Riv. Mat. Univ. Parma, Vol. **13** (2022), 47-72

Pietro Corvaja

On the local-to-global principle for value sets

Abstract. We consider the following problem: given a morphism $\mathcal{Y} \to \mathcal{X}$ of algebraic curves over a number field k, describe the rational points $x \in \mathcal{X}(k)$ lifting locally at every place to some rational point on $\mathcal{Y}$, but admitting no rational pre-image. In particular, we provide examples where there exist infinitely many such points.

Keywords. Local global principle, Diophantine equations.

Mathematics Subject Classification: 11D99, 11R09, 11G35.

1 - Introduction

A way to prove the unsolvability of certain Diophantine equations consists in proving that the corresponding congruence to some suitable modulus is not solvable, and this last fact can always be detected by finite computations. However, it may happen that each congruence associated to a given Diophantine equation admits a solution while the equation itself admits no integral (or rational) solution. Hence the problem arises: for which Diophantine equations does the solvability of all the associated congruences guarantees the existence of a solution for the original Diophantine equation?

While this problem has been widely studied for equations in several variables, it seems that little work has been done around equations in a single unknown.

We illustrate more precisely our setting: given a polynomial $f(X) \in \mathbb{Z}[X]$, we say that an integer number λ is a *strongly fake value* of the polynomial $f(X)$ if the Diophantine equation

$$f(x) = \lambda \tag{1}$$

Received: July 6, 2021; accepted in revised form: October 12, 2021.

admits no integral solution $x \in \mathbb{Z}$, while for each modulus $m \geq 1$ the corresponding congruence

$$f(x) \equiv \lambda \pmod{m}$$

admits a solution $x \in \mathbb{Z}$.

In another language, the equation (1) admits 'local' p-adic solutions $x \in \mathbb{Z}_p$ for every prime p, but no 'global' solution in $\mathbb{Z}$.

If the equation admits a p-adic solution for all but finitely many primes p, we shall say that λ is a *fake value* of the polynomial.

An analogous definition will be given for rational functions and rational values of λ, possibly over arbitrary number fields.

As we shall see, the first occurences of polynomials admitting fake values arise in degree five. Here is an example: the Diophantine equation

$$x^5 + x^4 - 19x^2 + x^3 - 19x = 19 \tag{2}$$

admits no integral solution (actually no rational solution), but does admit a solution in every ring of p-adic integers $\mathbb{Z}_p$. Note that the above equation can be written as

$$(x^2 + x + 1)(x^3 - 19) = 0,$$

so it corresponds to finding a root of a *reducible* polynomial. Replacing the number 19 by another non-cube integer in the second factor above leads to analogous examples where the equation admits p-adic solutions for all large primes; for instance, the choice of the integer 2 produces the polynomial $(x^2 + x + 1)(x^3 - 2)$ which admits roots in $\mathbb{Z}_p$ for all primes $p \geq 5$ (and, of course, no rational root).

Hence, in our language, 0 is a strongly fake value for the polynomial $(x^2 + x + 1)(x^3 - 19)$, and it is a fake value - but not a strongly fake one - for the polynomial $(x^2 + x + 1)(x^3 - 2)$.

One natural problem, which will be addressed in this work, is the following:

P r o b l e m: *Find polynomials admitting infinitely many fake values.*

The first example, and basically the only one known at present over the rational integers, is provided by the famous Grunwald-Wang example: *the number* 16 *is an eighth-power in the ring* $\mathbb{Z}_p$ *for all odd prime* p*, but is not an eight-power in* $\mathbb{Q}$.

So, the polynomial $f(X) = X^8$ admits 16 as a fake value, and then automatically all numbers of the form $16n^8$, for $n \in \mathbb{Z}, n \neq 0$, are fake values of f.

More generally, we shall consider a finite morphism between two (affine or projective) algebraic curves $f : \mathcal{Y} \to \mathcal{X}$ over a (ring of S-integers of a) number

field κ. In the case of projective curves we shall consider rational points, while for affine curves integral points shall be considered. Note that if $\mathcal{X}, \mathcal{Y}$ are affine and the morphism $f : \mathcal{Y} \to \mathcal{X}$ is finite, then there exists a ring of S-integers $\mathcal{O}_S \subset \kappa$ such that for each S-integral point $p \in \mathcal{X}(\mathcal{O}_S)$, every rational point $q \in f^{-1}(p)$ is necessarily S-integral. In the sequel, a number field κ and a ring of S-integers $\mathcal{O}_S \subset \kappa$ will be tacitly meant to have been chosen.

We say that a rational (resp. S-integral) point p on the projective (resp. affine) curve $\mathcal{X}$ is a fake value of the morphism f if for all but finitely many valuations ν of κ, the pre-image $f^{-1}(p)$ contains a ν-adic point in $\mathcal{Y}(\kappa_\nu)$ (κ_ν denoting the completion of κ at the place ν), but no point in $\mathcal{Y}(\kappa)$ (resp. in $\mathcal{Y}(\mathcal{O}_S)$).

Noting that the polynomial $f(X) = X^8$ appearing in Grunwald-Wang example can be viewed as an isogeny $\mathbb{G}_m \to \mathbb{G}_m$, R. Dvornicich and U. Zannier in [**4**], [**5**] treated the natural generalization to isogenies of elliptic curves or of more general commutative algebraic groups (see §7 for a compairison between their constructions and ours). To our knowledge, subsequent research concentrated only on the local-to-global principle/obstructions in the context of algebraic groups.

On the contrary, in this work we shall be interested in situations where no algebraic group structure is present, and especially on morphisms to the projective line.

To state our first result we need to introduce a definition: given an algebraic curve $\mathcal{X}$ over a number field κ, we say that a subset $A \subset \mathcal{X}(\kappa)$ is a value set over κ (or simply a value set) if there exists a morphism of algebraic curves $f : \mathcal{Y} \to \mathcal{X}$ over κ, where the curve $\mathcal{Y}$ might be reducible, such that $A = f(\mathcal{Y}(\kappa))$. It is easy to see that every finite set is a value set. Also, finite unions and intersections of value sets are again value sets (for the union, just take the disjoint union of the corresponding curves $\mathcal{Y}$, while for the intersection consider the fiber product over $\mathcal{X}$).

A value set is called *κ-thin* (or simply thin) if it is the union of the images of rational points under morphisms $\mathcal{Y} \to \mathcal{X}$ without rational sections (compare with [**15**], chap. 9, [**2**], chap. 4 and [**3**], chap. 5).

When $\mathcal{X} = \mathbb{P}_1$ is the projective line, Hilbert Irreducibility Theorem guarantees that $\mathcal{X}(\kappa)$ is not a thin set.

Theorem 1.1. *Let $f : \mathcal{Y} \to \mathcal{X}$ be a finite morphism of (projective or affine) algebraic curves over a number field κ. If f admits a fake value then* $\deg f \geq 5$. *The set of fake values for f is a thin set belonging to the Boolean algebra generated by the value sets. More explicitly, it is the complement of the set $f(\mathcal{Y}(\kappa))$ in a thin value set.*

The fact that no fake value can exist for morphisms of degree ≤ 4 was observed e.g. by D. Harari and F. Voloch in [**10**] (see the proof of their Theorem 3 therein).

It is known since the eighties (Faltings' theorem) that only curves of genus ≤ 1 can contain infinitely many rational points. Also, Siegel's theorem (see e.g. Chapter 3 of [**3**]), dating back to the twenties, asserts that the only affine curves admitting infinitely many integral points, on some ring of S-integers, are those parametrized (over an extension of the ground field) by $\mathbb{A}^1$ or by $\mathbb{G}_m$.

We can prove that stronger restrictions hold if a curve is the target curve of a morphism admitting infinitely many fake values:

Theorem 1.2. *Let $f : \mathcal{Y} \to \mathcal{X}$ a morphism admitting infinitely many fake values over any sufficiently large number field. Then $\mathcal{X}$ is a rational curve. If $\mathcal{X}, \mathcal{Y}$ are smooth affine curves and $f : \mathcal{Y} \to \mathcal{X}$ a finite map admitting infinitely many integral fake values, over sufficiently large rings of S-integers, then $\mathcal{X}$ is isomorphic to the affine line $\mathbb{A}^1$.*

Here, when we say that we require fake values over sufficiently large number fields we mean the following: there exists a number filed κ', such that over every number field κ'' containing κ' the morphism admits infinitely many fake values.

In the particularly interesting case of polynomials, i.e. finite morphisms $\mathbb{A}^1 \to \mathbb{A}^1$, we found examples of polynomials of degree 5 with infinitely many fake values, although only over rings of integers containing $\mathbb{Z}[\sqrt{5}]$ (see Section 5).

We also found examples of degree thirteen over suitable (i.e. sufficiently large) rings of integers, but again no example (with infinitely many f.v.) over the ring of rational integers.

In general, such examples, both for polynomials and for morphisms of complete curves, the 'generic Galois group' (see next section for the definition) has strong restrictions. Using this fact, we prove that a sufficiently generic polynomial (in the sense specified below of a Morse polynomial) as well as a generic rational function, can have only finitely many fake values.

Following [**7**] and other authors, we say that a polynomial $f(X) \in \mathbb{C}[X]$ of degree $n \geq 1$ is a *Morse polynomial* if its derivative has $n-1$ distinct zeros and f takes distinct values at the zeros of its derivative.

We shall prove the following

Theorem 1.3. *Let $f(X) \in \mathcal{O}_S[X]$ be a Morse polynomial with S-integral coefficients. Then its set of fake values in $\mathcal{O}_S$ is finite.*

For instance, the polynomial appearing on the left-hand side of equation (2), which is a Morse polynomial, admits only finitely many fake values.

An analogous notion is defined for rational functions: a rational function $f(x) \in \mathbb{C}(x)$ is said to be a Morse function if it is a Morse function as a map from the Riemann sphere to itself. This means that it has the maximal number (i.e. $2(\deg f - 1)$) of critical points [1].

We shall prove:

Theorem 1.4. *Let $f(X) \in \kappa(X)$ be a rational function defined over the number field κ. If f is a Morse function, it admits at most finitely many fake values over κ.*

We can also provide a procedure, for each fixed degree, to effectively find out whether there exist polynomials of that degree admitting infinitely many fake values.

The techniques to prove our theorems make use of three main ingredients: the Frobenius-Chebotarev density theorem, the Galois theory of covering of the line (over the complex number field) and Siegel's (and Faltings') finiteness theorems on integral (and rational) points on curves.

After this paper was written, an anonymous referee showed us the relevant reference [**17**], where M. Stoll studies the finite descent obstruction to the local-to-global principle, proving in particular that the finite abelian descent obstruction is the only obstruction in dimension zero.

The problem treated in this work, in the particular case of polynomial maps and strongly fake values, was considered from a different perspective, namely in the frame of Bohr topology, by K. Kudin and W. Rudin in [**11**].

As it will be explained in the sequel, these topics are closely related to the problem of *Kronecker conjugacy* of polynomials, apparently introduced by H. Davenport and studied in particular by M. Fried since the sixties (see the paper [**13**] by P. Müller for further results and a bibliography). We recall that two polynomials $f(X), g(X) \in \mathbb{Z}[X]$ are said to be *Kronecker conjugate* if they share the same values set in $\mathbb{A}^1(\mathbb{F}_p)$ for all but finitely many primes p. Of course, two linearly related polynomials. i.e. pairs of polynomials of the form $(f(X), f(aX+b))$, for $a, b \in \mathbb{Q}$, with $a \neq 0$ are Kronecker conjugate. The problem in this theory is to classify pairs of Kronecker conjugate polynomials which are not linearly related. As we shall see, each such pair gives rise to a polynomial with infinitely many fake values; however, there also exist polynomials with infinitely many fake values which do not admit any non-trivial Kronecker conjugate.

[1] Note however that a Morse polynomial of degree ≥ 3, viewed as a rational function, is not a Morse function, due to the fact that the point at infinity is totally ramified.

2 - Notation and preliminaries

N o t a t i o n. The following symbols will be used throughout in the paper:

- $\mathfrak{S}_n$, the symmetric group on n objects; $\mathfrak{A}_n \subset \mathfrak{S}_n$ is the alternating group.
- For a group G acting on a set X and a point $p \in X$, G_p denotes the stabilizer of p in G.
- If κ is a number field, we denote by $\mathcal{O}_\kappa$ its ring of integers.
- For a point $x \in \mathbb{P}_N(\kappa)$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_\kappa$, $x_\mathfrak{p}$ denotes the reduction of x mod. $\mathfrak{p}$.
- For an algebraic curve $\mathcal{X}$ of genus g, we set $\chi(\mathcal{X}) = 2g - 2$ (Euler characteristic)[2] .
- For a finite set A, we denote by $\sharp(A)$ its cardinality; when A is a group, we write also $|A|$.

Let κ be a number field, $f : \mathcal{Y} \to \mathcal{X}$ be a finite morphism of smooth absolutely irreducible algebraic curves defined over κ. The Galois closure of the covering $f : \mathcal{Y} \to \mathcal{X}$ is provided by another curve $\tilde{\mathcal{Y}}$ defined over κ, possibly geometrically reducible, and a morphism $\tilde{f} : \tilde{\mathcal{Y}} \to \mathcal{X}$ defined over κ. In the sequel of this section, we suppose to have fixed the number field κ and such covers over κ

$$\tilde{\mathcal{Y}} \to \mathcal{Y} \to \mathcal{X}.$$

The Galois group of the Galois extension $\kappa(\tilde{\mathcal{Y}})/\kappa(\mathcal{X})$ is called the Galois group of f over κ and denoted by $G_{f,\kappa}$ or simply G_f, omitting the reference to the ground field κ.

If $n = \deg f \geq 1$ is the degree of f, then $G_{f,\kappa}$ and $G_{f,\bar{\kappa}} =: G_f^{\mathrm{geo}}$ are naturally faithfully represented into $\mathfrak{S}_n$, as transitive subgroups, uniquely defined up to conjugation in $\mathfrak{S}_n$.

If $\tilde{\kappa}$ is the field of scalars in $\kappa(\tilde{\mathcal{Y}})$, then the Galois group of f is the middle term of the short exact sequence

$$\{0\} \to G_f^{\mathrm{geo}} \to G_{f,\kappa} \to \mathrm{Gal}(\tilde{\kappa}/\kappa) \to \{0\}. \tag{3}$$

In terms of field extensions, the above exact sequence corresponds to the tower

$$\kappa(\mathcal{X}) \subset \tilde{\kappa}(\mathcal{X}) \subset \kappa(\tilde{\mathcal{Y}}).$$

[2]For some authors, the Euler characteristic has opposite sign

The group G_f^{geo} does not change after extending the scalars from κ to the complex number field $\mathbb{C}$. Whenever $\mathcal{X} = \mathbb{P}_1$ is the projective line, this group can be described as follows: denoting by $S \subset \mathbb{P}_1(\mathbb{C})$ the (finite) set of branched points for the morphism f, we can view f as an unramified cover $\mathcal{Y}(\mathbb{C}) - f^{-1}(S) \to \mathbb{P}_1(\mathbb{C}) - S$. Fixing a base point $p \in \mathbb{P}_1(\mathbb{C}) - S$, the fundamental group $\pi_1(\mathbb{P}_1(\mathbb{C}) - S, p)$ acts on the fiber of p for f, which is a set of cardinality $n = \deg f$. The image of $\pi_1(\mathbb{P}_1(\mathbb{C}) - S, p)$ in $\mathfrak{S}_n$, depending only on a numbering of the fiber $f^{-1}(p)$, is isomorphic to G_f^{geo}.

Given a subgroup $H \subset G_{f,\kappa}$, we define the corresponding algebraic curve $\mathcal{U}_H$ over κ to be the quotient $\tilde{\mathcal{Y}}/H$; its function field is the fixed field $\kappa(\tilde{\mathcal{Y}})^H$ for the subgroup H. Each such curve is endowed with a projection $\mathcal{U}_H \to \mathcal{X}$. Note that $\mathcal{U}_H$ is absolutely irreducible if and only if the projection $H \to \mathrm{Gal}(\tilde{\kappa}/\kappa)$ is surjective.

Given a point $x \in \mathcal{X}(\kappa)$, its fiber $f^{-1}(x)$ is a finite union of Galois orbits for the action of $\mathrm{Gal}(\tilde{\kappa}/\kappa)$ on the set $\mathcal{X}(\bar{\kappa})$ of the geometric points of $\mathcal{X}$. We define the Galois group of $f^{-1}(x)$ to be the image of $\mathrm{Gal}(\tilde{\kappa}/\kappa)$ under this action.

The following result is well known.

P r o p o s i t i o n 2.1. *Let $f : \mathcal{Y} \to \mathcal{X}$ a finite morphism of algebraic curves over a number field κ. Let $x \in \mathcal{X}(\kappa)$ a rational point. The Galois group of $f^{-1}(x)$ is a sub-group of $G_{f,\kappa}$. Let $q \in \mathcal{Y}(\bar{\kappa})$ be an (algebraic) point in the fibre $f^{-1}(x)$ of x. Let $\kappa(q)$ be the field of definition of q. Then the Galois group of the Galois-closure of the field extension $\kappa(q)/\kappa$ is a quotient of a subgroup of $G_{f,\kappa}$.*

3 - Application of Frobenius-Chebotarev and Jordan's theorems

In this section we give a characterization of the set of fake values, by proving Theorem 1.1. We start with a definition:

D e f i n i t i o n - *Property* $(*)$. Given an integer $n \geq 1$ and a subgroup $H \subset \mathfrak{S}_n$ of the n-th symmetric group, we say that H has the *property* $(*)$ if it satisfies the following two conditions

1. *Every permutation in H has a fixed point.*

2. *For every point $p \in \{1, \ldots, n\}$ there exists an element $h \in H$ with $h(p) \neq p$.*

In other words, setting, for each point $p \in \{1, \ldots, n\}$, G_p the stabilizer of p

in $\mathfrak{S}_n$, a subgroup $H \subset \mathfrak{S}_n$ satisfies property $(*)$ if and only if

$$H \subset \bigcup_{p\in\{1,\dots,n\}} G_p = \bigcup_{g\in\mathfrak{S}_n} g\, G_n\, g^{-1}$$

but $H \not\subset G_p$ for any $p \in \{1, \dots, n\}$.

Note that if $G \subset \mathfrak{S}_n$ is a *transitive* subgroup, then the conditions above can be restated forgetting the reference to $\mathfrak{S}_n$: letting $K \subset G$ be the stabilizer of a point, noticing that the other stabilizers are the conjugates of K in G we can state condition $(*)$ as

$$\begin{array}{lllll} (*1) & H & \subset & \bigcup_{\gamma\in G} \gamma K \gamma^{-1} & \\ (*2) & H & \not\subseteq & \gamma K \gamma^{-1}, & \forall \gamma \in G. \end{array}$$

We can now classify the fake values by their Galois theoretic properties as follows:

P r o p o s i t i o n 3.1. *Let $f : \mathcal{Y} \to \mathcal{X}$ a finite morphism of algebraic curves over a number field κ and let $x \in \mathcal{X}(\kappa)$ be a fake value. Let $\tilde{\mathcal{Y}} \to \mathcal{X}$ be the Galois closure over κ of the cover $f : \mathcal{Y} \to \mathcal{X}$. Then the zero-dimensional variety $f^{-1}(x)$ is reducible over κ. Let $H \subset G_{f,\kappa} \subset \mathfrak{S}_n$ be the Galois group of its residue field. Then H has the property $(*)$.*

This proposition was essentially already known: for instance, the reducibility of the fiber was remarked by M. Stoll in [**17**] (see the proof of his Proposition 5.12). The proof of Proposition 3.1 makes use of the following two well-known results:

L e m m a 3.2 (Frobenius density theorem). *Let K/κ be a Galois extension of a number field, with Galois group H. Let $H \hookrightarrow \mathfrak{S}_n$ be a faithful permutation representation of H. Let $C \subset H$ be an equivalence class of elements of H which are conjugate in $\mathfrak{S}_n$. Then there exist infinitely many prime ideals $\mathfrak{p}$ in $\mathcal{O}_\kappa$ whose Frobenius class lies in C.*

The above lemma has actually be improved by Chebotarev, who replaced the equivalence relation induced by the embedding $H \hookrightarrow \mathfrak{S}_n$ by the finer relation of conjugation inside H.

L e m m a 3.3 (Theorem of Jordan). *Let G be a finite group acting transitively on a finite set with at least two elements. Then there exists an element of G fixing no point.*

This second lemma is a theorem of Jordan. It can be rephrased by saying that a group action with property $(*)$ is never transitive. In still another formulation: no finite group is covered by the union of the conjugates of a proper subgroup.

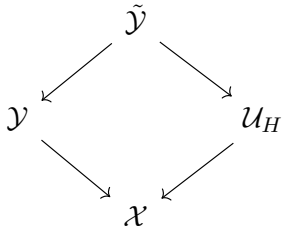
The reader is referred to Serre's paper [**16**], who provides two proofs of Jordan's theorem, as well as a proof of our Proposition 3.1 in the particular case of polynomial morphisms. Our proof is basically the same.

Proof of Proposition 3.1. Let $m \leq \deg f$ be the cardinality of the fiber $f^{-1}(x) \subset \mathcal{Y}(\bar{\kappa})$. The Galois group H of the residue field of the (geometric points of the) set $f^{-1}(x)$ acts on this set of cardinality m, so is (faithfully) represented in $\mathfrak{S}_m$. Let $h \in H$ be an element of the Galois group. For all but finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_\kappa$, the set $f^{-1}(x_\mathfrak{p})$ (where we used the symbol f also to designate the induced morphism on the reduced varieties $\mathcal{Y}_\mathfrak{p} \to \mathcal{X}_p$) is formed by m points in $\mathcal{Y}_\mathfrak{p}(\overline{\mathcal{O}_\kappa/\mathfrak{p}})$. The Frobenius automorphism of $\mathfrak{p}$ acts on this fiber. By Frobenius' theorem, there exist infinitely many primes $\mathfrak{p}$ of $\mathcal{O}_\kappa$ such that the corresponding Frobenius automorphism lifts to an element in the conjugacy class of h. Now, if x admits a $\mathfrak{p}$-adic lift to $\mathcal{Y}$, then $x_\mathfrak{p}$ admits a lift to a $\mathcal{O}_\kappa/\mathfrak{p}$-rational point in $\mathcal{Y}_\mathfrak{p}$. This means that one of the points of the fiber of $x_\mathfrak{p}$ is fixed by the Frobenius automorphism. But since this Frobenius automorphism lies in the class of h, the automorphism h itself must have a fixed point. This proves that every element of H has a fixed point. However, since x is a *fake* value, there is no point in $f^{-1}(x)$ fixed by the whole group H; these two facts mean precisely that H has the property $(*)$.

By the Theorem of Jordan, the action of H on the fiber $f^{-1}(x)$ cannot be transitive, so the fiber is reducible over κ. □

Take then a fake value x for a morphism $f : \mathcal{Y} \to \mathcal{X}$. Letting as before $\tilde{\mathcal{Y}} \to \mathcal{X}$ be the Galois closure of the cover $f : \mathcal{Y} \to \mathcal{X}$, there exists a subgroup $H \subset G_f$ with property $(*)$ such that the Galois group of the residue field of the fiber of $f^{-1}(x)$ is H. This means that if we let $\mathcal{U}_H$ be the algebraic curve $\tilde{\mathcal{Y}}/H$, corresponding to the fixed field $\tilde{\kappa}(\tilde{Y})^H$, then x is the image of a κ-rational point of $\mathcal{U}_H$. Below the diagram of algebraic curves and morphisms.

(4)



From the above discussion we obtain the

Theorem 3.4. *We keep the above notation. The set of fake values is contained in the union of the images of the rational points of the curves $\mathcal{U}_H$, for $H \subset G_f$ satisfying Property $(*)$.*

More precisely, the set of fake values is the complement of the set $f(\mathcal{Y}(\kappa))$ inside this union.

Note that, since H must always be a proper subgroup of G_f, the degree of each morphism $\mathcal{U}_H \to \mathcal{X}$ must be ≥ 2. Hence the above statement implies the last part of Theorem 1.1.

To end the proof of that theorem, it remains to exclude the existence of any fake value in degree ≤ 4. Indeed, suppose that x is a rational point of $\mathcal{X}$ whose fiber is reducible over κ; in degree 2 or 3, any reducible fiber has a rational point, so that x is actually a rational value of the morphism; in degree 4, the number field extension associated to a reducible fiber must be the compositum of two quadratic extensions: now, there are infinitely many primes which are inert for both extensions, and these primes do not admit lifting of the given rational point.

This achieves the proof of Theorem 1.1. □

Note that each fake value in degree five has the property that its fiber splits into two components, one of degree three and the other of degree two; the quadratic number field corresponding to the second component is the quadratic extension contained in the sextic extension obtained as the Galois closure of the field of definition of any (cubic) point in the degree-three component.

We now prove Theorem 1.2. Its proof needs the following elementary lemma from group theory:

Lemma 3.5. *Let G be a finite group, $K \subset G$ a subgroup and $H \lhd G$ a normal subgroup. If*

$$H \subset \bigcup_{\gamma \in G} \gamma K \gamma^{-1},$$

then $H \subset K$.

Proof. From the above inclusion and the fact that H is normal it follows that H is also included into $\bigcup_{\gamma \in G} \gamma K \cap H\gamma^{-1}$. By Jordan's Theorem, this implies that $K \cap H$ is not a proper subgroup of H, i.e. $H \subset K$ as wanted. □

Proof of Theorem 1.2. Suppose that $f : \mathcal{Y} \to \mathcal{X}$ is a finite morphism of degree n, defined over a number field κ, admitting infinitely many fake values over arbitrarily large number fields $\kappa' \supset \kappa$. By taking κ' sufficiently large, we can suppose that the group $G_{f,\kappa'}$ coincides with its geometric part G_f^{geo}.

Recall that we want to rule out the possibility that $\mathcal{X}$ has genus one (in the projective case) and that $\mathcal{X} \simeq \mathbb{G}_m$ (in the affine case).

Consider an infinite family of fake values provided by a cover $\mathcal{U}_H \to \mathcal{X}$ as described in the proof of Theorem 1.1 and suppose by contradiction that $\mathcal{X}$ has genus one (in the projective case) or $\mathcal{X} \simeq \mathbb{G}_m$ (in the affine case). Then, by Faltings' theorem in the projective case $\mathcal{U}_H$ must also have genus 1, while in the affine case by Siegel's theorem $\mathcal{U}_H \simeq \mathbb{G}_m$. In both cases the map $\mathcal{U}_H \to \mathcal{X}$ must be unramified, and must also be an abelian cover of $\mathcal{X}$. Then $H \lhd \mathbb{G}_f^{\mathrm{geo}}$ is a normal subgroup of G_f^{geo} (with abelian quotient). However, as proved in the above lemma, a normal subgroup H of a transitive group $G_f^{\mathrm{geo}} \subset \mathfrak{S}_n$ cannot have property $(*)$. □

To construct examples of morphisms $f : \tilde{\mathcal{Y}} \to \tilde{\mathcal{X}}$ with infinitely many fake values, one must then find a cover such that there exists a subgroup $H \subset G_f$ satisfying property $(*)$ such that the corresponding curve $\mathcal{U}_H$ in the diagram (4) has infinitely many rational (or integral) points. The subgroup H too can be viewed as the stabilizer of a point in a suitable action of G_f on a finite set (for instance the pre-image of an unramified point in the fiber of the morphism $g : \mathcal{U}_H \to \mathcal{X}$). Then condition $(*)$ can be rephrased in the following way: *the group G_f acts on two sets, one of cardinality* $\deg f$ *and one of cardinality* $\deg g$*, in such a way that whenever an element $\gamma \in G_f$ fixes a point in the second set it also fixes a point in the first one.*

In this work, we shall be interested in producing examples of infinite families of fake values over arbitrarily large number fields (or arbitrarily large rings of S-integers). Hence we shall consider mainly the geometric part G_f^{geo} of the Galois group G_f, and look for groups admitting two distinct "interesting" actions with the above property. In particular, our groups G_f^{geo} will never be abelian, which rules out the examples concerning isogenies of commutative algebraic groups considered in [**4**], [**5**].

4 - Proof of Theorems 1.3 and 1.4

Let $\mathcal{O}_S \subset \kappa$ be a ring of integers of a number field, and $f(X) \in \mathcal{O}_S[X]$ a Morse polynomial of degree $n \geq 5$.

We start by showing that the geometric Galois group G_f^{geo} is the full group $\mathfrak{S}_n$. This fact can be viewed by observing, as we did in §2, that the geometric Galois group is represented in $\mathfrak{S}_n$ as the monodromy action of the fundamental group of the complement in $\mathbb{P}_1(\mathbb{C})$ of the ramification values of the map f, viewed as a morphism of the Riemann sphere $\mathbb{P}_1(\mathbb{C})$ to itself. Due to the hypothesis on f, this permutation group is generated by transpositions; now,

every transitive subgroup of $\mathfrak{S}_n$ generated by transpositions is the full group.

Since the full Galois group G_f is always contained in $\mathfrak{S}_n$ (in its canonical representation) and contains its geometric part G_f^{geo}, which in the present case is the full group $\mathfrak{S}_n$, we must have $G_f = \mathfrak{S}_n$.

Now, letting as before $\tilde{\mathcal{Y}}$ be the Galois closure of the covering $f : \mathbb{P}_1 \to \mathbb{P}_1$, we can calculate the Euler characteristic of $\tilde{\mathcal{Y}}$ via Hurwitz formula: taking into account that the point $\infty \in \mathbb{P}_1$ is totally ramified (i.e. of index $n = \deg f$) in the cover $f : \mathbb{P}_1 \to \mathbb{P}_1$ and that $n-1$ points admit one single pre-image with ramification index 2 (the other pre-images being unramified), the morphism $\tilde{\mathcal{Y}} \to \mathbb{P}_1$ admits $n!/n$ ramified points of index n and $n!(n-1)/2$ ramified points of index 2. Hence

$$\chi(\tilde{\mathcal{Y}}) = -2n! + \frac{n!}{n}(n-1) + \frac{n!(n-1)}{2} = n!\left(\frac{n-1}{n} + \frac{n-1}{2} - 2\right). \tag{5}$$

Suppose now that the morphism $f : \mathbb{P}_1 \to \mathbb{P}_1$ admits infinitely many fake values. Then there must exist an infinite family of such fake values, all obtained as images of rational points from a curve $g : \mathcal{U}_H \to \mathbb{P}_1$, associated to a subgroup $H \subset \mathfrak{S}_n$ satisfying property $(*)$. Moreover, the affine curve $\mathcal{U}_H - g^{-1}(\infty)$ must contain infinitely many S-integral points. By Siegel's theorem, this forces the Euler characteristic of $\mathcal{U}_H$ to be strictly negative (and the set $g^{-1}(\infty)$ to have cardinality ≤ 2).

Consider then the cover $\tilde{\mathcal{Y}} \to \mathcal{U}_H$. Again by Hurwitz formula, the relation between the Euler charcateristics of the curves $\mathcal{U}_H$ and $\tilde{\mathcal{Y}}$ reads

$$\chi(\mathcal{U}_H) = \frac{\chi(\tilde{\mathcal{Y}}) - \mathrm{Ram}(\tilde{\mathcal{Y}}/\mathcal{U}_H)}{\sharp(H)},$$

where $\mathrm{Ram}(\tilde{\mathcal{Y}}/\mathcal{U}_H) = \sum_{p \in \tilde{\mathcal{Y}}}(e_p - 1)$, and e_p is the ramification at p of the cover $\tilde{\mathcal{Y}} \to \mathcal{U}_H$. Hence, in order to have $\chi(\mathcal{U}_H) < 0$, we must have

$$\mathrm{Ram}(\tilde{\mathcal{Y}}/\mathcal{U}_H) > \chi(\tilde{\mathcal{Y}}) = n!\left(\frac{n-1}{n} + \frac{n-1}{2} - 2\right). \tag{6}$$

Now, the ramified points of such a cover are those points $p \in \tilde{\mathcal{Y}}$ whose stabilizer H_p is non-trivial. Recall that there are $n!/n$ points in $\tilde{\mathcal{Y}}$ whose stabilizer in $\mathfrak{S}_n = G_f^{\mathrm{geo}}$ has order n and all the other points have a stabilizer which is either trivial or of order 2; these last stabilizers are generated by transpositions. Since the subgroup $H \subset \mathfrak{S}_n$ satisfies property $(*)$, no power of any n-cycle (apart the identity) can be contained in H. Hence the only elements of H fixing some point in $\tilde{\mathcal{Y}}$ are the transpositions.

Observe now that all the transpositions in $\mathfrak{S}_n$ are conjugate to each other, so their set of fixed points has the same cardinality. Since $\mathfrak{S}_n$ contains $\binom{n}{2}$

transpositions, and there are $n!(n-1)/2$ points fixed by a transposition, it follows that each transposition fixes exactly $[n!(n-1)/2]/\binom{n}{2} = (n-1)!$ points. This holds in particular for all the transpositions belonging to the subgroup H, so

$$\mathrm{Ram}(\tilde{\mathcal{Y}}/\mathcal{U}_H) = h(n-1)!,$$

where h is the number of transpositions in H. From (6) and the above identity we obtain

$$h(n-1)! > n!\left(\frac{n-1}{n} + \frac{n-1}{2} - 2\right),$$

i.e.

$$h > n - 1 + \frac{n(n-1)}{2} - 2n = \binom{n}{2} - n - 1. \tag{7}$$

In other words, H must contain all but at most n transpositions of the symmetric group $\mathfrak{S}_n$.

Recall also that H is non-transitive (otherwise, by Jordan's theorem, it cannot satisfy property $(*)$) and not contained in the stabilizer of a point. Then H conserves a partition of $\{1,\dots,n\}$ of the form $\{1,\dots,k\}\cup\{k+1,\dots,n\}$, for some $1 < k < n-1$. But then the number h of transpositions in H is bounded as

$$h \le \binom{k}{2} + \binom{n-k}{2} \le 1 + \binom{n-2}{2},$$

which, together with the lower bound (7), forces $n \le 4$. However, we are supposing here $n \ge 5$, and this concludes the proof. □

Theorem 1.4 is proved in a similar way. Again, a Morse function $f : \mathbb{P}_1 \to \mathbb{P}_1$ of degree n has a Galois group $G_f = G_f^{\mathrm{geo}} \simeq \mathfrak{S}_n$. Letting again $\tilde{\mathcal{Y}} \to \mathbb{P}_1$ be the Galois closure of the cover $f : \mathbb{P}_1 \to \mathbb{P}_1$, every ramified point in the cover $\tilde{\mathcal{Y}} \to \mathbb{P}_1$ has ramification index 2. Since the ramification divisor has degree $2n-2$, there are $n!(2n-2)/2$ ramified points for the cover $\tilde{\mathcal{Y}} \to \mathbb{P}_1$. Hence the Euler characteristic of $\tilde{\mathcal{Y}}$ equals

$$\chi(\tilde{\mathcal{Y}}) = n!(n-3).$$

As before, a subgroup $H \subset \mathfrak{S}_n$ giving rise to an infinite family of fake values must satisfy property $(*)$ and the corresponding curve $\mathcal{U}_H = \tilde{\mathcal{Y}}/H$ must satisfy $\chi(\mathcal{U}_H) \le 0$, by Faltings' theorem. An argument similar to the previous one shows that each transposition in $\mathfrak{S}_n$ fixes $2(n-1)!$ points of $\tilde{\mathcal{Y}}$. Hence H must contain at least $n!(n-3)/2(n-1)! = n(n-3)/2$ transpositions. Then the proof is concluded exactly as before.

5 - Examples in degree five

`The Icosahedral group`. The icosahedral group is defined as the group of rotations of the icosahedron. It is isomorphic to the alternating group $\mathfrak{A}_5$ and constitutes one of the "coincidences" in the classification of finite simple groups, in the sense that it belongs to three different series of simple groups. Namely, we have the isomorphisms

$$\mathfrak{A}_5 \simeq \mathrm{SL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_5).$$

It acts naturally on a five-point set, e.g. the set $\mathbb{P}_1(\mathbb{F}_4)$, but also on a ten-point set: the set of unordered pairs of points in $\mathbb{P}_1(\mathbb{F}_5)$, or the set of opposite pairs of sides of an icosahedron. It also acts on the set $\mathbb{P}_1(\mathbb{F}_{16}) - \mathbb{P}_1(\mathbb{F}_4) = \mathbb{F}_{16} - \mathbb{F}_4$, containing twelve points, the number of faces of a dodecahedron and of vertices of an icosahedron. Note that this last action is imprimitive, since the Frobenius automorphism of the extension $\mathbb{F}_{16}/\mathbb{F}_4$ acts on the twelve-point set $\mathbb{P}_1(\mathbb{F}_{16}) - \mathbb{P}_1(\mathbb{F}_4)$, and its action commutes with the action of $\mathrm{SL}_2(\mathbb{F}_4)$. This is in accordance wth the fact that the rotation group of the icosahedron too acts imprimitively on the vertices of the icosahedron, since its action commutes with the antipodal map. Hence, we obtain an action on a six-point set, namely the set of opposite pairs of vertices of the icosahedron. This last action can be viewed via the isomorphism $\mathfrak{A}_5 \simeq \mathrm{PSL}_2(\mathbb{F}_5)$ and the six-point set can be identified with $\mathbb{P}_1(\mathbb{F}_5)$. Using the same trick as above, we obtain an action on $\mathbb{P}_1(\mathbb{F}_{25}) - \mathbb{P}_1(\mathbb{F}_5)$, which contains twenty points, as many as the faces of an icosahedron. Again, this action is imprimitive, since it commutes with that of the Frobenius involution (corresponding again to the antipodal map on the icosahedron). Finally, recall that an icosahedron has thirty edges: the number thirty is the cardinality of the set of $\mathbb{F}_5$-rational points in the surface $\mathbb{P}_1 \times \mathbb{P}_1 - \Delta$, Δ being the diagonal of $\mathbb{P}_1 \times \mathbb{P}_1$, and the action of $\mathrm{PSL}_2(\mathbb{F}_5)$ on that surface being the obvious one.

As we observed, in order to produce infinite families of fake values it is important to realize a finite group as a Galois group of an extension of function fields, and to compare *two* actions of that group.

`A first example`. We shall start with the action of $G = \mathfrak{A}_5$ on a five-point set, deriving from the monodromy action of a degree five cover of the projective line. More precisely, we look for a polynomial $f(X) \in \mathbb{Q}[X]$ of degree five, inducing a cover $\mathbb{P}_1 \to \mathbb{P}_1$ whose monodromy group is the alternating group. We shall use a cover which ramifies only over three points (the minimal number of branched points for a non-abelian cover). Start from the identity

$$(1,2,4) \circ [(2,3) \circ (4,5)] = (1,2,3,4,5)$$

which shows that the groups $\mathfrak{A}_5$ can be generated by a three-cycle and a product of two disjoint transpositions, whose product is a five-cycle. We can then represent the fundamental group $\pi_1(\mathbb{P}_1(\mathbb{C}) - \{p_1, p_2, \infty\})$, for any choice of $p_1, p_2 \in \mathbb{C}$, in the alternating group $\mathfrak{A}_5$, by sending one generator, corresponding to a loop around p_1, to the three-cycle $(1, 2, 4)$, and the second generator, corresponding to a loop around p_2, to the permutation $(2, 3) \circ (4, 5)$. The product of these elements of the fundamental group will correspond to a loop around ∞. We then look for a cover which is totally ramified over ∞, and has two more branched points: for one of them the pre-image has a ramified point of order 3, for the second one two ramified points of order 2, all the remaining pre-images being unramified.

A concrete instance is represented by the polynomial

$$f(X) = 9X^5 + 15X^4 + 40X^3 = X^3(9X^2 + 15X + 40). \tag{8}$$

It ramifies over 0 and 64. It defines a cover $f : \mathbb{P}_1 \to \mathbb{P}_1$ whose Galois closure is given by a rational curve $\tilde{\mathcal{Y}} \simeq \mathbb{P}_1$, as it can be shown using the Hurwitz formula: indeed the degree of the cover $\tilde{\mathcal{Y}} \to \mathbb{P}_1$ is $60 = |\mathfrak{A}_5|$. The ramified points form three orbits: one of them is the pre-image of ∞ and contains 12 points with ramification index 5; a second one is the pre-image of 0: it contains 20 points with ramification index 3; the third one consists in the pre-image of 64, and contains 30 points with ramification index 2. Then the Euler characteristic of $\tilde{\mathcal{Y}}$ turns out to be $-2 \cdot 60 + 12 \cdot 4 + 20 \cdot 2 + 30 = -2$, which forces $\tilde{\mathcal{Y}}$ to be a rational curve (over $\bar{\mathbb{Q}}$ at least).

The icosahedral pattern is well recognizable. Since, however, the icosahedral group cannot act on $\mathbb{P}_1$ over the rationals, the Galois group $G_{f,\mathbb{Q}}$ must then be the full group $\mathfrak{S}_5$. However, after replacing $\mathbb{Q}$ by $\mathbb{Q}(\sqrt{5})$, we would obtain a Galois group $G_{f,\mathbb{Q}(\sqrt{5})} = G_f^{\mathrm{geo}} = \mathfrak{A}_5$.

We have now to look for a group H satisfying property $(*)$. Automatically the curve $\mathcal{U}_H = \tilde{\mathcal{Y}}/H$ will be rational and will provide infinitely many rational fake values for the morphism f. However, if we want to construct infinitely many *integral* fake values, we must also construct such a curve $\mathcal{U}_H$ so that, denoting by $g : \mathcal{U}_H \to \mathbb{P}_1$ the corresponding morphism, the pre-image $g^{-1}(\infty)$ of the point at infinity has cardinality ≤ 2. Otherwise, by Siegel's theorem, the affine curve $\mathcal{U}_H - \{g^{-1}(\infty)\}$ will have only finitely many integral points, so only finitely many fake values so constructed will be integral.

To construct the subgroup H, consider the mentioned action of $G = \mathfrak{A}_5$ on a ten point set and define H to be the stabilizer of one of these points. For instance, H can be taken to be the subgroup of G sabilizing the set $\{1, 2\} \subset \{1, \ldots, 5\}$, i.e. fixing one element in the set of cardinality $\binom{5}{2} = 10$ consisting of the cardinality-two subsets of $\{1, \ldots, 5\}$. We claim that H has the property

$(*)$. This means that every even permutation stabilizing $\{1,2\}$ admits at least one fixed point: indeed, if this permutation does not fix 1 and 2, it interchanges them and so acts on the set $\{3,4,5\}$ via an odd permutation, which necessarily fixes one of these last three points.

Let us study now the morphisms $\tilde{\mathcal{Y}} \to \mathcal{U}_H \to \mathbb{P}_1$, in order to detect the pre-image of ∞ with respect to the last arrow. Note that the index of H in G is 10, so the degree of the morphism $g : \mathcal{U}_H \to \mathbb{P}_1$ is also 10. Since H contains no 5-cycle, no point of $\tilde{\mathcal{Y}}$ lying over ∞ ramifies in the projection $\tilde{\mathcal{Y}} \to \mathbb{P}_1$. Hence the pre-image of ∞ in $\mathcal{U}_H$ must be ramified with index 5, so $g^{-1}(\infty)$ cosists in two points.

We then obtain that, over a suitable ring of S-integers, the polynomial $f(X)$ defined in (8) admits infinitely many fake values. These fake values are parametrized by the units in such a ring of S-integers, being values at S-units of a degree ten Laurent polynomial $g(t) \in \mathbb{Q}(\sqrt{5})[t^{\pm 1}]$.

We note that in this case the polynomial f and the Laurent polynomial g play symmetrical roles. If we let K be the stabilizer of a point for the action of $G = \mathfrak{A}_5$ on a five point set, while H is the stabilizer of a point in the ten point set acted on by the same group G, as described above, we have that each element of H fixes a point on the first set (of cardinality 5), while each element of K fixes a point in the second set (in other words: every even permutation of $\{1,\dots,5\}$ fixing one point admits an invariant subset of cardinality 2). It follows that not only each rational value of g is a fake value of f, unless it is a rational value of f too, but also that each rational value of f which is not a rational value of g is a fake value for g.

`A second example`. Here we construct another example of a degree five polynomial admitting infinitely many fake values, over arbitrary number fields; however, this second polynomial admits only finitely many *integral* fake values, over any ring of S-integers.

We start from the identity

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

holding in $\mathfrak{A}_5$. Interpreting as above the first permutation as a loop around, say, the point $0 \in \mathbb{P}_1$ and the second permutation as a loop around the point $1 \in \mathbb{P}_1$, their product corresponds to a loop around ∞. Hence we obtain a representation of $\pi_1(\mathbb{P}_1 - \{0,1,\infty\}) \to \mathfrak{A}_5$ which corresponds to a cover $f : \mathbb{P}_1 \to \mathbb{P}_1$, totally ramified over ∞, and such that the pre-images of 0 and 1 both consist in three points, one of which is ramified at order 3.

A concrete example is represented by the polynomial

$$f(x) = 6X^5 - 15X^4 + 10X^3.$$

The Galois closure of the corresponding cover is provided by a curve $\tilde{\mathcal{Y}}$ of genus 5. The quotient $\mathcal{U}_H = \tilde{\mathcal{Y}}/H$ by the same subgroup $H \subset \mathfrak{A}_n$ considered in the previous example turns out to have genus 1; it provides a cover $g : \mathcal{U}_H \to \mathbb{P}_1$ fitting in the diagram (4). Then, over a suitable number field, $\mathcal{U}_H$ contains infinitely many rational points, and their images in $\mathbb{P}_1$ are fake values for f, up to finitely many exceptions. However, only finitely many of such fake values are algebraic integers, or more generally S-integers for any fixed finite set of places S, since the affine curve $\mathcal{U}_H - g^{-1}(\infty)$ has only finitely many integral points by Siegel's theorem.

`An example involving elliptic curves`. This time we start from the Galois closure $\tilde{\mathcal{Y}}$ of our cover $f : \mathcal{Y} \to \mathbb{P}_1$, to be defined later.

We consider the so-called Bring's curve (see W.L. Edge's paper [**6**] or the one by M. Weber [**19**]), defined as the complete intersection in $\mathbb{P}_4$:

$$\tilde{\mathcal{Y}}: \quad \begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 &= 0 \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 &= 0 \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 &= 0. \end{cases} \tag{9}$$

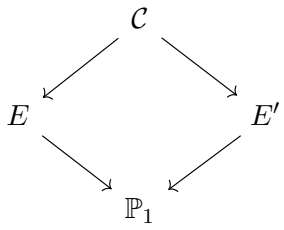
It has genus four and is acted on in the obvious way by the symmetric group $\mathfrak{S}_5$, the action being defined over $\mathbb{Q}$. We shall first consider the action of the subgroup $\mathfrak{A}_5 \subset \mathfrak{S}_5$ on $\tilde{\mathcal{Y}}$.

The elements of order five of $\mathfrak{A}_5$ have four fixed points each on $\tilde{\mathcal{Y}}$: for instance the five-cycle $(1, 2, 3, 4, 5)$ fixes the point $(1 : \zeta : \zeta^2 : \zeta^3 : \zeta^4)$, for each primitive fifth root of unity ζ. Since $\mathfrak{A}_5$ contains six cyclic subgroups of order five, and each subgroup has four fixed points, there are 24 points of $\tilde{\mathcal{Y}}$ whose stabilizer has order five. It follows that they form two orbits for the group $\mathfrak{A}_5$. The elements of order two in $\mathfrak{A}_5$ fix two points each: for instance the involution $(1, 2) \circ (3, 4)$ fixes the points $(1 : -1 : \xi : -\xi : 0)$ where $\xi^2 = -1$. This family of points forms a unique orbit.

It then follows from Hurwitz genus formula that the quotient $\tilde{\mathcal{Y}}/\mathfrak{A}_5$ is isomorphic to the projective line $\mathbb{P}_1$ (actually also over $\mathbb{Q}$). Letting $K \subset \mathfrak{A}_5$ be the stabilizer of a point for the action of $\mathfrak{A}_5$ on five points, the curve $E := \tilde{\mathcal{Y}}/K$ turns out to have genus one. The cover $f : E \to \mathbb{P}_1$ has degree five, and ramifies over three points with indices $5, 5, 2$. Letting again H be the stabilizer of a two-point subset of the five-point set acted on by $\mathfrak{A}_5$, we obtain that the curve $\mathcal{U}_H =: E'$ too has genus one. Also, it is isogenous to E (see [**19**], where M. Weber proves that the jacobian of Bring's curve $\tilde{\mathcal{Y}}$ is the fourth-power of a single elliptic curve).

If K stabilizes the point $5 \in \{1, \ldots, 5\}$ and H the sub-set $\{1, 2\}$, so that $K \cap H =< (1, 2) \circ (3, 4) >$ then the fiber product $\mathcal{C} = E \times_{\mathbb{P}_1} E'$ turns out to be

a genus-two curve. We then obtain the diagram

(10)


The morphism $g : E' \to \mathbb{P}_1$ has degree 10 and each of its rational values, apart finitely many of them - precisely those coming from rational points on the genus-two curve $\mathcal{C}$ - are fake values for the degree-five morphism $f : E \to \mathbb{P}_1$. The vice-versa also holds, since the subgroup K is also included in the union of the conjugates of H: not only the rational values of g are fake values for f, but also the rational values of f are fake values for g.

Up to now, this symmetry occured in every example of infinite families of fake values. However, this is not a general fact, as we shall se in our next example.

`Another example in degree five`. We slightly modify the last construction, by exploiting the action of the full group $\mathfrak{S}_5$ on Bring's curve $\tilde{\mathcal{Y}}$. The quotient curve $\tilde{\mathcal{Y}}/\mathfrak{S}_5$ is clearly rational, since it is dominated by $\tilde{\mathcal{Y}}/\mathfrak{A}_5$, which was proved to be rational (even over $\mathbb{Q}$). Letting K' be the stabilizer of a point for the action of $\mathfrak{S}_5$ on a five-point set, the curve $\tilde{\mathcal{Y}}/K'$ turns out to be rational, and the corresponding morphism $f' : \mathbb{P}_1 \to \mathbb{P}_1$ is represented by a rational function of degree five.

Since $H \supset K$ and $H \subset \bigcup_{\gamma\in\mathfrak{A}_5} \gamma K \gamma^{-1}$, *a fortiori* $H \subset \bigcup_{\gamma\in\mathfrak{S}_5} \gamma K' \gamma^{-1}$. However, this time it is not true that K' is included in the union of the conjugates of H.

The inclusion $K' \subset \mathfrak{S}_5$ corresponds to a morphism $g' : E' \to \mathbb{P}_1$, obtained as $g' = h \circ g$ where $g : E' \to \mathbb{P}_1$ is the arrow appearing in diagram (10) and $h : \mathbb{P}_1 \to \mathbb{P}_1$ is a quadratic morphism.

This time, the rational values of g' are fake values for f', with finitely many exceptions, but the vice-versa does not hold.

6 - Examples in degree seven and thirteen

We present two more examples, already known in the literature. They arise as examples of pairs of Kronecker conjugate polynomials, i.e. pairs of

polynomials, not linearly related, representing the same set of values modulo all but finitely many primes. However, this phenomenon does not occur over $\mathbb{Q}$, but only over sufficiently large number fields.

`The simple group with` 168 `elements`. Another coincidence in the list of finite simple groups is represented by the isomorphism

$$\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{SL}_3(\mathbb{F}_2) =: G. \tag{11}$$

The the group G admits two natural actions: on the projective line over $\mathbb{F}_7$, which contains eight rational points, and on the 'Fano plane', i.e. the set $\mathbb{P}_2(\mathbb{F}_2)$, consisting of seven points, arranged so that every line contains three points and every point is contained in three lines.

This group can be generated by three elements a, b satisfying $a^2 = b^3 = (ab)^7 = 1$. It is the "smallest" hyperbolic triangle group. Using the representation of G as 3×3 matrices in $\mathbb{F}_2$, the group G acts naturally on $\mathbb{P}_2(\mathbb{F}_2)$, consisting of seven points and seven lines. The two matrices

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

have indeed order 2 and 3, while their product has order 7.

Viewing G as the group $\mathrm{PSL}_2(\mathbb{F}_7)$, acting on $\mathbb{P}_1(\mathbb{F}_7) = \mathbb{F}_7 \cup \{\infty\}$, it can be generated by the projective automorphisms:

$$a : x \mapsto -1/x, \qquad b : x \mapsto -1/(x+1), \tag{12}$$

of respective order 2 and 3. Their product has order 7. In the isomorphism between $\mathrm{SL}_3(\mathbb{F}_2)$ and $\mathrm{PSL}_2(\mathbb{F}_7)$ the pair (A, B) can be identified with (a, b).

`An example in degree seven`. Using the realization of the group G defined in (11) as the automorphism group of $\mathbb{P}_2(\mathbb{F}_2)$, G can be viewed as the monodromy group of a degree seven polynomial map $f : \mathbb{P}_1 \to \mathbb{P}_1$, totally ramified over ∞ and ramified also over 0 and 1. The fiber of 0 consists of two points ramified at order 3 and one unramified points (the local monodromy over 0 being represented by the permutation induced by the matrix B), while the fiber of 1 consists in two ramified points (of index 2 each) and three unramified ones, in accordance to the fact that A induces an automorphism with three fixed points.

The Galois closure (over $\bar{\mathbb{Q}}$) of such a cover is represented by a genus-three curve, which is the famous Klein's quartic, studied e.g. in the monography [**12**], admitting the plane model

$$\tilde{\mathcal{Y}} : X^3Y + Y^3Z + Z^3X = 0.$$

Letting $K \subset G \subset \mathfrak{S}_7$ be the stabilizer of a point, the quotient $\tilde{\mathcal{Y}}/K$ is a $\mathbb{Q}$-rational curve and defines the mentioned cover $\mathcal{Y} = \mathbb{P}_1 \to \mathcal{X} = \mathbb{P}_1$ of degree 7.

It is easy to find a group $H \subset G \subset \mathfrak{S}_7$ having property $(*)$: indeed, take for H the stabilizer of a *line* in $\mathbb{P}_2(\mathbb{F}_3)$. The fact that $(*)$ holds follows from the duality principle in projective geometry. More explicitly: (1) every projective automorphism fixing a line has a fixed point; (2) given a line l and a point p, there exists an automorphism leaving l invariant and not fixing p. The assertion (1) is just the fact that if a matrix has a rational eigenvector its transpose too has one rational eigenvector.

From Hurwitz formula again it follows that $\mathcal{U}_H = \tilde{\mathcal{Y}}/H$ is a rational curve and the corresponding map $g : \mathcal{U}_H \simeq \mathbb{P}_1 \to \mathbb{P}_1$ has a totally ramified point, so in suitable coordinates it is a polynomial map.

This proves that over s suitable large number field, namely a number field κ over which the Galois groups $G_{f,\kappa}$ and G_f^{geo} coincide, the polynomial f admits infinitely many fake values, namely all the integral values of g outside finitely many (those which are common integral values of f and g, which are finite in number by Siegel's theorem).

`An example in degree` 13. Our next example is similar in nature to the one in degree 7. We shall use the group

$$G = \mathrm{PSL}_3(\mathbb{F}_3)$$

of order $2808 = 2^3 \cdot 3^3 \cdot 13$. It acts on the projective plane $\mathbb{P}_2(\mathbb{F}_3)$, which contains 13 points. The group G can be generated by elements of order 2 and of order 3 with product of order 13, for instance:

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

The projective automorphism induced by the matrix A has five fixed points and four two-cycles; the one induced by B has one fixed point and four three-cycles. The corresponding representation of $G \hookrightarrow \mathfrak{S}_{13}$ is the monodromy representation of a polynomial $f(X) \in \mathbb{Q}[X]$ of degree 13, inducing a cover $f : \mathbb{P}_1 \to \mathbb{P}_1$ unramified outside three points. The Galois closure of the cover is a curve of genus 127.

Consider, as in the previous construction, the dual action of G on the hyperplanes (i.e lines) of $\mathbb{P}_2(\mathbb{F}_3)$; letting H be the stabilizer of a point in the dual projective plane, i.e. a line of $\mathbb{P}_2$, we obtain that H has the property $(*)$. The induced cover $g : \mathcal{U}_H \to \mathbb{P}_1$ is again provided by a rational curve, and the point at infinity is again totally ramified, so that in suitable coordinates g is a polynomial.

As in previous examples, over every number fields the polynomials f and g share only finitely many common rational values. Over every sufficiently large number field κ, so large that the Galois action of G on $\tilde{\mathcal{Y}}$ can be defined over κ, the rational values of g which are not rational values of f are fake values for f and vice-versa.

7 - On the Grunewald-Wang and Dvornicich-Zannier examples

The Grunewald-Wang example (actually discovered first by Trost - see the reference in [**5**]) concerns the polynomial $g(X) = 16X^8$, whose values at integers are perfect eighth-power modulo every prime. Actually, they are also eighth power in the ring of p-adic integers, except for $p = 2$. For instance, the number $16 = g(1)$ is a fake value for $f(X) = X^8$, not a strongly fake one however since it is not an eighth-power in $\mathbb{Q}_2$.

Over the field $\mathbb{Q}(\sqrt{-17})$ it becomes a strong fake value. This is due to the fact that $16 = (1+i)^8$, $\mathbb{Q}_2(\sqrt{-17}) = \mathbb{Q}_2(i)$, but 16 is not an eighth power in $\mathbb{Q}(\sqrt{-17})$.

Note that over every number field containing any eighth root of 16, e.g. over any number field containing $i = \sqrt{-1}$ or $\sqrt{2}$, the polynomial $g(X)$ stops producing fake values for f. Indeed, the reason for the existence of fake values for the polynomial $f(X)$ lies in the 'arithmetic part' of its Galois group $G_{f,\mathbb{Q}}$, which is an extension

$$\{0\} \to \mathbb{Z}/8\mathbb{Z} \to G_{f,\mathbb{Q}} \to (\mathbb{Z}/2\mathbb{Z})^2 \to \{0\},$$

where $\mathbb{Z}/8\mathbb{Z} \simeq G_f^{\mathrm{geo}}$ and $(\mathbb{Z}/2\mathbb{Z})^2 \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$, ζ_8 being a primitive eighth root of unity. Then $|G| = |G_{f,\mathbb{Q}}| = 32$ and the group acts on an eight-point set as the group of affine transformations of the 'line' $\mathbb{A}^1(\mathbb{Z}/8\mathbb{Z})$ over the ring $\mathbb{Z}/8\mathbb{Z}$: the normal subgroup $\mathbb{Z}/8\mathbb{Z}$ identifies with the group of translations, and a general transformation is of the form

$$x \mapsto \alpha x + b$$

for $\alpha \in (\mathbb{Z}/8\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and $b \in \mathbb{Z}/8\mathbb{Z}$. The group K is the stabilizer of a point, say the origin; it identifies with the group of linear transformations $x \mapsto \alpha x$. For the group H one can take the group generated by

$$x \mapsto -x, \quad x \mapsto 3x + 4.$$

Now, $H \subset \bigcup_{\gamma \in G} \gamma K \gamma^{-1}$, but also $K \subset \bigcup_{\gamma \in G} \gamma H \gamma^{-1}$. This is in accordance with the fact that the rational values of g are fake values for f, but also the rational value of f are fake values of g. Note that the image of H in $(\mathbb{Z}/2\mathbb{Z})^2$ is

surjective: otherwise the curve $\mathcal{U}_H$ would not be geometrically irreducible, and would contain only finitely many rational points. Note also that H does not fix any point in $\mathbb{A}^1(\mathbb{Z}/8\mathbb{Z})$; it is the stabilizer of the set $\{0,4\} \subset \mathbb{A}^1(\mathbb{Z}/8\mathbb{Z})$.

Of course, extending the ground field so to eliminate the 'arithmetic part', represented by the group $(\mathbb{Z}/2\mathbb{Z})^2$ in the above exact sequence, reduces the Galois group to the commutative group $\mathbb{Z}/8\mathbb{Z}$, for which no pairs of subgroups (K,H) satisfying property $(*)$ can exist.

`The examples of Dvornicich-Zannier`. Let us now consider the examples coming from divisibility on elliptic curves. While Dvornicich and Zannier used a sligthly different point of view, we show how their constructions fit in our framework.

Given an elliptic curve E over a number field κ and an integer $m > 1$, consider the multiplication by m-map $f = [m] : E \to E$. Letting $\tilde{\kappa}$ be the field of definition of the m-torsion on E over κ, the Galois group $G_{f,\kappa}$ is an extension

$$\{0\} \to (\mathbb{Z}/m\mathbb{Z})^2 \to G_{f,\mathbb{Q}} \to \mathrm{Gal}(\tilde{\kappa}/\kappa) \to \{0\}. \tag{13}$$

The group $\mathrm{Gal}(\tilde{\kappa}/\kappa)$ injects into the group $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Since any rational point in $E(\kappa)$ provides a section of the morphism $G_{f,\mathbb{Q}} \to \mathrm{Gal}(\tilde{\kappa}/\kappa)$, the group $G_{f,\kappa} =: G$ is a semi-direct product of the normal abelian group $(\mathbb{Z}/m\mathbb{Z})^2 \simeq (\ker[m]) =: E[m]$ by the group $\mathrm{Gal}(\tilde{\kappa}/\kappa)$ similiarly to what happens in Grunewald-Wang example. The group G acts naturally on the group $E[m]$. Every fiber $f^{-1}(P)$ of any point of $E(\kappa)$ is a principal homogeneous space for $E[m]$ and indeed the action of G on the fibers is compatible with the action of G on $E[m]$.

We must look for pairs of subgroups $K, H \subset G$, where K is the stabilizer of a point of $E[m]$ and H satisfies property $(*)$ with respect to K. We also want that the projection of H into $\mathrm{Gal}(\tilde{\kappa}/\kappa)$ be surjective.

As shown in [**4**] there are no examples for m a prime number, while for $m = 4$ an example is constructed in [**5**].

As to the first assertion, we have to exclude the existence of a subgroup $H \subset G$ satisfying property $(*)$ and inducing a surjection $H \to \mathrm{Gal}(\tilde{\kappa}/\kappa) := \Delta$. Recall that here G is the semi-direct product of the additive group $(\mathbb{Z}/p\mathbb{Z})^2$, $p = m$ a prime, by the matrix group $\Delta \subset \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. The fact that every element of H admits a fixed point implies that the projection $H \to \Delta$ is injective (indeed, every non-trivial element of the kernel would be a non identical translation, admitting no fixed point). Then H is the image of a section $\Delta \to G$. It is well known that such sections come from points in $\mathbb{A}^2(\mathbb{Z}/p\mathbb{Z})$. In other terms, the first cohomology group $\mathrm{H}^1(\Delta, (\mathbb{Z}/p\mathbb{Z})^2)$ vanishes, so every section $\Delta \to G$ has for image the stabilizer of some point in $\mathbb{A}^2(\mathbb{Z}/p\mathbb{Z})$.

As to an explicit example with $m = 4$, Dvornicich and Zannier constructed an elliptic curve for which the field of rationality $\tilde{\kappa}$ for the four-torsion is quartic over the field of definition κ and the group $\Delta \simeq \mathrm{Gal}(\tilde{\kappa}/\kappa)$ identifies with the group of matrices

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}).$$

Now, the subgroup H can be generated by the transformations

$$v \mapsto \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix} \cdot v, \qquad v \mapsto \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \cdot v + \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Note that the projection $H \to \Delta$ is surjective. The first transformation fixes the points $\binom{0}{0}, \binom{2}{0}$, the second one the points $\binom{0}{\pm 1}$, so no point is fixed by the whole group H; the two transformations are indeed involutions and they commute; their product admits the fixed point $\binom{\pm 1}{0}$. It follows that property $(*)$ holds.

8 - Some relations with other topics

As mentioned in the Introduction, examples of polynomials admitting infinitely many fake values can be constructed via the so called pairs of Kronecker conjugates: these are pairs of polynomials $(f(X), g(X))$ in a polynomial ring $\mathcal{O}_S[X]$ representing the same sets modulo all but finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$.

In our setting, the polynomial $f(X)$ induces a finite morphism $f : \mathbb{A}^1 \to \mathbb{A}^1$. Defining the (affine) curve $\tilde{\mathcal{Y}}$ and the group $G_{f,\kappa}$ as explained in section 2, a subgroup H satisfying property $(*)$ and such that the quotient curve $\mathcal{U}_H = \tilde{\mathcal{Y}}/H$ is again isomorphic to $\mathbb{A}^1$ over κ provides a polynomial $g : \mathcal{U}_H \to \mathbb{A}^1$ whose set of values modulo every prime $\mathfrak{p}$ is contained in the reduction modulo $\mathfrak{p}$ of the value set of f.

Let $K \subset G_{f,\kappa} = G$ be the subgroup corresponding to the polynomial f, i.e. such that $\mathcal{X} = \tilde{\mathcal{Y}}/K$ and $f : \mathcal{X} = \mathbb{A}^1 \to \mathbb{A}^1$ be the induced morphism. Suppose now that

$$\bigcup_{\gamma \in G} \gamma H \gamma^{-1} = \bigcup_{\gamma \in G} \gamma K \gamma^{-1}. \tag{14}$$

Then f and g are Kronecker conjugate. Note that the above condition is symmetric, while condition $(*)$ is not.

A pair of Kronecker polynomials $(f(X), g(X))$ is said to be a *proper pair* over κ if the two polynomials are not linearly related over κ, i.e. $g(X)$ is not

of the form $f(\alpha x+\beta)$ for any $\alpha\in\kappa^*,\beta\in\kappa$. M. Fried [**7**], [**8**] (see also the bibliography of [**13**]) proved that there exist no *indecomposable* Kronecker pairs of polynomials over the integers. Also he found that over suitable number fields there are proper pairs of Kronecker conjugate polynomials $(f(X),g(X))$ with f of degree $7,11,13,15,21,31$, and only these degrees are allowed. Such pairs of polynomials are even linearly unrelated over the algebraic closure of their field of definition. Note that, on the contrary, the polynomials X^8 and $16X^8$, which are linearly unrelated over $\mathbb{Q}$, become linearly related over $\mathbb{Q}(\sqrt{2})$, or over $\mathbb{Q}(i)$.

The examples of degree 7 and 13 have been discussed in §6, and can be derived from the principle of projective duality in the plane.

In the paper [**13**] P. Müller extended Fried's research to the classification of proper pairs $(f(X),g(X))$ of Kronecker conjugates with f being decomposable with length two, i.e. of the form $f=f_1\circ f_2$ for indecomposable polynomials f_1,f_2. A complete classification in the general case seems hopeless at present.

The condition (14) can be further strengthened in the following way: given a finite group G, consider the pairs (H,K) of subgroups satisfying the condition

$(***)$ *For every conjugacy class* $C\subset G$, $\sharp(C\cap H)=\sharp(C\cap K)$.

This is again a symmetric condition on the pair (H,K). Clearly, condition $(***)$ is stronger then condition (14), so in particular stronger then $(*)$.

Pairs of subgroups (H,K) satisfying $(***)$ were first considered by F. Gassmann in [**9**]: the triple (G,H,K) is called a Gassmann triple.

They lead to arithmetically equivalent number fields, i.e. non-isomorphic pairs of number fields κ_1,κ_2 having the same Dedekind zeta function. The first example arises in degree 7, and is related to ours in §6, deriving from the principle of projective duality. See Perlis' article [**14**], where the relation between arithmetic equivalence and condition $(***)$ is shown and the fact that there are no examples in degree ≤ 6 is deduced.

In a different domain, T. Sunada [**18**] proved that pairs of subgroups satisfying $(***)$ lead to pairs of non-isometrical isospectral Riemannian manifolds. Namely, given a compact Riemannian manifold M and a free isometric action on it by a finite group G, a pair of non-conjugate subgroups (H,K) satisfying $(***)$ produces the two quotient varieties M/H and M/K which are non-isometric but isospectral. See also P. Buser's paper [**1**] for further remarks on this topic, and for an application in that context of the group-theoretic situation arising from Grunewald-Wang example (section 3 of [**1**]).

Acknowledgments. The results of this work were presernted at the Number Theory Web Seminar, organized by M. Bennett, Ph. Habegger and A. Ostafe. The author is grateful to the organizers for the invitation, and to

the listeners whose interventions enabled him to improve the presentation of the paper. In particular, the author is very grateful to P. Sarnak and D. Neftin who pointed out the connections to arithmetic equivalence and isospectrality, and to the references of P. Müller and R. Buser.

He is also grateful to J.-L. Colliot-Thélène for explaining him the relation with the theory of torsors, although this point of view has not been adopted in the present work, and to D. Dikranjan and U. Zannier for several conversations on these topics.

Finally, he wants to thank a competent anonymous referee, who pointed out to him the relevant references to works of M. Stoll [**17**] and Harari-Voloch [**10**].

References

[**1**] P. Buser, *Cayley graphs and planar isospectral domains*, in "Geometry and analysis on manifolds" (Katata/Kyoto 1987), Lecture Notes in Math., **1339**, Springer, Berlin, 1988.

[**2**] P. Corvaja, *Integral points on algebraic varieties*, An introduction to Diophantine geometry, Inst. Math. Sci. Lect. Notes, **3**, Hindustan Book Agency, New Delhi, 2016.

[**3**] P. Corvaja and U. Zannier, *Applications of Diophantine approximation to integral points and transcendence*, Cambridge Tracts in Math., **212**, Cambridge Univ. Press, Cambridge, 2018.

[**4**] R. Dvornicich and U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129** (2001), 317–338.

[**5**] R. Dvornicich and U. Zannier, *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Math. Acad. Sci. Paris **338** (2004), 47–50.

[**6**] W. L. Edge, *Bring's curve*, J. London Math. Soc. (2) **18** (1978), 539–545.

[**7**] M. Fried, *Arithmetical properties of value sets of polynomials*, Acta Arith. **15** (1968/69), 91–115.

[**8**] M. Fried, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–45.

[**9**] F. Gassmann, *Bemerkungen zur Vorstehenden Arbeit von Hurwitz: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppen*, Math. Z. **25** (1926), 661–675.

[**10**] D. Harari and J. F. Voloch, *The Brauer-Manin obstruction for integral points on curves*, Math. Proc. Cambridge Philos. Soc. **149** (2010), 413–421.

[**11**] K. Kunen and W. Rudin, *Lacunarity and the Bohr topology*, Math. Proc. Cambridge Philos. Soc. **126** (1999), 117–137.

[**12**] S. Levy (editor), *The eightfold way*, The beauty of Klein's quartic curve, Math. Sci. Res. Inst. Publ., **35**, Cambridge Univ. Press, Cambridge, 1999.

[**13**] P. Müller, *Kronecker conjugacy of polynomials*, Trans. Amer. Math. Soc. **350** (1998), 1823–1850.

[**14**] R. Perlis, *On the equation* $\zeta_{\mathbf{k}}(s) = \zeta_{\mathbf{k}'}(s)$, J. Number Theory **9** (1977), 342–360.

[**15**] J.-P. Serre, *Topics in Galois theory*, Res. Notes Math., **1**, Johnes & Bartlett Publisher, Boston, 1992.

[**16**] J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), 429–440.

[**17**] M. Stoll, *Finite descent obstructions and rational points on curves*, Algebra and Number Theory **1** (2007), 349–391.

[**18**] T. Sunada, *Riemannian coverings and isospectral manifolds*, Ann. of Math. **121** (1985), 169–186.

[**19**] M. Weber, *Kepler's small stellated dodecahedron as a Riemann surface*, Pacific J. Math. **220** (2005), 167–182.

Pietro Corvaja
Dipartimento di Scienze Matematiche,
Informatiche e Fisiche
Università di Udine
Via delle Scienze 206
33100 Udine, Italy
e-mail: pietro.corvaja@uniud.it