The Inverse Galois Problem over $\mathbb{Q}$ and Hilbert's Irreducibility Theorem
Bachelor Thesis

François Duhesme

June 27, 2018

Contents

Introduction: The inverse Galois problem

Galois theory is named after the famous 19*th* century mathematician Evariste Galois. He studied wether it was possible to express roots of polynomials using radicals. Galois theory answers that question by establishing a connection between field and group theory. This is done by associating to each finite field extension L/K its group of automorphims $\operatorname{Aut}(L/K)$. If the extension is normal and separable, then the fundamental theorem of Galois theory provides a bijection between the subgroups of $\operatorname{Aut}(L/K) =: \operatorname{Gal}(L/K)$ and field extensions M of the form $K \subset M \subset L$.

One can ask wether it is possible to go the other way around, that is given a finite group G, can it be realised as the Galois group of some field extension? Let's take a look at the symmetric groups: We can construct the group $\mathcal{S}_n$ as the Galois group associated to the polynomial $f(X) = (X - X_1) \cdots (X - X_n)$ over the field $\mathbb{Q}(X_1, ..., X_n)^{\mathcal{S}_n}$, where $X_1, ..., X_n$ are algebraically independent over $\mathbb{Q}$. Since any finite group can be embedded into a symmetric group, using the fundamental theorem of Galois theory we obtain that any finite group can be realised as the Galois group of some field extension.

Therefore it seems more adequate to adress the question in a more restricted context, fixing for example the base field K to be the rational numbers $\mathbb{Q}$. This question was first studied in depth by David Hilbert at the end of the 19*th* century. For finite abelian groups, the situation is relatively simple. Every finite abelian group G is isomorphic to a quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$, for some natural number n. Adjoining a primitive n-th root of unity ζ_n to $\mathbb{Q}$ we get a field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$. Using the fundamental theorem of Galois theory we obtain an extension of $\mathbb{Q}$ with Galois group G.

For nonabelian groups however, the situation is more complex. We already realised the symmetric groups over $\mathbb{Q}(X_1, ..., X_n)^{\mathcal{S}_n}$, which is isomorphic to $\mathbb{Q}(X_1, ..., X_n)$ over $\mathbb{Q}$. Thus the following question arises: given a finite group G that can be realized over a field of the form $\mathbb{Q}(X_1, ..., X_n)$, can we ‚descend' and realize G over $\mathbb{Q}$? We will show that this can be done. Our proof will be based on Hilbert's Irreducibility Theorem, first proved by Hilbert in 1892:

Theorem (Hilbert's Irreducibility Theorem). *The field $\mathbb{Q}$ has the Hilbert property, that is: For any irreducible polynomial $f \in \mathbb{Q}[X_1, ..., X_s, Y_1, ..., Y_r]$ of degre $\geqslant 1$ in $Y_1, ..., Y_r$, there exist infinitely many $b \in \mathbb{Q}^s$ such that $f(b_1, ..., b_s, Y_1, ..., Y_r) \in \mathbb{Q}[Y_1, ..., Y_r]$ is irreducible.*

The process of reducing the number of variables in a polynomial by evaluating it in some of its variables is called specialization. We will define this concept in a generalized context in the first section, where we will study its properties, and see how it relates to Galois theory. Notably, we will see under what circumstances the Galois group of the original and the specialised polynomials are isomorphic.

In the second section, we will introduce the following three equivalent formulations of the Hilbert property:

Theorem. *For a field K of characteristic zero the following conditions are equivalent:*

1. *For any irreducible polynomial $f \in K(X)[Y]$, there are infinitely many $b \in K$ such that f_b is irreducible.*

2. *For any finite collection of irreducible polynomials $f_1, ..., f_m \in K(X)[Y]$, there are infinitely many $b \in K$ such that all the $f_{1,b}, ..., f_{m,b}$ are irreducible simultaneously.*

3. *For any finite collection of irreducible polynomials $p_1, ..., p_m \in K(X)[Y]$ of degree > 1 in Y, there are infinitely many $b \in K$ such that none of the $p_{1,b}, ..., p_{m,b}$ has a root in K.*

We will then study the implications of the Hilbert property, still in the context of a field K of characteristic zero. From this study will in particular result that the case $s = r = 1$ in Hilbert's Irreducibility Theorem implies the case were s and r are arbitrary. This finishes our survey of the general situation over a field of characteristic zero, and opens the way to approach the specific situation with $K = \mathbb{Q}$.

As we will see at the end, to show that $\mathbb{Q}$ has the Hilbert property, it is sufficient to show that for any irreducible polynomial in two variables over $\mathbb{Q}$ we can find infinitely many specializations such that the specialized polynomial has no root in $\mathbb{Q}$. This provides the motivation for studying for which $x \in \mathbb{Q}$ the equation $f(x, y) = 0$ has a solution $y \in \mathbb{Q}$. For this, we will need an analytic tool: Puiseux series, which will be defined and introduced in the third section. They are special power series which contain rational exponents. They can be evaluated once the branches of the involved roots are chosen and convergence is well defined, thus inducing a function. We will use them to locally parametrize the solutions of the above equation in terms of x.

Now we have all the tools at hand to adress the situation over $\mathbb{Q}$. All that remains to be done is to bound asymptotically the proportion of integer entries x for which the corresponding Puiseux series takes rational values. This will permit us to estimate the number of pairs of rationals (x, y) which are solution to $f(x, y) = 0$, thus concluding the proof of the theorem.

Finally we close this work by coming back to the last question asked in the introduction, showing that every finite group G that can be realized as a Galois group over $\mathbb{Q}(X_1, ..., X_n)$ can be realized as a Galois group over $\mathbb{Q}$.

Danksagung

Zunächst möchte ich meiner Familie meinen Dank aussprechen, für all die gegenseitige Liebe die in ihr wirkt, für ihre tatkräftige Unterstütung allentlang meines Studiums, und dies obwohl ich ihren Mitgliedern den Inhalt desletzeren nicht immer in gerechter Weise vermitteln konnte.

Mein Dank gilt ebenfalls dem Studentenhaus Allenmoos in dem ich für drei Jahre ein Zuhause in der Fremde gefunden habe. Herzlichen Dank der Leitung, der Verwaltung und allen anderen Mitbewohnern mit denen ich zusammenwohnen konnte, und von denen ich in dieser Zeit einige ins Herz geschlossen habe.

Meinen Studienkamaraden möchte ich meinen Dank aussprechen für die unzähligen Momente des gemeinsamen Staunens vor Wahrzeichen der menschlichen Geisteskraft.

Meinen ganz besonderer Dank gilt Professor Richard Pink, dem Betreuer dieser Arbeit. Seine zahlreichen Anmerkungen, Korrekturen und Vorschläge sind mir wichtige Anhaltspunkte und Werkzeuge geworden, um zu sehen wie man Mathematik erarbeitet, ihren Inhalt strukturiert und ihre Formulierung zu Papier bringt. Bedanken möchte ich mich hier auch für drei Jahre lehrreicher Vorlesungen die mich auf meinen Entdeckungen der schönen Welt der Mathematik begleitet und meinen Blick auf sie geschult haben.

Vor allem bedanke ich mich aber für die angeregten und aufschlussreichen Gespräche, die nicht nur Themenbereich umfassten welche weit über die Mathematik hinausgingen, sondern auch immer in ehrlichen Ratschlägen mündeten, denen ich bei wichtigen Entscheidungsfindungen immer Vertrauen schenken konnte und deren Wert in denselben ich nicht genug hervorheben kann.

Herzlichen Dank!

1 Properties of specialization

Let K be a field. We denote by $K(X)$ the rational function field of K in the variable X. Suppose $f \in K(X)[\underline{Y}]$ is a polynomial in a finite set of variables $\underline{Y}$ over $K(X)$. Then we can write $f = \frac{\tilde{f}}{h}$ for $\tilde{f}$ a polynomial in $K[X][\underline{Y}]$ and $h \in K[X] \setminus \{0\}$ the lowest common denominator of the coefficients of f.

Definition 1.1. *For any $b \in K$ with $h(b) \neq 0$ we call $f_b(\underline{Y}) := f(b, \underline{Y}) := \frac{\tilde{f}(b,\underline{Y})}{h(b)} \in K[\underline{Y}]$* ***the polynomial*** f ***specialized at*** b.

Note that since h is nonzero, it vanishes only at finitely many points, hence for almost all $b \in K$ the specialized polynomial f_b is defined. We start by studying some basic properties of specialization. Unless mentioned otherwise, in the following we only consider the case of a single variable: $\underline{Y} = Y$.

Lemma 1.2. *For almost all $b \in K$ the degree of f_b is equal to the degree of f.*

Proof. If f is the zero polynomial the statement trivially holds. If f is nonzero, the leading coefficient of $\tilde{f}$ is a nonzero polynomial in X, which can only vanish at a finite number of $b \in K$. □

Lemma 1.3. *If f is separable, for almost all $b \in K$ the specialized polynomial f_b is also separable.*

Proof. Since f is separable, $\mathrm{Disc}_f(X)$ is a nonzero element of $K(X)$, excluding all the zeros of its denominator and its numerator, we obtain that $\mathrm{Disc}_{f_b} = \mathrm{Disc}_f(b) \neq 0$. □

Lemma 1.4. *Let p and f be polynomials in $K(X)[Y]$ such that $f|p$. Then for almost all $b \in K$ we have $f_b|p_b$.*

Proof. By definition there exists a $g \in K(X)[Y]$ such that $p = g \cdot f$. Consider only $b \in K$ such that p_b, g_b and f_b are defined. Then we have $p_b = g_b \cdot f_b$. □

Definition 1.5. *Let f be an irreducible polynomial over K. A field extension of the form $K[a_f]$, where $f(a_f) = 0$, is called a* stem field *of f.*

It is a standard result that every irreducible polynomial f over K possesses a stem field K_f over K. In the following we will always denote a stem field of f by K_f. It is easy to see that the pair (K_f, a_f) is determined up to unique isomorphism over K. When K_f/K is Galois, we denote its Galois group by G_f.

A useful property relating $K(X)_f$ and K_{f_b} is that polynomial equations from $K(X)_f$ translate to polynomial equations in K_{f_b} in the following sense:

Lemma 1.6 (Specialization preserves polynomial equalities)**.** *Let p, f be polynomials in $K(X)[Y]$. Suppose f is irreducible. If $a_f \in K(X)_f$ satisfies*

$$(\star) \qquad p(X, a_f) = 0$$

then for almost all $b \in K$ such that f_b is defined and irreducible, the element $a_{f_b} \in K_{f_b}$ satisfies

$$p_b(a_{f_b}) = 0 \ .$$

Proof. Recall that $K(X)_f$ is isomorphic to $K(X)[Y]/f(X,Y)$. Thus the equation $(\star)$ is equivalent to

$$p|f \ .$$

By Lemma 1.4 for almost all specializations this implies $p_b|f_b$, that is $p_b(a_{f_b}) = 0$. □

Proposition 1.7 (Preservation of the Galois group under specialization)**.** *Let $f \in K(X)[Y]$ be an irreducible polynomial, such that the extension $K(X)_f/K(X)$ is Galois. Then for almost all b in K such that f_b is defined, irreducible, separable and of the same degree as f it follows that the extension K_b/K is also Galois, with the same Galois group as $K(X)_f/K(X)$.*

Proof. Since the extension is Galois, f splits over K_f. So there exist a finite number of polynomials $w_1, ..., w_r \in K(X)[Z]$, with $w_1 = Z$ and $F \in K(X)^\times$ such that:

$$f(X,Y) = F(X) \prod_{i \in I} (Y - w_i(X, a_f)) \ .$$

In the rest of the proof we consider only $b \in K$ such that the specializations of all the polynomials involved are well defined, doing this we only exclude finitely many. By specialization we obtain:

$$f_b(Y) = F(b) \prod_{i \in I} (Y - w_i(b, a_{f_b})) \ .$$

Hence f_b splits over $K(a_{f_b}) = K_{f_b}$ and the extension K_{f_b}/K is normal. By assumption f_b is separable, hence K_{f_b}/K is also separable, thus Galois.

Because f and f_b are irreducible, G_f and G_{f_b} permute their roots transitively. Moreover any root $w_i(X, a_f)$ of f and $w_i(b, a_{f_b})$ of f_b generate the field extensions K_f and K_{f_b} respectively. Hence every assignment of some root $w_i(X, a_f)$ to some other root $w_j(X, a_f)$; and each assignment of some root $w_n(b, a_{f_b})$ to some other root $w_m(b, a_{f_b})$ uniquely determines an element of G_f and G_{f_b} respectively. Thus we can define a group isomorphism σ:

$$\begin{tikzcd}
G_f = \mathrm{Gal}(K(X)_f/K(X)) \arrow[r, "\sigma"] & G_{f_b} = \mathrm{Gal}(K_{f_b}/k) \\
(w_i(X, a_f) \mapsto w_j(X, a_f)) \arrow[r, mapsto, "\sigma"] & (w_i(b, a_{f_b}) \mapsto w_j(b, a_{f_b}))
\end{tikzcd}$$

□

Convention. *For simplicity all fields in this text considered from now on are supposed to have characteristic* 0. *The consequence we will use is that then every irreducible polynomial is separable.*

Given an irreducible polynomial $h \in K(X)[Y]$ we would like to know for which specializations $b \in K$ the specialized polynomial h_b is again irreducible.

Proposition 1.8 (descent of irreducibility)**.** *Let f and $h \in K(X)[Y]$ be irreducible polynomials which split over $K(X)_f$. Then for almost all $b \in K$ the following holds:*

If f_b is irreducible, then h_b is irreducible .

Proof. Since h is irreducible, it is nonzero. We only consider $b \in K$ for which h_b is well defined. As $K(X)_f$ contains a splitting field of h, there exist polynomials $v_1, ..., v_m \in K(X)[Z]$ and $H \in K(X)^\times$ such that:

$$h(X,Y) = H(X)\prod_{i=1}^{m}(Y - v_i(X, a_f)) \ . \tag{†}$$

We restrict to $b \in K$ such that h_b is again a separable polynomial of degree m. Moreover by Lemma 1.6 we can specialize both sides of (†) to obtain :

$$h_b(Y) = H(b)\prod_{i=1}^{m}(Y - v_i(b, a_{f_b})) \ .$$

Since h is irreducible G_f permutes the roots $v_1(X, a_f), ..., v_r(X, a_f)$ transitively. Pick an element $g \in G_f$ sending $v_1(X, a_f)$ to $v_i(X, a_f)$. Since $g(a_f)$ lies in $K(X)_f$ there is a polynomial $w \in K(X)[Z]$ such that $g(a_f) = w(X, a_f)$. Written out as an equation we get:

$$g(v_1(X, a_f)) = v_1(X, g(a_f)) = v_1(X, w(X, a_f)) = v_i(X, a_f)$$

Now we can apply the isormophism σ from Proposition 1.7. Then for almost all specializtions this implies $\sigma g(a_{f_b}) = w(b, a_{f_b})$, and restricting furthermore to specializations such that the polynomial equalities are preserved we obtain that

$$(\sigma g)(v_1(b, a_{f_b})) = v_1(b, \sigma g(a_{f_b})) = v_1(b, w(b, a_{f_b})) = v_i(b, a_{f_b}) \ .$$

Hence G_{f_b} acts transitively on the roots of h_b, and h_b is thus irreducible. □

We end this section with a lemma permitting us to transpose the question of the reducibility of a polynomial to the question of the existence of a root of some other polynomials.

Lemma 1.9. *Let $f \in K(X)[Y]$ be irreducible. Then there exists a finite collection of irreducible polynomials $p_1, ..., p_m \in K(X)[Y]$ of degree > 1, such that for almost all $b \in K$ the following holds:*

If f_b is reducible then one of the $p_{1,b}, ..., p_{m,b}$ has a root in K .

Proof. Restricting only to specializations for which the leading coefficient is well defined and non-zero, we can assume f to be monic. In a splitting field L of f we have

$$f = \prod_{i \in I} (Y - w_i)$$

with all $w_i \in L$. Since f is irreducible, for each nonempty $J \subsetneq I$ one of the coefficients of

$$\prod_{i \in J} (Y - w_i)$$

does not lie in $K(X)$. Pick one of these: it is a symmetric polynomial $s_J \in K(X)[\{Z_i\}_{i \in J}]$ evaluated at $\{Z_i \mapsto w_i\}_{i \in J}$. We denote the minimal polynomial of the coefficient $s_J(\{w_i\}_{i \in J})$ over $K(X)$ by $p_J \in K(X)[Y]$. So

$$p_J(X)(s_J(\{w_i\}_{i \in J})) = 0 \ .$$

We restrict to $b \in K$ such that f_b is separable. Then in a splitting field M of f_b we have $f_b = \prod_{i \in I}(Y - v_i)$, with $v_i \in M$. Suppose f_b is reducible. Then for some nonempty $J \subsetneq I$ the polynomial $\prod_{i \in J}(Y - v_i)$ lies in $K[Y]$. In particular the coefficient $s_J(\{v_i\}_{i \in J})$ lies in K. Since polynomial equalities are preserved for almost all specializations, we have

$$p_J(b)(s_J(\{v_i\}_{i \in J})) = 0$$

and thus the polynomial $p_{J,b}$ has a zero in K. So the polynomials $\{p_J\}_{\varnothing \neq J \subsetneq I}$ have the desired property. □

2 The Hilbert property

Theorem 2.1 (The equivalent formulations of the Hilbert property)**.** *For any field K the following conditions are equivalent:*

1. *For any irreducible polynomial $f \in K(X)[Y]$, there are infinitely many $b \in K$ such that f_b is irreducible.*

2. *For any finite collection of irreducible polynomials $f_1, ..., f_m \in K(X)[Y]$, there are infinitely many $b \in K$ such that all the $f_{1,b}, ..., f_{m,b}$ are irreducible simultaneously.*

3. *For any finite collection of irreducible polynomials $p_1, ..., p_m \in K(X)[Y]$ of degree > 1 in Y, there are infinitely many $b \in K$ such that none of the $p_{1,b}, ..., p_{m,b}$ has a root in K.*

Definition 2.2. *A field is called Hilbertian if it satisfies the above equivalent conditions.*

Proof. 1. implies 2. : Let the situation from (2.) be given. Take a finite Galois extension $L/K(X)$ containing splitting fields of all the $f_1, ..., f_m$. By the primitive element theorem, L is the stem field of an irreducible polynomial $f \in K(X)[Y]$. For each $i \in 1, ..., m$ and almost all $b \in K$ we obtain by Proposition 1.8:

$$\text{If } f_b \text{ is irreducible, then } f_{i,b} \text{ is irreducible.}$$

Since we can prove this for each $i \in 1, ..., m$ and since assuming (1.) provides infinitely many b in K such that f_b is irreducible it follows that there are infinitely many $b \in K$ such that all $f_{1,b}, ..., f_{m,b}$ are irreducible simultaneously, which is what we wanted to show.

2. implies 3. : Let the situation from (3.) be given. Using (2.) we can obtain infinitely many $b \in K$ with all $p_{1,b}, ..., p_{m,b}$ irreducible and of degree > 1. Then none of the $p_{1,b}, ..., p_{m,b}$ has a root in K, since that would contradict their irreducibility.

3. implies 1. : Let the situation from (1.) be given. Then using Lemma 1.9 we obtain irreducible polynomials $p_1, ..., p_m \in K(X)[Y]$ of degree > 1 such that for almost all $b \in K$ the following holds: If none of the $p_{1,b}, ..., p_{m,b}$ has a root in K then f_b is irreducible. Applying assumption (3) yields infinitely many $b \in K$ with none of the $p_{1,b}, ..., p_{m,b}$ having a root in K, thus with f_b being irreducible. □

In the above definition we considered only the case of a polynomial in one variable. Let $f \in K(X)[\underline{Y}]$ be an irreducible polynomial in a finite number of variables $\underline{Y} = Y_1, ..., Y_s$. To study the case of more variables we introduce:

Definition 2.3 (Kronecker specialization)**.** *For a base field K, and an integer d we define the Kronecker specialization of degree d to be the ring homomorphism:*

$$S_d : \ K[\underline{Y}] \longrightarrow K[Z]$$

$$f(Y_1, Y_2, ..., Y_s) \longmapsto f(Z, Z^d, ..., Z^{d^{s-1}})$$

By uniqueness of the d-adic extension of an integer, S_d defines a bijection:

$$K[\underline{Y}]_{\ll d} := \left\{ f \in K[\underline{Y}] \;\middle|\; \begin{array}{l} \text{each } Y_i \text{ has} \\ \text{order} < d \text{ in } f \end{array} \right\} \xrightarrow{\sim} \left\{ f \in K[Z] \;\middle|\; f \text{ is of total degree} < d^s \right\}$$

Since we are eventually interested in specializing irreducible polynomials, we would like to know how irreducible polynomials behave under the map S_d. However S_d does in general not map irreducible polynomials to irreducible polynomials, even if the we consider elements in $K[\underline{Y}]_{\ll d}$, as the following examples shows: Set d to be greater than 1. Then Y_2 lies in $K[\underline{Y}]_{\ll d}$ but $S_d(Y_2) = Z^d$ is reducible.

However we can handle irreducibility better by using the following trick:

Definition 2.4. *Fix an integer d. Let $F \in K[Z]$ be a polynomial of degree > 0. The polynomial F is said to be **d-mildly irreducible** if for any factorization $F = G \cdot H$, such that $G, H \in K[Z] \backslash K$ and G and H have preimages $g, h \in K[\underline{Y}]_{\ll d}$ under S_d, the product $g \cdot h$ does not lie in $K[\underline{Y}]_{\ll d}$.*

Note that there are polynomials in $K[Z]$ which are d-mildly irreducible but not irreducible. For instance every polynomial $F \in K[Z]$ of degree $\geqslant 2d^s$ is d-mildly irreducible: If we have a factorization $F = G \cdot H$, then one of G, H, say G has degree $\geqslant d^s$. Hence G has no preimage g under S_d in $K[\underline{Y}]_{\ll d}$, so the implication trivially holds.

The polynomial $Z^d = S_d(Y_2)$ is d-mildly irreducible: For any factorization $Z^d = Z^m \cdot Z^{d-m}$ with $0 < m < d$ the preimages of Z^m and Z^{d-m} under S_d in $K[\underline{Y}]_{\ll d}$ are Y_1^m and Y_1^{d-m}. But $Y_1^m \cdot Y_1^{d-m}$ does not lie in $K[\underline{Y}]_{\ll d}$, since it has degree d in Y_1.

Lemma 2.5. *Let f be a polynomial in $K[\underline{Y}]_{\ll d}$. Then f is irreducible if and only if $S_d(f)$ is d-mildly irreducible.*

Proof. We show the contrapositive in both directions:

Assume F is reducible, then $f = gh$, for some $g, h \in K[\underline{Y}]$. The degree of g and h with respect to each Y_i is smaller than that of f. Therefore g, h also lie in $K[\underline{Y}]_{\ll d}$. Since S_d is a ring homomorphism we have $S_d(f) = S_d(g)S_d(h)$, and $gh = f$ lies in $K[\underline{Y}]_{\ll d}$ hence $S_d(f)$ is not d-mildly irreducible .

Conversely assume $S_d(f)$ is not d-mildly irreducible. So there exists a factorization $S_d(f) = G \cdot H$, such that $G, H \in K[Z] \backslash K$ and G and H have preimages $g, h \in K[\underline{Y}]_{\ll d}$ under S_d, moreover $g \cdot h$ lies in $K[\underline{Y}]_{\ll d}$. Since S_d provides a bijection from $K[\underline{Y}]_{\ll d}$ to its image and $g \cdot h$ and f lie in $K[\underline{Y}]_{\ll d}$, with both having the same image $S_d(f) = G \cdot H = S_d(g) \cdot S_d(h) = S_d(g \cdot h)$, we have $f = g \cdot h$. Moreover $S_d(g), S_d(h)$ lie in $K[Z] \backslash K$, hence g, h lie in $K[\underline{Y}] \backslash K$ therefore f is reducible. □

Lemma 2.6. *Let F be a d-mildly irreducible polynomial in the variable Z over $K(X)$. We can write F as a product of irreducible factors $F_1, ..., F_m \in K(X)[Z]$:*

$$F = \prod_{j \in I} F_j \ .$$

Then for almost all $b \in K$ the following holds: If the polynomials $F_{1,b}, ..., F_{m,b}$ are irreducible and of same degree as $F_1, ..., F_m$, the specialized polynomial F_b is d-mildly irreducible.

Proof. Since we suppose all the $F_{j,b}$ to be irreducible and of same degree as F_j,

$$F_b(Z) = \prod_{j \in I} F_{j,b}(Z)$$

is a decomposition of F_b into irreducible factors. Fix a nonempty $J \subsetneq I$ and let $g, h \in K(X)[\underline{Y}]_{\ll d}$ be the preimages under S_d of $\prod_{j \in J} F_j$ and of $\prod_{j \in I \backslash J} F_j$. Because F is d-mildly irreducible the product

$$g \cdot h =: p$$

does not lie in $K(X)[\underline{Y}]_{\ll d}$. In other words, p has degree $\geqslant d$ in one of the variables $Y_1, ..., Y_s$. Now restrict to specializations such that p_b still has degree $\geqslant d$ in one of the

$Y_1, ..., Y_s$. Doing this we only exclude finitely many specializations. Then for the preimages $g_b, h_b \in k[\underline{Y}]_{\ll d}$ of $\prod_{j\in J} F_{j,b}$ and of $\prod_{j\in I\setminus J} F_{j,b}$ their product

$$g_b \cdot h_b = p_b$$

has degree $\geqslant d$ in one of the variables $Y_1, ..., Y_s$. Hence it does not lie in $K[\underline{Y}]_{\ll d}$. Varying $\varnothing \neq J \subsetneq I$ we obtain that, F_b is d-mildly irreducible. □

Now we are ready to prove a consequence of the Hilbert property for polynomials in multiple variables :

Theorem 2.7. *Let K be hilbertian. Then for any irreducible polynomial $f \in k(X)[\underline{Y}]$, there exist infinitely many $b \in K$ such that $f_b \in K[\underline{Y}]$ is irreducible.*

Proof. Fix an integer d large enough such that f lies in $K(X)[\underline{Y}]_{\ll d}$. Because f is irreducible, its Kronecker specialization $S_d(f) \in K(X)[Z]$ is d-mildly irreducible. We can write $S_d(f)$ as a product of irreducible factors $F_1, \cdots F_m \in K(X)[Z]$. Because K is hilbertian we can find infinitely many $b \in K$ such that the $F_{1,b}, ..., F_{m,b}$ are all irreducible and of same degree as $F_1, ..., F_m$ in Z. By Lemma 2.6 for almost all of these specializations $S_d(f)_b = S_d(f_b)$ is d-mildly irreducible. By Lemma 2.5, since f_b lies in $K[\underline{Y}]_{\ll d}$, this implies that f_b is irreducible. □

The last important result we will treat in this section is the preservation of the Hilbert property by finitely generated field extensions. First we treat the case of finite field extensions, which we will study using Galois theory: Consider a Galois extension M/K. Then the action of $\mathrm{Gal}(M/K)$ on M induces a unique action on $M(X)[Y]$ fixing X and Y.

Lemma 2.8. *Let M/K be a finite Galois extension. For any monic, irreducible polynomial $f \in M(X)[Y]$ we can find an element $t \in M(X)$ such that for $g(X, Y) := f(X, Y + t(X))$, when σ runs through $\mathrm{Gal}(M/K)$ all the σg are distinct.*

Proof. For the σg to be distinct it is sufficient, for their constant terms $\sigma g(X, 0) = \sigma f(X, t(X))$ to be distinct. Denote by $\alpha \in M$ a primitive element over K. We write $f(X, Y) = Y^m + c_{m-1}(X)Y^{m-1} + ... + c_0(X)$. We set $t(X) = X^N + \alpha X^{N-1}$ for a sufficiently large integer N. Then we have:

$$g(X, 0) = f(X, t(X)) = (X^N + \alpha X^{N-1})^m + c_{m-1}(X)(X^N + \alpha X^{N-1})^{m-1} + ... + c_0(X)$$

If we take N to be large enough such that for all $0 \leqslant i \leqslant m - 1$ we have

$$\deg c_i(X) + N \cdot i < m \cdot N - 1$$

then the terms of highest terms only come from $(X^N + \alpha X^{N-1})^m$:

$$g(X, 0) = X^{m\cdot N} + m\alpha X^{m\cdot N-1} + \text{lower order terms} .$$

Since $m\alpha$ is a primitive element, all the $\sigma(m\alpha)$ are distinct and a fortiori so are the σg. □

Lemma 2.9. *If K is hilbertian, every finite field extension L of K is hilbertian.*

Proof. Let M/K be a Galois closure of L/K. We say that two elements $h, g \in M(X)[Y]$ are conjugate over L if there exists a σ in $\mathrm{Gal}(M/L) \subset \mathrm{Gal}(M/K)$ such that $\sigma h = g$. Let $f \in L(X)[Y]$ be an irreducible polynomial. Excluding all specializations for which the leading coefficient vanishes or becomes ∞, we can assume f to be monic. In $M(X)[Y]$ the polynomial f decomposes into monic irreducible factors $f = f_1 \cdots f_m$ which are all conjugate over L and distinct. Lemma 2.8 yields a substitution $t \in M(X)$ using which we obtain a polynomial $g(X,Y) := f_1(X, Y + t(X))$ such that when σ runs through $\mathrm{Gal}(L/K)$ the σg are all distinct. Then

$$G := \prod_{\sigma \in \mathrm{Gal}(M/K)} \sigma g$$

lies in $K(X)[Y]$ and is irreducible. Because K is hilbertian, there are infinitely many $b \in K$ such that G_b is irreducible. This implies that g_b, and a fortiori $f_{1,b}(Y) = g_b(Y - t_b) \in M[Y]$ is irreducible. Furthermore we restrict to specializations such that all the $f_{1,b}, ..., f_{m,b}$ are distinct. Then the $f_{1,b}, ..., f_{m,b}$ are irreducible in $M(X)[Y]$, conjugate over L and distinct, hence their product $f_b = f_{1,b} \cdots f_{m,b}$ is irreducible in $L(X)[Y]$. □

Theorem 2.10. *If K is hilbertian every finitely generated field extension L is hilbertian.*

Proof. Since any finitely generated extension can be achieved as a sequence of simple, purely transcendental and finite extensions, in view of Lemma 2.9 it suffices to show that if K is hilbertian, any simple, purely transcendental field extension $K(U)$ of K is hilbertian. Let $f(U, X, Y) \in k(U)(X)[Y]$ be an irreducible polynomial. There exists a nonzero polynomial $h \in K[U]$ such that $f = \frac{\tilde{f}}{h}$ where $\tilde{f}$ is an irreducible polynomial in $K(X)[U, Y]$. By Theorem 2.7 there are infinitely many $b \in K$ such that $\tilde{f}(U, b, Y)$ is irreducible in $K[U, Y]$ and a fortiori with $\tilde{f}(U, b, Y) \cdot h(U) = f(U, b, Y)$ being irreducible in $K(U)[Y]$. □

3 Algebraic equations and Puiseux series

After the study of Hilbertian fields in general, we will in the rest of this work come back to the situation over $\mathbb{Q}$. For this we will use some tools from complex analysis, which will be the object of this section. In this whole section we consider an irreducible polynomial $P(x, y) \in \mathbb{C}[x, y]$ in the variables x and y. Let r be its degree in y. Then we can write $P(x, y) = \sum_{i=0}^{r} a_i(x) y^i$. We use the following notation:

We denote by $\mathrm{Disc}_y[P](x)$ the discriminant of the polynomial $P(x, y)$ viewed as a polynomial in y over $\mathbb{C}[x]$. A point $x_0 \in \hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ is called **critical** if $x_0 = \infty$ or $x_0 \in \mathbb{C}$ and $a_r(x_0) \cdot \mathrm{Disc}_y[P](x_0) = 0$. Since P is irreducible, $\mathrm{Disc}_y[P](x)$ is a non-zero polynomial and the set of critical points is finite.

We will study the equation

$$P(x, y) = 0 \tag{1}$$

We would like to express the solutions y of equation (1) as functions of x. If x_0 is not a critical point, $P(x_0, y)$ has r distinct roots $y_1, ..., y_r$ because its discriminant is non-zero. Since $\mathrm{Disc}_y[P](x_0) \neq 0$ also implies that $P(x_0, y)$ and $\frac{\partial P}{\partial y}(x_0, y)$ have no common factor over $\mathbb{C}$ we must have $\frac{\partial P}{\partial y}(x_0, y) \neq 0$.

Applying the implicit function theorem yields an open neighborhood U of x_0 and pairwise disjoint open neighborhoods $V_1, ..., V_r$ of $y_1, ..., y_r$ with analytic functions $\psi_i : U \to V_i$, such that for all $x \in U$:

$$P(x, y) = 0 \text{ if and only if there exists an } i \in \{1, ..., r\} \text{ such that } y = \psi_i(x).$$

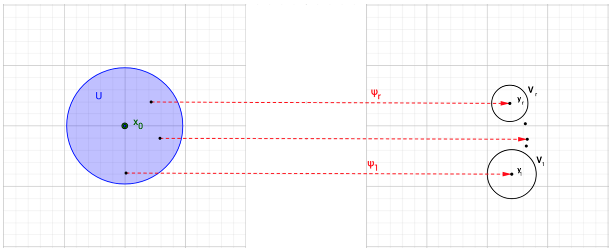


Figure 1:

If we now consider a critical point $x_0 \in \hat{\mathbb{C}}$ after a linear substitution $x \mapsto x - x_0$, or a substitution $x \mapsto 1/x$, we can assume $x_0 = 0$. Since the set of critical points is is discrete, around 0 we can pick three open discs B_1, B_2, B_3 such that $B_1 \cup B_2 \cup B_3$ forms a punctured neighborhood of 0 which does not contain a critical point (see Figure 2).

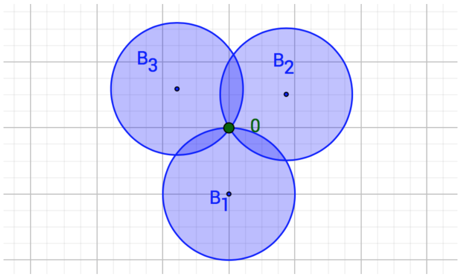


Figure 2:

By the above reasoning, at each point of our discs the possible solutions y of equation (1) are given by analytic functions of x. Denote these by $\psi_1, ..., \psi_r$ for B_1, by $w_1, ..., w_r$ for B_2 and $v_1, ..., v_r$ for B_3 respectively.

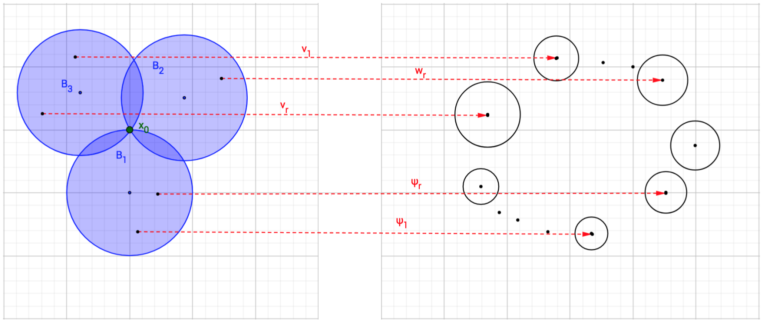


Figure 3:

On the intersection of any two discs the functions on one disc have to agree with the functions on the other disc in some order.

If we start with a function from the first disc B_1, then go to the corresponding function on B_2, then go to the corresponding function on B_3, and then go from B_3 to B_1 we may end up with a different function from the one we started with.

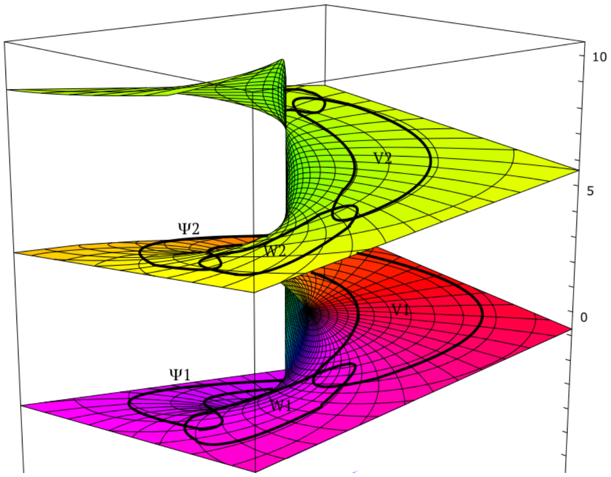


Figure 4: The Monodromy Operation

Since the monodromy operation is an element of S_r, after at most $r!$ turns we will come back to the function we started with, obtaining a cycle, for example $[\psi_1, w_1, v_1, \psi_2, ..., v_k]$. In this way the functions $\psi_1, ..., \psi_r; w_1, ..., w_r; v_1, ..., v_r$ fall into different cycle classes:

$$[\psi_1, w_1, v_1, \psi_2, ..., v_k][\psi_{k+1}, w_{k+1}, ..., v_m]...[\psi_{l+1}, ..., v_r]$$

In order to glue the elements of a cycle $[\psi_1, ..., v_k]$ together to an analytic function, we introduce the variable τ satisfying $x = \tau^{r!}$. If τ turns once around 0 then x turns $r!$ times around 0. Thus we can glue all the functions within a cycle, to an analytic function of τ:

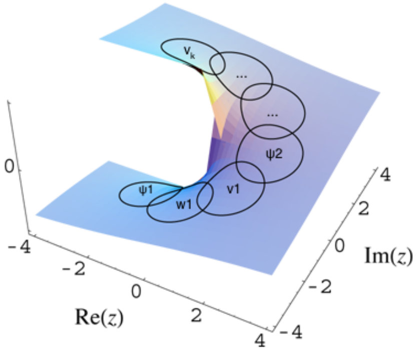


Figure 5:

Doing this for every cycle we obtain analytic functions $\varphi_1, ..., \varphi_\ell$ of τ, such that for all u in a punctured neigborhood D' of 0 and all $v \in \mathbb{C}$:

$$P(u, v) = 0 \text{ iff there exists a } \tau \in \mathbb{C} \text{ with } \tau^{r!} = u \text{ and } v = \varphi_i(\tau) \text{ for some } \varphi_i \ .$$

Theorem 3.1 (Puiseux series expansion)**.** *Let $P \in \mathbb{C}[x, y]$ be a polynomial of degree r in y. Then for all $x_0 \in \mathbb{C} \cup \{\infty\}$ there exists a punctured neighboorhood D' of x_0 and a finite collection of Laurent series $\varphi_1, ..., \varphi_k$ with finite principal part converging on a punctured neighborhood of 0, such that for all $u \in D'$ and $v \in \mathbb{C}$:*

$$P(u, v) = 0 \textit{ iff there is a } \tau \in \mathbb{C} \textit{ with } \tau^{r!} = \begin{cases} u - x_0, \textit{ if } x_0 \in \mathbb{C} \\ 1/u, \textit{ if } x_0 = \infty \end{cases} \textit{ and } v = \varphi_i(\tau) \textit{ for some } i.$$

Proof. After a substitution we can assume $x_0 = 0$. Moreover it is sufficient to show the statement for each irreducible factor. This is exactly the result showed above, hence we obtain different φ_i, which are defined on a punctured disc around 0. As analytic functions defined on a punctured disc, each φ_i has a Laurent expansion. As furthermore $\varphi_i(\tau)$ satisfies the polynomial equation $P(\tau^n, \varphi_i(\tau)) = 0$ as τ tends to 0 we can bound $\varphi_i(\tau) \cdot \tau^k$ by a constant for some k sufficiently large, and its Laurent expansion has finite principal part. □

4 The situation over $\mathbb{Q}$

This section will be devoted to proving that $\mathbb{Q}$ is hilbertian. We start by collecting some results needed for the proof of the main theorem of this section.

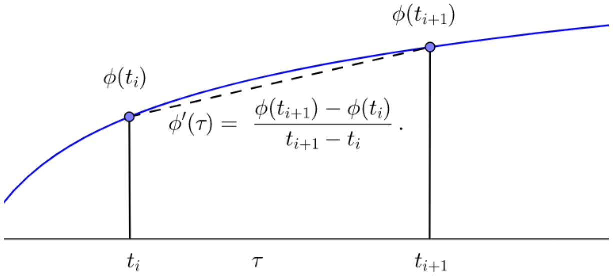
Given $c \in \mathbb{R}$ and some subset $N \subset \mathbb{C}$ we denote by $N^{>c}$ the set $\{n \in N \mid |n| > c\}$. Having a Puiseux series $\varphi(t)$, converging for all sufficiently large t, of the form

$$\varphi(t) = a_m t^{m/n} + ... + a_1 t^{1/n} + a_0 + a_{-1} t^{-1/n} + ...$$

we want to estimate the distribution of the sequence of natural numbers $\{t_i\}_{i\in\mathbb{N}} \in \mathbb{N}$, such that t_i and $\varphi(t_i)$ both lie in $\mathbb{Z}$.

This will be achieved in Lemma 4.2. For didactical purposes we sketch the simple case where $m = 1$, which illustrates the proof idea of the general case:

If $m = 1$, then $\varphi'(t)$ has only terms of the form $b_{-i}t^{-i/n}$, for $i > 0$, hence $\varphi'(t) \in \mathcal{O}(\frac{1}{t^{1/n}})$. Then we have the following situation:



$\phi(t_{i+1})$
$\phi(t_i)$
$\phi'(\tau) = \dfrac{\phi(t_{i+1}) - \phi(t_i)}{t_{i+1} - t_i}.$
t_i
τ
t_{i+1}

Figure 6:

and by the mean value theorem, for each pair t_i, t_{i+1} there exists a $\tau \in [t_i, t_{i+1}]$ such that:

$$\varphi'(\tau) = \frac{\varphi(t_{i+1}) - \varphi(t_i)}{t_{i+1} - t_i}.$$

which is equivalent to :

$$(\star) \qquad |t_{i+1} - t_i| = \frac{|\varphi(t_{i+1}) - \varphi(t_i)|}{|\varphi'(\tau)|}$$

Since $\varphi(t_{i+1})$ and $\varphi(t_i)$ are integers and we can assume t_{i+1} and t_i to be distinct, by equation $(\star)$, $\varphi(t_{i+1}) - \varphi(t_i)$ is a nonzero integer, in particular its absolute value is $\geqslant 1$. From equation $(\star)$ we deduce using $\varphi'(t) \in \mathcal{O}(\frac{1}{t^{1/n}})$:

$$|t_{i+1} - t_i| = \frac{|\varphi(t_{i+1}) - \varphi(t_i)|}{|\varphi'(\tau)|} \geqslant \frac{1}{|\varphi'(\tau)|} \overset{\tau \text{ large}}{\geqslant} c\tau^{1/n} \geqslant ct_i^{1/n}.$$

Now we will see a generalization of this result, which is stated in Lemma 4.2. For its proof we need a stronger version of the mean value theorem:

Lemma 4.1. *Let $\psi \in \mathcal{C}^m(\mathbb{R},\mathbb{R})$, for $m \in \mathbb{N}$. Let $t_0 < ... < t_m$ be real numbers. Then there exists a τ in the interval (t_0, t_m) satisfying:*

$$\left|\psi^{(m)}(\tau)\right| = \frac{\left| m! \cdot \det \begin{bmatrix} 1 & t_0 & ... & t_0^{m-1} & \psi(t_0) \\ . & . & & . & . \\ . & . & & . & . \\ 1 & t_m & ... & t_m^{m-1} & \psi(t_m) \end{bmatrix} \right|}{V_m},$$

where $V_m = \prod_{0 \leqslant j < k \leqslant m} (t_k - t_j)$ *is a Vandermonde determinant.*

Proof. Define the function

$$F(t) := \det \begin{bmatrix} 1 & t_0 & ... & t_0^{m-1} & \psi(t_0) \\ . & . & & . & . \\ . & . & & . & . \\ 1 & t_{m-1} & ... & t_{m-1}^{m-1} & \psi(t_{m-1}) \\ 1 & t & ... & t^{m-1} & \psi(t) \end{bmatrix} .$$

Note that the above matrix differs from a Vandermonde matrix only in the last column. Moreover $F(t)$ vanishes if t is equal to one of $t_0, ..., t_{m-1}$. Thus there is a constant C such that the function:

$$G(t) := F(t) - C(t - t_0)...(t - t_{m-1})$$

vanishes at $t = t_0, ..., t_{m-1}$ and $t = t_m$.

Thus $G(t)$ vanishes $m + 1$ times in $[t_0, t_m]$. Applying the mean value theorem between neighboring zeros of $G(t)$ we obtain m distinct zeros of $G'(t)$. Successively applying the mean value theorem we eventually obtain a zero τ in (t_0, t_m) of $G^{(m)}(t)$:

$$0 = G^{(m)}(\tau) = F^{(m)}(\tau) - m! \cdot C \ .$$

By construction $F(t) = p(t) + V_{m-1} \cdot \psi(t)$, for a polynomial p in t of degree $< m$ and $V_{m-1} = \prod_{0 \leqslant j < k \leqslant m-1} (t_k - t_j)$. So we can rewrite the above equation as:

$$\begin{aligned} m! \cdot C &= F^{(m)}(\tau) \\ &= \psi^{(m)}(\tau) \cdot V_{m-1} \ . \end{aligned}$$

Dividing by V_{m-1} and taking absolute values we obtain:

$$\left| \psi^{(m)}(\tau) \right| = \left| \frac{m! \cdot C}{V_{m-1}} \right|$$

Since

$$C = \frac{F(t_m)}{(t_m - t_0)...(t_m - t_{m-1})}$$

and the product of the denominator of C with V_{m-1} is precisely V_m we obtain the statement of the lemma. □

Note that $\varphi(t)$ being a Laurent series in t^{-1} with finite principal part means that there exists an integer k such that:

$$\varphi(t) = \sum_{j=-\infty}^{k} a_j t^j$$

Lemma 4.2. *Let $\varphi(t)$ be a Laurent series with coefficients in $\mathbb{R}$, and suppose there is an integer k such that*

$$\varphi(t) = \sum_{j=-\infty}^{k} a_j t^j \ .$$

Suppose moreover there exists a $c \in \mathbb{R}$ such that $\varphi(t)$ converges on $\mathbb{R}^{>c}$. Let n be a positive integer. For each $t > 0$ let $t^{1/n}$ denote its unique positive n-th root. Define the set M by

$$M := \{t \in \mathbb{Z}^{>c^n} \mid \varphi(t^{1/n}) \in \mathbb{Z}\} \ .$$

We can write the elements of M as a strictly increasing sequence of natural numbers $\{t_i\}_{i\in\mathbb{N}}$. Then if $\varphi(t)$ is not a polynomial in t^n there exists an $m \in \mathbb{N}$, a $\lambda \in \mathbb{R}^+$ and an $i_0 \in \mathbb{N}$ such that for all $i > i_0$:

$$t_{i+m} - t_i > t_i^{\lambda} \ .$$

Proof. Define the function mapping t to $\psi(t) := \varphi(t^{1/n}) = \sum_{j=-\infty}^{k} a_j t^{j/n}$, which is defined on $\mathbb{R}^{>c^n}$.

Because $\varphi(t)$ is not a polynomial in t^n, the function $\psi(t)$ is not a polynomial in t. So its expansion contains a nonzero term of the form $a_\ell t^{-\ell/n}$ where $n \nmid \ell$ or $\ell > 0$. So the derivative contains the term $\frac{-\ell}{n} a_\ell t^{-(\ell+n)/n}$, which again satisfies $n \nmid (\ell+n)$ or $\ell + n > 0$. Therefore none of the higher-order-derivatives of ψ is identically 0.

Choose m large enough such that $\psi^{(m)}(t)$ has the form:

$$\psi^{(m)}(t) = at^{-j/n} + bt^{-(j+1)/n} + ...$$

with $j > 0$ and $|a| > 2$. Then

$$\lim_{t\to\infty} |\psi^{(m)}(t) \cdot t^{j/n}| = |a| \ .$$

Thus as t tends to infinity $\left|\psi^{(m)}(t)\right|$ is asymptotically equivalent to$\left|at^{-j/n}\right|$. In particular $\left|\psi^{(m)}(t)\right|$ is nonzero for sufficiently large t.

Fix i in $\mathbb{N}$. We apply Lemma 4.1 to ψ and the points $t_i, ..., t_{i+m}$ in M. We obtain a τ in (t_i, t_{i+m}) satisfying:

$$\left|\psi^{(m)}(\tau)\right| = \frac{\left| m! \cdot \det \begin{bmatrix} 1 & t_i & ... & t_i^{m-1} & \psi(t_i) \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ 1 & t_{i+m} & ... & t_{i+m}^{m-1} & \psi(t_{i+m}) \end{bmatrix} \right|}{V_m} \ ,$$

If we suppose t_i and hence τ large enough, $\psi^{(m)}(\tau)$ is nonzero. Moreover, by assumption all the $t_i, ..., t_{i+m}$ and all the $\psi(t_i) = \varphi(t_i^{1/n}), ..., \psi(t_{i+m}) = \varphi(t_{i+m}^{1/n})$ lie in $\mathbb{Z}$. Therefore the determinant in the above formula is a nonzero integer, and so its absolute value is bounded below by 1. Thus:

$$|\psi^{(m)}(\tau)| \geqslant \left|\frac{1}{V_m}\right| \ .$$

Using the following estimation of the absolute value of the Vandermonde determinant,

$$|V_m| = \prod_{i \leqslant j < k \leqslant i+m} |(t_k - t_j)| \leqslant |(t_{i+m} - t_i)|^{\frac{m(m+1)}{2}}$$

we obtain that for t_i sufficiently large

$$|(t_{i+m} - t_i)|^{\frac{m(m+1)}{2}} \geqslant \left|\frac{1}{\psi^{(m)}(\tau)}\right| \underset{\psi^{(m)}(t)\sim at^{j/n}}{\geqslant} \frac{1}{2}\left|a\tau^{j/n}\right| .$$

Taking the $\frac{m(m+1)}{2}th$ root on both sides yields

$$t_{i+m} - t_i > \tau^{\lambda} \geqslant t_i^{\lambda}$$

with $\lambda \leqslant 1 + \frac{jm(m+1)}{2n}$. □

Definition 4.3. *A set $M \subset \mathbb{N}$ is called **sparse** if there exists a $\lambda \in [0,1)$ and an $n_0 \in \mathbb{N}$ such that for all $N > n_0$ we have $|M \cap \{1, ..., N\}| < N^{\lambda}$.*

Lemma 4.4. *Any finite set and any finite union of sparse sets is sparse.*

Proof. Follows by a straightforward application of the definition. □

Lemma 4.5. *Let $\{t_i\}_{i\in\mathbb{N}}$ be a strictly increasing sequence of natural numbers, for which there exists an $m \in \mathbb{N}$, a $\lambda \in \mathbb{R}^+$ and an $i_0 \in \mathbb{N}$ such that for all $i > i_0$ we have:*

$$t_{i+m} - t_i > t_i^{\lambda}$$

Then the set $M := \{t_i\}_{i\in\mathbb{N}}$ is sparse.

Proof. By Lemma 4.4 it is sufficient to prove the result for $m = i_0 = 1$. Let $N \in \mathbb{N}$, set $N_1 := |\{\ i \mid t_i \leqslant N^{\frac{1}{2}}\ \}|$ and $N_2 := |\{\ i \mid N^{\frac{1}{2}} < t_i \leqslant N\ \}|$. Then $M \cap \{1, ..., N\}$ is equal to $\{t_1, ..., t_{N_1+N_2}\}$. Representing $\mathbb{R}^+$ by a ray, we have the following illustration:

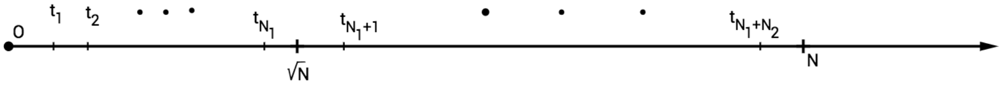


Figure 7: A representation of the set $M \cap \{1, ..., N\}$ in $\mathbb{R}^+$

First using $N \geqslant t_{N_1+N_2}$ and $N_1 < t_{N_1+1}$, and then using the assumption $t_{i+1} - t_i > t_i^{\lambda}$ we obtain the following inequalities:

$$N - N_1 \geqslant t_{N_1+N_2} - t_{N_1+1} = \sum_{i=N_1+1}^{N_1+N_2-1} t_{i+1} - t_i > \sum_{i=N_1+1}^{N_1+N_2-1} t_i^{\lambda} \geqslant (N_2 - 1) \cdot t_{N_1+1}^{\lambda} \geqslant (N_2 - 1) \cdot N^{\frac{\lambda}{2}} .$$

Dividing $N - N_1 > (N_2 - 1)N^{\frac{\lambda}{2}}$ by $N^{\frac{\lambda}{2}}$ we get an upper estimation for N_2 using which we obtain:

$$\begin{aligned} |M \cap \{1, ..., N\}| = N_1 + N_2 &\leqslant N_1 + \frac{N - N_1}{N^{\frac{\lambda}{2}}} + 1 \\ &\leqslant N^{\frac{1}{2}} + \frac{N - N_1}{N^{\frac{\lambda}{2}}} + 1 \\ &\leqslant N^{\frac{1}{2}} + N^{1-\frac{\lambda}{2}} + 1 \\ &\leqslant N^{\alpha} \end{aligned}$$

for some $\alpha \in [0, 1)$, and sufficiently large N. □

After these analytic lemmas we are now finally ready to state the first important result of this section.

Proposition 4.6. *Let $P \in \mathbb{Q}(X)[Y]$ be an irreducible polynomial of degree $r > 1$ in Y. Then the set*

$(\star)$ $\{ b \in \mathbb{N} \mid P(b, Y)$ *has a root in* $\mathbb{Q} \}$ *is sparse.*

Proof. After multiplying by the lowest common denominator, we can assume that P lies in $\mathbb{Z}[X, Y]$. We write $P(X, Y) = \sum_{i=0}^{r} p_i(X)Y^i$. After multiplying Y by a rational function of X if necessary, we can reduce furthermore to the case where $p_r(X) = 1$. Since for all $b \in \mathbb{Z}$, $P(b, Y)$ is a polynomial in $\mathbb{Z}[Y]$ with leading coefficient 1, every root of it which lies in $\mathbb{Q}$ already lies in $\mathbb{Z}$. Thus we are reduced to showing that:

$(*)$ $\{ b \in \mathbb{N} \mid P(b, Y)$ has a root in $\mathbb{Z} \}$ is sparse.

By Theorem 3.1 there exists a $c \in \mathbb{R}$ and a finite collection of Laurent series $\varphi_1, ..., \varphi_k$ each of which has only finitely many terms with positive exponent and converges for all $t \in \mathbb{C}^{>c}$; such that for all $u \in \mathbb{C}^{>c^n}$ and all $v \in \mathbb{C}$:

$$P(u, v) = 0 \text{ iff there exists a } \tau \in \mathbb{C} \text{ with } \tau^n = u \text{ and } v = \varphi_i(\tau) \text{ for some } \varphi_i \ .$$

Thus $(*)$ is equivalent to :

$\big\{b \in \mathbb{N}^{>c^n} \mid$ there is a $\tau \in \mathbb{C}$ with $\tau^n = b$ and an $1 \leqslant i \leqslant k$ such that $\varphi_i(\tau) \in \mathbb{Z}\big\}$ is sparse.

Denote by $t \mapsto {}^1t^{1/n}, ..., t \mapsto {}^nt^{1/n}$ the different branches of the complex n-th root function. With this notation $(*)$ is further equivalent to:

$$\bigcup_{i=1}^{k} \bigcup_{\ell=1}^{n} \{ b \in \mathbb{N}^{>c^n} \mid \varphi_i({}^{\ell}t^{1/n}) \in \mathbb{Z} \} \text{ is sparse.}$$

In Lemma 4.7 below we show that for every $i \in \{1, ..., k\}$ and every $\ell \in \{1, ..., n\}$ the set $\{b \in \mathbb{N}^{>c^n} \mid \varphi_i({}^{\ell}t^{1/n}) \in \mathbb{Z}\}$ is sparse. Because a finite union of sparse sets is sparse this concludes the proof. □

Lemma 4.7. *Let $\varphi(t)$ be a Laurent series with coefficients in $\mathbb{C}$, and suppose there is an integer k such that*

$$\varphi(t) = \sum_{j=-\infty}^{k} a_j t^j \ .$$

Suppose there is a $c \in \mathbb{R}$ such that $\varphi(t)$ converges for all $t \in \mathbb{C}^{>c}$. Suppose moreover that there exists an irreducible polynomial $P \in \mathbb{Z}[X,Y]$, of degree > 1 in Y and an $n \in \mathbb{N}$ such that for all $t \in \mathbb{C}^{>c}$:

$$P(t^n, \varphi(t)) = 0 \ .$$

Let $t \mapsto t^{1/n}$ be a branch of the complex n-th root function, which is defined on an open set containing $\mathbb{R}^+$. Then the set

$$\{ \ b \in \mathbb{N}^{>c^n} \mid \varphi(b^{1/n}) \in \mathbb{Z} \ \} \text{ is sparse.}$$

Proof. The different branches of the n-th root are obtained from each other by a multiplication with powers of $e^{2\pi i/n}$. Since after substituting $\psi(t) = \varphi(e^{2\pi i/n} \cdot t)$ the Laurent series $\psi(t)$ still fullfills the assumption of the Lemma, it is enough to treat the case where $t \mapsto t^{1/n}$ is the positive real valued branch of the n-th root function. We set

$$M := \{ \ b \in \mathbb{N}^{>c^n} \mid \varphi(b^{1/n}) \in \mathbb{Z} \ \} \ .$$

If M is finite it is also sparse, so we assume from now on that it is infinite.

First case: Assume $\varphi(t)$ is a polynomial in t^n. Then $\varphi(t^{1/n})$ is a polynomial in t, say $f(t)$. Then the value of f at any element b in M is $f(b) = \varphi(b^{1/n}) \in \mathbb{Z}$. So we have infintely many integers b such that $f(b)$ also lies in $\mathbb{Z}$. Therefore f lies in $\mathbb{Q}[t]$. Since the polynomial equation $P(t, f(t)) = 0$ is true for infinitely many $t \in \mathbb{R}$, it is identically zero as a polynomial. Hence $Y - f(X)$ divides $P(X,Y)$ in $\mathbb{Q}(X)[Y]$, but the latter was supposed to be irreducible and of degree > 1 in Y. We obtain a contradiction, so in this case the set M must be finite.

Second case: $\varphi(t)$ is not a polynomial in t^n. Consider the Laurent series $\Re\varphi(t), \Im\varphi(t)$, obtained by taking the real part of the coefficients and the imaginary part of the coefficients of $\varphi(t)$ respectively. One of $\Re\varphi(t), \Im\varphi(t)$, say for instance $\Re\varphi(t)$, also is not a polynomial in t^n. Note that then

$$M = \{ \ b \in \mathbb{N}^{>c^n} \mid \varphi(b^{1/n}) \in \mathbb{Z} \ \} \subset \{ \ b \in \mathbb{N}^{>c^n} \mid \Re\varphi(b^{1/n}) \in \mathbb{Z}\} =: N.$$

Combining lemma 4.2 and 4.5 yields that the set N is sparse. A fortiori M is also sparse. If $\Im\varphi(t)$ is not a polynomial in t^n then the argument works the same using the set $N := \{ \ b \in \mathbb{N}^{>c^n} \mid \Im\varphi(b^{1/n}) = 0\}$ instead.

□

Theorem 4.8 (Hilbert's irreducibility theorem)**.** *The field $\mathbb{Q}$ is Hilbertian.*

Proof. We prove that $\mathbb{Q}$ satisfies property (3) of Theorem 2.1.

Let $P_1, ..., P_r \in \mathbb{Q}(X)[Y]$ be irreducible polynomials of degree > 1 in Y. Then by Proposition 4.6 for each $1 \leqslant i \leqslant r$ the set

$$\{\ b \in \mathbb{N} \mid P_i(b, Y) \text{ has a root in } \mathbb{Q}\ \} \text{ is sparse.}$$

Since a finite union of sparse sets is sparse, the set

$$\{\ b \in \mathbb{N} \mid \text{ one of } P_1(b, Y), ..., P_r(b, Y) \text{ has a root in } \mathbb{Q}\ \} \text{ is sparse.}$$

Since a complement of a sparse set is infinite, the set

$$\{\ b \in \mathbb{N} \mid \text{ none of } P_1(b, Y), ..., P_r(b, Y) \text{ has a root in } \mathbb{Q}\ \} \text{ is infinite.} \qquad \square$$

Corollary 4.9. *If $f \in \mathbb{Q}(X)[Y]$ is irreducible, for any integers a, d there exist infinitely many integers b congruent to $a \mod d$, such that $f(b, Y)$ is irreducible.*

Proof. We have seen in the proof of Theorem 4.8 that the set of $b \in \mathbb{N}$ such that $f(b, Y)$ is reducible is sparse. Thus it cannot contain all but finitely many of the natural numbers congruent to $a \mod d$. □

Corollary 4.10. *Given an irreducible polynomial $f \in \mathbb{Q}(X)[Y]$, the set of $b \in \mathbb{Q}$ such that $f(b, Y)$ is irreducible is dense in $\mathbb{Q}$.*

Proof. If f is irreducible in $\mathbb{Q}(X)[Y]$, then for any $q \in \mathbb{Q}$ the polynomial $g(X, Y) := f(q + 1/X, Y)$ is also irreducible. Since we can find infinitely many integers b with $g(b, Y) = f(q + 1/b, Y)$ irreducible, we are done. □

5 Applications to the inverse Galois problem

We conclude by relating Hilbert's irreducibility theorem to the inverse Galois problem.

Theorem 5.1. *Every finite group G that can be realized as a Galois group over $\mathbb{Q}(X_1, ..., X_n)$ can be realized as a Galois group over $\mathbb{Q}$.*

Proof. Assume we have a Galois extension of $\mathbb{Q}(X_1, ..., X_n)$, whose Galois group is G. By the primitive element theorem, the field extension is generated by a primitive element whose minimal polynomial we denote by $f(X_1, ..., X_n, Y)$. We have:

$$\begin{tikzcd}
\mathbb{Q}(X_1, ..., X_n)[Y]/f(X_1, ..., X_n, Y) \arrow[d, dash, "G"'] \\
\mathbb{Q}(X_1, ..., X_n)
\end{tikzcd}$$

By Hilberts irreducibility Theorem we can specialize $X_1, ..., X_n \mapsto b_1, ..., b_n \in \mathbb{Q}$ such that $f(b_1, ..., b_n, Y)$ is irreducible. Then by Proposition 1.7 the extension $\mathbb{Q}[Y]/f(b_1, ..., b_n, Y)$ is Galois with Galois Group G. □

Corollary 5.2. *Every symmetric group $\mathcal{S}_n$ can be realized as a Galois group over $\mathbb{Q}$.*

Proof. For any integer n we know that the associated symmetric polynomials $s_1, ..., s_\ell$ are algebraically independent, and generate $\mathbb{Q}(X_1, ..., X_n)^{\mathcal{S}_n}$ over $\mathbb{Q}$, i.e $\mathbb{Q}(X_1, ..., X_n)^{\mathcal{S}_n} = \mathbb{Q}(s_1, ..., s_\ell) \cong \mathbb{Q}(X_1, ..., X_\ell)$. Then the result follows from Theorem 5.1. □

References

[1] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem (Mathematical Sciences Research Institute Publications)*. Cambridge University Press, 2002.

[2] Serge Lang. *Fundamentals of Diophantine Geometry*. Springer New York, 1983.

[3] Serge Lang. *Algebra (Graduate Texts in Mathematics)*. Springer, 2005.

[4] Yamashita Makoto. Computer image : Imaginary log analytic continuation.png. 2006.

[5] E.D. Solomentsev. *Encyclopedia of mathematics*, chapter Branch point. Springer Verlag, 2002.

[6] B. L. van der Waerden. *Einführung in die algebraische Geometrie*. Springer Berlin Heidelberg, 1973.

[7] Helmut Völklein. *Groups as Galois Groups*. Cambridge University Press, 1996.