CHEBYCHEFF AND BELYI POLYNOMIALS, DESSINS D'ENFANTS, BEAUVILLE SURFACES AND GROUP THEORY

I. BAUER, F. CATANESE, AND F. GRUNEWALD

Abstract. We start discussing the group of automorphisms of the field of complex numbers, and describe, in the special case of polynomials with only two critical values, Grothendieck's program of 'Dessins d' enfants', aiming at giving representations of the absolute Galois group. We describe Chebycheff and Belyi polynomials, and other explicit examples. As an illustration, we briefly treat difference and Schur polynomials. Then we concentrate on a higher dimensional analogue of the triangle curves, namely, Beauville surfaces and varieties isogenous to a product. We describe their moduli spaces, and show how the study of these varieties leads to new interesting questions in the theory of finite (simple) groups.

1. Introduction

This article is an extended version of the plenary talk given by the second author at the CIMMA 2005 in Almeria. It is intended for a rather general audience and for this reason we start with explaining very elementary and wellknown facts: we apologize to the expert reader, who will hopefully be satisfied by the advanced part.

We only give very selected proofs, and we often prefer to introduce concepts via examples in order to be selfcontained and elementary.

The general main theme of this article is the interplay between algebra and geometry. Sometimes algebra helps to understand the geometry of certain objects and vice versa. The absolute Galois group, i.e., the group of field automorphisms of the algebraic closure of $\mathbb{Q}$, which is a basic object of interest in algebraic number theory, is still very mysterious and since Grothendieck's proposal of "dessins d'enfants" people try to understand it via suitable actions on classes of geometrical objects. In this paper we address the simplest possible such action, namely the action of the absolute Galois group on the space of (normalized)

AMS Classification: 11S05, 12D99, 11R32, 14J10, 14J29, 14M99, 20D99, 26C99, 30F99.

Keywords: polynomials, Riemann existence theorem, monodromy, Galois group, dessins d'enfants, Belyi and Chebycheff, difference polynomials, algebraic surfaces, moduli spaces, Beauville surfaces, simple groups.

We would like to thank Fabio Tonoli for helping us with the pictures.

polynomials with exactly two critical values, and on some combinatorial objects related to them.
At the basis of such a correspondence lies the so called "algebraization" of (non constant) holomorphic functions $f : C \to \mathbb{P}^1$ from a compact Riemann surface C to the projective line: the Riemann existence theorem describes f completely through its set of critical values and the related monodromy homomorphism (the combinatorial object mentioned above).
The class of polynomials with two critical values is far from being understood, there are however two series of such polynomials, the so called Chebycheff polynomials, and the Belyi polynomials.
While the latter have a very simple algebraic description but are not so well known, the Chebycheff polynomials are ubiquitous in many fields of mathematics (probability, harmonic analysis,..) and everybody has encountered them some time (see e.g. [Riv74], [Riv90]).
We try to describe the Chebycheff polynomials from a geometric point of view, explaining its geometrical ties with the function $cos(z)$, which also has exactly two critical values (viz., ± 1). The group of symmetries for $cos(z)$ is the infinite dihedral group of transformations $z \mapsto \pm z + n, n \in \mathbb{Z}$, which has as fundamental domain an euclidean triangle of type $(2, 2, \infty)$, i.e., with angles $\frac{\pi}{2}, \frac{\pi}{2}, 0$.
Our complete mastering of the function $cos(z)$ allows us to achieve a complete and satisfactory description of the polynomials with finite dihedral symmetry, namely the Chebycheff polynomials.
This is a key idea for the program we address: the knowledge of the uniformizing triangular functions in the hyperbolic case (these are functions on the upper half plane, with group of symmetries determined by a hyperbolic triangle with angles $\frac{\pi}{m_1}, \frac{\pi}{m_2}, \frac{\pi}{m_3}$, cf. [Car54],part 7, chapter 2) sheds light on the class of the so called *triangle curves*, on which the absolute Galois group acts.
Triangle curves are pairs (C, f) of a curve C and a holomorphic Galois covering map $f : C \to \mathbb{P}^1$ ramified exactly over $\{0, 1, \infty\}$.
In fact, being ramified only in three points, triangle curves are *rigid* (i.e., they do not have any non trivial deformations) hence they are defined over $\overline{\mathbb{Q}}$. Belyi's famous theorem says almost the converse: every curve defined over $\overline{\mathbb{Q}}$ admits a holomorphic map $f : C \to \mathbb{P}^1$ ramified exactly over $\{0, 1, \infty\}$. Belyi's theorem in turn aroused the interest of Grothendieck to the possible application of this result to the construction of interesting representations of the absolute Galois group, on the set of the so called "dessins d'enfants", which we briefly describe in section 4.
Our main purpose is to explain how Grothendieck's sets of "dessins d'enfants" can be more conveniently replaced by the sets of fundamental groups of certain higher dimensional varieties X which admit an unramified covering which is isomorphic to a product of curves (these

are called *varieties isogenous to a product*). The Galois group acts transforming such a variety X to another variety of the same type, but whose fundamental group need not be isomorphic to the fundamental group of X.

The last chapter is thus devoted to an overview of [BCG05a], where the so-called *Beauville surfaces* are studied. Beauville surfaces are rigid surfaces which admit a finite unramified covering which is a product of two algebraic curves.

Giving a Beauville surface is essentially equivalent to giving two triangle curves with the same group G, and in such a way that G acts freely on the product of the two triangle curves.

Beauville surfaces (and their higher dimensional analogues) not only provide a wide class of surfaces quite manageable in order to test conjectures, but also show how close algebra and geometry are. The ease with which one can handle these surfaces is based on the fact that they are determined by discrete combinatorial data. Therefore one can translate existence problems, geometric properties etc. in a purely group theoretic language.

It was very fascinating for us that, studying Beauville surfaces, we found out that many geometric questions are closely related to some classical problems and conjectures in the theory of finite groups.

2. Field automorphisms

Let K be any field and let $\phi : K \to K$ be an automorphism of K: then, since $\phi(x) = \phi(1 \cdot x) = \phi(1) \cdot \phi(x)$, it follows that $\phi(1) = 1$, therefore $\phi(n) = n$ for all $n \in \mathbb{N}$. If K has characteristic 0, i.e., $n \neq 0$ for all n, thus $\mathbb{Q} \subset K$, then $\phi|_{\mathbb{Q}} = Id_{\mathbb{Q}}$.

The following exercise, quite surprising for first year students, asserts that the real numbers have no automorphisms except the identity, and the complex numbers have 'too many'.

Lemma 2.1. *1) $Aut(\mathbb{R}) = \{Id\}$;*
2) $|Aut(\mathbb{C})| = 2^{2^{\aleph_0}}$.

Proof. 1) $\phi(a^2) = \phi(a)^2$, thus ϕ of a square is a square, so ϕ carries the set of squares $\mathbb{R}_+$ to itself. In particular, ϕ is increasing, and since it is equal to the identity on $\mathbb{Q}$, we get that ϕ is the identity.
2) This follows from the fact that, if $\mathcal{B}$ and $\mathcal{B}'$ are two transcendency bases, i.e., maximal subsets of elements satisfying no nontrivial polynomial equations, then $\mathcal{B}$ and $\mathcal{B}'$ have the same cardinality $2^{\aleph_0}$, and for any bijection ϕ' between $\mathcal{B}$ and $\mathcal{B}'$ there exists an automorphism ϕ such that $\phi|_{\mathcal{B}} = \phi'$. *Q.E.D.*

Remark 2.2. *1) Part two of the previous lemma is essentially the theorem of Steinitz: two algebraically closed fields are isomorphic iff they have the same characteristic and the same absolute transcendence degree.*

2) In practice, the automorphisms of $\mathbb{C}$ *that we do understand are only the continuous ones, the identity and the complex conjugation* σ *(i.e.,* $\sigma(z) := \bar{z} = x - iy$*).*
3) The field of algebraic numbers $\overline{\mathbb{Q}}$ *is the set* $\{z \in \mathbb{C} | \exists P \in \mathbb{Q}[x] \setminus \{0\}, s.t.\ P(z) = 0\}$*. The fact that* $Aut(\mathbb{C})$ *is so large is due to the fact that the kernel of* $Aut(\mathbb{C}) \to Aut(\overline{\mathbb{Q}})$ *is very large.*
The group $Aut(\overline{\mathbb{Q}})$ *is called the* absolute Galois group *and denoted by* $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$*.*
Note that even if we have a presentation of a group G*, still our information about it might be quite scarce (even the question: "is the group nontrivial?" is hard to answer), and the solution is to have a* representation *of it, for instance, an action on a set* M *that can be very well described.*

Example 2.3. *The dihedral group* D_n *is best described through its action on* $\mathbb{C}$*, as the set of* $2n$ *transformations of the form* $z \mapsto \zeta z$*, where* $\zeta^n = 1$*, or of the form* $z \mapsto \zeta \bar{z}$*. We see immediately that the group acts as a group of permutations of the regular* $n-$*gon whose set of vertices is the set* μ_n *of* $n-$*th roots of unity* $\mu_n := \{\zeta | \zeta^n = 1\}$*.*
The group is generated by complex conjugation σ*, and by the rotation* $r(z) = exp(\frac{2}{n}\pi i)z$*, so its presentation is* $< r, \sigma | r^n = 1, \sigma^2 = 1, \sigma r \sigma = r^{-1} >$*.*

We end the section by invoking *Grothendieck's dream of dessins d' enfants (= children's drawings)*, which aims at finding concrete representations for the Galois Group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. We will try to explain some of the basic ideas in the next sections, trying to be as elementary as possible.
One can invoke as a catchword *moduli theory*, in order to soon impress the audience, but it is possible to explain everything in a very simple way, which is precisely what we shall do in the next sections, at least in some concrete examples.

3. Polynomials with rational critical values.

Let $P(z) \in \mathbb{C}[z]$, $P(z) = \sum_{i=0}^{n} a_i z^i$ be a polynomial of degree n.

Definition 3.1. *1)* $\zeta \in \mathbb{C}$ *is a* critical point *for* P *if* $P'(\zeta) = 0$*;*
2) $w \in \mathbb{C}$ *is a* critical value *for* P *if there is a critical point* ζ *for* P *such that* $w = P(\zeta)$*. Denote by* B_P *the set of critical values of* P*;* B_P *is called the* branch set *of* P*.*

Remark 3.2. *1)* $\phi \in Aut(\mathbb{C})$ *acts on* $\mathbb{C}[z]$*, by* $P(z) = \sum_{i=0}^{n} a_i z^i \mapsto \phi(P)(z) := \sum_{i=0}^{n} \phi(a_i) z^i$*.*
2) If $\zeta \in \mathbb{C}$ *is a critical point for* P*, then, since* $\sum_{i=0}^{n} i a_i \zeta^{i-1} = 0$*,* $\phi(\zeta)$ *is a critical point for* $\phi(P)$*. Similarly, if* $w \in \mathbb{C}$ *is a critical value for* P*, then* $\phi(w) = \phi(P(\zeta)) = \phi(P)(\phi(\zeta))$ *is a critical value for* $\phi(P)$*.*

Since for each $\phi \in Aut(\mathbb{C})$ we have $\phi(\mathbb{Q}) = \mathbb{Q}$, and $\phi(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}$, the class of polynomials $\{P | B_P \subset \overline{\mathbb{Q}}\}$, and $\{P | B_P \subset \mathbb{Q}\}$ are invariant under the action of $Aut(\mathbb{C})$.

Remark 3.3. *If $g : \mathbb{C} \to \mathbb{C}$, $g(z) = az + b$ is an invertible affine transformation, i.e., $a \neq 0$, then two* right affine equivalent *polynomials $P(z)$ and $P(g(z))$ are immediately seen to have the same branch set. In order not to have infinitely many polynomials with the same branch set, one considers the* normalized polynomials *of degree n:*

$$P(z) = z^n + a_{n-2} z^{n-2} + \cdots + a_0.$$

Any polynomial is right affine equivalent to a normalized polynomial, and two normalized polynomials are right affine equivalent iff they are equivalent under the group μ_n of n-th roots of unity, $P(z) \cong P(\zeta z)$ (i.e., $a_i \mapsto \zeta^i a_i$).

The usefulness of the above concept stems from the following

Theorem 3.4. *Let P be a normalized polynomial: then $P \in \overline{\mathbb{Q}}[z]$ if and only if $B_P \subset \overline{\mathbb{Q}}$.*

Proof. It is clear that $P \in \overline{\mathbb{Q}}[z]$ implies that $B_P \subset \overline{\mathbb{Q}}$.
Now, assume that $B_P \subset \overline{\mathbb{Q}}$ and observe that, by the argument of Steinitz, it suffices to show that $P \in \mathbb{C}[z]$ has only a finite number of transforms under the group $Aut(\mathbb{C})$.
Since a transform of a normalized polynomial is normalized, it suffices to show that the right affine equivalence class of P has only a finite number of transforms under the group $Aut(\mathbb{C})$.
Since the set $B_P \subset \overline{\mathbb{Q}}$ has only a finite number of transforms, it suffices to show that there is only a finite number of classes of polynomials having a fixed branch set B: but this follows from the well known Riemann's existence theorem, which we shall now recall. *Q.E.D.*

Theorem 3.5. *(Riemann's existence theorem) There is a natural bijection between:*
1) Equivalence classes of holomorphic mappings $f : C \to \mathbb{P}^1_{\mathbb{C}}$, of degree n and with branch set $B_f \subset B$, (where C is a compact Riemann surface, and $f : C \to \mathbb{P}^1_{\mathbb{C}}$, $f' : C' \to \mathbb{P}^1_{\mathbb{C}}$ are said to be equivalent if there is a biholomorphism $g : C' \to C$ such that $f' = f \circ g$).
2) Conjugacy classes of monodromy *homomorphisms $\mu : \pi_1(\mathbb{P}^1_{\mathbb{C}} - B) \to \mathcal{S}_n$ (here, $\mathcal{S}_n$ is the symmetric group in n letters, and $\mu \cong \mu'$ iff there is an element $\tau \in \mathcal{S}_n$ with $\mu(\gamma) = \tau \mu'(\gamma) \tau^{-1}$, for all γ).*
Moreover:
i) C is connected if and only if the subgroup $Im(\mu)$ acts transitively on $\{1, 2, \ldots n\}$.
ii) f is a polynomial if and only if $\infty \in B$, the monodromy at ∞ is a cyclical permutation, and $g(C) = 0$.

For a proof we refer to [Mir95], especially pp. 91,92.

Remark 3.6. *1) Assume that $\infty \in B$, so write $B := \{\infty, b_1, \dots b_d\}$. Then $\pi_1(\mathbb{P}^1_{\mathbb{C}} - B)$ is a free group generated by $\gamma_1, \dots \gamma_d$ and μ is completely determined by the local monodromies $\tau_i := \mu(\gamma_i)$.*
2) To give then a polynomial of degree n with branch set $B_P = \{b_1, \dots b_d\}$ it suffices to give nontrivial permutations $\tau_1, \dots \tau_d$ such that

$$\tau_1 \cdot \dots \cdot \tau_d = (1, 2, \cdots, n),$$

and such that, if we write each τ_j as a product of disjoint cycles of length m_{ij}, then $\sum_{i,j} m_{ij} = n - 1$.
3) Riemann's existence theorem holds more generally also for maps of infinite degree, and it was generalized by Grauert and Remmert (cf. [GR58]*) to describe locally finite holomorphic maps between normal complex spaces.*

4. Polynomials with two critical values

Observe that there is only one normalized polynomial of degree n with only 0 as critical value, namely $P(z) = z^n$. In fact, there is only one choice for τ_1: $\tau_1 = (1, 2, \cdots, n)$.
If we consider polynomials P with only two critical values, we shall assume, without loss of generality (and for historical reasons) that $B_P = \{-1, 1\}$ or $B_P = \{0, 1\}$.
We have to give two permutations τ_1, τ_2 such that $\tau_1 \cdot \tau_2 = (1, 2, \cdots, n)$. If τ_1 has a cycle decomposition of type $m_1, \dots, m_r$, τ_2 has a cycle decomposition of type $d_1, \dots, d_s$, then, counting the roots of the derivative of P, we find that

$$(**) \qquad \sum_j (m_j - 1) + \sum_i (d_i - 1) = n - 1.$$

Theorem 4.1. *There is only one class of a polynomial T_n of degree n, called* Chebycheff polynomial of degree n*, such that*
a) the critical values of T_n are just $\{-1, 1\}$,
b) the derivative of T_n has simple roots.
We have

$$T_n(z) = \sum_{2r \leq n} (-1)^r z^{n-2r} (1 - z^2)^r =$$

$$= cos(n(arcos(z))) = \frac{1}{2}((z \pm \sqrt{z^2 - 1}\ )^n + (z \pm \sqrt{z^2 - 1}\ )^{-n}).$$

Proof. By condition b), the permutations τ_1, τ_2 are a product of disjoint transpositions, so $m_j = n_i = 2$ and formula $(**)$ says that we have exactly $n - 1$ transpositions: one sees immediately that there is only one combinatorial solution (cf. figure 2).
The monodromy image is in fact exactly the Dihedral group D_n: this explains the above fomulas, because if we set $u := T_n(z)$, then there is a quadratic extension of $\mathbb{C}(z)$, yielding the Galois closure of $\mathbb{C}(u) \subset \mathbb{C}(z)$.

We have, if $w := t^n$, $u = \frac{1}{2}(w + w^{-1}) = \frac{w^2+1}{2w}$, and similarly $z = \frac{t^2+1}{2t}$, thus $t^2 - 2zt + 1 = 0$.
Therefore, we have the following basic diagram (cf. also figure 1).

(1)
$$\begin{tikzcd} \Psi : t \arrow[r] \arrow[d] & z = \frac{1}{2}(t + t^{-1}) = \frac{t^2+1}{2t} \arrow[d, "T_n"'] \\ \Psi : t^n = w \arrow[r] & u = T_n(z) = \Psi(w). \end{tikzcd}$$

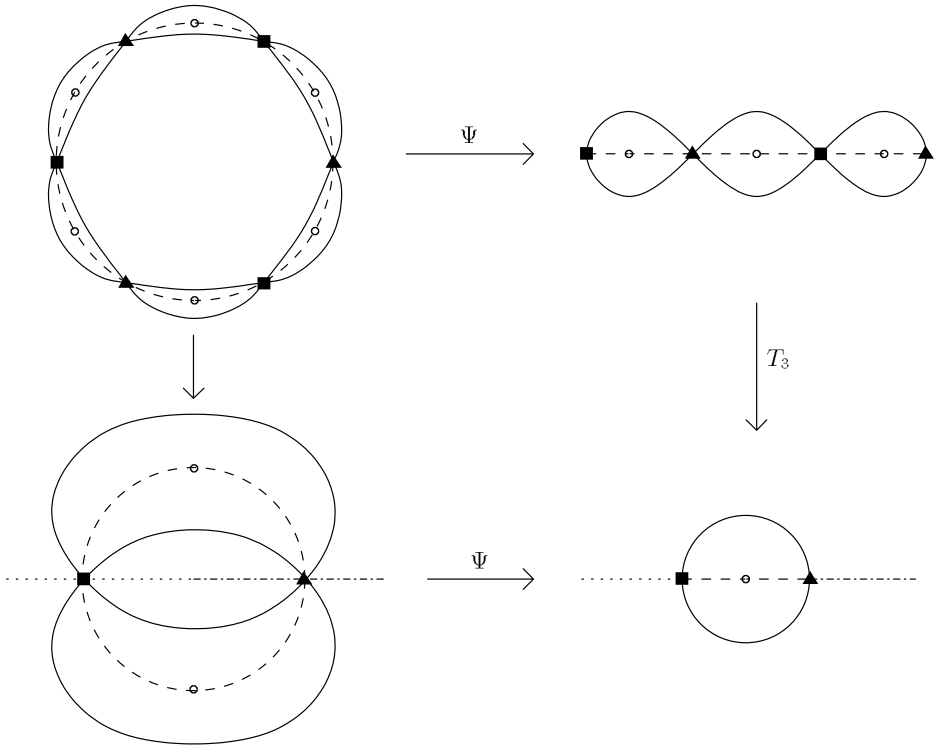


FIGURE 1. Chebycheff basic diagram

The relation with the function $cos(y) = \frac{1}{2}(e^{iy} + e^{-iy})$ comes in because the monodromy of T_n factors through the mondromy of cos, namely, the infinite Dihedral group

$$D_\infty =< a, b | a^2 = b^2 = 1 >= AL(1, \mathbb{Z}) := \{g | g(z) = \pm z + c,\ c \in \mathbb{Z}\}.$$

Q.E.D.

Note that in the first picture of figure 2 ($n = 6$) we have two disjoint transpositions corresponding to the reflection of the hexagon with horizontal axis, and three disjoint transpositions corresponding to the reflection with axis the dotted line.
In the second picture ($n = 5$), we have two disjoint transpositions corresponding to the reflection with horizontal axis and two other disjoint transpositions corresponding to the reflection with axis the dotted line.

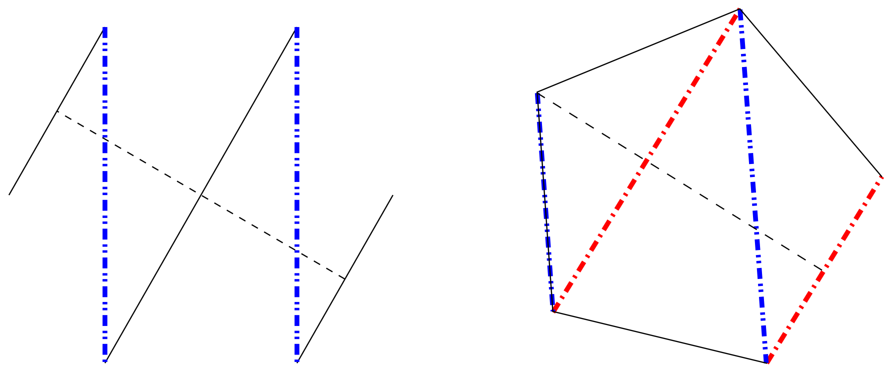


FIGURE 2. Chebycheff monodromies: even and odd

Another very simple class of polynomials with two critical values is given by the *Belyi polynomials*.
Take a rational number $q \in \mathbb{Q}$ such that $0 < q < 1$: writing q as a fraction $q = \frac{m}{m+r}$, we get a polynomial

$$P_{m,r} := z^m (1-z)^r (m+r)^{m+r} m^{-m} r^{-r}.$$

The critical points of $P_{m,r}$ are just $\{0, 1, q = \frac{m}{m+r}\}$, and its only critical values are $\{0, 1\}$. Observe that $P_{m,r}(0) = P_{m,r}(1) = 0$, while the coefficient of $P_{m,r}$ is chosen exactly in order that $P_{m,r}(q) = 1$. Hence it follows that the monodromy τ_1' corresponding to the critical value 1 is a transposition, whereas the monodromy τ_0' corresponding to the critical value 0 has a cycle decomposition of type (m, r) (but be aware of the possibility $m = 1, r = 1$).

Definition 4.2. *Let $P \in \mathbb{C}[z]$ be a polynomial with critical values $\{0, 1\}$, and observe that $1 - P$ is also a polynomial with critical values $\{0, 1\}$. We say that $1 - P$ is* extendedly *equivalent to P, and we shall call the union of the equivalence class of P with the equivalence class of $1 - P$ the* extended equivalence class.

In particular, for degree ≤ 4, Chebycheff polynomials are extendedly equivalent to Belyi polynomials.

Proposition 4.3. *Consider the extended equivalence classes of polynomials with two critical values: among them are the classes of Chebycheff and Belyi polynomials.*
i) In degree ≤ 4 there are no other classes.
ii) In degree 5 there is also the class of the polynomial $\frac{3}{16}(z^5 - \frac{10}{3}z^3 + 5z + \frac{8}{3})$.
Observing that all the above polynomials are in $\mathbb{Q}[z]$, we have also that
iii) in degree 6 we first find a polynomial P which is not extendedly equivalent to any polynomial in $\mathbb{R}[z]$, and which more precisely is not extendedly equivalent to its complex conjugate.

Proof. i) We leave as an exercise to the interested reader to find out that all the possible (extended classes of) monodromies in degree ≤ 4 are either Chebycheff monodromies ($\iff$ τ_j for $j = 1, 2$ is a product of disjoint transpositions) or Belyi monodromies ($\iff$ τ_1 is a transposition, and τ_2 is a product of at most two cycles).
ii) Similarly one sees that in degree 5 the only remaining case is the one where each τ_j is a 3-cycle. Up to affine transformations we may assume that the sum of the critical points equals 0, so that we get the polynomial

$$Q(z) = 5\int (z-a)^2(z+a)^2 = z^5 - \frac{10}{3}a^2z^3 + 5a^4z + c.$$

Imposing the condition $Q(-a) = 0$, $Q(a) = 1$ we obtain $c = \frac{1}{2}$, $a^5 = \frac{3}{16}$. Thus we obtain a normalized polynomial which has coefficients which do not lie in $\mathbb{Q}$. However, if we set $a = 1$ and we multiply Q by $\frac{3}{16}$, we obtain a nonnormalized polynomial $P \in \mathbb{Q}[z]$ with critical values $\{0, 1\}$.
To see iii) is not difficult: it suffices to exhibit a polynomial P whose monodromy is not conjugate to the monodromy of $\bar{P}$. We choose now (cf. figure 3) $\frac{1}{2}$ as base point, and basis of the fundamental group of $\mathbb{C} \setminus \{0, 1\}$ such that complex conjugation sends $\gamma_j \mapsto \gamma_j^{-1}$, $j = 1, 2$.

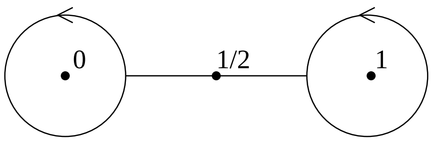


FIGURE 3.

It follows that if τ_j, $j = 1, 2$ yield the monodromy of P , then τ_j^{-1}, $j = 1, 2$ yield the monodromy of $\bar{P}$. We choose $\tau_1 = (1, 3, 6)(4, 5), \tau_2 = (1, 2)(3, 5)$, and observe that if there were a permutation α conjugating τ_i to τ_i^{-1} for $i = 1, 2$, then α would leave invariant the sets $\{1, 3, 6\}$, $\{4, 5\}$, $\{1, 2\}$, $\{3, 5\}$, hence their mutual intersections. This immediately implies that $\alpha = id$, a contradiction.
Another example is given by setting $\tau_1 = (5, 6)(1, 2, 3), \tau_2 = (3, 4, 6)$.

Q.E.D.

Let $P \in \mathbb{C}[z]$ be a polynomial with critical values $\{0, 1\}$. Then we know by theorem 3.4 that P has coefficients in $\overline{\mathbb{Q}}$, and in fact then in some number field K. We want to show this fact again, but in a more explicit way which will allow us to find effectively the field K.
Let us now introduce several affine algebraic sets which capture the information contained in all the number fields arising this way.
Let $P(z) := z^n + a_{n-2}z^{n-2} + \dots a_0$ be a normalized polynomial with only critical values $\{0, 1\}$. Once we choose the types of the respective

cycle decompositions $(m_1, \dots, m_r)$ and $(n_1, \dots, n_s)$, we can write our polynomial P in two ways, namely

$$P(z) = \prod_{i=1}^{r} (z - \beta_i)^{m_i},$$

$$P(z) - 1 = \prod_{k=1}^{s} (z - \gamma_k)^{n_k}.$$

Since P is normalized we have the equations $F_1 = \sum m_i \beta_i = 0$ and $F_2 = \sum n_k \gamma_k = 0$. We have: $m_1 + \dots m_r = n_1 + \dots n_s = n = degP$ and therefore, since by $(**)$ $\sum_j (m_j - 1) + \sum_i (n_i - 1) = n - 1$, we get $r + s = n + 1$.
Since we have $\prod_{i=1}^{r} (z - \beta_i)^{m_i} = 1 + \prod_{k=1}^{s} (z - \gamma_k)^{n_k}$ comparing coefficients we obtain further $n - 1$ polynomial equations with integer coefficients in the variables β_i, γ_k which we denote by $F_3 = 0, \dots, F_{n+1} = 0$.
Let

$$\mathbf{V}\left(n, \begin{bmatrix} m_1 & \dots & m_r \\ n_1 & \dots & n_s \end{bmatrix}\right)$$

be the algebraic set in affine $(n+1)$-space corresponding to the equations $F_1 = 0, \dots, F_{n+1} = 0$. Mapping a point of this algebraic set to the vector $(a_0, \dots, a_{n-1})$ of coefficients of the corresponding polynomial P we obtain (by elimination of variables) an algebraic set

$$\mathbf{C}\left(n, \begin{bmatrix} m_1 & \dots & m_r \\ n_1 & \dots & n_s \end{bmatrix}\right)$$

in affine $(n-1)$ space. Both these algebraic sets are defined over $\mathbb{Q}$. This does not imply that each of their points has coordinates in $\mathbb{Q}$ (cf. proposition 4.3). We encounter this phenomenon also later, in the more complicated situation of Beauville surfaces (cf. theorem 7.20). We have

Proposition 4.4. *Each of the algebraic sets*

$$\mathbf{V}\left(n, \begin{bmatrix} m_1 & \dots & m_r \\ n_1 & \dots & n_s \end{bmatrix}\right), \quad \mathbf{C}\left(n, \begin{bmatrix} m_1 & \dots & m_r \\ n_1 & \dots & n_s \end{bmatrix}\right)$$

is either empty or has dimension 0.

This follows from Riemann's existence theorem since this theorem shows that there are only a finite number of normalized polynomials having critical points $\{0, 1\}$ and fixed ramification types. We are going to describe this set of polynomials in the following case $n = 6$, $r = 4$, $s = 3$. We shall give now information on the algebraic sets $\mathbf{C}$ for all possible choices of the ramification indices.

I. $(m_1, m_2, m_3, m_4) = (2, 2, 1, 1)$, $(n_1, n_2, n_3) = (2, 2, 2)$:
The algebraic set $\mathbf{C}$ is defined by the equations

$$a_0 = -1, \quad a_1 = 0, \quad 4a_2 = a_4^2, \quad a_3 = 0, \quad a_4^3 = -54,$$

it is irreducible over $\mathbb{Q}$ and consists of 3 points over $\bar{\mathbb{Q}}$ (in the Chebycheff class).

II. $(m_1, m_2, m_3, m_4) = (2, 2, 1, 1)$, $(n_1, n_2, n_3) = (3, 2, 1)$:
The algebraic set $\mathbf{C}$ is defined by the equations

$$a_0 = \frac{a_4^6}{8748} + \frac{a_4^3}{81} - \frac{2}{3}, \quad a_1 = -\frac{a_3 a_4^4}{324} + \frac{a_3 a_4}{3}, \quad a_2 = -\frac{25 a_4^8}{314928} + \frac{2a_4^5}{729} + \frac{8a_4^2}{27},$$
$$a_3^2 + \frac{5a_4^6}{2187} - \frac{4a_4^3}{81} - \frac{4}{3} = 0, \quad a_4^9 - \frac{324 a_4^6}{25} - \frac{17496 a_4^3}{25} - \frac{314928}{25} = 0,$$

it is irreducible over $\mathbb{Q}$ and consists of 18 points over $\bar{\mathbb{Q}}$.

III. $(m_1, m_2, m_3, m_4) = (2, 2, 1, 1)$, $(n_1, n_2, n_3) = (4, 1, 1)$:
Here the algebraic set $\mathbf{C}$ falls into two irreducible components $\mathbf{C}_1$, $\mathbf{C}_2$ already over $\mathbb{Q}$. The variety $\mathbf{C}_1$ is defined by

$$a_0 = -1, \quad a_1 = 0, \quad a_2 = 0, \quad a_3 = 0, \quad a_4^3 = \frac{27}{4},$$

it is irreducible over $\mathbb{Q}$ and consists of 3 points over $\bar{\mathbb{Q}}$. The variety $\mathbf{C}_2$ is defined by

$$a_0 = -\frac{2527}{2500}, \quad a_1 = \frac{19 a_3 a_4}{150}, \quad a_2 = \frac{21 a_4^2}{20}, \quad a_3^2 = -\frac{243}{125}, \quad a_4^3 + \frac{27}{50} = 0,$$

it is irreducible over $\mathbb{Q}$ and consists of 6 points over $\bar{\mathbb{Q}}$.

IV. $(m_1, m_2, m_3, m_4) = (3, 1, 1, 1)$, $(n_1, n_2, n_3) = (2, 2, 2)$:
Here the algebraic set $\mathbf{C}$ falls into two irreducible components $\mathbf{C}_1$, $\mathbf{C}_2$ already over $\mathbb{Q}$. The components $\mathbf{C}_1$, $\mathbf{C}_2$ are defined by

$$a_0 = 0, \quad a_1 = 0, \quad a_2 = 0, \quad a_3 = \pm 2, \quad a_4 = 0.$$

V. $(m_1, m_2, m_3, m_4) = (3, 1, 1, 1)$, $(n_1, n_2, n_3) = (3, 2, 1)$:
The algebraic set $\mathbf{C}$ is defined by the equations

$$a_0 = \frac{29 a_4^3}{2700} - \frac{9}{50}, \quad a_1 = \frac{7 a_3 a_4^4}{432} + \frac{3 a_3 a_4}{8}, \quad a_2 = -\frac{5a_4^5}{324} + \frac{5a_4^2}{12},$$
$$a_3^2 = \frac{11 a_4^3}{135} - \frac{2}{5}, \quad a_4^6 - \frac{324 a_4^3}{25} + \frac{2916}{25} = 0,$$

it is irreducible over $\mathbb{Q}$ and consists of 12 points over $\bar{\mathbb{Q}}$.

VI. $(m_1, m_2, m_3, m_4) = (3, 1, 1, 1)$, $(n_1, n_2, n_3) = (4, 1, 1)$:
The algebraic set $\mathbf{C}$ is defined by the equations

$$a_0 = -\frac{513}{625}, \quad a_1 = \frac{24 a_3 a_4}{25}, \quad a_2 = \frac{16 a_4^2}{45}, \quad a_3^2 = \frac{32}{125}, \quad a_4^3 = -\frac{729}{100},$$

it is irreducible over $\mathbb{Q}$ and consists of 6 points over $\bar{\mathbb{Q}}$.

We return now to the general situation and we consider the following set
$M_n := \{$right affine equivalence classes of polynomials P of degree n with critical values $\{0, 1\}\}$. As seen in thm. 3.4, the Galois group

$Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on M_n, and Grothendieck's expression: "Dessins d' enfants" refers to the graph $P^{-1}([0,1])$.
It has n edges, corresponding to the inverse image of the open interval $(0,1)$, and its set of vertices is *bipartite*, since we have two different types of vertices, say the black vertices given by $P^{-1}(\{0\})$, and the blue vertices corresponding to $P^{-1}(\{1\})$.
Moreover, around each vertex, we can give a cyclical counterclockwise ordering of the edges incident in the vertex (cf. figure 3).
It is easy to show that these data completely determine the monodromy, which acts on the set $P^{-1}(\{\frac{1}{2}\})$, i.e., on the midpoints of the edges. In fact, e.g. the "black monodromy" is given as follows: for each midpoint of a segment: go first to the black vertex, then turn to the right, until you reach the next midpoint.
Figure 4 gives the dessin d'enfant for a Chebycheff polynomial, whereas figure 5 is the children 's drawing of a rational function of degree 9, whose monodromy at ∞ is $(A,B,C,D,E)(a,b)(\alpha,\beta)$.

FIGURE 4. Dessins d'enfants: Chebycheff polynomial

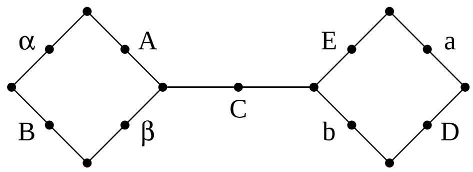


FIGURE 5. A rational function of degree 9

Remark 4.5. *The action of the Galois group is still very mysterious, the only obviously clear fact is that the conjugacy classes of τ_1, resp. τ_2 (in other words, the multiplicities of the critical points in $P^{-1}(\{0\})$, resp. $P^{-1}(\{1\})$) remain unchanged.*

5. RIEMANN'S EXISTENCE THEOREM AND DIFFERENCE POLYNOMIALS

In this section we briefly discuss some applications of Riemann's existence theorem, and in particular of Chebycheff polynomials to the problem of irreducibility of difference polynomials (cf. [DLS61], [Sch67], [Fr70], [Fr73]).

Definition 5.1. *Let f, $g \in \mathbb{C}[x]$ be two polynomials. Then a* difference polynomial *is a polynomial in $\mathbb{C}[x,y]$ of the form $f(x) - g(y)$.*

Consider the curve $\Gamma := \{(x, y) \in \mathbb{C}^2 | f(x) = g(y)\}$, which can be thought of as the the fibre product of the two maps $f : \mathbb{C} \to \mathbb{C}$ and $g : \mathbb{C} \to \mathbb{C}$ (or as $(f \times g)^{-1}(\Delta \subset \mathbb{C} \times \mathbb{C})$, Δ being the diagonal in $\mathbb{C} \times \mathbb{C}$).
Denoting the respective branch loci of f and g by B_f and B_g, we have that the singular locus of Γ is contained in the intersection of the respective inverse images of the branch loci, i.e., $Sing(\Gamma) \subset p_x^{-1}(B_f) \times p_y^{-1}(B_g)$. Moreover, if we denote by C' the normalization of Γ, then the branch locus B of $\pi : C' \to \mathbb{C}$ (which has degree $deg(f) \cdot deg(g)$) is equal to $B_f \cup B_g$.
We have the monodromy homomorphisms $\mu_f : \pi_1(\mathbb{C} - B_f) \to \mathfrak{S}_n$, $\mu_g : \pi_1(\mathbb{C} - B_g) \to \mathfrak{S}_m$ and via the epimorphism $\pi_1(\mathbb{C} - B) \to \pi_1(\mathbb{C} - B_f)$ (resp. the one for g), we get

$$\Phi = \mu_f \times \mu_g : \pi_1(\mathbb{C} - B) \to \mathfrak{S}_n \times \mathfrak{S}_m.$$

Therefore Riemann's existence theorem and the fact that a variety is irreducible iff its nonsingular locus is connected yields the following:

Proposition 5.2. *$f(x) - g(y)$ is irreducible if and only if the product of the two monodromies $\Phi = \mu_f \times \mu_g$ is transitive.*

An easier irreducibility criterion is obtained by the following observation.
Homogenizing the equation $f(x) = g(y)$ as $y_0^m x_0^n f(\frac{x_1}{x_0}) = x_0^n y_0^m g(\frac{y_1}{y_0})$ we obtain a compactification $\overline{\Gamma} \subset \mathbb{P}^1 \times \mathbb{P}^1$ such that the only point at infinity is $(\infty, \infty) = ((0, 1)(0, 1))$.
In this point there are local holomorphic coordinates (u, v) such that the local equation of $\overline{\Gamma}$ reads out as $u^n = v^m$. Set $d := G.C.D.(n, m)$: then we have $u^n - v^m = \prod_{i=1}^d (u^{\frac{n}{d}} - \zeta^i v^{\frac{m}{d}})$, ζ being as usual a primitive d-th root of 1. Thus we obtain

Proposition 5.3. *The curve $\overline{\Gamma}$ has exactly d branches at infinity, and is in particular irreducible if $d = 1$. Letting C be the normalization of $\overline{\Gamma}$, the algebraic function $f(x) = g(y)$ has branch locus equal to $B_f \cup B_g \cup \{\infty\}$ if $n, m \geq 1$.*

A trivial example of a non irreducible difference polynomial is given by $f = g$, since then $(x - y)|(f(x) - f(y))$.
A less trivial counterexample is given by the Chebycheff polynomial $T_{2n}(x) + T_{2n}(y)$ (cf. [DLS61]). In fact, $T_{2n}(x) + T_{2n}(y) = T_{2n}(x) - (-T_{2n}(y))$ and the monodromy of $(-T_{2n}(y))$ is simply obtained by exchanging the roles of τ_1, τ_2.
It is easier to view the dihedral monodromies of $T_{2n}(x)$, respectively $(-T_{2n}(y))$, as acting on $\mathbb{Z}/2n$:

$$\tau_1(i, j) = (-i, -j - 1), \quad \tau_2(i, j) = (-i - 1, -j).$$

We see immediately that $\tau_1\tau_2(i, j) = (i + 1, j + 1)$, thus the cyclic subgroup of D_{2n} operates trivially on $(i - j)$ and we conclude that

we have exactly n orbits of cardinality $4n$ in the product $(\mathbb{Z}/2n)^2$, and correspondingly a factorization of $T_{2n}(x) + T_{2n}(y)$ in n irreducible factors.
Schinzel asked (cf. [Sch67]) whether one could give examples without using the arithmetic of Chebycheff polynomials. Riemann's existence provides plenty of examples, as the following one where two degree 7 polynomials yield a difference polynomial with exactly two irreducible factors, of respective bidegrees $(4,4),(3,3)$.

Proposition 5.4. *Consider the following three matrices in* $GL(3,\mathbb{Z}/2)$, $A_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, *and let* f *be the degree* 7 *polynomial associated to the monodromy action of* $\pi_1(\mathbb{C} \setminus \{0,1,\lambda\})$ *determined by the above three matrices on the Fano projective plane associated to the vector space* $V := (\mathbb{Z}/2)^3$.
Let moreover g *be the degree* 7 *polynomial associated to the monodromy action of* $\pi_1(\mathbb{C} \setminus \{0,1,\lambda\})$ *on the dual projective plane (associated to the vector space* $V^\vee := (\mathbb{Z}/2)^3$*) determined by the (inverses of the) transposes of the above three matrices, which have order* 2.
Then the difference polynomial $f(x) - g(y)$ *is the product of two irreducible factors, of respective bidegrees* $(4,4),(3,3)$.

Proof. Each linear map A_i has a fixed subspace of dimension 2, and has order two: hence the associated permutation is a double transposition. One sees easily that the A_i's generate a transitive subgroup, therefore the associated covering yields the class of a polynomial f of degree 7, and similarly for g. By construction, the product action on $\mathbb{P}(V) \times \mathbb{P}(V^\vee)$ leaves invariant the incidence correspondence, which is a correspondence of type $(3,3)$.
Moreover, one sees immediately that $A_1, A_2 = {}^t A_1$ leave the vector e_3 fixed, and they operate transitively on the projective line generated by e_1, e_2. Therefore the action on the product $\mathbb{P}(V) \times \mathbb{P}(V^\vee)$ is easily seen to have exactly two orbits, the incidence correspondence and its complementary set.

Q.E.D.

Another very interesting occurrence of Chebycheff polynomials concerns *Schur's problem*, which asks: given a polynomial $f \in \mathbb{C}[z]$, when is $\frac{f(x)-f(y)}{x-y}$ irreducible?
Nontrivial non irreducible Schur polynomials are obtained again through the Chebycheff polynomials: $\frac{T_n(x)-T_n(y)}{x-y}$. Let us briefly explain how, using again the description of the product monodromy (this procedure shows how one can find many more examples of non irreducible Schur polynomials, although without an explicit determination of the coefficients of the polynomial f).

Using the previous notation, we get this time the action

$$\tau_1(i,j) = (-i,-j), \quad \tau_2(i,j) = (-i-1,-j-1) \text{ on } (\mathbb{Z}/n)^2,$$

thus in particular $\tau_1\tau_2(i,j) = (i+1, j+1)$ and obviously the difference $i-j$ is only transformed into $\pm(i-j)$.
Thus the corresponding Schur polynomial has exactly $\frac{n-1}{2}$ factors for n odd, and $\frac{n}{2}$ factors for n even.
We already said that Chebycheff polynomials are quite ubiquitous.
Let us point out another beautiful application of Chebycheff polynomials: namely, Chmutov (cf. [Ch92]) used them to construct surfaces in $\mathbb{P}^3$ with "many" nodes, obtaining the best known asymptotic lower bounds.

6. Belyi's Theorem and Triangle curves

Grothendieck's enthusiasm was raised by the following result, where Belyi made a very clever and very simple use of the Belyi polynomials in order to reduce the number of critical values of an algebraic function

Theorem 6.1. *(Belyi, cf.* [Bel79]*) An algebraic curve C can be defined over $\overline{\mathbb{Q}}$ if and only if there exists a holomorphic map $f : C \to \mathbb{P}^1_{\mathbb{C}}$ branched exactly in $\{0, 1, \infty\}$.*

Again here the monodromy of f is determined by the children's drawing $f^{-1}([0,1])$. If, moreover, we assume that f is Galois, then we call C a triangle curve.

Definition 6.2. *C is a* triangle curve *if there is a finite group G acting effectively on C and with the property that $C/G \cong \mathbb{P}^1_{\mathbb{C}}$, and $f : C \to \mathbb{P}^1_{\mathbb{C}} \cong C/G$ has $\{0, 1, \infty\}$ as branch set.*

Belyi's construction of triangle curves is rather complicated. Easier examples can be constructed using, as in the previous section, difference polynomials associated (as in 5.3) to polynomials with $0, 1$ as only critical values.
Gabino Gonzalez (cf. [Gon04]) was recently able to extend Belyi's theorem to the case of complex surfaces (in terms of Lefschetz maps with three critical values).
In the next section we shall describe some higher dimensional analogues of triangle curves.

7. Beauville surfaces

Inspired by a construction of A. Beauville (cf [Bea78]) of a surface with $K^2 = 8$, $p_g = q = 0$ as a quotient of the product of two Fermat curves of degree 5 by the action of $\mathbb{Z}/5\mathbb{Z}$ the second author gave in [Cat00] the following definition.

Definition 7.1. *A* Beauville surface *is a compact complex surface S which*
1) is rigid*, i.e., it has no nontrivial deformation,*
2) is isogenous to a (higher) product*, i.e., it is a quotient $S = (C_1 \times C_2)/G$ of a product of curves of resp. genera ≥ 2 by the free action of a finite group G.*

In the above cited paper, the second author introduced and studied extensively surfaces isogenous to a higher product. Among others it is shown there that the topology of a surface isogenous to a product determines its deformation class up to complex conjugation. The following theorem contains a correction to thm. 4.14 of [Cat00].

Theorem 7.2. *Let $S = (C_1 \times C_2)/G$ be a surface isogenous to a product. Then any surface X with the same topological Euler number and the same fundamental group as S is diffeomorphic to S. The corresponding subset of the moduli space $\mathcal{M}_S^{top} = \mathcal{M}_S^{diff}$, corresponding to surfaces homeomorhphic, resp, diffeomorphic to S, is either irreducible and connected or it contains two connected components which are exchanged by complex conjugation.*
In particular, if X is orientedly diffeomorphic to S, then X is deformation equivalent to S or to $\bar{S}$.

The class of surfaces isogenous to a product and their higher dimensional analogues provide a wide class of examples where one can test or disprove several conjectures and questions (cf. e.g. [Cat03], [BC04], [BCG05a]).
Notice, that given a surface $S = (C_1 \times C_2)/G$ isogenous to a product, we obtain always three more, exchanging C_1 with its conjugate curve $\bar{C}_1$, or C_2 with $\bar{C}_2$, but only if we conjugate both C_1 and C_2, we obtain an orientedly diffeomorphic surface. However, these four surfaces could be all biholomorphic to each other.
If S is a Beauville surface (and X is orientedly diffeomorphic to S) this implies: $X \cong S$ or $X \cong \bar{S}$. In other words, the corresponding subset of the moduli space $\mathcal{M}_S$ consists of one or two points (if we insist on keeping the orientation fixed, else we may get up to four points).
The interest for Beauville surfaces comes from the fact that they are the rigid ones amongst surfaces isogenous to a product. We recall that an algebraic variety X is *rigid* if and only if it does not have any non trivial deformation (for instance, the projective space is rigid). There is another (stronger) notion of rigidity, which is the following

Definition 7.3. *An algebraic variety X is called* strongly rigid *if any other variety homotopically equivalent to X is either biholomorphic or antibiholomorphic to X.*

Remark 7.4. *1) It is nowadays wellknown that smooth compact quotients of symmetric spaces are rigid (cf.* [CV60]*).*

2) Mostow (cf. [Mos73] *proved that indeed locally symmetric spaces of complex dimension ≥ 2 are strongly rigid, in the sense that any homotopy equivalence is induced by a unique isometry.*

These varieties are of general type and the moduli space of varieties of general type is defined over $\mathbb{Z}$, and naturally the absolute Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of their connected components. So, in our special case, $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the isolated points which parametrize rigid varieties.
In particular, rigid varieties are defined over a number field and work of Shimura gives in special cases a way of computing explicitly their fields of definition. By this reason these varieties were named *Shimura varieties* (cf. Deligne's Bourbaki seminar [Del71]).
A quite general question is

Question 7.5. *What are the fields of definition of rigid varieties? What is the $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit of the point in the moduli space corresponding to a rigid variety?*

Coming back to Beauville surfaces we observe the following:

Remark 7.6. *The rigidity of a Beauville surface is equivalent to the condition that (C_i, G^0) is a triangle curve, for $i = 1, 2$ ($G^0 \subset G$ is the subgroup of index ≤ 2 which does not exchange the two factors).*
It follows that a Beauville surface is defined over $\overline{\mathbb{Q}}$, whence the Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ operates on the discrete subset of the moduli space $\mathcal{M}_S$ corresponding to Beauville surfaces.
By the previous theorem, the Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ may transform a Beauville surface into another one with a non isomorphic fundamental group. Phenomena of this kind were already observed by J.P. Serre (cf. [Ser64]*).*

It looks therefore interesting to address the following problems:

Question 7.7. *Existence and classification of Beauville surfaces, i.e.,*
a) which finite groups G can occur?
b) classify all possible Beauville surfaces for a given finite group G.

Question 7.8. *Is the Beauville surface S biholomorphic to its complex conjugate surface $\bar{S}$?*
Is S real (i.e., does there exist a biholomorphic map $\sigma : S \to \bar{S}$ with $\sigma^2 = id$)?

The major motivation to find these surfaces is rooted in the following so called *Friedman-Morgan speculation (1987)* (cf. [FM94]), which we briefly explain in the following.
One of the fundamental problems in the theory of complex algebraic surfaces is to understand the moduli spaces of surfaces of general type, and in particular their connected components, which parametrize the deformation equivalence classes of minimal surfaces of general type.

Definition 7.9. *Two minimal surfaces S and S' are said to be* def - equivalent *(we also write: $S \sim_{def} S'$) if and only if they are elements of the same connected component of the moduli space.*

By the classical theorem of Ehresmann ([Ehr43]), two def - equivalent algebraic surfaces are (orientedly) diffeomorphic.
In the late eighties Friedman and Morgan (cf. [FM94]) conjectured that two algebraic surfaces are diffeomorphic if and only if they are def - equivalent (**def = diff**).
Donaldson's breaktrough results had made clear that diffeomorphism and homeomorphism differ drastically for algebraic surfaces (cf. [Don83]) and the success of gauge theory led Friedman and Morgan to "speculate" that the diffeomorphism type of algebraic surfaces determines the deformation class. After the first counterexamples of M. Manetti (cf. [Man01]) appeared, there were further counterexamples given by Catanese, Kharlamov-Kulikov, Catanese-Wajnryb, Bauer-Catanese-Grunewald (cf. [Cat03], [K-K02],[BCG05a], [CW04]).
The counterexamples are of quite different nature: Manetti used $(\mathbf{Z}/\mathbf{2})^{\mathbf{r}}$-covers of $\mathbb{P}^1_{\mathbf{C}} \times \mathbb{P}^1_{\mathbf{C}}$, his surfaces have $b_1 = 0$, but are not 1-connected. Kharlamov - Kulikov used quotients S of the unit ball in $\mathbf{C}^2$, thus $b_1 > 0$, and the surfaces are rigid. Catanese used surfaces isogenous to a product (which are not rigid).
Our examples are given by Beauville surfaces. The great advantage of these is that, being isogenous to a product, they can be described by combinatorial data and the geometry of these surfaces is encoded in the algebraic data of a finite group.
In order to reduce the description of Beauville surfaces to some group theoretic statement, we need to recall that surfaces isogenous to a higher product belong to two types:

- S is of *unmixed type* if the action of G does not mix the two factors, i.e., it is the product action of respective actions of G on C_1, resp. C_2.
- S is of *mixed type*, i.e., C_1 is isomorphic to C_2, and the subgroup G^0 of transformations in G which do not mix the factors has index precisely 2 in G.

The datum of a Beauville surface can be completely described group theoretically, since it is equivalent to the datum of two triangle curves with isomorphic groups with some additional condition assuring that the diagonal action on the product of the two curves is free.

Definition 7.10. *Let G be a finite group.*
1) A quadruple $v = (a_1, c_1; a_2, c_2)$ of elements of G is an unmixed Beauville structure for G *if and only if*
(i) the pairs a_1, c_1, and a_2, c_2 both generate G,

(ii) $\Sigma(a_1, c_1) \cap \Sigma(a_2, c_2) = \{1_G\}$, *where*

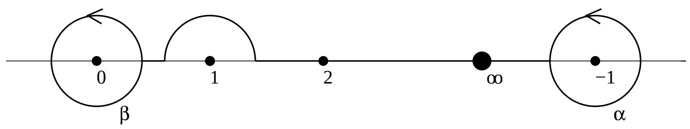
$$\Sigma(a, c) := \bigcup_{g \in G} \bigcup_{i=0}^{\infty} \{ga^i g^{-1}, gc^i g^{-1}, g(ac)^i g^{-1}\}.$$

We write $\mathbb{B}(G)$ *for the set of unmixed Beauville structures on* G.
2) A mixed Beauville quadruple for G *is a quadruple* $M = (G^0; a, c; g)$ *consisting of a subgroup* G^0 *of index* 2 *in* G, *of elements* $a, c \in G^0$ *and of an element* $g \in G$ *such that*
i) G^0 *is generated by* a, c,
ii) $g \notin G^0$,
iii) for every $\gamma \in G^0$ *we have* $g\gamma g\gamma \notin \Sigma(a, c)$.
iv) $\Sigma(a, c) \cap \Sigma(gag^{-1}, gcg^{-1}) = \{1_G\}$.
We call $\mathbb{M}(G)$ *the set of mixed Beauville quadruples on the group* G.

Remark 7.11. *We consider here finite groups* G *having a pair* (a, c) *of generators. Setting* $(r, s, t) := (\mathrm{ord}(a), \mathrm{ord}(c), \mathrm{ord}(ac))$, *such a group is a quotient of the triangle group*

$$T(r, s, t) := \langle x, y \mid x^r = y^s = (xy)^t = 1 \rangle.$$

We defined some algebraic structures on a finite group in the above. As the name "Beauville structure" already suggests, these data give rise to a Beauville surface as follows:
Take as base point $\infty \in \mathbb{P}^1$, let $B := \{-1, 0, 1\}$, and take the following generators α, β of $\pi_1(\mathbb{P}^1_{\mathbf{C}} - B, \infty)$ $(\gamma := (\alpha \cdot \beta)^{-1})$:



We observe that we now prefer to take as branch locus the set $\{-1, 0, 1\}$, since it is more convenient for describing the complex conjugation group theoretically.
Let now G be a finite group and $v = (a_1, c_1; a_2, c_2) \in \mathbb{B}(G)$. We get surjective homomorphisms

$$\pi_1(\mathbb{P}^1_{\mathbf{C}} - B, \infty) \to G, \qquad \alpha \mapsto a_i, \ \gamma \mapsto c_i \tag{2}$$

and Galois coverings $\lambda_i : C(a_i, c_i) \to \mathbb{P}^1_{\mathbf{C}}$ ramified only in $\{-1, 0, 1\}$ with ramification indices equal to the orders of a_i, b_i, c_i and with group G) (*Riemann's existence theorem*).

Remark 7.12. *1) Condition (1), ii) assures that the action of* G *on* $C(a_1, c_1) \times C(a_2, c_2)$ *is free.*
2) Let be $\iota(a_1, c_1; a_2, c_2) = (a_1^{-1}, c_1^{-1}; a_2^{-1}, c_2^{-1})$. *Then* $S(\iota(v)) = \overline{S(v)}$. *(Note that* $\bar{\alpha} = \alpha^{-1}$, $\bar{\gamma} = \gamma^{-1}$.*)*
3) We have: $g(C(a_1, c_1)) \geq 2$ *and* $g(C(a_2, c_2)) \geq 2$. *This is a nontrivial fact, whcih comes from group theory. It is equivalent to the fact that* $\mu(a_i, c_i) := \frac{1}{ord(a_i)} + \frac{1}{ord(c_i)} + \frac{1}{ord(a_i c_i)} < 1$ *(cf. prop. 7.26).*

In order to address reality questions of Beauville surfaces, we have to translate the two questions:

- Is S biholomorphic to its complex conjugate $\bar{S}$?
- Is S real, i.e., does there exist a biholomorphism $\sigma : S \to \bar{S}$, such that $\sigma^2 = id$?

into group theoretic conditions.

Remark 7.13. *Actually we can define a finite permutation group $\mathrm{A}_{\mathbb{B}}(G)$ such that for $v, v' \in \mathbb{B}(G)$ we have : $S(v) \cong S(v')$ if and only if v is in the $\mathrm{A}_{\mathbb{B}}(G)$-orbit of v'. Under certain assumptions on the orders of the generating elements these orbits are easy to describe as shows the following result.*

Proposition 7.14. *Let G be a finite group and $v = (a_1, c_1; a_2, c_2) \in \mathbb{B}(G)$.*
Assume that $\{\mathrm{ord}(a_1), \mathrm{ord}(c_1), \mathrm{ord}(a_1c_1)\} \neq \{\mathrm{ord}(a_2), \mathrm{ord}(c_2), \mathrm{ord}(a_2c_2)\}$ and that $\mathrm{ord}(a_i) < \mathrm{ord}(a_ic_i) < \mathrm{ord}(c_i)$.
Then $S(v) \cong \overline{S(v)}$ if and only if there are inner automorphisms ϕ_1, ϕ_2 of G and an automorphism $\psi \in Aut(G)$ such that, setting $\psi_j := \psi \circ \phi_j$, we have

$$\psi_1(a_1) = a_1^{-1}, \quad \psi_1(c_1) = c_1^{-1},$$

$$\psi_2(a_2) = {a_2}^{-1}, \quad \psi_2(c_2) = {c_2}^{-1}.$$

In particular $S(v)$ is isomorphic to $\overline{S(v)}$ if and only if $S(v)$ has a real structure.

The following is an immediate consequence of the above

Remark 7.15. *If G is abelian, $v \in \mathbb{B}(G)$. Then $S(v)$ always has a real structure, since $g \mapsto -g$ gives an automorphism of G of order two.*

Concerning the existence of (unmixed) Beauville groups respectively unmixed Beauville surfaces we have among others the following results:

Theorem 7.16. *1) A finite abelian group G admits an unmixed Beauville structure iff $G \cong (\mathbb{Z}/n)^2$, $(n, 6) = 1$.*
2) The following groups admit unmixed Beauville structures:
a) $\mathfrak{A}_n$ for large n,
b) $\mathfrak{S}_n$ for $n \in \mathbb{N}$ with $n \geq 7$,
c) $\mathbf{SL}(2, \mathbb{F}_p)$, $\mathbf{PSL}(2, \mathbb{F}_p)$ for $p \neq 2, 3, 5$.

We checked all finite simple nonabelian groups of order ≤ 50000 and found unmixed Beaville structures on all of them with the exception of $\mathfrak{A}_5$. This led us to the following

Conjecture 7.17. *All finite simple nonabelian groups except $\mathcal{A}_5$ admit an unmixed Beauville structure.*

We have checked this conjecture for some bigger simple groups like the Mathieu groups $\mathbf{M}12$, $\mathbf{M}22$ and also matrix groups of size bigger than 2.
We call $(r,s,t) \in \mathbb{N}^3$ *hyperbolic* if

$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1.$$

In this case the triangle group $T(r,s,t)$ is hyperbolic. From our studies also the following looks suggestive:

Conjecture 7.18. *Let (r,s,t), (r',s',t') be two hyperbolic types. Then almost all alternating groups $\mathcal{A}_n$ have an unmixed Beauville structure $v = (a_1, c_1; a_2, c_2)$ where (a_1, c_1) has type (r,s,t) and (a_2, c_2) has type (r', s', t').*

The above conjectures are variations of a conjecture of Higman (proved by B. Everitt (2000), [Ev00]) asserting that every hyperbolic triangle group surjects onto almost all alternating groups.
The next result gives explicit examples of rigid surfaces not biholomorphic to their complex conjugate surface.

Theorem 7.19. *The following groups admit unmixed Beauville structures v such that $S(v)$ is not biholomorpic to $\overline{S(v)}$:*

1) *the symmetric group $\mathfrak{S}_n$ for $n \geq 7$,*
2) *the alternating group $\mathfrak{A}_n$ for $n \geq 16$ and $n \equiv 0$ mod 4, $n \equiv 1$ mod 3, $n \not\equiv 3, 4$ mod 7.*

The following theorem gives examples of surfaces which are not real, but biholomorphic to their complex conjugates, or in other words, they give real points in their moduli space which do not correspond to real surfaces.

Theorem 7.20. *Let $p > 5$ be a prime with $p \equiv 1$ mod 4, $p \not\equiv 2, 4$ mod 5, $p \not\equiv 5$ mod 13 and $p \not\equiv 4$ mod 11. Set $n := 3p + 1$. Then there is an unmixed Beauville surface S with group $\mathfrak{A}_n$ which is biholomorphic to the complex conjugate surface $\bar{S}$, but is not real.*

For *mixed* Beauville surfaces the situation is far more complicated, as already the following suggests.

Theorem 7.21. *1) If a finite group G admits a mixed Beauville structure, then the subgroup G^0 is non abelian.*
2) No group of order ≤ 512 admits a mixed Beauville structure.

We give a general construction of finite groups admitting a mixed Beauville structure.
Let H be a non-trivial group. Let $\Theta : H \times H \to H \times H$ be the automorphism defined by $\Theta(g,h) := (h,g)$ $(g, h \in H)$. We consider the semidirect product

$$H_{[4]} := (H \times H) \rtimes \mathbb{Z}/4\mathbb{Z} \tag{3}$$

where the generator 1 of $\mathbb{Z}/4\mathbb{Z}$ acts through Θ on $H \times H$. Since Θ^2 is the identity we find

$$H_{[2]} := H \times H \times 2\mathbb{Z}/4\mathbb{Z} \cong H \times H \times \mathbb{Z}/2\mathbb{Z} \tag{4}$$

as a subgroup of index 2 in $H_{[4]}$.
We have now

Lemma 7.22. *Let H be a non-trivial finite group and let a_1, c_1, a_2, c_2 be elements of H. Assume that*
1. the orders of a_1, c_1 are even,
2. a_1^2, a_1c_1, c_1^2 generate H,
3. a_2, c_2 also generate H,
4.$(\mathrm{ord}(a_1) \cdot \mathrm{ord}(c_1) \cdot \mathrm{ord}(a_1c_1), \mathrm{ord}(a_2) \cdot \mathrm{ord}(c_2) \cdot \mathrm{ord}(a_2c_2)) = 1$.
Set $G := H_{[4]}$, $G^0 := H_{[2]}$ as above and $a := (a_1, a_2, 2)$, $c := (c_1, c_2, 2)$. Then $(G^0; a, c)$ is a mixed Beauville structure on G.

Proof. It is easy to see that a, c generate $G^0 := H_{[2]}$.
The crucial observation is

$$(1_H, 1_H, 2) \notin \Sigma(a, c). \tag{5}$$

If this were not correct, it would have to be conjugate of a power of a, c or b. Since the orders of a_1, b_1, c_1 are even, we obtain a contradiction. Suppose that $h = (x, y, z) \in \Sigma(a, c)$ satisfies $\mathrm{ord}(x) = \mathrm{ord}(y)$: then our condition 4 implies that $x = y = 1_H$ and (5) shows $h = 1_{H_{[4]}}$.
Let now $g \in H_{[4]}$, $g \notin H_{[2]}$ and $\gamma \in G^0 = H_{[2]}$ be given. Then $g\gamma = (x, y, \pm 1)$ for appropriate $x, y \in H$. We find

$$(g\gamma)^2 = (xy, yx, 2)$$

and the orders of the first two components of $(g\gamma)^2$ are the same, contradicting the above remark.
Therefore the third condition is satisfied.
We come now to the fourth condition of a mixed Beauville quadruple. Let $g \in H_{[4]}$, $g \notin H_{[2]}$ be given, for instance $(1_H, 1_H, 1)$. Conjugation with g interchanges then the first two components of an element $h \in H_{[4]}$. Our hypothesis 4 implies the result. *Q.E.D.*
As an application we find the following examples

Theorem 7.23. *Let p be a prime with $p \equiv 3$ mod 4 and $p \equiv 1$ mod 5 and consider the group $H := \mathbf{SL}(2, \mathbb{F}_p)$. Then $H_{[4]}$ admits a mixed Beauville structure u such that $S(u)$ is not biholomorphic to $\overline{S(u)}$.*

Remark 7.24. *Note that the smallest prime satifying the above congruences is $p = 11$ and we get that G has order equal to* 6969600.

So it is natural to ask the following:

Question 7.25. *What is the minimal order of a group G admitting a mixed Beauville structure?*

It is interesting to observe that one important numerical restriction follows automatically from group theory:

Proposition 7.26. *Assume* $(a_1, c_1; a_2, c_2) \in \mathbb{B}(G)$. *Then* $\mu(a_1, c_1) := \frac{1}{\mathrm{ord}(a_1)} + \frac{1}{\mathrm{ord}(c_1)} + \frac{1}{\mathrm{ord}(a_1 c_1)} < 1$ *and* $\mu(a_2, c_2) < 1$. *Whence we have:* $g(C(a_1, c_1)) \geq 2$ *and* $g(C(a_2, c_2)) \geq 2$.

Proof. We may without loss of generality assume that G is not cyclic. Suppose (a_1, c_1) satisfies $\mu(a_1, c_1) > 1$: then the type of (a_1, c_1) is up to permutation amongst the

$$(2, 2, n)\ (n \in \mathbb{N}),\ (2, 3, 3),\ (2, 3, 4),\ (2, 3, 5).$$

These can be excluded easily. If $\mu(a_1, c_1) = 1$ then the type of (a_1, c_1) is up to permutation amongst the

$$(3, 3, 3),\ (2, 4, 4),\ (2, 3, 6)$$

and G is a finite quotient of one of the wall paper groups and cannot admit an unmixed Beauville structure. *Q.E.D.*

We finish sketching the underlying idea for the examples of Beauville surfaces not isomorphic to their conjugate surface obtained from symmetric groups.

Lemma 7.27. *Let* G *be the symmetric group* $\mathfrak{S}_n$ *in* $n \geq 7$ *letters and let* p *be an odd prime. We set* $a := (1, p+2, p+1)(2, p+3)$, $c := (1, 2, \dots, p)(p+1, \dots, n)$. *Then the following holds:*
1) there is no automorphism of G *carrying* $a \to a^{-1}$, $c \to c^{-1}$;
2) $\mathfrak{S}_n = < a, c >$.

Proof. 1) Since $n \neq 6$, every automorphism of G is an inner one. If there is a permutation g conjugating a to a^{-1}, c to c^{-1}, g would leave each of the sets $\{1, p+1, p+2\}$, $\{2, p+3\}$, $\{1, 2, \dots, p\}$, $\{p+1, \dots, n\}$ invariant. By looking at their intersections we conclude that g fixes the elements $1, 2, p+3$. But then $gcg^{-1} \neq c^{-1}$.
2) Let $G' := < a, c >$. Note that G' contains the transposition $a^3 = (2, p+3)$ and it contains the n-cycle $c \cdot (2, p+3)$. Therefore $G' = \mathfrak{S}_n$. *Q.E.D.*

Remark 7.28. *1)* $a' := \sigma^{-1}$, $c' := \tau\sigma^2$, *where* $\tau := (1, 2)$ *and* $\sigma := (1, 2, \dots, n)$. *It is obvious that* $\mathfrak{S}_n = < a', c' >$.
2) Let $n \geq 7$ *and let* p *be an odd prime such that* n *is not congruent to* 0 *or* 1*(mod* p*) (cf. 7.29), we get by the same arguments as in* [BCG05a], *prop. 5.5. that* $\Sigma(a, c) \cap \Sigma(a', c') = \{1\}$.
In fact, one has to observe that conjugation preserves the types (coming from the cycle decomposition). The types in $\Sigma(a, c)$ *are derived from* (3), (2), (p), $(n-p)$ *and* $(n-p-1)$ *(since we assume that* p *does neither divide* n *nor* $n-1$*), whereas the types in* $\Sigma(a', c')$ *are derived from* (n), $(n-1)$, *or* $(\frac{n-1}{2}, \frac{n+1}{2})$.

The existence of an odd prime p as above is assured by the following lemma.

Lemma 7.29. *Let $n \geq 5$ be any integer $\neq 6$. Then there is an odd prime number p such that n is not congruent to 0 or $1(mod\ p)$.*

Proof. If n is odd, then $n-2 \geq 3$ and we choose an odd prime p dividing $n-2$. Then $n \equiv 2(mod\ p)$ and we are done.
Assume now n to be even and let p be a prime dividing $n-3$. If there exists such a prime $\neq 3$, then we are done, since $n \equiv 3(mod\ p)$. Otherwise, $n-3 = 3^k$, for some $k \geq 2$. Then it is obvious that $n+3 = 3^k+6$ is not a power of 3 and we take a prime $p > 3$ dividing $n+3$ and we are done, since $n \equiv -3(mod\ p)$ and -3 is not congruent to 0 or $1(mod\ p)$: *Q.E.D.*

References

[Ba-Cat04] I. Bauer, F. Catanese, '*Some new surfaces with $p_g = q = 0$.* Proceedings of the Fano Conference (Torino 2002), 123–142, Univ. Torino, Turin (2004)

[BC04] Bauer, I., Catanese, F.: *Symmetry and Variation of Hodge Structures.* Asian Jour. Math., 8, no.2, Volume in honour of Siu's 60-th birthday, 363–390 (2004)

[BCG05a] Bauer, I., Catanese, F., Grunewald, F.: *Beauville surfaces without real structures.* In: Geometric methods in algebra and number theory, 1–42. Progr. Math., 235. Birkhäuser Boston, Boston, MA (2005)

[Bea78] A. Beauville, *Surfaces algébriques complexes.* Asterisque 54, Soc. Math. France (1978).

[Bel79] Belyĭ, G.V.: *On Galois extensions of a maximal cyclotomic field.* Izv. Akad. Nauk SSSR Ser. Mat. 43:2, 269–276 (1979); translation in Math. USSR- Izv. 14, 247–256 (1980)

[CV60] Calabi, E., Vesentini, E.: *On compact, locally symmetric Kähler manifolds.* Ann. of Math. (2) 71, 472–507 (1960)

[Car54] Caratheodory, C., *Theory of functions of a complex variable.* Vol. 2. Translated by F. Steinhardt. Chelsea Publishing Company, New York, (1954)

[Cat00] F. Catanese, '*Fibred surfaces, varieties isogenous to a product and related moduli spaces.*', Amer. J. Math. 122 (2000), no.1, 1–44.

[Cat03] F. Catanese, '*Moduli Spaces of Surfaces and Real Structures,* Ann. Math. 158 (2003), no.2, 577-592.

[CW04] Catanese, F., Wajnryb, B.: *Diffeomorphism of simply connected algebraic surfaces.* Preprint math.AG/0405299 (2004)

[Ch92] Chmutov, S. V.: *Examples of projective surfaces with many singularities.* J. Algebraic Geom. 1 , no. 2, 191–196 (1992)

[CIW94] P.B. Cohen, C. Itzykson, J. Wolfart : *Fuchsian triangle groups and Grothendieck dessins. Variations on a theme of Belyĭ.* Comm. Math. Phys. 163 no. 3, 605–627 (1994)

[DLS61] Davenport, H.; Lewis, D. J.; Schinzel, A.: *Equations of the form $f(x) = g(y)$.* Quart. J. Math. Oxford Ser. (2) 12, 304–312 (1961)

[Del71] Deligne, P.: *Travaux de Shimura.* In: Séminaire Bourbaki, 23ème année (1970/71), Exp. no. 389, 123–165 Lecture Notes in Math., Vol. 244. Springer, Berlin (1971)

[Don83] Donaldson, S.K.: *An application of gauge theory to four-dimensional topology.* J. Differential Geom. 18, no. 2, 279–315 (1983)

[Ehr43] C. Ehresmann, *Sur les espaces fibrés différentiables.* C.R. Acad. Sci. Paris 224, 1611-1612, (1947)

[Ev00] B. Everitt, '*Alternating quotients of Fuchsian groups*', Journal of Algebra 223, 457–476 (2000)

[Fr70] Fried, M.: *On a conjecture of Schur.* Michigan Math. J. 17, 41–55 (1970)

[Fr73] Fried, M.: *The field of definition of function fields and a problem in the reducibility of polynomials in two variables.* Illinois J. Math. 17, 128–146 (1973)

[FM94] Friedman, R., Morgan, J.W.: *Smooth four-manifolds and complex surfaces.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 27. Springer, Berlin (1994)

[Gon04] González-Diez, G.: *Variations on Belyi's theorem.* Preprint, to appear on Q. J. Math. (2004)

[GR58] Grauert, H., Remmert, R.: *Komplexe Räume.* Math. Ann. 136, 245–318 (1958)

[Gro97] Grothendieck, A.: *Esquisse d'un programme.* In: Geometric Galois actions, 1, 5–48. London Math. Soc. Lecture Note Ser., 242. Cambridge Univ. Press, Cambridge, 1997

[K-K02] V. Kharlamov and V. Kulikov, *On real structures of rigid surfaces* , ' Izv. Ross. Akad. Nauk Ser. Mat. 66 (2002), no. 1, 133–152.

[Man01] Manetti, M.: *On the moduli space of diffeomorphic algebraic surfaces.* Invent. Math. 143, no. 1, 29–76 (2001)

[Mir95] Miranda, R.: *Algebraic curves and Riemann surfaces.* Graduate Studies in Mathematics, 5. American Mathematical Society, Providence, RI, (1995)

[Mos73] Mostow, G.D.: *Strong rigidity of locally symmetric spaces.* Annals of Mathematics Studies, no. 78. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo (1973)

[Riv74] Rivlin, T.J., *The Chebychev Polynomials.* Pure and Applied Mathematics. Wiley Interscience, New York-London-Sydney, (1974)

[Riv90] Rivlin, T.J., *Chebyshev polynomials. From approximation theory to algebra and number theory.* Second edition. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, (1990)

[Sch67] Schinzel, A.:, *Reducibility of polynomials of the form* $f(x) - g(y)$. Colloq. Math. 18, 213–218 (1967)

[Ser64] Serre, P.: *Exemples de variétés projectives conjuguées non homéomorphes.* C. R. Acad. Sci. Paris 258, 4194–4196 (1964)

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
E-mail address: Ingrid.Bauer@uni-bayreuth.de

Lehrstuhl Mathematik VIII, Universität Bayreuth, 95440 Bayreuth, Germany
E-mail address: Fabrizio.Catanese@uni-bayreuth.de

Mathematisches Institut der, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany
E-mail address: grunewald@math.uni-duesseldorf.de