C \quad \sim \quad \varphi^*(K_D) + R,$$

where

$$R = \sum_{P \in C(k)} \quad \delta_P {\cdot} P,$$

see [15], Proposition IV.2.3. Also see [16], page 42. Also see [12], page 219 in case $k = \mathbb{C}$. Note that $\deg(K_X) = 2{\cdot}\mathrm{genus}(X) - 2$. From this (RH) and (RHH) follow; here we use Section 6 in the case of RHH.

Exercise 4.4. Let k be a field *of characteristic zero,* and let $C \to \mathbb{P}^1 = D$ be a (possibly ramified) covering defined over k. Then either this covering is an isomorphism or the number of branch points in D is at least two.

See 7.3 for a counterexample in positive characteristic.

In exercises below the characteristic of the base field is arbitrary, unless otherwise specified. For some exercises results in Sections 3, 4, 6 might be useful.

Exercise 4.5. Suppose $\mathrm{genus}(C) < \mathrm{genus}(D)$. Show there does not exist a surjective morphism $\varphi : C \to D$.

Exercise 4.6. Use 1.1 and give a proof of the Hurwitz bound (HB) = 1.6. See [15], Exercise 2.5 in IV.2.

Exercise 4.7. Show the Hurwitz bound is not sharp for every g (hint: show that a curve of genus $g = 2$ does not admit an automorphism of order 7).

Find a curve of genus 7 over $\mathbb{C}$ with $\#(\mathrm{Aut}(C)) = 504$; see [28].

Show the Hurwitz bound is sharp for infinitely many values of g; see [29].

4.8. Remark (The Klein quartic). Let $K \subset \mathbb{C}$ be a field containing $\mathbb{Q}(\zeta_4, \zeta_7)$; notation: $\zeta_n = e^{2\pi\sqrt{-1}/n} \in \mathbb{C}$. Let $C \subset \mathbb{P}^2_K$ be defined as the set of zeros of $X^3Y+Y^3Z+Z^3X$; this is a curve of genus 3. In this case $\#(\mathrm{Aut}(C)) = 84{\cdot}2 = 164$. In fact, in this case $\mathrm{Aut}(C) \cong PSL(2, \mathbb{F}_7)$.

Exercise 4.9. Let p be a prime number and let C be a curve over a field of characteristic p with $1 < \mathrm{genus}(C) = g < p-1$. Show that $\#(\mathrm{Aut}(C)) \leq 84{\cdot}(g-1)$.

Exercise 4.10 (Roquette)**.** See [35]. Let $p \geq 5$ be a prime number and let C be given by $Y^2 = X^p - X$ (i.e. C is the complete, non-singular curve given as the completion of this affine model) over $\overline{\mathbb{F}_p}$. Compute genus(C). Compute $\#(\mathrm{Aut}(C))$, and note that this curve does not satisfy the Hurwitz bound.

4.11. Remark. For curves in positive characteristic an upper bound of $\#(\mathrm{Aut}(C))$ in terms of genus(C) exists, and has been given by B. Singh, 1974 and by H. Stichtenoth, 1973; see [46], [37]. For examples and theory see [31].

5 The valence of a correspondence

Consider algebraic curves over $\mathbb{C}$.

5.1. The valence $\gamma = \gamma(\Lambda)$ of a correspondence Λ, if it exists, is defined by

$$\Lambda \quad \sim \quad a_1C_1 + b_2C_2 - \gamma{\cdot}\Delta;$$

see [11], 16.1.5. A correspondence allowing a valence is said to be a non-singular correspondence, see [45], p. 331 (confusing with the terminology that $\Lambda \subset C \times C$ can be singular or non-singular). It can be proved that for a curve of genus $g > 0$ every correspondence that has a valence this is unique, e.g. see [12], page 284; see [3], Th. 10 on page 125. For a generic curve of genus $g > 0$ every correspondence does have a valence see [12], page 286.

The notion of a singular correspondence has studied by Abel, Hurwitz and many others, see [45], pp. 331–348.

For a correspondence $\Lambda \subset C \times C$ the valence is γ if for every $P \in C$ the linear equivalence class $T(P) + \gamma{\cdot}P$ on C is independent of $P \in C$.

It seems Felix Klein was the first to observe that there exist algebraic curves and a correspondence on $C \times C$ that does not possess a valence, see [25], [26], [1]. For more references about correspondences see V. Snyder – *Correpondences on non-rational curves*, Chapter VII in [45], pp. 166–196.

In S. Lefschetz – *Singular correspondences between algebraic curves*, Chapter XVI in [45], pp. 331–348 we find another description of singular and non-singular correspondences. Lefschetz defines a correspondence on $C \times C$ to be "singular" if it poses restrictions on the Riemann Matrices of the curves, i.e. if the correspondence cannot be extended to all deformations of the curves involved. In [12], Lemma on page 285 we see that the definition given earlier, and this definition coincide for $C \times C$.

The Chasles-Cayley-Brill, or the Cayley-Brill formula was formulated by Chasles for a rational curve (1864), Cayley considered the formula for curves of arbitrary genus (1866), and Brill proved this theorem (1873, 1874), see [3], page 129; see [42], pp. 176, 183/184.

5.2. Exercises. **(1)** Suppose $\Lambda \subset E \times E$ is the graph of an automorphism φ of an elliptic curve E over $\mathbb{C}$ such that $\varphi \neq \pm 1$. Show that the valence of Λ does not exist; see [12], p. 286.
(2) Suppose $g \geq 1$, and let C be given as the complete, nonsingular curve over $\mathbb{C}$ given by $Y^2 = X^{2g+1} - 1$. We define φ by

$$\varphi^*(X) = \zeta{\cdot}X, \quad \varphi^*(Y) = Y, \quad \zeta = e^{2\pi\sqrt{-1}/(2g+1)}.$$

Show that the graph of φ does not admit a valence.

6 Algebraic curves in positive characteristic

6.1. Ramification and the different. We take notation $\varphi : C \to D$ and e_P for $\varphi(P) = Q$ as in Section 3. We write

$$\varphi^*(t) = u{\cdot}s^e = \beta_e{\cdot}s^e + \sum_{i>e} \beta_i{\cdot}s^i, \quad u(P) = \beta_e; \quad \varphi^*(t) \in \mathcal{O}_{C,P}^{/P} \cong k[[s]];$$

here u is a unit at P, hence $\beta_e \neq 0$, and the sum is a formal, a priori infinite sum (convergent in the case of Riemann surfaces).

As we assumed that φ is separable, there is at least one index i not a multiple of p with $\beta_i \neq 0$. We define the *different* δ_P of φ at P as the value

$$\delta_P := v_P \left(\frac{\partial}{\partial s}(\varphi^*(t)) \right).$$

Clearly $\delta_P = i - 1$ where i is the smallest index i not divisible by p with $\beta_i \neq 0$.

In case e_P is *not divisible by p* (or in case we are in characteristic zero, or in case we consider Riemann surfaces) we have $\delta_P = e_P - 1$.

However if $\mathrm{char}(k) = p > 0$ divides e_P we have $\delta_P > e_P - 1$; in this case, $p = \mathrm{char}(k)$ divides the ramification index e_P, we say the covering is *wildly ramified* at P. We will study several examples.

Theorem 6.2 (The Riemann-Hurwitz-Hasse formula, see Theorem 1.10)**.** *For a separable, finite morphism $\varphi : C \to D$ of complete, nonsingular, irreducible algebraic curves we have:*

$$2g - 2 = n{\cdot}(2g' - 2) + \delta(\varphi); \qquad \delta(\varphi) = \sum_{P \in C} \delta_P \quad \text{(RHH)}.$$

See [16], in particular see page 42 for the different in the case of $e_P = p$; for a proof [15], IV.2.

6.3. (a) Assume $p = 2$ and $g \in \mathbb{Z}_{>0}$. For $g = 1$ we define $E = C$ by

$$E = \mathcal{Z}(Y^2Z + X^2Y + XZ^2) \subset \mathbb{P}^2.$$

This is a supersingular elliptic curve, actually over an algebraically closed field of characteristic two the unique one up to isomorphism.

More generally: Assume $p > 0$ is a prime number and C given by

$$C = \mathcal{Z}(X^pY + Y^pZ + Z^pX)$$

over a field of characteristic p. This curve is non-singular of genus $p(p-1)/2$. Consider the map $[x : y : 1] \mapsto x$; this is the projection with center $[0 : 1 : 0]$ on the X-axis. This extends to a morphism $\varphi : C \to D = \mathbb{P}^1$, a covering of degree p with

$$\varphi(P) = Q = (x = 0 : z = 1), \quad P = [0 : 0 : 1], \quad \text{with} \quad e_P = p,$$

and

$$\varphi(P') = Q' = (x = 1 : z = 0), \quad P' = [0 : 1 : 0] \quad \text{with} \quad e_{P'} = p - 1.$$

At P the function y is a local parameter on C and x is a local parameter on $\mathbb{P}^1$, and

$$x \sim_P y^p + y^{p^2+1} + \text{h.o.t.}; \quad \text{hence} \quad \delta_P = p^2;$$

here $\sim_P$ stand for: up to unit in P and h.o.t. means "higher order terms". Clearly $\delta_{P'} = e_{P'} - 1 = p - 2$. This checks with the Rieman-Hurwitz-Hasse formula:

$$2g_C - 2 = p(p-1) - 2 = p\cdot(g_D - 2) + \delta(\varphi) = p\cdot(-2) + \delta_P + \delta_{P'} = -2p + p^2 + p - 2.$$

(b) Hyperelliptic curves in characteristic 2. For $g \in \mathbb{Z}_{>1}$ we define C by a covering by two open sets:

$$U_0 = \mathcal{Z}(Y^2 + h_0(X)Y + r_0(X)) \subset \mathbb{A}^2, \quad U_\infty = \mathcal{Z}(\eta^2 + h_\infty(\xi)\eta + r_\infty(\xi)) \subset \mathbb{A}^2,$$

with identification on $U_0 \cap U_\infty$, given by $x \neq 0$ and $\xi \neq 0$, by the transformation

$$Y = \frac{\eta}{\xi^{g+1}}, \quad X = \frac{1}{\xi}.$$

The polynomials involved are submitted to:

$$\deg(h_0(X)) = g + 1, \quad 0 < \deg(r_0(X)) \leq 2g + 2,$$

and

$$h_\infty(\xi) = \xi^{g+1}h_0(\frac{1}{\xi}), \quad r_\infty(\xi) = \xi^{2g+2}r_0(\frac{1}{\xi});$$

we assume that for every $\beta \in k$ with $h_0(\beta) = 0$ we have $r_0(\beta) = 0$ and $(X - \beta)^2$ does not divide $r_0(X)$. Let us write

$$r_0(X) = \prod (X - \beta_i)^{d_i} \quad \text{for mutually different} \quad \beta_i,$$

and $P_i = (x = \beta_i, y = 0)$. We write $\varphi : C \to \mathbb{P}^1$ for the projection on the X-axis. We see:

$$\mathrm{genus}(C) = g; \quad \sum \beta_i = g + 1, \ \ \delta_{P_i} = 2\beta_i; \quad \text{indeed } \ 2g - 2 = 2\cdot(-2) + \sum \delta_{P_i}.$$

6.4. Remark. Suppose $\varphi : C \to D$ and $\psi : B \to D$ are given, with degree(φ) = degree(ψ) and where all ramification indices of φ are the same as those for ψ. These data do not imply that C and B have the same genus (if $\delta(\varphi) \neq \delta(\psi)$).

Here is an easy example. Let C be given as zeros of $Y^2 + X^2Y + X^3 + X$ (and then complete and normalize) over a field of characteristic 2. It is clear that C is an elliptic curve. We define $\varphi : (x, y) \mapsto x$. This is a double cover $C \to \mathbb{P}^1$, branching is only at $x = 0$, with $P = (0, 0)$, and $e_P = 2$ and $\delta_P = 4$. Indeed $2g - 2 = 2\cdot(-2) + 4$ yields $g = 1$.

Choose any $h \in \mathbb{Z}_{>1}$ and define D by $Y^2 + X^{h+1}Y + X^{2h+1} + X$, and $\psi(x, y) = x$. At the point $R = (0, 0) \in D$ we have $e_P = 2$ and $\delta_P = 2h + 2$, and genus$(D) = h$. In this example many numerical values are the same (excepts the differents), but genus$(C) = 1 <$ genus$(D) = h$.

Many more examples can be given, in any positive characteristic.

7 An equivalent of Belyi's theorem ?

7.1. We have seen that an algebraic curve C given over $\mathbb{C}$ that admits a covering $C \to \mathbb{P}^1$ branched in at most three points actually can be defined over $\overline{\mathbb{Q}}$ (Belyi's theorem), see Theorem 1.8. Can this be generalized to fields of arbitrary characteristic? We see that Belyi knew this was not the case: see [9], footnote (3) on page 3. In this section an algebraically closed field k of characteristic $p > 0$ will be fixed. Note that k need not be an algebraic closure of a finite field.

7.2. Proposition. *Every curve C of genus at least one over a field $k \supset \mathbb{F}_p$ admits a covering $C \to \mathbb{P}^1_k$ branched in precisely one point in $\mathbb{P}^1_k$.*
See [23], pp. 91/92 and [50], Corollary 3 on page 715.
For a proof we first explain two examples.

7.3. Example (Artin-Schreier). *For every two different points $P \neq P'$ on $\mathbb{P}^1$ there exists a degree p covering*

$$\varphi : \mathbb{P}^1 \to \mathbb{P}^1, \quad \varphi(P) = \varphi(P')$$

branched in exactly one point different from $\varphi(P)$.
After a coordinate change, if necessary, we assume

$$P = [a : 1], \ \ P' = [b : 1] \in C = \mathbb{P}^1(k), \quad \text{with} \quad a \neq b.$$

Consider

$$\varphi : C = \mathbb{P}^1 \to \mathbb{P}^1 = D, \quad \varphi([s : 1]) := [s^p - \beta s : 1], \ \ \beta \neq 0.$$

This morphism, extended to the whole $\mathbb{P}^1$, is unramified for every $[s:1]$; further $\varphi(\infty) = \infty$, where $\infty = [1:0]$ is a ramification point (the unique one) and $\varphi(\infty) = \infty$ is the branch point of φ. Moreover if

$$\beta = \frac{a^p - b^p}{a - b} \quad \text{then} \quad \varphi(P) = \varphi(P').$$

This is the desired example.

We note the ZHH formula is satisfied: in projective coordinates $[S:U]$ on $C = \mathbb{P}^1$ and $[T:Q]$ on $D = \mathbb{P}^1$ the transformation φ is given by

$$\frac{S^p}{U^p} - \beta\frac{SU^{p-1}}{U^p} = \frac{T}{W};$$

substituting $S = 1$, and $T = 1$ we obtain the morphism on a chart near ∞:

$$W = \frac{U^p}{1 - \beta U^{p-1}}; \quad \text{then} \quad W \sim U^p(1 + \beta U^{p-1}) + \cdots = U^p + \beta U^{2p-1} + \cdots .$$

We see $\delta(\varphi) = \delta_\infty = 2p - 2$. This fits into ZHH:

$$-2 = -2{\cdot}p + \delta(\varphi).$$

7.4. Example. see [23], pp. 91/92. *For $P = [0:1] \in C = \mathbb{P}^1(k)$ there exists a morphism*

$$\varphi : C = \mathbb{P}^1 \to \mathbb{P}^1 = D, \quad \varphi(P) = \infty = \varphi(\infty),$$

of degree $\deg(\varphi) = p + 1$,
non-ramified on $\mathbb{P}^1 - \{\infty\}$, in particular $e_P = 1$ and
ramified of degree p at $\infty \mapsto \infty$.

We give the morphism by

$$s \mapsto s^p + \frac{1}{s},$$

and extend to $C = \mathbb{P}^1 \to D$. Clearly this map is unramified on $\mathbb{P}^1 - \{\infty\}$, and $\varphi(P) = \infty$.

Indeed we can compute:

$$\frac{S^{p+1}}{SU^p} + \frac{U^{p+1}}{SU^p} = \frac{T}{W}, \quad W \sim U^p - U^{2p+1}, \quad e_\infty = p,$$

which gives $\delta(\varphi) = \delta_\infty = 2p + 1 - 1 = 2p$. In this case RHH reads:

$$-2 = -2{\cdot}(p+1) + \delta(\varphi).$$

Using these examples we show that an equivalent of Belyi's theorem does not hold in positive characteristic.

7.5. Proof of Proposition (7.2). Suppose C over k given; assume genus$(C) > 0$. We choose any separable, finite morphism

$$\varphi_1 : C \to D_1 = \mathbb{P}^1;$$

let $P_1, \cdots, P_r \in D_1(k)$ be the branch points of φ_1. We perform a linear transformation, if necessary, to achieve $P_r = \infty$. Using 7.3 inductively we construct

$$C \to D_1 \to \cdots \to D_j$$

such that $C \to D_j$ branches at ∞ and at at most $1 \leq r - j$ points; after at most $r-2$ steps we arrive at $C \to D' = \mathbb{P}^1$ branching at ∞ and possibly at one other point. We finish by 7.4, constructing

$$C \longrightarrow D' = \mathbb{P}^1 \longrightarrow D'' = \mathbb{P}^1$$

where $C \to D''$ is branched only at ∞. This finishes the proof of 7.2.

7.6. In [50] we find Corollary 3 on page 715: *For any curve X of genus ≥ 2 over a field $k \supset \mathbb{F}_p$ there exists a finite set $S \subset X(k)$ and a finite etale cover $X \setminus S \to \mathbb{P}^1_k \setminus \{\infty\}$.* This also proves 7.2.

Exercise 7.7. For every $k \supset \mathbb{F}_p$ and every $n \in \mathbb{Z}_{\geq p}$ there exists a covering $C \to D$ of degree n with at least one point of wild ramification.

8 Galois covers and wild ramification

8.1. Suppose $\varphi : C \to D$ is a (separable) cover of algebraic curves (non-singular, irreducible and complete) over an algebraically closed field k. We define the Galois closure $B \to C \to D$ of this cover. One way is the following; we have a finite separable extension of fields $k(C) \supset k(D)$. Let $L \supset k(D)$ be the Galois closure of $k(C)/k(D)$ in the sense of field theory; we define $B \to D$ as the normalization of D in the field L.

We explain the procedure of constructing the Galois closure of a covering in geometric terms. Suppose $\varphi : X \to Y$ is a cover, with X irreducible. The fiber product $X \times_Y X$ contains the diagonal

$$\Delta = \Delta_X \subset X \times_Y X,$$

and, say the projection on the first factor,

$$X \times_Y X \setminus \Delta_X =: Z \to X$$

induces a cover of X. This is of degree one less than the degree of $X \to Y$. Note that $Z \to X$ is not branched at $P \in X$ if $\varphi(P) \in Y$ is not a branch point of φ. Repeating this process (taking an irreducible component of Z, etc.) we arrive at a Galois cover. Note that we can determine precisely in every step geometrically the ramification indices.

For the rest of this section we work over an algebraically closed field k of characteristic $p > 0$. We have seen that for any curve in characteristic $p > 0$ there exists a covering $C \to \mathbb{P}^1$ branched in at most one point. Hence the Galois closure $B \to C \to \mathbb{P}^1$ is a separable Galois cover, i.e. $\Gamma \subset \mathrm{Aut}(B)$ and

$$B \to B/\Gamma \cong \mathbb{P}^1,$$

that is branched in at most one point. Hence the previous section implies there are "many" Galois covers of curves (in positive characteristic) branched in one point.

8.2. For an algebraic curve C we define the *p-rank*, written as $f(C)$. One way of doing this is to consider its Jacobian variety $J = \mathrm{Jac}(C)$, an abelian variety of dimension equal to $g = \mathrm{genus}(C)$, and $f = f(C) = f(\mathrm{Jac}(C))$ is given by

$$\mathrm{Ker}\left(J \xrightarrow{\times p} J\right)(K) \cong (\mathbb{Z}/p)^f.$$

We know $0 \leq f \leq g$, and al possibilities show up for an appropriate choice of C.

Another way is using the Hasse-Witt matrix for C; we will not go into details here.

Suppose $\varphi : C \to D$ is a separable finite cover. What is the relation between $f(C)$ and $f(D)$?

Theorem 8.3. *Let $B \to B/\Gamma = D$ be a Galois cover of algebraic curves in characteristic p. Suppose Γ is a p-group* (i.e., the order of Γ is a power of p). *Then*

$$f(C) - 1 = (\#(\Gamma))(f(D) - 1) + \sum_{P \in C(k)} (e_P - 1).$$

Note the curious fact that the RHH formula involves the different at the ramification points, however this formula on the p-ranks only uses the ramification indices.

8.4. The case of p-covers. The theorem was proved for the case of etale Galois covers of degree p by Shafarevich, see [44].

See [47], Theorem 4.1 for the case of (possibly ramified) Galois covers of degree p. Note that in case $\#(\Gamma) = p$ and S is the set of ramification points in $C(k)$ (and note that φ maps the set of ramification points in this case bijectively onto the set branch points) then

$$(f(C) - 1 + \#(S)) = p\cdot(f(D) - 1 + \#(S)).$$

Observation. *A cyclic p-cover branched in exactly one point satisfies $f(C) = p{\cdot}f(D)$.*

The general case. For the general case of Galois covers by a p-group see [47], Theorem 4.2; see [30]; see [6], Corollary 1.8. Also see [14] for the general formalism.

8.5. Observation. *If $\varphi : D \to D/\Gamma = C$ is a Galois cover branched in precisely one point and $\#(\Gamma)$ is a power of p and $f(D) = 0$ then $f(C) = 0$*: indeed in this case $\#(S) = 1$, hence

$$\sum_{P \in C(k)} (e_P - 1) = e_P - 1 < \#(\Gamma);$$

hence

$$f(C)-1=(\#(\Gamma))(f(D)-1)+\sum_{P\in C(k)}(e_P-1)=-\#(\Gamma)+e_P-1<0.$$

8.6. In particular, let us take the situation of Proposition 7.2 with $f(C)>0$, in particular $C\to D=\mathbb{P}^1$ having only one branch point. Let $B\to D$ be its Galois closure. Because $f(C)>0$ we conclude $f(B)>0$, and we see that the Galois group of $B\to D$ is not a p-group in this case.

8.7. Example. Let char$(k)=2$, and let C be given as the plane curve

$$C=\mathcal{Z}(Y^4+X^3Y+X^2Y^2+XY^2+XZ^3)\subset\mathbb{P}^2.$$

This is a non-singular quartic curve, hence genus$(C)=3$. We project from the center $[0:1:0]$ onto the X-axis; this gives a degree 4 cover $\varphi : C\to\mathbb{P}^1=D$. This morphism is totally ramified at $P=[0:0:1]$.We see that this is the only ramification point. Indeed, $x\sim_P y^4+y^{13}+$h.o.t, and $\delta(\varphi)=\delta_P=12$. The RHH formula reads

$$2g-2=4=4P\cdot(-2)+\delta(\varphi)=-8+12.$$

We see that the lines given by $Y=X+Z$ and by $X=0$ are bitangents; hence $f(C)>0$. (Alternative argument: compute the Hasse-Witt matrix of C.) If φ would be a Galois cover, we would have

$$0<(f(C)-1+\#(S))=p\cdot(f(D)-1+\#(S))=0,\quad\text{because}\quad\#(S)=1,$$

a contradiction. We conclude that φ is not a Galois cover; the Galois closure $C^{\sim}\to\mathbb{P}^1$ of $\varphi : C\to\mathbb{P}^1$ has a Galois group that is not a p-group, because $f(C^{\sim})>0$.

References

[1] A. Adler – *Modular correspondence on* $X_0(11)$. Proceedings of the Edinburgh Mathematical Society **35** (1992), 427–435. `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.7216&rep=rep1&type=pdf`

[2] C. Chevalley – *Fondements de la géométrie algébrique.* Notes, Sécr. Math., Paris, 1985.

[3] J. Coolidge – *A treatise on algebraic plane curves.* Clarendon Press, Oxford, 1931; reprinted by Dover Publ., 1959.

[4] J. Coolidge – *A history of geometrical methods.* Clarendon Press, Oxford, 1940; reprinted by Oxford University Press, 1947.

[5] *Modular forms and Fermat's last theorem.* Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995. Edited by Gary Cornell, Joseph H. Silverman and Glenn Stevens. Springer-Verlag, New York, 1997.

[6] R. Crew – *Etale p-covers in characteristic p.* Compositio Math. **52** (1984), 31–45.

[7] M. De Franchis – *Un teorema sulle involuzioni irrazionali.* Rend. Circ. Mat. Palermo **36** (1913), 368.

[8] G. Faltings – *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), 349–366.

[9] I. Fesenko – *Arithmetic deformation theory via arithmetic fundamental groups and nonarchimedean theta functions, notes on the work of Shinichi Mochizuki.* `https://www.maths.nottingham.ac.uk/personal/ibf/notesoniut.pdf` `https://www.maths.nottingham.ac.uk/personal/ibf/mp.html`

[10] W. Fulton – *Algebraic topology.* A first course. Graduate Texts in Mathematics, 153. Springer-Verlag, New York, 1995.

[11] W. Fulton – *Intersection theory.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics 2, Berlin, New York: Springer-Verlag, 1984. Second edition 1998.

[12] Ph. Griffiths and J. Harris – *Principles of algebraic geometry.* Pure and Applied Mathematics. Wiley-Interscience, John Wiley & Sons, New York, 1978.

[13] A. Grothendieck – *Séminaire de géométrie algébrique* 1960/1961: SGA 1. *Revêtements étales et groupe fondamental.* Lect. Notes Math. 224, Springer-Verlag, 1971.

[14] A. Grothendieck – *Formule d'Euler-Poincaré en cohomologie étale* (rédigé par I. Bucur). SGA 5: Sém. Géom. Algébrique 1965 – 1966: Cohomologie ℓ-adique et function L. Lect. Notes Math. 589, Springer-Verlag, 1977, pp. 372–406.

[15] R. Hartshorne – *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[16] H. Hasse – *Theorie de relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstanenkörper.* Journ. reine angew. Math. (Crelle) **172** (1935), 37–54.

[17] H. Hauser, J. Lipman, F. Oort and A. Quirós – *Resolution of singularities.* Obergurgl (1997); Progr. Math., 181, Birkhäuser, Basel, 2000.

[18] H. Hironaka – *Resolution of singularities of an algebraic variety over a field of characteristic zero* I, II. Ann. of Math. **79** (1964), 109–203; **79** (1964) 205–326.

[19] *The Abel Prize, 2003-2007. The first five years.* Editors: Helge Holden and Ragni Piene. Springer-Verlag, Berlin, 2010.

[20] A. Hurwitz – *Über Riemann'sche Fläche mit gegebenen Verzweigungspunkten.* Math. Ann. **39** (1891), 1–61.

[21] A. Hurwitz – *Über algebraische Gebilde mit eindeutigen Transformationen in sich.* Math. Ann. **41** (1893), 403–442.

[22] A. J. de Jong – *Families of curves and alterations.* Ann. Inst. Fourier (Grenoble) **47** (1997), no. 2, 599–621.

[23] N. Katz – *L-Functions and Monodromy: Four Lectures on Weil II.* Advances in Mathematics **160** (2001), 81–132.

[24] S. Kleiman – *Hieronymus Georg Zeuthen* (1839-1920). In: Enumerative Algebraic Geometry: Proceedings of the 1989 Zeuthen Symposium, Editors S. Kleiman and A. Thorup. Amer. Math. Soc., Contemporary Mathematics **123**, 1991.

[25] F. Klein – *Zur Theorie der elliptischen Modulfunctionen.* Math. Ann. **17** (1880), 62–70. `https://www.digizeitschriften.de/en/dms/img/?PPN=PPN235181684_0017&DMDID=dmdlog12`

[26] F. Klein – *Über gewisse Theilwerthe der* Θ*-Function.* Math. Ann. **17** (1880), 565–574. `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.7216&rep=rep1&type=pdf`

[27] N. Koblitz – *Introduction to elliptic curves and modular forms.* Graduate Texts in Mathematics 97. Springer-Verlag, New York, 1984.

[28] A. Macbeath – *On a curve of genus* 7. Proc. London Math. Soc. **15** (1965), 527–542.

[29] A. Macbeath – *On a theorem of Hurwitz.* Proc. Glasgow Math. Assoc. **5** (1961) 90–96.

[30] M. Madan – *On a theorem of M. Deuring and I. R. Safarevic.* Manuscriptia Math. **23** (1977), 91–102.

[31] M. Matignon and M. Rocher – *Smooth curves having a large automorphism* p*-group in characteristic* $p > 0$. Algebra Number Theory **2** (2008), 887–926.

[32] D. Mumford – *Curves and their Jacobians.* Univ. Michigan Press, 1976.

[33] B. Riemann, Gesammelte Mathematisch Werke. Dover Publications, 1985; pp. 3–43: B. Riemann – *Grundlagen für eine allgemeine Theorie der Funktionen einer veränderlichen complexen Grösse.* Inauguraldissertion, Göttingen 1851; pp. 88–142: B. Riemann – *Theorie der Abel'schen Functionen.* Journ. reine angew. Math. (Crelle) **54** (1857), 115–155.
English translation: Bernhard Riemann, Collected Papers. Paperback, Kendrick Press, 2004.

[34] G. Roch – *Über die Anzahl der willkurlichen Constanten in algebraischen Functionen.* Journ. reine angew. Math. (Crelle) **64** (1865), 372–376.

[35] P. Roquette – *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik.* Math. Zeitschr. **117** (1970), 157–163.

[36] A. Seidenberg – *Comments on Lefschetz's Principle.* The American Mathematical Monthly, **65** (1958), pp. 685–690.

[37] B. Singh – *On the group os automorphisms of a function field of genus at least two.* Journ. Pure Appl. Algebra **4** (1974), 205–229.

[38] J-P. Serre – *Faisceaux algébriques cohérents.* Ann. of Math. **61** (1955), 197–278.

[39] J-P. Serre – *Géométrie algébrique et géométrie analytique.* Ann. Inst. Fourier, Grenoble **6** (1955–1956), 1–42.

[40] J-P. Serre – *Groupes algébriques et corps de classes.* Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959.

[41] J-P. Serre – *Lectures on the Mordell-Weil theorem.* Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. Asp. of Math. E15, Vieweg, 1989.

[42] F. Severi - *Vorlesungen über algebraische Geometrie.* Translation by E. Löffler, Leipzig, 1921. Reprinted: Johnson Reprint Corporation, 1968.

[43] I. Shafarevich – *Basic algebraic geometry,* Vol. 1. Varieties in projective space. Translated by Miles Reid. Springer-Verlag, 1994.
Basic algebraic geometry, Vol. 2. Schemes and complex manifolds. Translated by Miles Reid. Springer-Verlag, 1994.

[44] I. Shafarevich – *On p-extensions.* Mat. Sb. Nov. Ser. 20, **62** (1947), 351–363. Amer. Math. Soc. Translations, Series II, **4** (1956), 59–72.

[45] V. Snyder et. al. – *Selected topics in algebraic geometry* (two volumes in one). Second edition. Chelsea Publishing Co., New York, 1970.

[46] H. Stichtenoth – *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik* I, II. Arch. Math. (Basel) **24** (1973), 527–544, 615–631.

[47] D. Subrao – *The p-rank of Artin-Schreier curves.* Manuscr. Math. **16** (1975), 169–193.

[48] H. Weyl – *Die Idee der Riemannschen Fläche.* Teubner, 1913.
A translation: H. Weyl – *The concept of a Riemann surface*, translated by G. R. MacLane, Addison-Wesley Pub. Co., 1964, Snowball Publishing, 2010.

[49] E. E. Whittaker and G. Watson – *A course of modern analysis.* Cambridge University Press, third edition, 1920.

[50] L. Zapponi – *On the* 1*-pointed curves arising as étale covers of the affine line in positive characteristic.* Math. Zeitschr. **258** (2008), 711–727.

[51] H. Zeuthen – *Nouvelle démonstration des théorèmes sur les séries de points correspondants sur deux courbes.* Math. Ann. **3** (1871), 150–156. http://reader.digitale-sammlungen.de/de/fs1/object/display/bsb11043309_00160.html