ABC for polynomials, dessins d'enfants, and uniformization — a survey

JÜRGEN WOLFART (Frankfurt)

Prof. Wolfgang Schwarz zum 70. Geburtstag gewidmet
— und zum 25–jährigen Bestehen guter Zusammenarbeit!

Abstract. The main subject of this survey are Belyi functions and dessins d'enfants on Riemann surfaces. Dessins are certain bipartite graphs on 2–manifolds defining there a conformal and even an algebraic structure. In principle, all deeper properties of the resulting Riemann surfaces or algebraic curves should be encoded in these dessins, but the decoding turns out to be difficult and leads to many open problems.
We emphasize arithmetical aspects like Galois actions, the relation to the ABC theorem in function fields and arithmetic questions in uniformization theory of algebraic curves defined over number fields.

Dessins d'enfants have their origin in Grothendieck's *Esquisse d'un programme* [G] from 1984. In the meantime they turned out to be a fascinating source of links to many fields of mathematics like Inverse Galois Theory, Teichmüller Spaces, Maps and Hypermaps, Mathematical Physics or even Dense Circle Packings on 2–Manifolds. This survey makes a special choice, but it contains basic material and references for further studies in all directions. It should be accessible and useful (I hope) for all mathematicians interested in function theory and/or arithmetics e.g. as a base for a seminar or a graduate course. Aspects of algebraic geometry are presented in a rather oldfashioned way — at the price that some proofs are omitted or only sketched.
The paper grew out of lectures given in Southampton, Vilnius and on the ELAZ conference, of an old preprint [Wo0] partly published in [CoWo] and [CIW], and of an unpublished manuscript written in german for graduate students. Besides of some examples, some new aspects and proofs (e.g. of Thm. 5) most of the content of this paper is known. For important hints and improvements of earlier versions I am grateful to F. Berg, B. Köck, D. Singerman, J. Steuding, M. Streit and R. Remmert.

1. ABC for polynomials — a motivation from number theory

One of the most important contemporary Diophantine problems is the *abc conjecture* formulated first by Oesterlé and Masser in 1985. In its simplest form it can be stated as follows.

CONJECTURE. *All coprime integers* a, b, c *satisfying*

$$a + b + c = 0$$

are bounded by a small power of the kernel $K := \prod_{p|abc} p$ *, i.e. the product of all prime divisors of abc not counting multiplicities, more precisely: For any* $\varepsilon > 0$ *there is a constant* C_ε *such that*

$$\max\{|a|, |b|, |c|\} < C_\varepsilon K^{1+\varepsilon} .$$

In the meantime many generalizations and more sophisticated versions arose from this conjecture. For these, for the history of the problem, for many consequences and examples see Nitaj's homepage [Ni]. One of the reasons to believe in some form of this conjecture is the fact that an analogous statement was proven for function fields already some years before by W.W. Stothers [Sto] and then in much more general form by R. Mason [Mas]. It can be formulated for arbitrary genera and arbitrary fields of constants, see Chapter 7 of [Ro], but we present here the simplest version only.

THEOREM 1. *Let* A, B, C *be coprime polynomials in* $\mathbb{C}[x]$ *, not all constant, and satisfying* $A + B + C = 0$ *. Let* $n_0 := |\{\, \delta \in \mathbb{C} \mid ABC(\delta) = 0 \,\}|$ *be the number of zeros of* ABC *, i.e. the degree of the kernel* $K := \prod(x - \delta)$ *, the product running over all prime factors of* ABC *not counting multiplicities. Then we have*

$$\max\{\deg A, \deg B, \deg C\} < n_0 .$$

We give a very elementary argument due to Serge Lang [La]: Let

$$A := \alpha \prod (x - \alpha_i)^{n_i} \ , \ B := \beta \prod (x - \beta_j)^{m_j} \ , \ C := \gamma \prod (x - \gamma_k)^{l_k}$$

be the decompositions into linear factors with disjoint sets of zeros $\{\alpha_i\}$, $\{\beta_j\}$, $\{\gamma_k\}$. Without loss of generality, we may suppose that $\deg A = \sum n_i$ is the maximal degree of A, B, C . Put $f := -A/C$, $g := B/C$. Then we have

$$-f + g + 1 = 0 \ , \quad \text{hence} \quad f' = g' \ ,$$

and

$$-\frac{A}{B} = \frac{f}{g} = \frac{g'/g}{f'/f} = \frac{\sum \frac{m_j}{x-\beta_j} - \sum \frac{l_k}{x-\gamma_k}}{\sum \frac{n_i}{x-\alpha_i} - \sum \frac{l_k}{x-\gamma_k}} .$$

We multiply above and below with the kernel $K = \prod_{i,j,k}(x-\alpha_i)(x-\beta_j)(x-\gamma_k)$ of degree n_0 and observe that in each term of the sums involved precisely one linear factor cancels. We obtain therefore

$$-\frac{A}{B} = \frac{n(x)}{d(x)},$$

with polynomials n and d both of degree $< n_0$. Unique factorization in $\mathbb{C}[x]$ shows therefore $\deg A < n_0$.

The argument shows in particular the advantage of treating function fields instead of number fields: differentiation provides a powerful additional tool. The consequences of the ABC theorem are parallel to those in the number field case, e.g. Fermat's Theorem for functions, here for polynomials. And as in the number field case, we are interested in the limits of Theorem 1, i.e. in the question if it gives a sharp estimate. In the terminology of the proof above, this estimate would be sharp if $\deg A = n_0 - 1$. This is true if and only if $\deg n = n_0 - 1$, i.e. if two conditions are satisfied:

1. $\sum m_j \neq \sum l_k$, i.e. $\deg B \neq \deg C$
2. n and d are coprime.

Now observe that for all i, j, k

$$n(\alpha_i) = 0\,, \quad n(\beta_j) \neq 0\,, \quad n(\gamma_k) \neq 0$$

$$d(\alpha_i) \neq 0\,, \quad d(\beta_j) = 0\,, \quad d(\gamma_k) \neq 0\,,$$

since e.g. $n(\beta_j) = m_j \prod_i(\beta_j - \alpha_i) \prod_{j' \neq j}(\beta_j - \beta_{j'}) \prod_k(\beta_j - \gamma_k) \neq 0$ the $\alpha_i, \beta_j, \gamma_k$ all being pairwise distinct. Common factors of n and d therefore cannot have zeros which are zeros or poles of f and g. If n and d are not coprime, their common factor has zeros of $f' = g'$ outside the zeros of the kernel K. Taking into account that the f–preimages of $0, 1, \infty$ are precisely the α_i, the β_j and the γ_k, we have the following result (Zannier [Za]).

Proposition 1. *Let A, B, C, be coprime polynomials in $\mathbb{C}[x]$, not all constant and satisfying $A+B+C = 0$. Let $n_0 := |\{\,\delta \in \mathbb{C} \mid ABC(\delta) = 0\,\}|$. Then,*

$$\max\{\deg A, \deg B, \deg C\} = n_0 - 1$$

implies that the meromorphic function $f = -\frac{A}{C}$ is ramified at most above $0, 1, \infty$.

We remark in passing that our assumption that A is of maximal degree among A, B, C is not needed for this statement because the functions $-C/A$, $-B/C$ have the same ramification property. Note also another reason for the first condition $\deg B \neq \deg C$ in the critical cases: at least one of both polynomials has the same degree as A, and an easy argument of Vaserstein [V] shows that the other has degree $\leq n_0 - 2$. Proposition 1 holds for much more general situations ([Za], [Ro]), giving a first justification for the following

Definition 1. A non–constant meromorphic function $\beta : X \to \overline{\mathbb{C}} = \mathbb{P}^1(\mathbb{C})$ on a compact Riemann surface X is called a *Belyi function* if it ramifies at most above three points. (If not stated otherwise, we will assume these three critical values to be normalized as $0, 1, \infty$.)

In this terminology we have the following converse to Proposition 1.

Proposition 2. *Let $\beta : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ be a Belyi function, written as $\beta = -\frac{A}{C}$ with coprime polynomials A, C. Suppose $B \in \mathbb{C}[x]$ to be defined by*

$$A + B + C \;=\; 0\,,$$

and suppose ∞ to be a ramification point of β. Then

$$\max\{\deg A, \deg B, \deg C\} \;=\; n_0 - 1 \;=\; |\{\,\delta \in \mathbb{C} \,|\, ABC(\delta) = 0\,\}| - 1\;.$$

We can follow the arguments for the proof of Proposition 1. The condition $\deg B \neq \deg C$ is equivalent to $\beta(\infty) = 1$ or ∞ and implies the claim of Prop. 2 with $n_0 - 1 = \deg A$. In the case $\beta(\infty) = 0$ replace β by the Belyi function $1 - \beta$ and use again the arguments for Proposition 1.

2. Dessins d'enfants on Riemann surfaces

2.1. Belyi's theorem. For a direct application of Belyi functions to number theory see Elkies' work [El] about the impact of the abc conjecture on the Mordell–Faltings theorem. Here we will consider another reason why Belyi functions are important for arithmetics.

Recall that nonsingular algebraic curves in a projective space $\mathbb{P}^n(\mathbb{C})$ are compact Riemann surfaces. This is known already by Riemann's fundamental [R] work on abelian functions, and in principle he knew also that the converse is true, i.e. that every compact Riemann surface is isomorphic to a smooth projective algebraic curve over $\mathbb{C}$. Still it was a long way up to a conclusive proof: nowadays we may consider it as an equivalence between categories, a special case of Serre's GAGA–principle. We will make free use of this equivalence, e.g. considering holomorphic mappings between compact Riemann surfaces as rational mappings between projective algebraic curves. However, in this equivalence are hidden some solved and unsolved problems, the subjects of the present paper.

A fundamental problem can be described as follows. Can function theory give conditions under which a compact Riemann surface X — as an algebraic curve — is defined over a number field? In other words, when can

X be defined by algebraic equations with coefficients in $\overline{\mathbb{Q}}$ by choosing appropriate coordinates in $\mathbb{P}^n$? Or in other words again, when is it possible to write the function field of X as $\mathbb{C}(X) = \mathbb{C} \otimes_F F(X)$ for some function field $F(X)$ with constant field $F \subset \overline{\mathbb{Q}}$? We begin by stating the fundamental and simple answer of Belyi ([B1], 1979).

THEOREM 2. *Let X be a smooth algebraic curve in $\mathbb{P}^n(\mathbb{C})$. The following statements are equivalent.*
A) X is defined over a number field.
B) There exist Belyi functions β on X.

Of course, we want to have the field of definition F of X (and β) as small as possible, but we postpone this more sophisticated question as well as the proof of Theorem 2, see Sections 2.4 and 4.4.

2.2. Examples. Since $\mathbb{P}^1$ is defined over $\mathbb{Q}$ we should expect the existence of Belyi functions according to Theorem 2. There are in fact many series of Belyi functions. We will discuss only two of them.

EXAMPLE 1. $\beta : \mathbb{P}^1 \to \mathbb{P}^1$, $\beta(z) := z^n$ for a positive integer n. We may visualize the topological behavior of β by the β–preimage of the real interval $[0,1]$ as given in Figure 1 for $n = 6$.

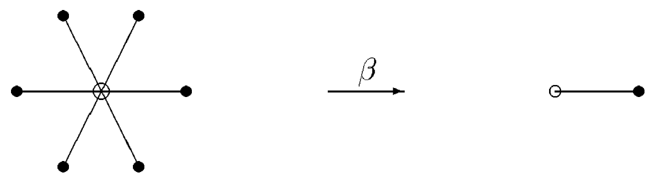

FIGURE 1. $[0,1]$–preimage of $\beta(z) = z^6$

EXAMPLE 2. Let $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ be the function

$$\beta(z) \ := \ T_n^2(z)$$

where T_n is the n–th Tchebychev polynomial defined by the property

FIGURE 2. Topological $[0,1]$–preimage of $\beta(z) = T_5^2(z)$

$T_n(\cos\theta) = \cos n\theta$. Up to an homeomorphism $\beta^{-1}[0,1]$ looks like the picture given in Figure 2 where the black vertices indicate the preimages $\cos k\pi/n$ of 1 and the white vertices the preimages $\cos\frac{(2k-1)\pi}{2n}$ of 0. We will see in Proposition 3 that only the topological structure of this graph and its embedding into the surface are important.

Example 3. There are not only polynomial Belyi functions, of course. The rational function

$$\beta(z) := \frac{4}{27}\,\frac{(1-z+z^2)^3}{z^2\,(1-z)^2}$$

is well known in modular function theory, describing the relation between the elliptic modular invariant j and Legendre's λ–function. Figure 3 shows again $\beta^{-1}[0,1]$. Ramification points of β are the double poles in $0,\,1,\,\infty$, the triple zeros in $\frac{1}{2}(1\pm\sqrt{-3})$ and the double zeros of $\beta-1$ in $-1,\,\frac{1}{2},\,2$.

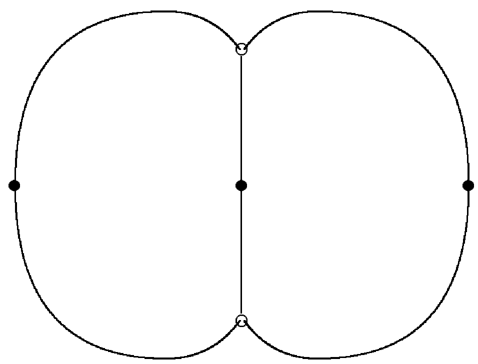

Figure 3. $[0,1]$–preimage of β, Example 3

These simple examples already show some principles valid for all Belyi functions.

1. $\beta^{-1}[0,1]$ is a connected graph on the surface X.
2. The β–preimages of 0 and 1 become the respective white and black vertices of the graph. With this convention we obtain a *bipartite* graph, i.e. every white vertex has only black neighbour vertices and conversely. The edges are the connected components of $\beta^{-1}]0,1[$.
3. The valencies of the graph in the vertices are the ramification orders of β in these points, i.e. above 0 and 1 respectively.
4. The graph cuts X into simply connected open cells. Each cell contains as "center" precisely one pole of β, and the order m of this pole (the ramification order above ∞) corresponds to the valency $2m$ of its cell. In other words, the cell is bounded by $2m$ edges, m white and m black vertices. Caution: if — as in Examples 1 and 2 — edges or vertices belong at both sides to the same cell, they have to be counted twice.

As an illustration, we continue with two examples for Belyi functions on elliptic curves.

EXAMPLE 4. (F. Berg) Let $X = X(\cos\frac{\pi}{10})$ be given by the affine equation

$$y^2 = (x-1)(x+1)(x - \cos\frac{\pi}{10}) .$$

Then $\beta(x,y) = T_5^2(x)$ is a Belyi function on X where T_5 is the Tchebychev polynomial we met already in Example 2. The ramification behaviour of β can be visualized according to the composition of maps

$$(x,y) \mapsto x \mapsto T_5^2(x) .$$

The first mapping is ramified of order 2 above the points $x = \infty,\ 1,\ -1$ and $\cos\frac{\pi}{10}$, and for the second consult Example 2. The bipartite graph then has the topological shape described in Figure 4 on the torus X. If we cut the

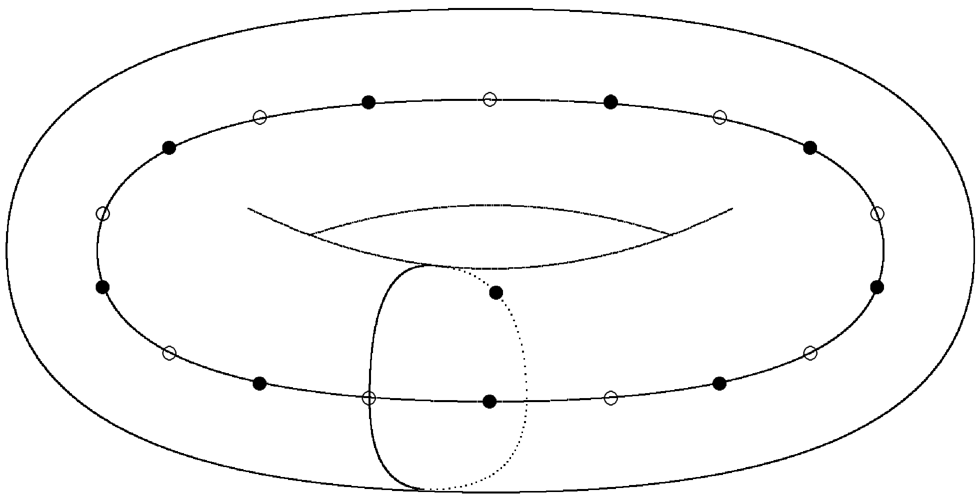

FIGURE 4. $[0,1]$–preimage of $\beta(x,y) = T_5^2(x)$ on $X(\cos\frac{\pi}{10})$

torus along the edges we may use it in the euclidean or Gaussian plane as fundamental domain of the universal covering group, i.e. in our case of a

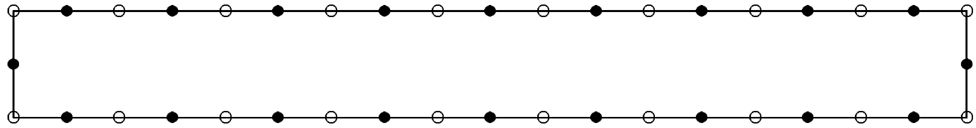

FIGURE 5. $[0,1]$–preimage of $\beta(x,y) = T_5^2(x)$ on $X(\cos\frac{\pi}{10})$

lattice of translations. In this picture the bipartite graph looks like Figure 5 where the opposite sides have to be identified to obtain again the graph on the torus. Besides a zero of order 4 in the point

$$(x,y) \;=\; (\cos\frac{\pi}{10},0)$$

we have as ramification points only double zeros of β and $\beta-1$ and one pole of order 20.

Example 5. On the elliptic curve with the affine equation

$$y^2 \;=\; x\,(x-1)\,(x\;-\;\frac{1}{\sqrt[3]{2}})$$

(real third root) $\beta(x,y)=4x^3(1-x^3)$ is a Belyi function. The ramification of β can be understood by decomposing β into the maps

$$(x,y)\;\mapsto\;x\;\mapsto\;x^3\;\mapsto\;4x^3(1-x^3)\;.$$

If we determine the preimage of the $[0,1]$–interval following these maps backwards step by step, we obtain a bipartite graph homeomorphic to that one given in Figure 6 (again, opposite sides have to be identified). For example the zero of order 6 and the 1–point of order 4 are the points

$$(x,y) \;=\; (0,0) \qquad \text{and} \qquad (\frac{1}{\sqrt[3]{2}},0)\;, \quad \text{respectively.}$$

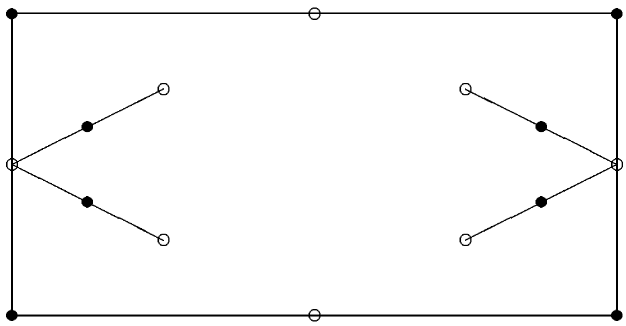

Figure 6. $\beta^{-1}[0,1]$ on the Torus of Example 5

2.3. Children's drawings — dessins d'enfants. The structure of these bipartite graphs is simple, and Grothendieck [G] pointed out that they encode important information about the curve X. So we follow his proposal introducing the following terminology.

Definition 2. Let M be a compact oriented 2–manifold and D a bipartite graph on M such that $M-D$ is a disjoint union of simply connected open sets. Then D is called a *dessin d'enfant* on M.

Grothendieck introduced this terminology for an even simpler class of Belyi functions and graphs: if β has ramification order 2 in all preimages of 1, i.e. if D has valency 2 in all black vertices, we may omit these black vertices and consider D as the usual connected graph on M cutting M into simply connected open cells. In this case we call β a *clean* Belyi function and also the resulting dessin a *clean* one. We can always get this simplification replacing β by $4\beta(1-\beta)$. On the other hand, this simplification has some disadvantages like doubling the degree, so we will not use it in the sequel.
The notion of dessins presented here has also some disadvantages. It does not reflect the equal right among the three types of ramification points above $0, 1, \infty$: as already mentioned in Section 1, we may replace β by $1-\beta$ or by β^{-1} interchanging the colours of the vertices of D or interchanging white vertices and centers of the faces of D, respectively. These equal rights are better reflected in the language of *hypermaps*, see [JS2], [JS3], but then the drawings become more complicated. For several reasons there is still no standard terminology for dessins, so we will use the definitions given here.

Why does the definition speak about 2–manifolds only and not about Riemann surfaces? The answer is given by the following striking fact, first pointed out by Grothendieck [G] but proven essentially before by Jones and Singerman [JS1] and independently by Malgoire and Voisin [MV].

PROPOSITION 3. *Let M be a compact oriented 2–manifold with dessin d'enfant D. Then there is a unique conformal structure on M and a Belyi function β on M such that $D = \beta^{-1}[0,1]$ is the dessin belonging to β.*

According to Theorem 2 M is then not only a Riemann surface but moreover a smooth projective algebraic curve defined over $\overline{\mathbb{Q}}$. We will give an idea of the proof in Sections 3.5 and 3.6. For the moment, we continue with some complements to the definition.

DEFINITION 3. The dessin D on the 2–manifold M is called *uniform* if all white vertices, all black vertices, all cells have the same valency p, q, $2r$ respectively. It is called *regular* if the automorphism group of D acts transitively on the set of edges. By an *automorphism* we understand a graph automorphism of D preserving the colours of the vertices and resulting from the restriction of an orientation preserving homeomorphism of M onto itself.

Examples 1 and 3 above are in fact regular dessins. Some comments concerning Definition 3 are in order. Every automorphism of the dessin is a graph automorphism of D but the converse is not true in general. Regular dessins are uniform but again the converse is not true in general: in genus 2 there are 11 non–isomorphic regular dessins (for a list see e.g. [Wo2]), but more than 500 non–isomorphic uniform dessins, see [SSy2]. We may complete Proposition 3 by saying that every automorphism of D can be considered as restriction of an automorphism of the conformal structure of M and that regular dessins belong precisely to Belyi functions defining normal (ramified, of course) coverings $\beta : M \to \mathbb{P}^1$, see Theorem 4 in Sec. 4.6. One may even show that on any smooth algebraic curve X defined over $\overline{\mathbb{Q}}$ and of genus $g > 1$ there is a dessin having $\operatorname{Aut} X$ as automorphism group.

2.4. Proof of A) $\Rightarrow$ B).

Lemma 1. *Let X be a Riemann surface, $f : X \to \overline{\mathbb{C}}$ a non–constant meromorphic function, W the set of its critical values, i.e. the images of the ramification points of f, and let $g : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ be a nonconstant rational function with critical values in the set V. Then the critical values of $g \circ f$ are contained in $V \cup g(W)$.*

The proof of this lemma is evident. We use it as follows. On a curve X defined over a number field F take a rational function f defined over F and observe that the critical values of f consist of finitely many algebraic numbers and perhaps ∞. There is a minimal polynomial g of these algebraic numbers, defined over $\mathbb{Q}$ and of degree $m > 1$, say. Then the critical values of $g \circ f$ are $0, \infty$ and at most $m-1$ algebraic numbers of degree $\leq m-1$. As g–images of the zeros of $g' \in \mathbb{Q}[x]$ this set of critical values is even invariant under algebraic conjugations, its minimal polynomial over $\mathbb{Q}$ has therefore some degree $\leq m-1$. Therefore we can iterate the procedure to decrease the degree of the critical values and obtain finally

Lemma 2. *Suppose that the smooth projective algebraic curve X is defined over a number field. There is a rational function on X whose critical values are contained in $\mathbb{Q} \cup \{\infty\}$.*

For the next step Belyi [B1] uses induction again which leads in concrete examples often to very complicated Belyi functions. For this part of the proof there are now several alternatives like e.g. [B2]. Here we follow an idea by Leonardo Zapponi [Z2] relying on a simple identity between rational functions.

Lemma 3. *Let $r_1, \ldots, r_n \in \mathbb{Q}$ be pairwise different and put*

$$y_i := \Big(\prod_{j \neq i} (r_i - r_j) \Big)^{-1} .$$

Then we have

$$\sum_i \frac{y_i}{x - r_i} = \frac{1}{\prod_i (x - r_i)} .$$

PROOF. Consider the polynomials $p(x) = \prod_i (x - r_i)$ and

$$q(x) \; = \; p(x) \sum_i \frac{y_i}{x - r_i} \; = \; \sum_i y_i \prod_{j \neq i} (x - r_j) \; \in \; \mathbb{Q}[x] \, .$$

Then $\deg q \leq n - 1$ and $q(r_1) = \ldots = q(r_n) = 1$, therefore $q(x) = 1$.

For the PROOF of part $A) \Rightarrow B)$ of Theorem 2 we use Lemma 2 to construct a meromorphic function on X with critical values at most ∞ and some $r_1, \ldots, r_n \in \mathbb{Q}$. Let N be the least common denominator for the numbers y_i in Lemma 3. That means $a_i := N y_i \in \mathbb{Z}$, and the rational function

$$g(x) \; := \; \prod_i (x - r_i)^{a_i} \; \in \; \mathbb{Q}(x)$$

satisfies

$$\frac{g'(x)}{g(x)} \; = \; \sum_i \frac{a_i}{x - r_i} \; = \; \sum_i \frac{N y_i}{x - r_i} \; = \; \frac{N}{\prod_i (x - r_i)}$$

according to Lemma 3. Therefore g is ramified at most in ∞ and in the r_i. By Lemma 1, $g \circ f$ has at most $0, 1, \infty$ as critical values.

3. Uniformization

3.1. Covering groups and arithmetic. As usual we consider Riemann's generalized mapping theorem as main theorem of uniformization theory, saying that every simply connected Riemann surface is biholomorphically equivalent to $\overline{\mathbb{C}}$, $\mathbb{C}$ or the unit disc $\mathbb{U}$ which we may replace by the upper half plane $\mathbb{H}$. By construction, the universal covering U of a Riemann surface X has the structure of a simply connected Riemann surface. Therefore we can write X as quotient space $\Gamma \backslash U$ where Γ denotes the covering group of X, acting discontinuously and without torsion on U. In the case $U = \overline{\mathbb{C}}$ we have trivial Γ, for X compact of genus 1, i.e. for elliptic curves, we have $U = \mathbb{C}$ and Γ is the translation group of the period lattice, and for compact Riemann surfaces of higher genus we have $U = \mathbb{H}$ and $\Gamma \subset \mathrm{PSL}_2\mathbb{R}$ a cocompact torsion free Fuchsian group, sometimes called a *surface group*. In the following, we will often admit torsion, in other words we will admit ramified coverings by the upper half plane.
The aim of uniformization of Riemann surfaces is to replace their function theory by function theory in a simply connected region. Unfortunately, uniformization is not very explicit: in general it is very hard to determine the covering group of some curve of genus $g > 1$ by giving e.g. their generators in explicit matrix form, see e.g. [Se]. And conversely, given a Fuchsian group Γ by matrices, it is in general difficult to write down the defining equations

of the curve $X \cong \Gamma\backslash\mathbb{H}$. In special cases like Klein's quartic which played an important role for the history of uniformization theory both problems are solvable. Why are we here in a better position? This became understandable by Belyi's theorem. To this aim, we will present it in another version but first we recall an arithmetic question related to the uniformization of smooth projective algebraic curves X of genus $g > 1$. *In which cases is* X *defined over* $\overline{\mathbb{Q}}$ *and at the same time the covering group* Γ *— at least after a suitable conjugation in* $\mathrm{PSL}_2\mathbb{R}$ *— is contained in* $\mathrm{PSL}_2(\mathbb{R} \cap \overline{\mathbb{Q}})$ *?* The Chudnovsky brothers ([Chu], Section 7) have a very general conjecture saying in this special case: These should be those curves whose covering group Γ is arithmetic (see [Bo], [Ka] or [MR]) or a subgroup of some triangle group. Triangle groups share even more interesting properties with arithmetic groups, compare [CoWo], and have a special meaning for dessins whence we will define and discuss them in a moment.
As an illustration for this kind of questions let's have a short look on the case of elliptic curves. There, the two conditions that

- X is defined over $\overline{\mathbb{Q}}$ and
- its covering group, i.e. its period lattice $\Gamma \subset \mathbb{C}$, can be chosen in $\overline{\mathbb{Q}}$

are satisfied simultanuously if and only if X has complex multiplication (Th. Schneider [Schn]).

3.2. Triangle groups. If p, q, r are positive integers such that

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1 ,$$

take a hyperbolic triangle in $\mathbb{H}$ with vertices P, Q, R and angles π/p, π/q, π/r. The triangle is uniquely determined by these angles up to orientation and hyperbolic transformation. (If the sum of the angles is $= \pi$ or $> \pi$ we get euclidean or spherical triangles and define in the same way as below euclidean or spherical triangle groups acting on $\mathbb{C}$ or $\overline{\mathbb{C}}$.)

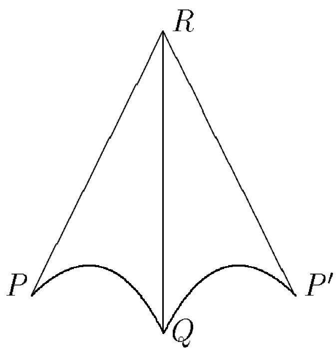

FIGURE 7. Fundamental domain of a triangle group in the unit disc with center R, signature $< 12, 6, 6 >$

Let γ_0, γ_1, γ_∞ be hyperbolic counterclockwise rotations around P, Q, R with angles $2\pi/p$, $2\pi/q$, $2\pi/r$. Then they generate a *triangle group* Δ with presentation

$$< \gamma_0, \gamma_1, \gamma_\infty \mid \gamma_0^p = \gamma_1^q = \gamma_\infty^r = \gamma_0\gamma_1\gamma_\infty = 1 > ,$$

acting discontinuously on the upper half plane $\mathbb{H}$. A fundamental domain of Δ can be given as the union of the triangle PQR with a triangle constructed by hyperbolic reflection in one side as e.g. $P'QR$ in Figure 7 (the drawing is given in the unit disc $\mathbb{U}$ instead of $\mathbb{H}$, and without loss of generality we take R as center of $\mathbb{U}$).
Up to conjugation in $\mathrm{PSL}_2\mathbb{R}$, the triangle group Δ is uniquely determined by p, q, r whence we replace the letter Δ often by its *signature* $< p, q, r >$. One can admit as well triangle groups for which e.g. P or other vertices lie on the border of the upper half plane, then as a *cusp* with angle 0. Then we define $p := \infty$ and omit the relation $\gamma_0^p = 1$ from the presentation — γ_0 becomes a parabolic element with fixed point P — and proceed as in the case $p \in \mathbb{N}$. Here the quotient space $\Delta\backslash\mathbb{H}$ is no longer compact and sometimes has to be compactified. Therefore we will concentrate in the following on the *cocompact* triangle groups, i.e. those without cusps.

There is a classical isomorphism

$$\Delta\backslash\mathbb{H} \cong \overline{\mathbb{C}}$$

defined by the j–function for the group Δ. This function can be defined by Riemann's mapping theorem as a biholomorphic mapping of the open triangle PQR onto the upper half plane $\mathbb{H}$, normalized by sending P, Q, R to $0, 1, \infty$ respectively. By Schwarz' reflection principle we can continue j analytically to the reflected triangles and by successive reflection in the border sides of all Δ–images of the fundamental domain finally as a meromorphic function on $\mathbb{H}$. Clearly j is a Δ–automorphic function, i.e. satisfies

$$j(\gamma z) = j(z) \quad \text{for all} \quad z \in \mathbb{H}\,,\ \gamma \in \Delta\,,$$

and is locally biholomorphic everywhere outside the Δ–images of P, Q, R, where it has zeros, 1–points and poles of orders p, q, r respectively. The boundary sides of the triangle and all their Δ–images form the j–preimages of $\overline{\mathbb{R}}$.
Another possibility to define j is to use the hypergeometric differential equation with monodromy group Δ: the quotient of two linearly independent solutions is the Schwarz triangle function, mapping — suitably normalized — the upper half plane onto the open triangle PQR. Its inverse function is j. This is the main ingredient for the following useful variant of Belyi's theorem, first published in [Wo0], [CoWo], [ClW].

3.3. Belyi functions and uniformization.

THEOREM 3. *Let X be a smooth algebraic curve in $\mathbb{P}^n(\mathbb{C})$. The following statements are equivalent.*
B) There exist Belyi functions β on X.
C) There is a subgroup Γ of some triangle group Δ such that $X \cong \Gamma\backslash\mathbb{H}$.

PROOF of C) $\Rightarrow$ B). A Belyi function on X is given by

$$\Gamma\backslash\mathbb{H} \rightarrow \Delta\backslash\mathbb{H} \rightarrow \overline{\mathbb{C}} : \quad \Gamma z \mapsto j(z) .$$

For $\Delta = < p, q, r >$ the ramification orders above $0, 1, \infty$ divide p, q, r, respectively.

PROOF of B) $\Rightarrow$ C). Suppose we have a Belyi function β on X whose ramification orders above $0, 1, \infty$ divide p, q, r, respectively (w.l.o.g. with sum of the inverses < 1). Consider the triangle group $\Delta = < p, q, r >$ and its j–function. Outside of its ramification points, β is locally biholomorphic, therefore in any simply connected domain inside $\overline{\mathbb{C}} - \{0, 1, \infty\}$ there is a holomorphic branch of β^{-1}. We cannot continue this branch analytically to $\overline{\mathbb{C}}$ across the singularities $0, 1, \infty$ but we can continue the composition $\beta^{-1} \circ j$ along any path in $\mathbb{H}$ since the multiplicities of the values of j are multiples of the respective ramification orders of β. Using the monodromy theorem we can even define $\beta^{-1} \circ j$ globally as a covering map $\mathbb{H} \rightarrow X$ whose covering group Γ is contained in Δ by construction. This proves Theorem 3.

The covering map constructed here is unramified only if p, q, r are the respective precise ramification orders in every ramification point of β above $0, 1, \infty$. If we choose in this case $\Delta = < p, q, r >$ we obtain just the universal covering group of X. As a consequence concerning our initial problem in uniformization theory we obtain

PROPOSITION 4. *The universal covering group Γ of a smooth algebraic curve $X \subset \mathbb{P}^n(\mathbb{C})$ of genus $g > 1$ is contained in a triangle group if and only if X has a uniform dessin.*

This proposition remains true for genera 1 and 0: observe that for $g = 1$ the valency triples of uniform dessins lead to the signatures of euclidean triangle groups

$$< 3, 3, 3 > , \quad < 2, 3, 6 > , \quad < 2, 4, 4 >$$

(for the resulting curves, see [SSy1]), and that for $g = 0$ uniform dessins correspond to the well known spherical triangle groups already classified by H.A. Schwarz as monodromy groups of the algebraic hypergeometric functions.

3.4. An example. We mentioned already that regular dessins are uniform. In Theorem 3, regular dessins correspond to torsion free normal subgroups Γ of Δ since the quotient $G := \Delta/\Gamma$ acts then as a group of biholomorphic automorphisms on the quotient space $X = \Gamma\backslash\mathbb{H}$, preserving the tesselation which is induced on X by the fundamental domains of Δ. Normal subgroups of Δ are of course kernels of homomorphisms

$$h : \Delta \to G ,$$

and the condition "torsion free" is satisfied if and only if the generators of Δ go under this map to elements of the same order: Fuchsian group theory says that every torsion element in Δ (hence also in Γ) is conjugate in Δ to some power of $\gamma_0, \gamma_1, \gamma_\infty$. If h maps these generators to elements of the same order, only trivial powers of torsion elements lie in the kernel whence Γ is torsion free, and the converse is true as well. As an application we consider

Example 6. Let h be the homomorphism $< 2, 8, 8 > \to G = \mathbb{Z}/8\mathbb{Z}$ given by

$$h(\gamma_0) = 4 \, , \; h(\gamma_1) = 3 \, , \; h(\gamma_\infty) = 1$$

(read the right hand sides $\bmod 8$). Then the kernel Γ of h gives a Riemann surface $X = \Gamma\backslash\mathbb{H}$. The Riemann–Hurwitz formula or a volume consideration for the fundamental domains of Δ and Γ show that its genus is 2.

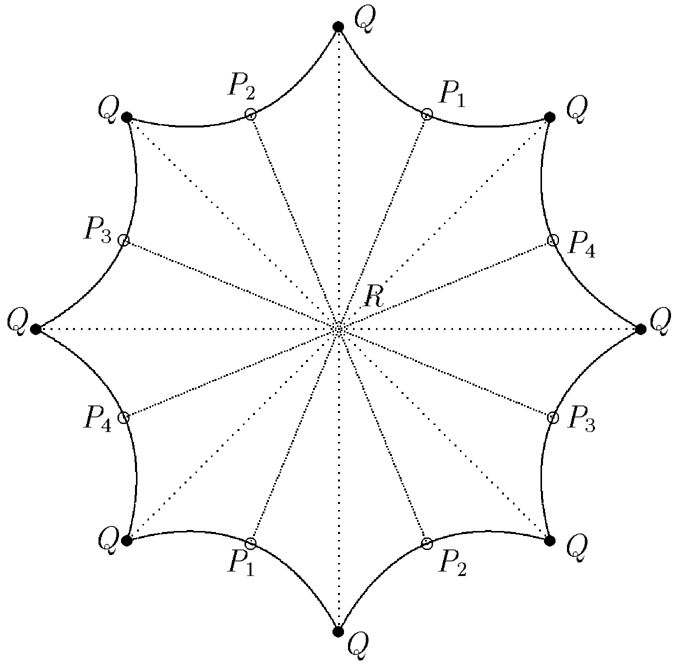

Figure 8. Fundamental domain of Γ in Example 6, drawing in the unit disc

Figure 8 shows a fundamental domain of Γ (in the unit disc, the center is chosen as the center R of the fundamental domain) consisting of $8 = \operatorname{ord} G$ fundamental domains of Δ. These are the hyperbolic quadrangles $P_i Q P_{i+1} R$, where we read $i \bmod 4$. The letters indicate how to identify sides and vertices to obtain the quotient X. Euler's formula provides another possibility to see that $g = 2$.
Following the ideas explained above, the border of the polygon will become a dessin d'enfant on X, here with 4 white and one black vertex, 8 edges and one cell. Observe that we have to count the edges twice since on X they have the same cell on both sides. Figure 8 also visualizes the action of G on X: the automorphisms are rotations around the center with rotation angle $2\pi k/8$, $k \in \mathbb{Z}$. Fixed points are R and *the* black vertex Q of the dessin, and fixed points of order 2 (rotation of angle π) are in addition all white vertices P_i. According to Proposition 3, a dessin determines uniquely the conformal and the algebraic structure on X, so we should be able to determine equations for X and the Belyi function corresponding to the dessin. This is possible but difficult in general, see [Bi], [Sn2], [LZ] and the completely different approaches in [St1] and [BS], all with instructive examples. In simple cases like the present example we can try a good guess: β has degree 8, has four double zeros and is ramified above 1 and ∞ of order 8. The quotient $Z_2 \backslash X$ of X by the unique order 2 subgroup in G is still the Riemann sphere, again with a regular dessin with valencies $1, 4, 4$ and cyclic automorphism group of order 4. Its Belyi function is easily seen to be $x^4 + 1$. Now observe that X is a double cover of $\mathbb{P}^1$ ramified over the points where $x^4 + 1 = 0,\ 1,\ \infty$. The result is

$$K \ : \ y^2 \ = \ x(x^4+1) \quad , \quad \beta \ : \ (x,y) \ \mapsto \ x^4 + 1 \ ,$$

and G is generated by

$$(x,y) \ \mapsto \ (ix \, , \, e^{\pi i/4} y) \ .$$

The full automorphism group of X is in fact larger because Γ is even a normal subgroup of the triangle group $< 2,3,8 > \ \supset \ < 2,8,8 >$ (index 6 inclusion). One may tesselate the fundamental domain of Γ by 48 fundamental domains of $< 2,3,8 >$ giving X an automorphism group isomorphic to $\mathrm{GL}_2\mathbb{F}_3$ of order 48, see [Wo2] and the literature quoted there.

3.5. Determining the conformal structure. We will describe two ideas how to prove Proposition 3, i.e. how to use a dessin to determine the conformal structure. We explain these ideas in

Example 7. Let D be a dessin on a torus with one cell, five edges, two white and two black vertices of respective valencies 1 and 4. Up to isomorphism (i.e. orientation preserving homeomorphisms of the torus onto itself preserving the colours of the vertices) there are three such dessins. We fix one of these possibilities given in Figure 9 in the plane instead on the torus — identify opposite sides to get the picture on the torus as indicated also by the numbering of vertices and edges.

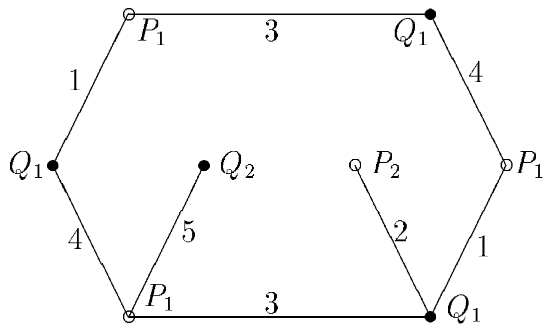

Figure 9. Dessin on a torus, Example 7

If there is a conformal structure on the torus with a Belyi function leading to D, then according to the proof of Theorem 3 the manifold should be a quotient space $\Gamma\backslash\mathbb{H}$ (having a unique conformal structure, of course) for some index 5 subgroup Γ of $\Delta = < p, q, r > = < 4, 4, 5 >$ (exercise: show that we could replace 4 and 5 by multiples without changing the conformal structure!). The Belyi function has to be

$$\Gamma\backslash\mathbb{H} \to \Delta\backslash\mathbb{H} \to \overline{\mathbb{C}} : \quad \Gamma z \mapsto j(z) ,$$

and on $\Gamma\backslash\mathbb{H}$ the dessin must be part of the triangle grid coming from the border of the fundamental domain of Δ and all its Δ–images in the hyperbolic plane, under the projection

$$\mathbb{H} \to \Gamma\backslash\mathbb{H} : z \mapsto \Gamma z .$$

How do we find the subgroup Γ of Δ? By variation of an idea of Shabat and Voevodsky [SV1] we cut the manifold along the edges of D until we have a simply connected domain. This cut has to meet all vertices whose valencies are proper divisors of p and q, i.e. in our example we have to cut along the edges 2 and 5 meeting the vertices P_2 and Q_2. Every cut edge — in our example all five edges — occurs twice as border edge of the resulting domain. Now we deform the domain homeomorphically such that it fits into the triangle grid defined by the Δ–tesselation on $\mathbb{H}$. In particular, all edges have to become hyperbolic lines between Δ–fixed points of orders p and q. Figure 10 may illustrate that we can perform that program.
Now recall Poincaré's theorem that — under suitable hypotheses concerning the angles — a Fuchsian group can be generated by elements of $\mathrm{PSL}_2\mathbb{R}$ mapping the sides of the polygon pairwise onto each other. The cut procedure and the numeration determine the side pairing. Here Γ will be of genus 1 with two inequivalent fixed points P_2, Q_2 of order 4, the other vertices

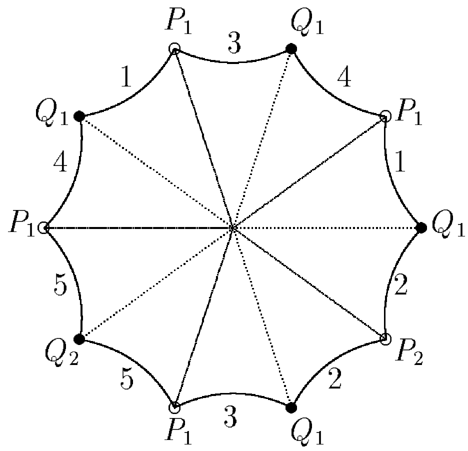

FIGURE 10. Fundamental domain for Γ, Example 7

belong to two orbits of accidental vertices. The resulting Riemann surface $\Gamma\backslash\mathbb{H}$ of genus 1 has precisely the dessin we started with.

3.6. The cartographic group. It is difficult to make precise the cut and paste technique described above if we consider more complicated dessins. More comfortable is a group theoretic procedure based on a description of dessins by means of permutation groups acting on the set of edges ([JS1], [JS2], [BaIt]), also better adapted to computations than graphical methods. Let $1, \ldots, n$ be the numbers of the edges and define the *(hyper)cartographic group* $G \subseteq S_n$ as generated by two permutations w, b permuting for all white (respective black) vertices the incident edges in cyclic counterclockwise order. To every white (resp. black) vertex corresponds therefore a cycle in the cycle representation of w resp. b, e.g. in Example 7

$$w = (1\,3\,5\,4)\,, \qquad b = (1\,2\,3\,4)$$

(recall the border identifications in Figures 9 and 10 and the fact that vertices of valency 1 give respective cycles (2) and (5) which do not appear in the usual description of permutations). The element $c = (wb)^{-1} \in G$ describes for every cell a cyclic couterclockwise permutation of all edges which have the cell on its left going from the black to the white border vertex. In Example 7

$$c = (1\,3\,4\,5\,2)$$

generates a normal subgroup of order 5 in G. The cartographic group is here a semidirect product of this normal subgroup Z_5 with a cyclic group Z_4 generated by w and acting on c by $wcw^{-1} = c^2$.
A SIDE REMARK about terminology. The term *cartographic group* is used in the literature mainly for clean dessins (see Section 2.3) or in more general

cases for the clean dessin we can get from D replacing β by $4\beta(1-\beta)$. Since we do not use this procedure we will speak of *cartographic groups* also in the general case.

Since the graph of the dessin is connected, G acts transitively. This is already one direction of the following

Proposition 5. *There is a bijection between*

1. *isomorphism classes of dessins on oriented* 2*–manifolds and*
2. *conjugacy classes of* "algebraic hypermaps"*, i.e. triples* (G, w, b) *of transitive permutation groups* $G \subseteq S_n$ *with two generators* w, b*.*

Proof. *Conjugacy class* means of course conjugation in S_n, i.e. renumbering the edges. It is almost evident how to construct a dessin for the algebraic hypermap (G, w, b): every number $1, \ldots, n$ represents an edge, and the cycles of w and b define the white and the black vertices. The cycles define also the local orientation of the edges around their border vertices. The cells are uniquely determined up to isomorphisms by the cycle decomposition of $c = (wb)^{-1} \in G$. These cells and how they fit together around the vertices define an atlas for the orientable compact 2–manifold M.

Let $H \subset G$ be the stabilizer subgroup of a fixed edge of the dessin D. Then we may identify the edges of D with the residue classes gH, $g \in G$, and we may read the operation of G on these edges as left multiplication on residue classes. In Example 7 and for edge no. 5 the group H is generated by $b = (1\,2\,3\,4)$. Note that the stabilizer group of any other edge is conjugate to H in G.

Now we return to a second proof of Proposition 3: how to construct from a dessin, i.e. an algebraic hypermap (G, w, b), a conformal structure on M, i.e. a triangle group Δ and a subgroup Γ to find a reasonable identification of M with the Riemann surface $\Gamma\backslash\mathbb{H}$? If we know already that D corresponds to the Belyi function $\beta : \Gamma\backslash\mathbb{H} \to \Delta\backslash\mathbb{H} \cong \mathbb{P}^1$ then G plays the role of the monodromy group of β because the edges of D represent the different branches of β^{-1} and the elements of G describe the change of branches under analytic continuation following paths in $\mathbb{P}^1 - \{0, 1, \infty\}$. These paths have to be composed from simple closed counterclockwise loops around 0 and 1 giving the generators w, b of G. How is G related to Δ and Γ?

Let Φ be the *kernel* of $\Gamma \subset \Delta$, i.e. the maximal normal subgroup of Δ contained in Γ. Let k be the hyperbolic line between P and Q, the fixed points of the generators $\gamma_0, \gamma_1 \in \Delta$, see Section 3.2, and let Γk be its image on $\Gamma\backslash\mathbb{H}$. Therefore the edges of D are the $\Gamma\delta k$, $\delta \in \Delta$, corresponding bijectively to the right residue classes $\Gamma\delta \in \Gamma\backslash\Delta$, and Δ acts by multiplication from the right permuting these residue classes. Such a permutation is trivial precisely if it belongs to the normal subgroup Φ, hence

- $G := \Delta/\Phi$ is the monodromy group of β acting by right multiplication on their residue classes $\Gamma\delta$,
- G is generated by $w = \gamma_0\Phi = \Phi\gamma_0$ and $b = \gamma_1\Phi = \Phi\gamma_1$,
- $H := \Gamma/\Phi$ is the stabilizer subgroup of k in the corresponding dessin.

This leads to the following proof for Proposition 3. Let D be a dessin on a topological oriented 2–manifold M and let (G, w, b) be the corresponding algebraic hypermap. Let p, q, r be the orders of $w, b, c = (wb)^{-1}$ and H the stabilizer subgroup of some fixed edge. As triangle group take $\Delta := < p, q, r >$ and consider the epimorphism $\pi : \Delta \to G$ defined by

$$\gamma_0 \mapsto w\,, \quad \gamma_1 \mapsto b$$

(strictly speaking we take an *antiepimorphism* because Δ acts by right multiplication and G from the left). Then the preimage $\Gamma := \pi^{-1}(H)$ is the good candidate to identify M with the Riemann surface $\Gamma\backslash\mathbb{H}$. Here $\mathbb{H}$ has to be replaced by $\mathbb{C}$ or $\overline{\mathbb{C}}$ if Δ is euclidean or finite, respectively.

In our Example 7 the complex and even the algebraic structure is explicitely known by Birch [Bi]: an affine model is

$$y^2 = x^3 + \frac{35}{4}x^2 + 25x + 25\,,$$

and he gives even the corresponding Belyi function which is *not* defined over $\mathbb{Q}$. The shape of the dessin already suggests that complex conjugation leaves the curve invariant but changes the colours of the vertices hence interchanges β and $1-\beta$. Considerations of this kind will play a major role in Section 4.

3.7. Automorphisms. The automorphism group of a dessin shows also the power of the notion *cartographic group*, see [Si1], [BaIt].

Proposition 6. *Let D be a dessin with algebraic hypermap group (G, w, b), $G \subseteq S_n$, let $H \subset G$ be the stabilizer subgroup of an edge in D and let $N(H)$ be its normalizer in G. Then the automorphism group of D is isomorphic to*

1. *the centralizer of G in S_n,*
2. *the quotient $N(H)/H$.*

D is a regular dessin if and only if $H = \{\mathrm{id}\}$, and this is the case if and only if $G \cong \mathrm{Aut}\,D$.

The proof relies on two possible descriptions of the automorphisms. First they are of course permutations p of the set of edges preserving

incidence and local orientation. That means they have to preserve the generators w, b of G. Since permutation of the entries in the cycle representation of $g \in G$ coincides with conjugation pgp^{-1}, such a p has to centralize the generators, hence G.
For the second claim identify the edges with the residue classes $\Gamma\delta k$, $\delta \in \Delta$, see the proof of Proposition 3 given above. Any automorphism of D preserves the conformal structure of $X = \Gamma\backslash\mathbb{H}$, therefore lifts to an automorphism α of $\mathbb{H}$. Because it preserves the colours of vertices, this lift has to be an element of Δ. On the other hand it defines an action on $\Gamma\backslash\mathbb{H}$ by left multiplication, i.e. maps Γ–orbits into Γ–orbits hence normalizes Γ. This action is trivial on $\Gamma\backslash\mathbb{H}$ if and only if $\alpha \in \Gamma$, so the automorphism group in question is $N(\Gamma)/\Gamma$, $N(\Gamma)$ denoting the normalizer of Γ in Δ. Taking quotients by Φ the isomorphism theorem of group theory proves the claim with $H = \Gamma/\Phi$. We have regularity of D if and only if Γ is normal in Δ, hence $\Gamma = \Phi$.
Caution: regularity does not mean $G = \operatorname{Aut} D$ since both groups act in a different way on the edges of D, see Section 3.6.

4. Galois actions

4.1. Examples. Let $X \subset \mathbb{P}^n(\mathbb{C})$ be a smooth algebraic curve defined over a number field F with Belyi function β also defined over F and with corresponding dessin D. What happens if some algebraic conjugation $\sigma \in \operatorname{Gal} \overline{\mathbb{Q}}/\mathbb{Q}$ acts on the constants in β and the defining equations for X? Regularity conditions are controlled by the nonvanishing of certain equations and "nonvanishing" is σ–invariant, therefore we obtain again a smooth curve $X^\sigma \subset \mathbb{P}^n(\mathbb{C})$. As a point set we get this curve also by extending σ to a field automorphism of $\mathbb{C}$ and applying σ to the coordinates of the points. The same idea gives a Belyi function β^σ on X^σ since $0, 1, \infty$ remain invariant and ramification orders are again defined by vanishing or nonvanishing of polynomials. Consequently we obtain a dessin d'enfant D^σ on X^σ.

Example 4'. There is an automorphism σ of the cyclotomic field $\mathbb{Q}(e^{\pi i/10})$ sending the elliptic curve $X = X(\cos\frac{\pi}{10})$ of Example 4 to the curve $X^\sigma = X(\cos\frac{3\pi}{10})$ defined by

$$y^2 \;=\; (x+1)\,(x-1)\,(x \;-\; \cos\frac{3\pi}{10})\,.$$

Having rational coefficients, the Belyi function $\beta(x, y) = T_5^2(x)$ remains formally unchanged. But the dessin D^σ has to look different from D in Figures 4 and 5 as we know by Proposition 3 : both elliptic curves are non–isomorphic as we can verify using their j–invariant. The first mapping $(x, y) \mapsto x$ in the composition of β is now ramified above another point

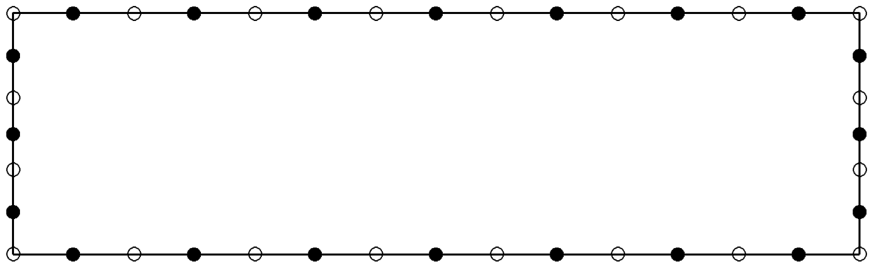

FIGURE 11. $[0,1]$–preimage of $\beta(x,y) = T_5^2(x)$ on $X(\cos\frac{3\pi}{10})$

than before. This D^σ looks like Figure 11 (as always up to homeomorphism, and opposite edges have again to be identified to obtain the dessin on a torus).

EXAMPLE 5'. Conjugate the elliptic curve in Example 5 by

$$\sigma \in \mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q} \quad \text{with} \quad \sigma : \frac{1}{\sqrt[3]{2}} \mapsto \frac{e^{2\pi i/3}}{\sqrt[3]{2}}$$

getting X^σ with the equation

$$y^2 \;=\; x\,(x-1)\,(x \;-\; \frac{e^{2\pi i/3}}{\sqrt[3]{2}})$$

and the Belyi function $\beta(x,y) = 4x^3(1-x^3)$. The resulting dessin D^σ — see Figure 12 — is again different from D in Figure 5 (as before, up to homeomorphism and with identification of opposite sides).

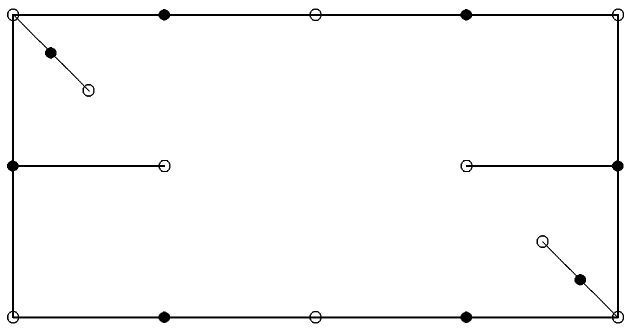

FIGURE 12. $\beta^{-1}[0,1]$ on the torus of Example 5'

What happens if we use instead the conjugate third root of unity? We will obtain an elliptic curve, complex conjugate to the present one, and it is not surprising that we get its dessin by reflection in one of the middle axes of Figure 12.

4.2. Invariants. Examples 4' and 5' show that D and D^σ are certainly not isomorphic but share many common properties like e.g. the (unordered) list of valencies or the numbers of white resp. black vertices or the number of cells. The proof of this invariance is straightforward if we consider how the Belyi function behaves under algebraic conjugation of the constants. It does not matter that X or β are defined over $\overline{\mathbb{Q}}$, only their existence (part B in Theorem 2 and 3) are important. We can state this invariance as follows.

PROPOSITION 7. *Let X be a smooth algebraic curve in $\mathbb{P}^n(\mathbb{C})$ with Belyi function β and corresponding dessin D. For the passage to D^σ under field automorphisms σ of $\mathbb{C}$ we have the following invariants:*

- *the valencies of white vertices (resp. black vertices, resp. cells),*
- *the number of white vertices with given valency (resp. black vertices, resp. cells),*
- *the genus of X,*
- *the isomorphism class of the automorphism group of X,*
- *regularity and uniformity.*

[JSt] contains a detailed proof and a much more general statement about the invariance of the cartographic group. Some more Galois invariants are known, see [Z1] and [StWo], but we seem to be far from having a complete list.— The next proposition shows how interesting these Galois actions are.

PROPOSITION 8. *Let $\mathbb{D}$ be the set of dessins with one cell for a fixed genus $g \geq 0$. Then $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$ acts faithfully on $\mathbb{D}$.*

A second look to Examples 4, 4', 5, 5' should make clear that this claim is true for genus 1. It relies on the fact that elliptic curves can be defined over the field $\mathbb{Q}(j)$ generated by the value of its j invariant, and that we can construct a Belyi function defined as well over $\mathbb{Q}(j)$ and having only one pole. Leonardo Zapponi extended this fact to higher genera by a covering argument (unpublished). Surprisingly, the proposition is even true for genus 0, i.e. for trees in $\overline{\mathbb{C}}$. The proof, written up by Leila Schneps [Sn] following an idea of H.W. Lenstra jr., is tricky but not difficult.

So dessins d'enfants become a wonderful playground for the absolute Galois group. In Grothendieck's ideas [G] they are — classifiying coverings of $\mathbb{P}^1$ minus three points — only the first step for what we call now the *Grothendieck–Teichmüller Lego* what should give a better understanding of $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$, compare [Sn], [LoSn1], [LoSn2], [Lu], [Oe] and [HS]. In the sequel we will however concentrate on the meaning of dessins and Galois actions for the curve X itself.

4.3. Moduli field and field of definition.

DEFINITION 4. Let D be a dessin on the smooth algebraic curve $X \subset \mathbb{P}^n(\mathbb{C})$. The *moduli field* $M(D)$ of D is the fixed field of the subgroup $U(X, \beta, \mathrm{id})$ of all field automorphisms σ of $\mathbb{C}$ with the property that D is isomorphic to D^σ, i.e. for which there is an isomorphism $f_\sigma : X \to X^\sigma$ such that

$$\beta = \beta^\sigma \circ f_\sigma$$

where $\beta : X \to \mathbb{P}^1$ denotes the Belyi function for D and β^σ its σ–conjugate. In the same way we define subgroups $U(X, \pi, \mathrm{id}) \subseteq \mathrm{Aut}\,\mathbb{C}$ for other covering maps $\pi : X \to \mathbb{P}^1$ instead of β. Similarly, the moduli field $M(X)$ of the curve X is the fixed field of the group

$$U(X) := \{\sigma \in \mathrm{Aut}\,\mathbb{C} \,|\, X^\sigma \cong X\} .$$

A *field of definition* of X is every field F containing the coefficients of the defining equations of a curve isomorphic to X (see Section 2.1), and a *field of definition* of D is every field over which we can define X and the corresponding Belyi function β.
For the following it will be useful to introduce even a further moduli field $M(X, \beta)$ for the *Belyi pair* (X, β) as the fixed field of the subgroup $U(X, \beta)$ of all $\sigma \in U(X)$ for which there are isomorphisms f_σ and g_σ with the property

$$f_\sigma : X \to X^\sigma , \quad g_\sigma : \mathbb{P}^1 \to \mathbb{P}^1 , \quad \beta^\sigma \circ f_\sigma = g_\sigma \circ \beta .$$

Then we call the Belyi pairs $(X, \beta), (X^\sigma, \beta^\sigma)$ *weakly isomorphic.* Note that in the definition of $U(X, \beta, \mathrm{id})$, i.e. of $M(D)$, we admit only the identity in the place of g_σ.

PROPOSITION 9. *Let $X \subset \mathbb{P}^n(\mathbb{C})$ be a smooth algebraic curve with dessin d'enfant D and corresponding Belyi function β. Then*

1. *$M(X)$ depends only on the isomorphism class of X,*
2. *$M(D)$ depends only on the isomorphism class of D,*
3. *$M(X) \subseteq M(X, \beta) \subseteq M(D)$,*
4. *$M(D)$, $M(X, \beta)$ and $M(X)$ are number fields,*
5. *every field of definition of X (resp. of D) contains the moduli field.*

PROOF. 1. Let $i : X \to Y$ be an isomorphism and $\sigma \in U(X)$, in other words suppose that there is an isomorphism $f_\sigma : X \to X^\sigma$, then $i^\sigma \circ f_\sigma \circ i^{-1}$ is an isomorphism $Y \to Y^\sigma$, i.e. $U(Y) \subseteq U(X)$. The converse inclusion is proved in the same way, whence $M(X) = M(Y)$. The proof of the second claim is similar.
3. follows from

$$U(X) \supseteq U(X, \beta) \supseteq U(X, \beta, \mathrm{id}) .$$

4. There are only finitely many possibilities to draw dessins d'enfants with a given list of valencies on an oriented 2–manifold of given genus. By Proposition 7, the orbit of D under the action of $\mathrm{Aut}\,\mathbb{C}$ is therefore finite. Another possibility is the use of Theorem 3: by a standard result of combinatorial group theory a given triangle group contains only finitely many subgroups of given index (= degree of the Belyi function, hence also invariant under $\mathrm{Aut}\,\mathbb{C}$). Consequently the subgroup $U(D)$ sending D to isomorphic dessins is of finite index in $\mathrm{Aut}\,\mathbb{C}$. It is easy to see that its fixed field $M(D)$ is a number field.
5. According to 1. we can replace X by a model defined over a field of definition L, then $U(X)$ contains all σ fixing L elementwise. A similar argument applies to D.

4.4. Remarks about B) $\Rightarrow$ A). This direction of the PROOF of Theorem 2 would be a consequence of the last proposition if we knew that the curve X can be defined over $M(X)$. Unfortunately this is not true in general. Interesting counterexamples were given by Earle [Ea] and Shimura [Sh], see also [DE]. They all have in common that X can be isomorphic to its complex conjugate curve without having a model defined over the reals. However, sufficient for Theorem 2 is a much weaker property:

PROPOSITION 10. *The curve X can be defined over a finite extension of its moduli field $M(X)$.*

Even that simpler statement is surprisingly difficult to prove. The reader is referred in the literature often to Weil's Theorem 4 in [W] but nowhere an explanation is given how to apply Weil's results. His ideas (see next section) stand certainly behind any reasonable proof, but for a modern and convincing treatment one should refer to [HH], [De] or to Bernhard Köck's paper [K] which gives even upper bounds for the degree of the field of definition, and also some history of the problem and translation hints how to pass from the language of schemes to polynomial equations. His presentation is optimal, so I omit a PROOF of this proposition.

4.5. Conditions for "moduli field = field of definition". We will however care about some more specialized versions of Proposition 10 by the following reason. Proposition 3 suggests that all properties of curves X defined over $\overline{\mathbb{Q}}$ should be somehow encoded in its dessin — which is not uniquely defined, of course, see Section 2. One may imagine that it has impact on automorphism groups, and that Weierstrass points could have to do something with vertices of dessins, see [SW], but properties of deeper nature lead to fascinating problems. In the following, we will concentrate on the determination of a (minimal, if possible) field of definition for X. The easiest way to see that X can be defined over the rationals, say, would be to have a dessin D on X uniquely determined by its Galois invariants, see Proposition 7, implying $M(D) = \mathbb{Q} = M(X)$ (we will see that such examples exist). Then we were done if we could prove that X can be defined over its field of moduli. A good criterion to do so is Theorem 1 of Weil [W]; we state it in a special form only.

PROPOSITION 11. *Suppose $X \subset \mathbb{P}^n(\mathbb{C})$ to be a smooth algebraic curve defined over a finite extension L of its moduli field $M := M(X)$. This field M is a field of definition for X if for every $\sigma \in \mathrm{Gal}\,\overline{M}/M$ there is an isomorphism*

$$f_\sigma \; : \; X \; \to \; X^\sigma$$

defined over L such that for all $\sigma, \tau \in \mathrm{Gal}\,\overline{M}/M$ the compatibility condition

$$f_{\tau\sigma} \; = \; f_\sigma^\tau \circ f_\tau$$

holds. An analogous statement is true for moduli fields and fields of definition of dessins (here the f_σ have to satisfy in addition $\beta = \beta^\sigma \circ f_\sigma$).

Together with the fact that such a curve can always be defined over a finite extension of its moduli field, Weil's criterion has the following nice and well–known consequence in all cases where f_σ is uniquely determined by σ. Since two such isomorphisms f_σ, f'_σ arise from each other by composition with an automorphism, we conclude

PROPOSITION 12. *A smooth algebraic curve $X \subset \mathbb{P}^n(\mathbb{C})$ with trivial automorphism group $\mathrm{Aut}\,X = \{\mathrm{id}\}$ can be defined over its field of moduli.*

This proposition shows in particular that "generic" curves of genus $g > 2$ are defined over their moduli fields. This is true also for the other extreme.

PROPOSITION 13. *Smooth algebraic curve $X \subset \mathbb{P}^n(\mathbb{C})$ of genus 0 and 1 can be defined over their field of moduli.*

The case $g = 0$ is trivial since $X \cong \mathbb{P}^1$ can be defined over $\mathbb{Q}$, and for $g = 1$ recall that the isomorphism class of an elliptic curve X is characterized by its j–invariant which can be calculated from any model for X, whence the moduli field is $M = \mathbb{Q}(j)$. On the other hand it is well known how to write down an equation for X with coefficients in $\mathbb{Q}(j)$.
For the intermediate case $g = 2$ all curves are hyperelliptic, i.e. have at least one nontrivial automorphism, on the other hand their moduli theory is already complicated. Explicit results were given by Mestre [Me].

4.6. Quasiplatonic curves. Another extreme contrast to the curves considered in Proposition 12 are the *quasiplatonic curves* or *quasiplatonic surfaces*, in older literature called *surfaces with many automorphisms* [Wo1]. They can be defined in many different ways by the following properties, see also [StWo].

THEOREM 4. *Let* $N\backslash\mathbb{H} \cong X \subset \mathbb{P}^n(\mathbb{C})$ *be a smooth algebraic curve of genus* $g > 1$ *with universal covering group* $N \subset \mathrm{PSL}_2\mathbb{R}$ *. The following statements are equivalent.*

1. *The lifts of all automorphisms of* X *to the upper half plane* $\mathbb{H}$ *form a triangle group* Δ *.*
2. N *is a normal subgroup of a triangle group* Δ *.*
3. X *has a regular dessin.*
4. *There is a Belyi function on* X *defining a normal (ramified) covering* $\beta : X \to \mathbb{P}^1(\mathbb{C})$ *.*
5. $(\mathrm{Aut}\, X)\backslash X \cong \mathbb{P}^1$ *, and the canonical projection*
$$X \;\to\; (\mathrm{Aut}\, X)\backslash X$$
is ramified above at most three points.
6. *All deformations* X' *sufficiently near to* X *in the moduli space of compact Riemann surfaces of genus* g *are either isomorphic to* X *or have a strictly smaller automorphism group than* X *.*

SIDE REMARKS. Recall that Proposition 6 gives other properties equivalent to statement 3.
The tesselation of the upper half plane $\mathbb{H}$ by the usual fundamental domains of Δ induces via statement 2 a tesselation of X by (double) geodesic triangles. The automorphism group Δ/N acts transitively on these double triangles — like the action of the symmetry group of a platonic solid on the induced grid of triangles on the Riemann sphere $\overline{\mathbb{C}}$, hence the name “quasiplatonic”. Famous examples for such surfaces are the Fermat curves of exponent $n > 3$ having an universal covering group N normal in the triangle groups $< 2, 3, 2n >$, and the *Hurwitz curves* whose automorphism group have the order $84(g-1)$ — the maximal possible order according to Hurwitz. These are characterized by the fact that their universal covering groups N are normal in $< 2, 3, 7 >$.

For the PROOF of Theorem 4 recall that X as compact Riemann surface of genus > 1 has only finitely many automorphisms and that all automorphisms of X lift to elements of $\mathrm{PSL}_2\mathbb{R}$ acting on $\mathbb{H}$. All these lifts form a Fuchsian group Δ containing N as normal subgroup with $\mathrm{Aut}\, X \cong \Delta/N$. The implications $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 2$ follow from Theorem 3, its proof, and from the considerations in the beginning of Section 3.4. For $2 \Rightarrow 1$ observe that Δ/N acts as a group of automorphisms of $X = N\backslash\mathbb{H}$, so the full automorphism group $\mathrm{Aut}\, X$ lifts to the upper half plane $\mathbb{H}$ as a supergroup $\overline{\Delta} \supseteq \Delta$ of finite index, and it is a classical fact that $\overline{\Delta}$ is a triangle group as well. $1 \Rightarrow 5$ follows from $\mathrm{Aut}\, X \cong \Delta/N$, so the canonical projection is just
$$N\backslash\mathbb{H} \;\to\; \Delta\backslash\mathbb{H}\,,$$

and $5 \Rightarrow 4$ is obvious. The equivalence $1 \Leftrightarrow 6$ results from the fact that deformations of X preserving its automorphism group (or its order) induce deformations of the covering group N and its extension Δ by the liftings of the automorphisms. Triangle groups are the only Fuchsian groups not admitting proper deformations ([Wo1]).

COROLLARY 1. *Every smooth algebraic curve $Y \subset \mathbb{P}^n(\mathbb{C})$ defined over a number field is a quotient of some quasiplatonic curve X by a subgroup of its automorphism group* $\mathrm{Aut}\, X$.

PROOF. According to Theorem 3, write Y as a quotient $\Gamma\backslash\mathbb{H}$ with a subgroup Γ of some Fuchsian triangle group Δ . There is a normal torsion free subgroup N of Δ contained in Γ, so we may take $X = N\backslash\mathbb{H}$. We can give these choices more precisely as follows ([Wo2]).

COROLLARY 2. *Let the Riemann surface Y have a dessin D with algebraic hypermap group (G, w, b) . Then, Y is the quotient $H\backslash X$ of a quasiplatonic curve X by a subgroup $H \subseteq \mathrm{Aut}\, X$ where $G \cong \mathrm{Aut}\, X$ and H is isomorphic to the stabilizer subgroup in G of an edge of D .*

4.7. The fields of definition of quasiplatonic curves. We call the projection β in statement 5 of Theorem 4 *canonical* because it is uniquely determined by X up to the identification of $(\mathrm{Aut}\, X)\backslash X$ with $\mathbb{P}^1$. In the terminology of Section 4.3 — observe that in the definition of $U(X, \beta)$ the fractional linear transformation g_σ is uniquely determined by $\beta, \beta^\sigma, f_\sigma$ — we have therefore

LEMMA 4. *$M(X) = M(X, \beta)$ for quasiplatonic surfaces and their canonical Belyi functions.*

Another important observation is the following ([CH], [DE], [Wo1])

PROPOSITION 14. *Let $\pi : X \to \mathbb{P}^1$ be a normal (ramified) covering map, let M be the fixed field of $U(X, \pi, \mathrm{id})$, see Definition 4, and suppose that the critical values of π, i.e. the images of the ramification points, are invariant under $U(X, \pi, \mathrm{id})$. Then X and π can be defined over M.*
In particular, a quasiplatonic curve X and its canonical Belyi function β with critical values $0, 1, \infty$ can be defined over $M(D)$.

PROOF. Choose some non–critical $x_0 \in \mathbb{P}^1(M)$ whose π–preimages in X form a G–orbit Gx under the covering group G of π, for some fixed x in this fibre. By definition we have for every $\sigma \in U(X, \pi, \mathrm{id})$ an isomorphism

$$f_\sigma \; : \; X \; \to \; X^\sigma \quad \text{with} \quad \pi^\sigma \circ f_\sigma \; = \; \pi \; .$$

Now $x_0 \in \mathbb{P}^1(M)$, and G acts transitively on the fibre $\pi^{-1}(x_0)$, so we can choose f_σ such that $f_\sigma(x) = \sigma(x) \in (\pi^\sigma)^{-1}(x_0) \subset X^\sigma$, and by this choice f_σ is uniquely determined. Moreover the compatibility criterion of Weil's criterion (Prop.11) is easily seen to be satisfied whence the claim follows.

We will see that this Proposition clearifies the situation in other important cases with hypotheses opposite to Proposition 12.

Theorem 5. *Every quasiplatonic curve can be defined over its field of moduli.*

Remark. Recall the problems discussed in the beginning of Section 4.5. For every genus (> 1) there are only finitely many quasiplatonic curves, and for low genera they are even uniquely determined by their automorphism groups and the ramification data of their canonical Belyi functions. Theorem 5 together with Proposition 7 implies therefore that all these curves can be defined over $\mathbb{Q}$ (for lists of quasiplatonic curves up to genus 4 see [Wo2]). Even in much more complicated higher genera cases Theorem 5 is an important tool to determine the (minimal) field of definition, see [St2], [StWo], [ScSm].

Proof of Theorem 5 (I learned from Bernhard Köck that the proof given in [Wo1] is incomplete). By Proposition 14, X can be defined over $M(D)$ where D is the regular dessin arising from the canonical Belyi function

$$\beta \;:\; X \;\to\; (\mathrm{Aut}\, X)\backslash X \;\cong\; \mathbb{P}^1(\mathbb{C})$$

with critical values $0, 1, \infty$. Lemma 4 and Proposition 9.3 say

$$M(X) \;=\; M(X, \beta) \;\subseteq\; M(D)\;,$$

so it would be sufficient to show that the extension $M(D)/M(X,\beta)$ is trivial. "Generically" this is true:

Lemma 5. *Under these conditions, suppose that the ramification orders p, q, r of β are pairwise different. Then $M(D) = M(X)$.*

It is sufficient to prove $U(X,\beta) = U(X,\beta,\mathrm{id})$. In fact, suppose $\sigma \in U(X,\beta)$ (see Def. 4), in other words (X,β) and (X^σ,β^σ) are weakly isomorphic, i.e. we have isomorphisms f_σ and g_σ with the property

$$f_\sigma \;:\; X \;\to\; X^\sigma\;, \quad g_\sigma \;:\; \mathbb{P}^1 \;\to\; \mathbb{P}^1\;, \quad \beta^\sigma \circ f_\sigma \;=\; g_\sigma \circ \beta\;,$$

which implies $g_\sigma = \mathrm{id}$ by the following reason. Proposition 7 shows that β^σ has the same ramification orders as β above $0, 1, \infty$. Since these are pairwise different, f_σ has to map the set $\beta^{-1}(0)$ of zeros onto the set of zeros $(\beta^\sigma)^{-1}(0)$, and the same argument works for $\beta^{-1}(1)$ and $\beta^{-1}(\infty)$. Therefore g_σ has to be a Möbius transformation fixing $0, 1, \infty$, hence $g_\sigma = \mathrm{id}$ for all $\sigma \in U(X,\beta)$, in other words $U(X,\beta) \subseteq U(X,\beta,\mathrm{id})$. The other inclusion $U(X,\beta) \supseteq U(X,\beta,\mathrm{id})$ is trivial.

If p,q,r are not pairwise different, these arguments are no longer valid. It can happen that f_σ, $\sigma\in U(X,\beta)$, maps the fiber triple of critical values

$$(\beta^{-1}(0),\beta^{-1}(1),\beta^{-1}(\infty)) \;\mapsto\; ((\beta^\sigma)^{-1}(\tau_\sigma(0)),(\beta^\sigma)^{-1}(\tau_\sigma(1)),(\beta^\sigma)^{-1}(\tau_\sigma(\infty))$$

where τ_σ denotes a nontrivial permutation of the critical values, see the examples given in [StWo]. The strategy of the proof is now to replace β by a Belyi function π with a non–standard normalization of its critical values. We will choose this normalization in such a way that the Galois actions on the critical values and on their fibers are compatible.
By Definition 4 of $U(X,\beta)$, the permutation τ_σ is the restriction of g_σ to $\{0,1,\infty\}$, and g_σ is uniquely determined by τ_σ. Recall that f_σ is unique up to composition with an automorphism $\alpha\in\operatorname{Aut}X^\sigma$, and that $\beta^\sigma\circ\alpha=\beta^\sigma$. This implies the first two statements of

LEMMA 6. *Let X be quasiplatonic with canonical Belyi function β and suppose $\sigma\in U(X,\beta)$.*

1. *On the set $\{0,1,\infty\}$ of critical values of β we have $\tau_\sigma=\beta^\sigma\circ f_\sigma\circ\beta^{-1}$.*
2. *The permutation τ_σ depends only on $\sigma\in U(X,\beta)$, not on the choice of f_σ.*
3. *If S_3 denotes the permutation group of $\{0,1,\infty\}$, the map*

   $$U(X,\beta)\;\to\;S_3\;:\;\sigma\;\mapsto\;\tau_\sigma$$

   defines an antihomomorphism with kernel $U(X,\beta,\mathrm{id})$.
4. *$M(D)/M(X)$ is a Galois extension.*
5. *τ_σ depends only on the restriction of σ to $M(D)$ and defines an injective antihomomorphism*

   $$\operatorname{Gal}M(D)/M(X)\;\to\;S_3\;:\;\sigma\;\mapsto\;\tau_\sigma\,.$$

For the PROOF of point 3. recall that τ_σ is a restriction of g_σ and that this g_σ is a fractional linear transformation with rational coefficients. For all $\sigma,\omega\in U(X,\beta)$ we have therefore

$$g_{\sigma\omega}\;=\;g_\omega^\sigma\circ g_\sigma\;=\;g_\omega\circ g_\sigma\,.$$

By Proposition 9.4 we know that $M(D)$ and $M(X)$ are number fields. Then 4. and 5. follow from Galois theory if we restrict σ to $\overline{\mathbb{Q}}$.

Therefore the field extension $M(D)/M(X)$ is either trivial or cyclic of order 2 or 3 or of order 6 with Galois group S_3 (I know no example for the last possibility). We continue the proof of Theorem 5 by changing the usual normalization of β.

LEMMA 7. *Under the same hypotheses as in Lemma 6 suppose w.l.o.g. (see Prop.14) that X and β are defined over $M(D)$. Then there exists a* *fractional linear transformation* μ *and isomorphisms* f_σ *such that*

$$(\mu \circ \beta)^\sigma \circ f_\sigma \;=\; \mu^\sigma \circ \beta^\sigma \circ f_\sigma \;=\; \mu \circ \beta$$

for all $\sigma \in \mathrm{Gal}\, M(D)/M(X)$, *and such that the set* $\mu\{0,1,\infty\}$ *of critical values of* $\mu \circ \beta$ *is invariant under* $\mathrm{Gal}\, M(D)/M(X)$.

PROOF. From Lemma 4 we know $M(X) = M(X,\beta)$, hence the existence of isomorphisms f_σ and $g_\sigma = \beta^\sigma \circ f_\sigma \circ \beta^{-1}$ for all $\sigma \in \mathrm{Gal}\, M(D)/M(X)$. These g_σ are uniquely determined by τ_σ. It is therefore sufficient to choose μ such that the invariance condition on the critical values $\mu(0), \mu(1), \mu(\infty)$ is satisfied and that — restricted to $0, 1, \infty$ —

$$(\mu \circ \beta)^\sigma \circ f_\sigma \circ \beta^{-1} \;=\; \sigma \circ \mu \circ \beta^\sigma \circ f_\sigma \circ \beta^{-1} \;=\; \sigma \circ \mu \circ \tau_\sigma \;=\; \mu\ .$$

This can be done with a case–by–case analysis of the different possibilities for the Galois group in question. For $M(D) = M(X)$ we may take $\mu = \mathrm{id}$. For quadratic extensions and the nontrivial conjugation σ suppose e.g. that the corresponding permutation is

$$\tau_\sigma(0,1,\infty) \;=\; (1,0,\infty)\ .$$

Then choose μ such that

$$\mu(\infty) \;=\; \infty\ , \quad \sigma(\mu(0)) \;=\; \mu(1) \in M(D)$$

to satisfy the claim. If $M(D)/M(X)$ is cyclic of order 3, choose μ such that $\mu(0), \mu(1), \mu(\infty)$ form a normal basis of the field extension. We can fix the order of the three points such that for all $\sigma \in \mathrm{Gal}\, M(D)/M(X)$ the composite map satisfies $\sigma \circ \mu \circ \tau_\sigma = \mu$.
The same construction principle works for S_3–extensions: one has to choose μ such that $\sigma \circ \mu = \mu \circ \tau_\sigma^{-1}$ on $0, 1, \infty$. This can be performed either with some representation theory — the Galois action of S_3 on a normal basis defines a regular representation containing a permutation representation as rational subrepresentation — or by fixing $\mu(0), \mu(1), \mu(\infty)$ as roots of an irreducible cubic polynomial generating the (non–normal, conjugate) cubic subfields of $M(D)/M(X)$.

END OF THE PROOF of Theorem 5. Let π denote the normal covering

$$\pi \;=\; \mu \circ \beta \;:\; X \;\to\; \mathbb{P}^1(\mathbb{C})$$

with μ constructed in Lemma 7. It says that $M(X)$ is the fixed field of $U(X, \pi, \mathrm{id})$ with critical values of π invariant under the action of this group. Therefore, Theorem 5 follows from Proposition 14.

5. Open questions

For important questions concerning the Grothendieck–Teichmüller Lego, Moduli Spaces, Physics and Inverse Galois Theory the reader should consult [LoSn2], [MM], [Lu], [Oe] or [HS]. Here I will enumerate some other open problems, most of them hidden in the preceding sections.

1. Quasiplatonic curves have canonical Belyi functions, and also on curves with uniform dessins we can define some sort of "canonical" Belyi functions. But is there a notion of *canonical* in general? More generally: are different dessins on the same curve somehow related? Is it possible to obtain them by a finite class of procedures from a given canonical one? If one restricts to the very special case of regular dessins, there is a rather complete knowledge by [Si2], [Gi], [GiWo].

2. Find a complete collection of Galois invariants for dessins! Still we have very few examples for actions of nonabelian Galois groups, and even for Belyi pairs defined over abelian extensions of $\mathbb{Q}$ it is an open question if the known invariants ([JSt], [StWo], [Z1]) are sufficient, or how to complete them.

3. As far as I know, all known curves not definable over their moduli field can be defined over quadratic extensions of this moduli field. Is this always true? Proof or counterexample needed!

4. The number of isomorphism classes of quasiplatonic curves (or regular dessins) for given genus g seems to depend on g in a rather irregular way. Is there a reasonable asymptotic behaviour, maybe a growth function of some meanvalue? This could be a problem for analytic number theory, but also for group theory or graph theory! [dFIt], [MSS], [MSP] or [SPW] give some hints. Caution: the problems *for quasiplatonic curves* and *for regular dessins* are certainly related but not the same: a quasiplatonic curve can have several regular dessins, see [Si2], [Gi], [GiWo].

5. How to detect deeper properties of curves in the dessins, e.g. how to see that the Jacobian is of CM type? There are very few attempts to answer this question in [Wo2], [Wo3], [St3], but even for elliptic curves we have no convincing answers.

6. How to generalize Belyi functions and dessins to higher dimensions? Despite some recent progress ([Br], [We], [Go]) we are far from a good understanding. Here is a nice elementary question with a onedimensional flavour: *suppose that the curve X has a moduli field of transcendence degree*

k. Does a meromorphic function exist on X ramified above at most k + 3 points?

References.

[BaIt] M. Bauer, Cl. Itzykson: *Triangulations*, pp.179–236 in [Sn]

[B1] G.V. Belyĭ: *On Galois Extensions of a Maximal Cyclotomic Field*, Math. USSR Izvestija 14 (1980), 247–265

[B2] G.V. Belyĭ: *Another proof of the three points theorem*, Preprint Bonn 1997.

[Bi] B. Birch: *Noncongruence Subgroups, Coverings and Drawings*, pp.25–46 in [Sn]

[Bo] A. Borel: *Commensurability classes and volumes of hyperbolic 3–manifolds*, Ann. Schuola Norm. Sup. Pisa (Ser. IV) 8 (1981), 1–33

[BS] Ph.L. Bowers, K. Stephenson: *Uniformizing Dessins and Belyĭ Maps via Circle Packing*, Memoirs of the AMS 805, Vol. 170, 2004

[Br] V. Braungardt: *Überlagerungen von Modulräumen für Kurven*, PhD Thesis, Karlsruhe 2001

[Chu] D.V. Chudnovsky, G.V. Chudnovsky: *Computer algebra in the service of mathematical physics and number theory*, pp. 109–232 in *Computers and Mathematics*, Proceedings Stanford 1986, Lecture Notes in Pure and Applied Mathematics 125, Dekker 1990.

[CIW] P. Cohen, Cl. Itzykson, J. Wolfart: *Fuchsian Triangle Groups and Grothendieck Dessins: Variations on a Theme of Belyi*, Commun. Math. Phys. 163 (1994), 605–627

[CoWo] P. Cohen, J. Wolfart: *Dessins de Grothendieck et variétés de Shimura*, C.R. Acad. Sci. Paris 315 (Sér.I) (1992), 1025–1028

[CH] K. Coombes, D. Harbater: *Hurwitz families and arithmetic Galois groups,* Duke Math. J. 52 (1985), 821–839

[DE] P. Dèbes, M. Emsalem: *On Fields of Moduli of Curves,* J. Algebra 211 (1999), 42–56

[De] G. Derome: *Descente algébriquement close*, J. Algebra 266 (2003), 418–426

[dFIt] P. di Francesco, C. Itzykson: *A generating function for fatgraphs*, Ann. Inst. H. Poincaré, Phys. th., 59 (1993), 117–139

[Ea] C.J. Earle: *On the Moduli of Closed Riemann Surfaces with Symmetries*, pp. 119–130 in L.V. Ahlfors et al.: *Advances in the Theory of Riemann Surfaces*, Ann. of Math. Studies 66, Princeton 1971

[El] N. Elkies: *ABC implies Mordell*, Internat. Math. Res. Notices 1991, no. 7, 99–109

[Gi] E. Girondo: *Multiply quasiplatonic Riemann surfaces*, Experimental Mathematics 12 (4) (2003), 463–475

[GiWo] E. Girondo, J. Wolfart: *Conjugators of Fuchsian groups and quasiplatonic surfaces*, to appear in Quarterly J. Math., `http://www.math.uni-frankfurt.de/~wolfart`

[Go] G. González–Diez: *Around Belyi's Theorem. The Case of Complex Surfaces*, preprint 2004

[G] A. Grothendieck: *Esquisse d'un Programme*, pp. 5–48 in [LoSn1]

[HH] H. Hammer, F. Herrlich: *A Remark on the Moduli Field of a Curve*, Arch. Math. 81 (2003), 5–10

[HS] D. Harbater, L. Schneps: *Fundamental groups of moduli spaces and the Grothendieck–Teichmüller group*, Trans. Am. Math. Soc. 352 (2000) no. 7, 3117–3148

[JS1] G. Jones, D. Singerman: *Theory of maps on orientable surfaces*, Proc. London Math. Soc. (3) 37 (1978), 273–307

[JS2] G. Jones, D. Singerman: *Maps, hypermaps and triangle groups*, pp. 115-145 in [Sn]

[JS3] G. Jones, D. Singerman: *Belyi Functions, Hypermaps and Galois Groups*, Bull. London Math. Soc. 28 (1996), 561–590

[JSt] G. Jones, M. Streit: *Galois groups, monodromy groups and cartographic groups*, pp. 25–65 in [LoSn2]

[Ka] S. Katok: *Fuchsian Groups*, Chikago 1992

[K] B. Köck: *Belyi's Theorem Revisited*, Beiträge zur Algebra und Geometrie 45 (2004), 253–275

[LZ] S.K. Lando, A.K. Zvonkin: *Graphs on Surfaces and Their Applications, with an appendix by* D. Zagier, Enc. of Math. Sc. Vol. 141, Springer 2004

[La] S. Lang: *Die abc–Vermutung*, Elemente der Math. 48 (1993), 89–99

[LoSn1] P. Lochak, L. Schneps: *Geometric Galois Actions 1. Around Grothendieck's Esquisse d'un Programme*, London Math. Soc. Lecture Note Ser. 242, Cambridge UP 1997

[LoSn2] P. Lochak, L. Schneps: *Geometric Galois Actions 2. The Inverse Galois Problem, Moduli Spaces and Mapping Class Groups*, London Math. Soc. Lecture Note Ser. 243, Cambridge UP 1997

[Lu] F. Luo: *Grothendieck's reconstruction principle and 2–dimensional topology and geometry*, Commun. Contemp. Math. 1 (1999), no. 2, 125–153

[MR] C. Maclachlan, A.W. Reid: *The Arithmetic of Hyperbolic 3–Manifolds*, Springer GTM 219, 2003

[MM] G. Malle, B.H. Matzat: *Inverse Galois Theory*, Springer 1999

[MaVo] J. Malgoire, C. Voisin: *Cartes Cellulaires*, Cahiers Mathématiques de Montpellier 12 (1977)

[Mas] R. Mason: *Diophantine equations over function fields*, London Math. Soc. LNS 96, Cambridge UP 1984

[Me] J.–F. Mestre: *Construction de courbes de genre 2 à partir de leurs modules*, pp. 313–334 in: Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., 94, Birkhäuser Boston, 1991

[MSS] St. Monni, J.S. Song, Y.S. Song: *The Hurwitz enumeration problem of branched covers and Hodge integrals*, J. Geometry and Physics 50 (2004), 223–256

[MSP] T.W. Müller, J.–Chr. Schlage–Puchta: *Normal growth of large groups, II*, to appear in Archiv der Mathematik

[Ni] A. Nitaj: `http://www.math.unicaen.fr/~nitaj/abc.html`

[Oe] J. Oesterlé: *Dessins d'enfants*, Sém. Bourbaki 2001–2002 no. 907, 285–305, Astérisque 290

[R] B. Riemann: *Theorie der abelschen Funktionen*, Journal für die Reine und Angewandte Mathematik 54 (1857), 115–155

[Ro] M. Rosen: *Number Theory in Function Fields*, Springer GTM 210, 2001

[SPW] J.–Chr. Schlage–Puchta, J. Wolfart: *How many quasi-platonic surfaces?*, manuscript,
`http://www.math.uni-frankfurt.de/~wolfart`

[ScSm] Th.A. Schmidt, K.M. Smith: *Galois Orbits of Principal Congruence Hecke Curves*, J. London Math. Soc. (3) 67 (2003), 673–685

[Schn] Th. Schneider: *Arithmetische Untersuchungen elliptischer Integrale*, Math. Ann. 113 (1937), 1–13

[Sn] L. Schneps (ed.): *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lecture Note Ser. 200, Cambridge UP 1994

[Sn2] L. Schneps: *Dessins d'enfants on the Riemann sphere*, pp.47–77 in [Sn]

[Se] M. Seppälä: *Myrberg's numerical uniformization for hyperelliptic curves*, Ann. Acad. Sci. Fenn. Math. 29 (2004), 3–20

[SV1] V.A. Voevodsky, G. Shabat: *Equilateral Triangulations of Riemann Surfaces and Curves over Algebraic Number Fields*, Soviet Math. Dokl. 39 (1989), 38–41

[SV2] G. Shabat, V.A. Voevodsky: *Drawing curves over number fields*, pp.199–227 in *The Grothendieck Festschrift III* (ed. P. Cartier et al.), Birkhäuser 1990

[Sh] G. Shimura: *On the Field of Rationality of an Abelian Variety*, Nagoya Math. J. 45 (1972), 167–178

[Si1] D. Singerman: *Automorphisms of maps, permutation groups and Riemann surfaces*, Bull. London Math. Soc. 8 (1976), 65–81

[Si2] D. Singerman: *Riemann Surfaces, Belyi Functions and Hypermaps*, pp. 43–68 in *Topics on Riemann Surfaces and Fuchsian Groups* (ed.: E. Bujalance, A.F. Costa, E. Martinez), London Math. Soc. LNS 287, Cambridge UP 2001

[SSy1] D. SINGERMAN, R.I. SYDDALL: *Belyi Uniformization of Elliptic Curves*, Bull. London Math. Soc. 139 (1997), 443–451

[SSy2] D. SINGERMAN, R.I. SYDDALL: *The Riemann Surface of a Uniform Dessin*, Beiträge zur Algebra und Geometrie 44 (2003), 413–430

[SW] D. SINGERMAN, P.D. WATSON: *Weierstrass Points on Regular Maps*, Geometriae Dedicata 66 (1997), 69–88

[Sto] W.W. STOTHERS: *Polynomial identities and hauptmoduln*, Quart. J. Math. (2) 32 (1981), 349–370

[St1] M. STREIT: *Homology, Belyi Functions and Canonical Curves*, Manuscripta Math. 90 (1996), 489–509

[St2] M. STREIT: *Field of definition and Galois orbits of Macbeath–Hurwitz curves*, Arch. Math. 74 (2000), 342–349

[St3] M. STREIT: *Period Matrices and Representation Theory*, Abh. Math. Sem. Hamburg 71 (2001), 279–290

[StWo] M. STREIT, J. WOLFART: *Characters and Galois invariants of regular dessins*, Revista Mat. Complutense 13 (2000), 1–33

[V] L. VASERSTEIN: *Quantum (abc)–theorems*, J. Number Theory 81 (2000), 351–368

[W] A. WEIL: *The field of definition of a variety,* Amer. J. Math. 78 (1956), 509–524

[We] A. WENG: *Endliche Überlagerungen von Varietäten und der Satz von Belyi*, PhD Thesis, Frankfurt 2004

[Wo0] J. WOLFART: *Mirror–invariant triangulations of Riemann surfaces, triangle groups and Grothendieck dessins: variations on a theme of Belyi*, Frankfurt 1992

[Wo1] J. WOLFART: *The 'Obvious' Part of Belyi's Theorem and Riemann Surfaces with Many Automorphisms*, pp. 97–112 in [LoSn1]

[Wo2] J. WOLFART: *Triangle groups and Jacobians of CM type,* manuscript, `http://www.math.uni-frankfurt.de/~wolfart`

[Wo3] J. WOLFART: *Regular Dessins, Endomorphisms of Jacobians, and Transcendence*, pp. 107–120 in *A Panorama of Number Theory or The View from Baker's Garden* (ed. G. Wüstholz), Cambridge UP 2002

[Za] U. ZANNIER: *On Davenport's bound for the degree of* $f^3 - g^2$ *and Riemann's Existence Theorem*, Acta Arithmetica 71 (1995), 107–137

[Z1] L. ZAPPONI: *Dessins d'enfants en genre 1*, pp. 79–116 in [LoSn2]

[Z2] L. ZAPPONI: *Le théorème de Belyi revisité*, preprint

JÜRGEN WOLFART, Mathematisches Seminar der Universität,
Postfach 11 19 32, D–60054 Frankfurt a. M.
`wolfart@math.uni-frankfurt.de`