HAL
open science

Diagonal Representation of Algebraic Power Series: A Glimpse Behind the Scenes

Sergey Yurkevich

To cite this version:

Sergey Yurkevich. Diagonal Representation of Algebraic Power Series: A Glimpse Behind the Scenes. Alin Bostan and Kilian Raschel. Transcendence in Algebra, Combinatorics, Geometry and Number Theory, TRANS19 (373), Springer, pp.309-339, 2021, Springer Proceedings in Mathematics & Statistics, 978-3-030-84303-8. 10.1007/978-3-030-84304-5_13 . hal-03150958

HAL Id: hal-03150958

https://hal.science/hal-03150958v1

Submitted on 24 Feb 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Diagonal Representation of Algebraic Power Series: A Glimpse Behind the Scenes*

Sergey Yurkevich§

February 24, 2021

Abstract

There are many viewpoints on algebraic power series, ranging from the abstract ring-theoretic notion of Henselization to the very explicit perspective as diagonals of certain rational functions. To be more explicit on the latter, Denef and Lipshitz proved in 1987 that any algebraic power series in n variables can be written as a diagonal of a rational power series in one variable more. Their proof uses a lot of involved theory and machinery which remains hidden to the reader in the original article. In the present work we shall take a glimpse on these tools by motivating while defining them and reproving most of their interesting parts. Moreover, in the last section we provide a new significant improvement on the Artin-Mazur lemma, proving the existence of a 2-dimensional code of algebraic power series.

1 Introduction

1.1 Basic Notions and Motivation

In all this text, K will denote a field of characteristic zero, even though most presented results are known to work even for excellent local integral domains. By default, $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are sets (equipped with the appropriate algebraic structure) of natural numbers (including 0), rationals, reals and complex numbers respectively. A ring is always commutative with 1 and a ring homomorphism is always unital. By R^* we denote the set of units of a ring R, and $\widehat{R}$ stands for the algebraic completion of a local ring with respect to its maximal ideal. If not indicated otherwise, $x = (x_1, \ldots, x_n)$ is a vector of n variables and $x' = (x_1, \ldots, x_{n-1})$. In contrast, t is always one variable and when we write xt, we mean $(x_1 t, \ldots, x_n t)$. Given an n-dimensional index $\alpha \in \mathbb{N}^n$ we write $|\alpha|$ for $\alpha_1 + \cdots + \alpha_n$ and x^α for $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Definition. A formal power series $h(x) \in K[\![x]\!]$ is called *algebraic* if there exists a non-zero polynomial $P(x,t) \in K[x,t]$ such that $P(x, h(x)) = 0$. Such a polynomial with minimal degree in t is called a *minimal polynomial of* $h(x)$. The set of algebraic power series is denoted by $K\langle x \rangle$. A power series which is not algebraic is called *transcendental*.

*This work is based on the author's master's thesis (U. of Vienna, 2020), supervised by H. Hauser.

§Supported by the Austrian Science Fund (FWF): P-31338.

Consider $(x) \subseteq K[x]$, the maximal ideal inside $K[x]$ generated by the elements $x_1, \ldots, x_n$. Then, algebraically speaking, $K\langle x\rangle$ is the algebraic closure of the localization of $K[x]$ with respect to this ideal, $K[x]_{(x)}$, inside $K[\![x]\!]$. Hence the ring of algebraic power series is a subring of formal power series. Moreover it is easy to see that $K\langle x\rangle^* = K\langle x\rangle \cap K[\![x]\!]^*$. Here are several examples in one variable, $x = x_1$.

Example 1: Any polynomial $p(x) \in K[x]$ is an algebraic power series since we may chose $P(x,t) := t - p(x)$.

Example 2: The power series given by

$$(1+x)^r = \sum_{k\geq 0} \binom{r}{k} x^k,$$

for some rational number $r \in \mathbb{Q}$ is algebraic[1]. This holds true, because when $r = p/q$ for non-zero integers p, q, we may choose $P(x,t) = t^q - (1+x)^p$ if $p, q > 0$ and $P(x,t) = t^q(1+x)^{-p} - 1$ if p happens to be negative. We obtain again that $P(x, (1+x)^r) = 0$.

Example 3: Consider the exponential power series:

$$\exp(x) = \sum_{k\geq 0} \frac{x^k}{k!}.$$

We claim that it is transcendental: assume it was algebraic, then after dividing the minimal polynomial by the coefficient of the leading term in t, we would find a $Q(x,t) = q_0(x) + \cdots + q_{m-1}(x)t^{m-1} + t^m \in K(x)[t]$ with $Q(x, \exp(x)) = 0$. Now, taking the derivative of $Q(x, \exp(x)) = 0$ with respect to x and using $\exp'(x) = \exp(x)$, it follows that

$$q_0'(x) + \cdots + (q_{m-1}'(x) + (m-1)q_{m-1}(x)) \exp(x)^{m-1} + m \exp(x)^m = 0.$$

Subtracting this from $mQ(x, \exp(x)) = 0$ and using the simple fact that no rational function $q(x)$ can satisfy $q(x) = cq'(x)$ for $c \in K^*$, we can find a non-zero polynomial of lower degree than m also annihilating $\exp(x)$. This is a contradiction with the minimality of m.

Example 4: The function $f(x) = \sqrt{x}$ is not an algebraic power series, because it is not a formal power series.

Example 5: Set $f(x) = \sqrt{x+1}$ and $g(x) = \sqrt[3]{x+1}$; we already saw in Example 2 that both $f, g \in K\langle x\rangle$. To see that $f(x) + g(x) = \sqrt{x+1} + \sqrt[3]{x+1}$ is algebraic as well, just consider the polynomial

$$P(x,t) = t^6 - 3\,(x+1)\,t^4 - 2\,(x+1)\,t^3 + 3\,(x+1)^2\,t^2 - 6\,(x+1)^2\,t - x\,(x+1)^2$$

and verify that it indeed satisfies $P(x, f(x) + g(x)) = 0$. Finding such a $P(x,t)$ is not straightforward and may require some work.

[1] The function $(1+x)^r$ exists for any $r \in \mathbb{Q}$, because the characteristic of K is assumed to be zero.

Algebraic power series appear in many mathematical areas, such as combinatorics, algebraic geometry and number theory. In order to motivate their deep ring-theoretic study in the next sections, we first introduce a very explicit viewpoint.

Definition. Let $g(x), f(x,t)$ be formal power series:

$$g(x) = \sum_{i_1,\dots,i_n} g_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n} \in K[\![x]\!],$$
$$f(x,t) = \sum_{i_1,\dots,i_n,j} f_{i_1,\dots,i_n,j} x_1^{i_1} \cdots x_n^{i_n} t^j \in K[\![x,t]\!].$$

Then the *small diagonal* $\Delta(g)$ of $g(x)$ is the (univariate) formal power series given by:

$$\Delta(g(x)) = \Delta(g(x))(t) := \sum_{j\geq 0} g_{j,\dots,j} t^j \in K[\![t]\!].$$

The *big diagonal* $\mathcal{D}(f)$ of $f(x,t)$ is given by the (multivariate) formal power series:

$$\mathcal{D}(f(x,t)) = \mathcal{D}(f(x,t))(x) := \sum_{i_1+\cdots+i_n=j} f_{i_1,\dots,i_n,j} x_1^{i_1} \cdots x_n^{i_n} \in K[\![x]\!].$$

Clearly, for $n = 2$ it holds that $\Delta(g(x_1,x_2)) = \mathcal{D}(g(x_1,t))$. We shall always refer to the big diagonal whenever we do not specify which diagonal we use.

Example 1: Let $x = x_1$ be one variable and $f(x,t) = 1/(1-x-t)$. Then we obtain

$$\mathcal{D}(f(x,t))(x) = \mathcal{D}\Big(\sum_{i,j\geq 0} \binom{i+j}{i} x^i t^j\Big)(x).$$

Therefore it follows that $\mathcal{D}(f(x,t))(x) = \sum_{n\geq 0} \binom{2n}{n} x^n = (1-4x)^{-1/2}$. This function is an algebraic power series with minimal polynomial $P(x,t) = (1-4x)t^2 - 1$.

Example 2: Define the Hadamard product of two power series $f(x) = \sum_{\alpha\in\mathbb{N}^n} f_\alpha x^\alpha$ and $g(x) = \sum_{\alpha\in\mathbb{N}^n} g_\alpha x^\alpha$ to be the series $(f * g)(x) := \sum_{\alpha\in\mathbb{N}} f_\alpha g_\alpha x^\alpha$. Now let again $x = x_1$ and $f(x,t) = \sum_{i,j\geq 0} c_{i,j} x^i t^j$. Define $D := \{(i,j) \in \mathbb{N}^2 : i = j\}$ and its indicator function $\mathbb{1}_D : \mathbb{N}^2 \to \{0,1\}$, then we obtain:

$$\begin{aligned}\Big(f(x,t) * \frac{1}{1-xt}\Big)(x,t) &= \Big(\sum_{i,j\geq 0} c_{i,j} x^i t^j * \sum_{i,j\geq 0} \mathbb{1}_D x^i t^j\Big)(x,t) = \sum_{i,j\geq 0} c_{i,j} \mathbb{1}_D x^i t^j \\ &= \sum_{n\geq 0} c_{n,n} (xt)^n = \mathcal{D}(f(x,t))(xt),\end{aligned}$$

the diagonal of $f(x,t)$, with xt substituted by x. This gives another viewpoint on the diagonal operator and was one historic reason for its definition.

Example 3: Consider the well-known power series

$$f(t) = \sum_{n\geq 0}\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 t^n \in \mathbb{Z}[\![t]\!] \subseteq \mathbb{C}[\![t]\!].$$

This series appears in Apéry's proof of the irrationality of $\zeta(3)$. It is known to be transcendental and to satisfy a Picard-Fuchs differential equation, see [ABD19, AB13]. A lengthy but simple computation shows that $f(t)$ is the small diagonal of the rational power series

$$\frac{1}{1-x_1} \cdot \frac{1}{(1-x_2)(1-x_3)(1-x_4)(1-x_5) - x_1x_2x_3} \in \mathbb{Z}[\![x_1, x_2, x_3, x_4, x_5]\!].$$

In [Str14] a diagonal representation with four variables is shown:

$$f(t) = \Delta\left(\frac{1}{(1-x_1-x_2)(1-x_3-x_4) - x_1x_2x_3x_4}\right).$$

Is is not known whether a similar rational expression using only 3 variables exists; in fact no power series is known for which 4 is provably the least number such that it is possible to write it as a small diagonal of some rational power series in that many variables [BLS17].

There are many theorems in the literature connecting algebraic power series and diagonals of rational functions. For example, Pólya observed already in 1922 that the diagonal of any rational power series in two variables is necessarily algebraic [Pó22]. Furstenberg's trick from 1967 implies that if $f \in K[\![x]\!]$ is algebraic and $x = x_1$ one variable, then there exists a rational power series $R(x,t)$ with $\mathcal{D}(R(x,t)) = f(x)$ [Fur67]; see also [Saf87], [AB13, Section 6] and [Dum16, Lemma 87]. In the same paper, Furstenberg proved that the small diagonal of any rational power series with coefficients in a field of positive characteristic is algebraic. In 1984 Deligne improved on the second result: the small diagonal of any *algebraic* power series over a field of positive characteristic is algebraic [Del84]. Note that for fields of characteristic 0 neither Deligne's nor Furstenberg's statements hold (cf. Example 3 above). Some elementary proofs of Deligne-Furstenberg's theorem have been found later by Harase [Har88], as well as by Sharif and Woodcock [SW88]. More recent and quantitative progress on this theorem is done by Adamczewski and Bell in [AB13]. Denef and Lipshitz gave a simpler proof already in 1987 and generalized the first theorem of Furstenberg to several variables [DL87]. This generalization stated below uses very abstract theory about the ring $K\langle x\rangle$ and we will present its proof in the last section using the discussed theorems of previous sections. A recent algorithmic confrontation to the viewpoint of algebraic power series as diagonals of rational functions is explained in [BDS17]. Finally, the reader can find Christol's survey about diagonals of rational functions in [Chr15].

Theorem 1.1 (Denef & Lipshitz). *Let $f(x) \in K\langle x\rangle$ be an algebraic power series in n variables over a field K of characteristic zero.*[2] *Then there exists a rational power series in $n+1$ variables $R(x,t) \in K(x,t) \cap K[\![x,t]\!]$ such that $f(x) = \mathcal{D}(R(x,t))$.*[3]

While the statement of this theorem is completely elementary, its proof uses quite involved techniques of commutative algebra and algebraic geometry. The goal of this text is not only to motivate and explain them to a non-expert reader, but also to provide intuition for the main steps of the original proof. After the prefatory discussion about the ring of algebraic power series in Section 1, we advance to Section 2 which is devoted to the notion of Henselization and its connection to $K\langle x\rangle$. In Section 3 we introduce étale ring maps and use this tool to prove an important fact about the Henselization of certain rings. Finally, in Section 4 we demonstrate the proof of Theorem 1.1 and present a new application of it, Theorem 4.3, in which we improve on the so-called Artin-Mazur lemma. We will recall all non-trivial definitions and try to be self-contained throughout the whole article.

Even though the proof of Theorem 1.1 is quite difficult, we can easily show it by the same trick as Furstenberg for a subclass of algebraic power series, which we call *étale-algebraic*. As we will see, the difficulty is then reducing the general case to the étale-algebraic one. This is done by proving that any algebraic power series can be represented as a rational function in an étale-algebraic series.

Definition. An algebraic power series $h(x) \in K\langle x\rangle$ with minimal polynomial $P(x,t) \in K[x,t]$ is called *étale-algebraic* if $h(0) = 0$ and $\partial_t P(0,0) \neq 0$.

Note that it immediately follows from the implicit function theorem that the minimal polynomial (as a function in t) of an étale-algebraic power series has a unique power series root vanishing at 0, which must be the étale-algebraic series itself. Therefore, étale-algebraic power series are exactly those series which are encoded uniquely by their minimal polynomial.

Example: Take $x = x_1$; the algebraic power series $\tilde{h}(x) = x\sqrt{1-x}$ has minimal polynomial $\tilde{P}(x,t) = t^2 + x^3 - x^2$ which admits $\partial_t \tilde{P}(0,0) = 0$ and therefore $\tilde{h}(x)$ is not étale-algebraic. Clearly, $\tilde{P}(x,t) = (t - x\sqrt{1-x})(t + x\sqrt{1-x})$ has two power series solutions, both vanishing at 0. However, consider $h(x) = \sqrt{1-x} - 1$. Then still $h(0) = 0$ and for the new minimal polynomial we find $\partial_t P(0,0) = 2 \neq 0$, meaning that $h(x)$ is étale-algebraic.

Lemma 1.2. *Let $h \in K\langle x\rangle$ be étale-algebraic with minimal polynomial $P(x,t) \in K[x,t]$. Then the following rational function is a power series*

$$F := t\frac{\partial_t P(xt,t)}{P(xt,t)} \in K[\![x,t]\!].$$

[2] In the original paper [DL87] the statement is more general, allowing for excellent local integral domains instead of only fields of characteristic 0, but the ideas of the proof are the same in the special case we consider.

[3] For completeness we mention that Denef and Lipshitz also proved another similar theorem in their paper. Using a slightly different notion of diagonal, they showed that an algebraic power series in n variables is the diagonal of a rational function in $2n$ variables, see [DL87, Theorem 6.2 (ii)].

Moreover, for any $i \in \mathbb{N}^n$ and $j \in \mathbb{N}$, the series $x^i h(x)^j$ is the diagonal of $(xt)^i t^{j+1} F$. In particular, Theorem 1.1 holds if f is étale-algebraic.

Proof. Since $h(x)$ is a root of $P(x,t)$, we can write $P(x,t) = (t - h(x))Q(x,t)$ for some $Q(x,t) \in K[\![x]\!][t]$. Differentiating both sides with respect to t gives

$$\partial_t P(x,t) = Q(x,t) + (t - h(x))\partial_t Q(x,t), \tag{1}$$

hence, after dividing through by $P(x,t)/t$, we obtain

$$t\frac{\partial_t P(x,t)}{P(x,t)} = \frac{t}{t - h(x)} + t\frac{\partial_t Q(x,t)}{Q(x,t)}. \tag{2}$$

Equation (1) implies that $Q(0,0) \neq 0$, therefore $Q(x,t) \in K[\![x,t]\!]^*$ and consequently the second summand in the equation above is a power series. Furthermore, since $h(0) = 0$, we have

$$\frac{t}{t - h(xt)} = \frac{1}{1 - t^{-1}h(xt)} \in K[\![x,t]\!].$$

This concludes, using equation (2), the proof of the first part of the Lemma. For the second part, consider

$$R(x,t) = (xt)^i t^{j+1} \frac{\partial_t P(xt,t)}{P(xt,t)}.$$

A straightforward computation together with equation (2) yields

$$\begin{aligned} \mathcal{D}(R(x,t)) &= \mathcal{D}\Big((xt)^i t^j \frac{1}{1 - t^{-1}h(xt)}\Big) = \mathcal{D}\Big((xt)^i \sum_{k \geq 0} t^{j-k} h(xt)^k\Big) \\ &= \mathcal{D}\big((xt)^i h(xt)^j\big) = x^i h(x)^j. \end{aligned} \tag{3}$$

Finally, by setting $i = 0$ and $j = 1$ in (3), we obtain the theorem of Denef and Lipshitz for étale-algebraic power series. □

Now we dive into a more fundamental and basic study of our ring of interest $K\langle x \rangle$.

1.2 Weierstrass Theorems

The Weierstrass division theorem (WDT) and the preparation theorem (WPT) are fundamental classical results about the rings of formal and convergent power series. WDT is in some sense a form of the Euclidean division algorithm, but requires an extra property on the divisor. Often, applications and implications of the division algorithm for the polynomial ring can be translated via the Weierstrass division theorem to $K[\![x]\!]$. For example, it implies that the ring of formal power series is Noetherian, Henselian and a unique factorization domain. However, our main interest lies in the fact that both WDT and WPT hold true for algebraic power series and yield the same implications also for this ring. This fact was first proven by Lafon in 1965 [Laf65] and is much less known. We shall reprove it following the ideas from [LT70].

Definition. We introduce the following notation and object:

(1) The *order* of a non-zero formal power series $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$, denoted by $\mathrm{ord}(f)$, is the smallest integer $d \geq 0$ such that $a_\alpha \neq 0$ for some $\alpha \in \mathbb{N}^n$ with $|\alpha| = d$. For $f = 0$ we say that $\mathrm{ord}(f) = +\infty$.

(2) A power series $g \in K[\![x]\!]$ is called *x_n-regular of order d* if $g(0, \ldots, 0, x_n) = x_n^d f(x_n)$ for some power series $f(x_n) \in K[\![x_n]\!]$ with $f(0) \neq 0$.

(3) A polynomial $p \in K[\![x']\!][x_n]$ is called *distinguished* if it is of the form $p = x_n^d + a_{d-1}(x')x_n^{d-1} + \cdots + a_0(x')$ for some power series $a_i(x') \in K[\![x']\!]$ with $a_i(0) = 0$ for $i = 0, \ldots, d-1$.

Theorem 1.3 (WPT)**.** *Let $g \in K[\![x]\!]$ be an x_n-regular power series of order d. Then there exist a unique $p \in K[\![x']\!][x_n]$ which is a distinguished polynomial in x_n of degree d and a unique unit $u \in K[\![x]\!]^*$, such that $g = up$.*

Theorem 1.4 (WDT)**.** *Let $g \in K[\![x]\!]$ be an x_n-regular power series of order d. For any $f \in K[\![x]\!]$ there exist uniquely a power series $q \in K[\![x]\!]$ and an $r \in K[\![x']\!][x_n]$ which is a distinguished polynomial in x_n of degree less than d, such that $f = qg + r$.*

There are several different known ways to prove these classical theorems. The standard literature for their proofs and implications is the book "The Basic Theory of Power Series" by Ruiz [Rui93], a more recent and very short proof can be found in [Hau17]. A very explicit approach is followed by Lang in [Lan84]. Now we state and prove Lafon's algebraic versions of these theorems.

Theorem 1.5 (Algebraic WPT)**.** *Let $g \in K\langle x \rangle$ be an x_n-regular algebraic power series of order d. Then there exist a unique $p \in K\langle x' \rangle[x_n]$ which is a distinguished polynomial in x_n of degree d with coefficients given by algebraic power series in x' and a unique unit $u \in K\langle x \rangle^*$, such that $g = up$.*

Proof. First note that we may assume without loss of generality that g is irreducible as a power series. Write $g = up$ with $u \in K[\![x]\!]^*$ and $p \in K[\![x']\!][x]$ a distinguished polynomial of degree d. It follows that p has d distinct roots in an algebraic closure of the quotient ring of the formal power series $\Omega = \overline{\mathrm{Frac}(K[\![x']\!])}$, say $\alpha_1, \ldots, \alpha_d$. Now let $G(x,t) = G_0(x) + G_1(x)t + \cdots + G_e(x)t^e \in K[x,t]$, $G_0 \neq 0$ be a minimal polynomial of g, i.e. we have

$$0 = G(x, g(x)) = G_0(x) + G_1(x)g(x) + \cdots + G_e(x)g(x)^e.$$

For every $i = 1, \ldots, d$ we can replace x by (x', α_i) and, using $g(x', \alpha_i) = 0$, we obtain for every of those i's

$$0 = G(x', \alpha_i, g(x', \alpha_i)) = G_0(x', \alpha_i).$$

As $0 \not\equiv G_0(x', x_n) \in K[x', x_n] \subseteq K(x', x_n)$ and annihilates α_i, we get that α_i is algebraic over $K(x')$. It follows that $x_n - \alpha_i$ is algebraic over $K(x', x_n) = K(x)$. Therefore, $p = \prod_{j=1}^d (x_n - \alpha_j)$ is an algebraic power series and the same holds for $u = g/p$. Uniqueness is guaranteed by uniqueness of Weierstrass formal preparation (Theorem 1.3). $\square$

Theorem 1.6 (Algebraic WDT). *Let $g \in K\langle x\rangle$ be an x_n-regular algebraic power series of order d. For any $f \in K\langle x\rangle$ there exist uniquely an algebraic power series $q \in K\langle x\rangle$ and an $r \in K\langle x'\rangle[x_n]$ which is a distinguished polynomial in x_n of degree less than d with coefficients given by algebraic power series in x', such that $f = qg + r$.*

Proof. Again, we may assume that g is irreducible and by the algebraic Weierstrass preparation theorem, we may also assume without loss of generality that $g \in K\langle x'\rangle[x_n]$ is a distinguished polynomial of degree d. We can divide formally:

$$f = qg + r = qg + \sum_{j=0}^{d-1} b_j(x')x_n^j, \tag{4}$$

for $q \in K[\![x]\!]$ and $b_0(x'), b_1(x'), \ldots, b_{d-1}(x') \in K[\![x']\!]$ formal power series. Because g is assumed to be a distinguished polynomial, we may write $g = \sum_{j=0}^{d} c_j(x')x_n^j$ for some $c_0(x'), \ldots, c_d(x') \in K\langle x'\rangle$ algebraic power series. We get that g has d distinct roots in $\Omega = \overline{\mathrm{Frac}(K[\![x']\!])}$, say $\alpha_1, \ldots, \alpha_d$. From (4), by replacing x_n with α_i, we get for every $i = 1, \ldots, d$ that $f(x', \alpha_i) = \sum_{j=0}^{d-1} b_j(x')\alpha_i^j$. This can be rephrased in terms of a matrix multiplication:

$$\begin{pmatrix} f(x',\alpha_1) \\ \vdots \\ f(x',\alpha_d) \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} b_0(x') \\ \vdots \\ b_{d-1}(x') \end{pmatrix}.$$

The matrix above is the Vandermonde matrix and it is invertible since the α_i's are pairwise different. Therefore, each $b_i(x')$ is uniquely given by some rational expression in the $f(x', \alpha_j)$'s and α_k's for $j, k \in \{1, \ldots, d\}$. On the other hand, by the same argument as in the proof of Theorem 1.5, we obtain that each α_i is algebraic over $K(x')$. Moreover, by assumption $f(x', x_n)$ is algebraic over $K(x', x_n)$. It follows that both field extensions $K(x') \subseteq K(x', \alpha_i)$ and $K(x', \alpha_i) \subseteq K(x', \alpha_i, f(x', \alpha_i))$ are finite. Hence, $K(x') \subseteq K(x', f(x', \alpha_i))$ is finite and consequently $f(x', \alpha_i)$ is algebraic over $K(x')$. As this holds for every $i = 1, \ldots, d$, it follows that also any rational expression in the $f(x', \alpha_j)$'s and α_k's for $j, k \in \{1, \ldots, d\}$ is algebraic over $K(x')$. Recall that each $b_i(x')$ is such an expression, therefore each $b_i(x')$ is algebraic over $K(x')$ and hence an algebraic power series. It follows that $r = \sum_{j=0}^{d-1} b_j(x')x_n^j$ is an algebraic power series and finally the same holds for $q = (f - r)/g$. Uniqueness is clear by the formal WDT (Theorem 1.4). □

As already mentioned, this theorem has many implications. For example, the proofs from [Rui93] and [Lan84] that $K[\![x]\!]$ is Noetherian and a UFD can be directly carried out for $K\langle x\rangle$. Another corollary is the following:

Theorem 1.7 (Hensel's Lemma). *Let $f \in K\langle x\rangle[t]$ be a monic polynomial in t over $K\langle x\rangle$. Assume $\alpha \in K$ is a root of multiplicity d of the polynomial $f(0, t) \in K[t]$. Then there exist unique monic polynomials $p, u \in K\langle x\rangle[t]$ with $u(0, \alpha) \neq 0$, p of degree d in t, $p(0, t) = (t - \alpha)^d$ and $f = up$.*

Proof. After the change of the variable t to $t+\alpha$, we may assume that $\alpha = 0$. Since α is a d-multiple root of $f(0,t)$, it follows that $f(x,t)$ is t-regular of order d. By the algebraic WPT in $n+1$ variables we may write uniquely $f = up$ where $p \in K\langle x\rangle[t]$ is a distinguished polynomial in t of degree d and $u \in K\langle x,t\rangle^*$ a unit, hence $u(0,\alpha) = u(0,0) \neq 0$. Moreover, since $p(x,t)$ is distinguished of degree d it follows by definition that $p(0,t) = t^d = (t-\alpha)^d$. $u(x,t) \in K\langle x\rangle[t]$ because of polynomial division in this ring. Uniqueness follows from the uniqueness of the algebraic Weierstrass division theorem. $\square$

The statement above ensures that a root $\alpha \in K$ of $f(0,t)$ gives rise to a factorization $f = up$. This factorization is called the *lifting* of α. Lifting all roots separately, one by one, it is possible to prove that coprime factorizations can be lifted as well.

Theorem 1.8 (Hensel's Lemma)**.** *Let $f \in K\langle x\rangle[t]$ be a monic polynomial in t over $K\langle x\rangle$. Assume $f(0,t) = \bar{p}(t)\bar{q}(t)$ factors into two monic coprime polynomials. Then there exist two unique monic polynomials $p, q \in K\langle x\rangle[t]$ with $p(0,t) = \bar{p}(t)$, $q(0,t) = \bar{q}(t)$ and $f = qp$.*

We omit the detailed proof here, because the equivalence on these two versions of Hensel's lemma will be justified in Section 3 in a more general setting. Instead, we explain the importance of these theorems following the motivation in [Eis95, pp. 185].

1.3 The Importance of Hensel's Lemma

Consider the nodal plane cubic curve over a field K (of characteristic 0 as always or positive but not equal to 2) given by the equation $t^2 - x^2(1+x) = 0$ for $x = x_1$. The associated affine coordinate ring is $S = K[x,t]/(t^2 - x^2(1+x))$. Of course, the curve is irreducible and S is a domain. When looking at the picture over $\mathbb{R}$ (Figure 1), one may think that localizing S at the maximal ideal $\mathfrak{m} = (\bar{x}, \bar{t})$ will make the ring have zero divisors, however this is not the case: every Zariski neighborhood of 0 of the node is irreducible. The reason is that over the complex numbers a neighborhood of the omitted origin is a punctured disc and therefore the curve remains irreducible. We would still like to factor $t^2 - x^2(1+x)$ somehow, in order to study the easier rings into which S will decompose. Examining a "really small neighborhood" of the node, we would expect the curve to become reducible there: for example over the ring of formal power series the expression $t^2 - x^2(1+x)$ is in fact reducible. This comes from the fact that $1+x$ has a square root in $K[\![x]\!]$ and we may therefore write $t^2 - x^2(1+x) = (t - x\sqrt{1+x})(t + x\sqrt{1+x})$. One can argue the reason why it is immediately clear that $1+x$ is a square over $K[\![x]\!]$ is that this ring satisfies Hensel's lemma! More precisely, take the polynomial $f(x,t) = t^2 - (1+x)$, then $f(0,t) =$

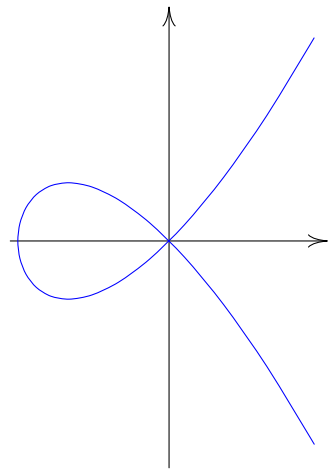

Figure 1: The node: $\mathbb{R}[x,t]/(t^2 - x^2(1+x))$.

$(t-1)(t+1) = \bar{p}(t)\bar{q}(t)$ and these polynomials are coprime. Therefore, by Hensel's lemma, this factorization must admit a lifting and therefore $\sqrt{1+x} \in K[\![x]\!]$. This is also the reason why we explicitly do not allow the characteristic of K to be 2: in this case $\bar{p}(t)$ and $\bar{q}(t)$ would not be relatively prime and the lifting would not be guaranteed, in fact it would not exist. However, we also see that in order to make the node reducible, we do not have to go from $K[x,t]$ all the way up to the polynomial ring over the completion $K[\![x]\!][t]$: it suffices to take *any* Henselian ring extension of S or of $K[x]_{(x)}$. This is exactly the idea and motivation for defining the Henselization.

2 Algebraic Power Series and Henselization

The main goal of this section is to stress the connection between the algebraic closure in the completion of a ring and the property of being Henselian, that is to satisfy Hensel's lemma. We will be able to prove that, under certain conditions, any Henselian ring is algebraically closed in its completion, that is, if $a \in \widehat{R}$ is algebraic over a Henselian R then it must already hold that $a \in R$. This will allow us to look at the ring of algebraic power series from a different viewpoint. The conditions may appear technical at first sight, however they have the purpose of excluding pathologies while still allowing for a large class of rings. A considerably different approach to this theory can be found in the book [KPR75] by Kurke, Pfister and Roczen.

We will work with *local rings*, i.e with those rings R, which have exactly one maximal ideal. Usually, we will denote this maximal ideal by $\mathfrak{m}$ and let $K := R/\mathfrak{m}$ be the residue field with respect to $\mathfrak{m}$. Sometimes, we write triples $(R, \mathfrak{m}, K)$ when talking about local rings, combining these three objects. It is immediate to see that R has only one maximal ideal $\mathfrak{m}$ if and only if $R^* = R \setminus \mathfrak{m}$. Recall that given two local rings $(R, \mathfrak{m}, K), (S, \mathfrak{n}, L)$, a homomorphism $\phi : R \to S$ is called *local* if $\phi(\mathfrak{m}) \subseteq \mathfrak{n}$ holds and this condition is equivalent to $\phi^{-1}(\mathfrak{n}) = \mathfrak{m}$. Note that both, the rings of formal and algebraic power series, are local with maximal ideal $\mathfrak{m} = (x) = (x_1, \ldots, x_n)$. It is also obvious that the residue field $K[\![x]\!]/(x) \cong K\langle x\rangle/(x)$ is (isomorphic to) K. Recall that the *completion* of a local ring $(R, \mathfrak{m}, K)$ is defined as the inverse limit $\varprojlim R/\mathfrak{m}^i$. A local ring $(R, \mathfrak{m}, K)$ is called *complete* if the canonical map to its completion $R \to \widehat{R}$ is an isomorphism. Note that $\cap_i \mathfrak{m}^i$ goes to zero under this mapping, therefore completeness implies $\cap_i \mathfrak{m}^i = 0$. Krull's intersection theorem justifies that the completion of a *Noetherian* ring (i.e. a ring with only finitely generated ideals) is complete, however this is false in general. Finally, recall that the completion $\widehat{R}$ of R satisfies the universal property that for any local $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ with $(S, \mathfrak{n})$ complete there exists a unique factorization $R \to \widehat{R} \to S$.

2.1 Henselian Rings

Given a $p \in R[t]$, we will denote by $\bar{p} \in K[t]$ the reduction of p mod $\mathfrak{m}R[t]$, given by reducing all coefficients of p mod $\mathfrak{m}$.

Definition. A local ring $(R, \mathfrak{m}, K)$ is called *Henselian* if the following property holds: Let $f(t) \in R[t]$ be a monic polynomial. Assume that $\bar{f}(t) = p_0(t)q_0(t)$ holds for two monic

coprime polynomials $p_0(t), q_0(t) \in K[t]$. Then there exist two unique monic polynomials $p(t), q(t) \in R[t]$ satisfying $\bar{p}(t) = p_0(t), \bar{q}(t) = q_0(t)$, $\deg p(t) = \deg p_0(t)$, $\deg q(t) = \deg q_0(t)$ and $f(t) = p(t)q(t)$.

The notion of Henselian rings (or Hensel rings) was first introduced by Azumaya in [Azu51]. The property above is usually referred to as "Hensel's lemma" even though it is used as a definition. One often reads in the literature "A ring is called Henselian, if Hensel's lemma holds [in this ring]". To avoid confusion, we will call the statement above Hensel's property. The actual "lemma" of Hensel is the following classical theorem (see for example [Eis95, Chapter 7]):

Theorem 2.1 (Hensel's lemma for complete rings)**.** *Let $(R, \mathfrak{m}, K)$ be a complete local ring. Then R is Henselian.*

Standard references for Henselian rings are [Nag62, Ray70, Gro67]. For the purpose of this work, a very significant fact is that Theorem 1.8 implies the following:

Theorem 2.2. *The ring of algebraic power series $K\langle x\rangle$ is Henselian.*

Another key fact about Henselian rings is the following lemma. Its statement and proof appear in [Nag62] and give an introductory flavor to this section. Recall that given an extension of rings $R \subseteq S$, an element $s \in S$ is called *integral over* R if there exists a monic polynomial $P(t) \in R[t]$ with $P(s) = 0$. The extension is said to be *integral* if this holds for any $s \in S$.

Lemma 2.3. *Let R be a Henselian integral domain and R' an integral extension of R. Then R' is a local ring.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of R and assume that R' has two maximal ideals $\mathfrak{m}'_1 \neq \mathfrak{m}'_2$. Take some $a \in \mathfrak{m}'_1$ which is not in $\mathfrak{m}'_2$. We have an irreducible monic polynomial $f(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0 \in R[t]$ which has a as root. Now, as $a \in \mathfrak{m}'_1$, we must have $c_0 \in \mathfrak{m}'_1 \cap R \subseteq \mathfrak{m}$. We also have that $a^n \notin \mathfrak{m}R[a]$, because $a \notin \mathfrak{m}'_2$, hence there must be a c_i which is not in $\mathfrak{m}$. Take $j \in \mathbb{N}$ such that $c_j \notin \mathfrak{m}$ but $c_{j-s} \in \mathfrak{m}$ for $0 < s \leq j$. Clearly $1 \leq j \leq n-1$ and we have

$$f(t) \equiv (t^j + c_{n-1}t^{j-1} + \cdots + c_{n-j})t^{n-j} \mod \mathfrak{m}R[t].$$

But this means that the image of f is reducible mod $\mathfrak{m}R[t]$ and using that R is Henselian we obtain that f must be reducible in $R[t]$. This is a contradiction and the assertion is proved. □

To state the main theorem of this section we will need some conditions on our local ring R. Therefore we define the necessary terms:

Definition. Let R be a ring.

(1) R is called *analytically irreducible* if it is local and its completion $\widehat{R}$ is a domain. R is called *analytically normal* if it is local and $\widehat{R}$ is normal[4].

[4]Recall that a local ring is called normal if is integrally closed in its quotient field.

(2) Assume R be an integral domain with quotient field L. R is called *Japanese*[5] if it satisfies the so-called finiteness condition for integral extensions. This means, for every finite extension L' of the quotient field L, the integral closure of R in L' is a finitely generated R-module.

(3) R is called a *Nagata ring*[6] if R is Noetherian and for every prime ideal $\mathfrak{p} \subseteq R$, the ring $R/\mathfrak{p}$ is Japanese.

Lemma 2.4. *If R is a Nagata ring, then every ring which is a finite module over R or a ring of quotients of R is also Nagata. Any localization of R is also Nagata. Any finitely generated R-algebra is Nagata.*

We see that the category of Nagata rings is reasonably large and closed under many operations. Good references for the proofs of the lemma above are [Nag62, Section 36] and [Mat80, Section 31]. Of course, most facts can also be found in [Sta20, Section 032E].

Finally, for our purposes we need the following version of the Zariski Main Theorem, which is Theorem 37.8 in [Nag62]. Recall that S is said to be of *finite type* over R if S is isomorphic to a quotient of $R[x_1, \ldots, x_n]$ as an R-algebra.

Lemma 2.5. *Let R be an analytically normal ring. If a normal and local Nagata ring S is of finite type over R, then S analytically irreducible.*

We are ready to prove one central theorem of this section, connecting Henselian rings with the property of being algebraically closed in the completion, and which will be a crucial ingredient in the proof of Theorem 2.7. This theorem explains why the study of algebraic power series essentially comes down to studying Henselian rings. Its statement can be found in [Nag62, (44.1)], however the proof given there is very concise and in some places unclear. Therefore we shall reprove the theorem here.

Theorem 2.6. *Let R be a Henselian, analytically normal Nagata ring. Then R is algebraically closed in its completion, i.e. if $a \in \widehat{R}$ algebraic over R, then $a \in R$.*

Proof. Let a be an element of $\widehat{R}$ which is algebraic over R. Then we can find $b \neq 0$ in R such that $c := ab$ is integral over R. We claim that $R[c] = R$. Assume otherwise and let $f \in R[t]$ be the minimal polynomial of c. We wish to use the lemma above on $R[c]$, but we lack the assumption of normality. So we define R' to be the integral closure of $R[c]$ in $L[c]$, where $L = \mathrm{Frac}(R)$, so R' is normal by definition. By an easy observation it follows that R' is also the integral closure of R in $L[c]$. Since R is analytically normal, it is a domain and therefore the ideal (0) is prime. By the definition of a Nagata ring, it follows that the integral closure of $R = R/(0)$ in any finite extension of L is a finitely generated R-module. Since c is integral and in particular algebraic, it follows that $L[c]$ is a finite extension of L and therefore R' is a finitely generated R-module. Furthermore,

[5] According to [Sta20] this name was first used by Grothendieck in order to contribute to Nakayama, Takagi, Nagata and many others.

[6] In the book "Local Rings" Nagata calls these rings pseudo-geometric.

R', being finitely generated over a Nagata ring, is still Nagata by Proposition 2.4 and also R' is indeed local by Lemma 2.3[7], hence we may apply Lemma 2.5 to get that R' is analytically irreducible. However, we have that $\widehat{R'} = R' \otimes_R \widehat{R}$ and this must be a domain. Now look at the completion of $R[c]$, which is given by $R[c] \otimes_R \widehat{R}$. Now, $R \to \widehat{R}$ is flat, meaning that we also have the inclusion $R[c] \otimes_R \widehat{R} \subseteq R' \otimes_R \widehat{R}$ and hence $\widehat{R[c]}$ must be a domain as well. On the other hand, we have $\widehat{R[c]} = R[c] \otimes_R \widehat{R} = \widehat{R}[t]/(f)$, identifying f with its image in $\widehat{R}[t]$. However $c \in \widehat{R}$ is a root of f, hence $\widehat{R}[t]/(f)$ cannot be a domain: a contradiction. So $c \in R$ and hence $a \in \mathrm{Frac}(R)$. Because $R = \mathrm{Frac}(R) \cap \widehat{R}$ and since a is in both rings, we get that $a \in R$ as wanted. $\square$

2.2 Henselian Characterization of Algebraic Power Series

We saw that Henselian rings are closely connected to algebraic closures in the completion. In particular, at this point, one may conjecture that for some, not necessarily Henselian, ring R, if we can define the "smallest" Henselian extension of R, it will be exactly the algebraic closure of R in $\widehat{R}$. Since algebraic power series are by definition the algebraic closure of $K[x]_{(x)}$ in its completion, this approach will also give a different viewpoint on our main ring of interest. Note that obviously any field is Nagata, therefore by Lemma 2.4 it follows that $K[x]$ is also a Nagata ring. Then $K[x]_{(x)}$ is again Nagata, since it is a localization.

Definition. Let $(R, \mathfrak{m}, K)$ be a local ring. We say a Henselian ring R^{h} together with a local homomorphism $i : R \to R^{\mathrm{h}}$ is the *Henselization* of R, if any local homomorphism from R to a Henselian ring factors uniquely through i.

In other words, the Henselian ring R^{h} together with $i : R \to R^{\mathrm{h}}$ is the Henselization of R, if for any Henselian ring H and local $\psi : R \to H$ there exists a unique local ϕ such that the following diagram commutes:

$$\begin{tikzcd} R \arrow[r, "i"] \arrow[d, "\psi"'] & R^{\mathrm{h}} \arrow[dl, dashed, "\phi"] \\ H & \end{tikzcd}$$

This notion was first introduced by Nagata in the article "On the theory of Henselian rings", which became the first of a trilogy [Nag53, Nag54, Nag59]. Since then, the Henselization of a ring became a very well studied object; we shall only explain those facts which are of importance for our purpose.

Note that from the definition it follows that if R^{h} exists, then it must be unique up to isomorphism. For Noetherian rings one has the inclusion $R \hookrightarrow \widehat{R}$; this together with Hensel's lemma immediately implies that i must be injective as well in this case. Moreover, the following fact follows also easily from the universal property: Assume the existence of a Henselian ring R' such that $R \subseteq R' \subseteq R^{\mathrm{h}}$, then $R' = R^{\mathrm{h}}$. In this sense we can view the Henselization as the "smallest" Henselian ring extension of R. Note that it

[7] This is where we use the Henselian assumption.

is not obvious that R^{h} exists for any local R, however this is true and we will prove this in the next section (Section 3.3).

The following theorem allows a purely ring-theoretic viewpoint on $K\langle x\rangle$.

Theorem 2.7. *Let $R = K[x]_{(x)}$ be the localization of $K[x]$ at the maximal ideal (x). Assume that the Henselization of R exists*[8]*. Then it is isomorphic to the ring of algebraic power series: $R^{\mathrm{h}} \cong K\langle x\rangle$.*

For the proof we need two lemmas: we provide a proof for the first, and a reference for the second.

Lemma 2.8. *Let R^{h} be the Henselization of a Noetherian local ring R. Then $\widehat{R^{\mathrm{h}}} = \widehat{R}$.*

Proof. By Hensel's lemma $\widehat{R}$ is Henselian, thus there exists a unique factorization $R \to R^{\mathrm{h}} \to \widehat{R}$. Let S be a complete local ring with maximal ideal $\mathfrak{n}$ and assume $R^{\mathrm{h}} \to S$ is a local map. Precomposing with i gives $R \to R^{\mathrm{h}} \to S$. By the universal property of the completion and then by the factorization of $R \to \widehat{R}$ we also find $R \to R^{\mathrm{h}} \to \widehat{R} \to S$. Now, since S being complete is also Henselian, the uniqueness in the universal property of R^{h} implies that these factorizations are equal. Hence, for every $R \to S$ with S complete we find $R^{\mathrm{h}} \to \widehat{R} \to S$. The universal property of the completion forces $\widehat{R^{\mathrm{h}}} = \widehat{R}$. □

Lemma 2.9. *Let R be a local Nagata ring. Then its Henselization R^{h} is also Nagata. Moreover, if R is also analytically normal then so is R^{h}.*

For the proof see [Nag62, (44.2,44.3)].

Proof of Theorem 2.7. By Lemma 2.9 it follows that $K[x]^{\mathrm{h}}_{(x)}$ is both analytically normal and Nagata. Because the ring of algebraic power series is Henselian (Theorem 2.2) and the Henselization is the smallest Henselian ring extension of a given ring, it suffices to show $K\langle x\rangle \subseteq K[x]^{\mathrm{h}}_{(x)}$. Let $f \in K\langle x\rangle \subseteq K[\![x]\!] = \widehat{K[x]_{(x)}}$. Then obviously f is algebraic over $K[x]^{\mathrm{h}}_{(x)}$ and by Lemma 2.8 we must have $f \in \widehat{K[x]^{\mathrm{h}}_{(x)}}$. We can apply Theorem 2.6 to see that $f \in K[x]^{\mathrm{h}}_{(x)}$. □

3 Étale Ring Maps and Henselization

3.1 Motivation for Étale Ring Maps

Before giving the rigorous definition of an étale map $R \to S$ between two rings R, S, we will try to explain the motivation behind it. Milne writes in his lecture notes [Mil13]:

> *"An étale morphism is the analogue in algebraic geometry of a local isomorphism of manifolds in differential geometry, a covering of Riemann surfaces with no branch points in complex analysis, and an unramified extension in algebraic number theory."*

[8] In the next section (Section 3.3) we will prove that the Henselization of a local ring always exists.

Of course, the importance of these objects makes it clear that one needs a definition in the setting of algebraic geometry and that this definition might be involved. There are many equivalent ways to define this analogue and we will try to motivate the one that is mostly geometric and closest to a universal property.

Consider the case of two affine algebraic varieties $X = V(f_1, \dots, f_r) \subseteq K^n, Y = V(g_1, \dots, g_s) \subseteq K^m$ and a morphism $f_\phi : X \to Y$ coming from $\phi : R \to S$, where

$$\begin{aligned} R &\coloneqq K[Y] = K[y_1, \dots, y_m]/(g_1, \dots, g_s) \text{ and} \\ S &\coloneqq K[X] = K[x_1, \dots, x_n]/(f_1, \dots, f_r) \end{aligned}$$

are the corresponding coordinate rings. Recall that a local diffeomorphism is characterized by its bijective differential. We want to achieve an analogous property for f_ϕ by putting only algebraic conditions on ϕ.

By definition, f_ϕ maps any K-point $a \coloneqq (a_1, \dots, a_n) \in X$ to a K-point $b \coloneqq (b_1, \dots, b_m) \in Y$. To formulate this in an algebraic way, we can require the following diagram to commute:

$$\begin{tikzcd} S = K[X] \arrow[r] & K \\ R = K[Y] \arrow[u, "\phi"] \arrow[ur] & \end{tikzcd}$$

To see that this algebraic formulation indeed corresponds to the geometric viewpoint of sending $a \in X$ to some $b \in Y$, note that the map $K[X] \to K$ defines a K-point of X, since it maps each x_i to a_i for some $a \coloneqq (a_1, \dots, a_n) \in K^n$ with the condition that each $f_j(a_1, \dots, a_n) = 0$, $1 \leq j \leq r$, hence, by definition, $a \in X$. Similarly, $K[Y] \to K$ is a K-point, say $b = (b_1, \dots, b_m) \in Y$, because $g_j(b_1, \dots, b_m) = 0$ for $j = 1, \dots, s$. The commutativity of the diagram means that sending $(y_1, \dots, y_m) \mapsto (b_1, \dots, b_m)$ by the diagonal map is the same as sending $(y_1 \dots, y_m) \mapsto (\phi_1(x_1, \dots, x_n), \dots, \phi_m(x_1, \dots, x_n)) \mapsto (\phi_1(a), \dots, \phi_m(a))$: K-points are sent to K-points.

Now we want to describe the behavior of f_ϕ on tangent vectors. We can formulate this in an algebraic way, by requiring the commutativity of the following diagram, adding the ring $K[\varepsilon]/(\varepsilon^2)$ to the above:

$$\begin{tikzcd} S = K[X] \arrow[r] & K \\ R = K[Y] \arrow[u, "\phi"] \arrow[r] & K[\varepsilon]/(\varepsilon^2) \arrow[u] \end{tikzcd}$$

Since

$$\begin{gathered} K[Y] \longrightarrow K[\varepsilon]/(\varepsilon^2) \longrightarrow K \\ (y_1, \dots, y_m) \mapsto (b_1 + \varepsilon c_1, \dots, b_m + \varepsilon c_m) \mapsto (b_1, \dots, b_m), \end{gathered}$$

we see that this intermediate ring does not destroy the considerations above. Moreover, we claim that the map $K[Y] \to K[\varepsilon]/(\varepsilon^2)$ corresponds to a tangent vector of Y: say, we

have

$$K[Y] = K[y_1, \ldots, y_m]/(g_1, \ldots, g_s) \to K[\varepsilon]/(\varepsilon^2)$$
$$y_i \mapsto b_i + \varepsilon c_i, \quad 1 \le i \le m,$$

for some $b \in K^m$ and $c := (c_1, \ldots, c_m) \in K^m$. Then it must hold that $g_j(b_1+\varepsilon c_1, \ldots, b_m+\varepsilon c_m) = 0$ for $1 \le j \le s$. Using Taylor expansion and the fact that $\varepsilon^2 = 0$ in $K[\varepsilon]/(\varepsilon^2)$, we obtain:

$$0 = g_j(b_1 + \varepsilon c_1, \ldots, b_m + \varepsilon c_m) = g_j(b) + \sum_{i=1}^{m} \frac{\partial g_j}{\partial y_i}(b) c_i \varepsilon.$$

Comparison of the coefficients in ε gives that $g_j(b_1, \ldots, b_n) = 0$ for each j, i.e. b is a K-point of Y (what we already knew), and that

$$\sum_{i=1}^{m} \frac{\partial g_j}{\partial y_i}(b) c_i = 0, \quad 1 \le j \le s.$$

This is of course equivalent to $c \cdot \nabla g_j(b) = 0$, i.e. c is a tangent vector of Y at b and we may say $c \in T_b Y$, the tangent space of Y at b.

Up to now, we have reformulated the property of f_ϕ to map K-points to K-points and added the potential of considering tangent vectors in terms of a commutative diagram. We can now add the final requirement to ϕ, making it the analogue of a local diffeomorphism: we want its "differential" $T_a X \to T_{f_\phi(a)} Y = T_b Y$ to be bijective. Surprisingly, this condition is very easy to add in our commutative diagram formalism: we require additionally the existence and uniqueness of the diagonal arrow, preserving commutativity:

$$\begin{tikzcd}
S = K[X] \arrow[r] & K \\
R = K[Y] \arrow[u, "\phi"] \arrow[r] \arrow[ur] & K[\varepsilon]/(\varepsilon^2) \arrow[u]
\end{tikzcd}$$

By the same argument as above, we can easily convince ourselves that this diagonal map writes $K[X] \to K[\varepsilon]/(\varepsilon^2) : x_i \mapsto a_i + \varepsilon d_i$ for $i = 1, \ldots, n$ and some $d := (d_1, \ldots, d_n)$ which corresponds to a tangent vector of X. The commutativity of the upper-right triangle just means that this vector is in the tangent space $T_a X$. Finally, consider the commutativity of the lower triangle. On the one hand, we can map by the horizontal homomorphism $y_j \mapsto b_j + \varepsilon c_j$, $1 \le j \le m$ as we already saw. On the other hand, going the other path, we have again by Taylor's expansion for $j = 1, \ldots, m$:

$$y_j \mapsto \phi_j(x_1, \ldots, x_n) \mapsto \phi_j(a_1 + \varepsilon d_1, \ldots, a_n + \varepsilon d_n) = \phi_j(a) + \sum_{i=1}^{n} \frac{\partial \phi_j}{\partial x_i}(a) d_i \varepsilon.$$

Since the lower-left triangle commutes, we have by comparison of the coefficient of ε that

$$c_j = \sum_{i=1}^{n} \frac{\partial \phi_j}{\partial x_i}(a) d_i, \quad 1 \le j \le m.$$

Putting these m equations together, we define the Jacobian matrix

$$J_\phi(a) := \left(\frac{\partial \phi_j}{\partial x_i}(a)\right)_{\substack{1\le i\le n\\ 1\le j\le m}}.$$

Then, the equation above is, of course, equivalent to $J_\phi(a)d = c$.

Hence, the existence of the diagonal arrow makes sure that for any tangent vector at $b \in Y$, we have at least one tangent vector at $a \in X$ mapping to it, in other words it ensures the surjectivity of $J_\phi(a)$. Analogously, the uniqueness of the diagonal map translates into injectivity of the differential. Equipped with this good understanding of what it means to define the algebraic analogue of a local diffeomorphism, we can step forward to its rigorous definition.

3.2 Étale Ring Maps

We will present only those results about étale ring maps that are important for the construction of the Henselization. For other statements and some omitted proofs we refer to standard literature such as [Mil80, Gro67, Ray70] and of course [Sta20, Section 00U0].

Definition. Given an R-algebra S with the homomorphism $\phi : R \to S$, we call S *formally étale* if the following condition is satisfied:
Suppose that T is some R-algebra, $\mathfrak{n} \subseteq T$ some ideal with $\mathfrak{n}^2 = 0$ and the following diagram of R-algebra maps commutes:

$$\begin{tikzcd} S \arrow[r, "\bar{u}"] & T/\mathfrak{n} \\ R \arrow[u, "\phi"] \arrow[r] & T \arrow[u, "\pi"'] \end{tikzcd}$$

Then there is a unique R-algebra morphism $u : S \to T$, which lifts $\bar{u}$, i.e. the following diagram also commutes:

$$\begin{tikzcd} S \arrow[r, "\bar{u}"] \arrow[dr, dashed, "u"] & T/\mathfrak{n} \\ R \arrow[u, "\phi"] \arrow[r] & T \arrow[u, "\pi"'] \end{tikzcd}$$

This property is known under the name *infinitesimal lifting*. As we saw above, it reflects the definition of a local diffeomorphism inside of algebraic geometry. When dealing with a formally étale S, we will often refer to the map $\phi : R \to S$ as formally étale rather than to the R-algebra itself.

To go from *formally* étale to étale ring maps, we need to recall the notion of finitely presented algebras. It is evident that an R-algebra S is always of the form $S \cong R[x_i : i \in \mathcal{I}]/\mathfrak{a}$ for some index set $\mathcal{I}$ and an ideal $\mathfrak{a} \subseteq R[x_i : i \in \mathcal{I}]$. In practice we are often interested in a finite number of generators and a finitely generated ideal, hence we define:

Definition. Let R be a ring. We say an R-algebra S is *finitely presented* if it is of the form $S \cong R[x_1, \dots, x_n]/(f_1, \dots, f_m)$ for some $f_i \in R[x_1, \dots, x_n]$, $i = 1, \dots, m$.

Naturally, we have immediately the following fact about transitivity: If S if finitely presented over R and T is finitely presented over S, then T is finitely presented over R. Note that a localization of R at one element, say $a \in R$, is finitely presented, since $R_a \cong R[t]/(at - 1)$. Therefore a localization at finitely many elements is still finitely presented, but this does not have to be true for any multiplicative system.

Definition. Let S be an R-algebra. S is called *étale* if it is formally étale and finitely presented.

The following lemma is a direct consequence of our definitions and observations.

Lemma 3.1. *Let S be an R-algebra and S' an S-algebra. Assume that $R \to S$ and $S \to S'$ are (formally) étale, then the induced map $R \to S'$ is also (formally) étale.*

Another important fact which again follows easily from chasing the correct diagram states that the property of being étale is stable under base change. Before proving this statement, we want to recall the definition and add a simple remark: Let S be an R-algebra with $\phi : R \to S$ the corresponding map and let $R \to R'$ be any ring homomorphism. Then the *base change of ϕ by $R \to R'$* is the ring map $R' \to R' \otimes_R S =: S'$.

$$\begin{tikzcd} S \arrow[r] & S' = R' \otimes_R S \\ R \arrow[u, "\phi"] \arrow[r] & R' \arrow[u, "\text{base change of } \phi"'] \end{tikzcd}$$

Note that the explicit description of a base change is very natural when a presentation is given: We already saw that S, being an R-algebra, is of the form

$$S \cong R[x_i : i \in \mathcal{I}]/(f_j : j \in \mathcal{J}),$$

for some index sets $\mathcal{I}, \mathcal{J}$ and polynomials $f_j \in R[x_i : i \in \mathcal{I}]$. Then, for the base change one has

$$R' \otimes_R S = R'[x_i : i \in \mathcal{I}]/(f'_j : j \in \mathcal{J}),$$

where each f'_j is the image of f_j under the map $R[x_i : i \in \mathcal{I}] \to R'[x_i : i \in \mathcal{I}]$ induced by the map $R \to R'$. In [Sta20, Tag 05G3] this fact is described as "the key to understanding base change".

Lemma 3.2. *Let $R \to S$ be étale and $R \to R'$ be arbitrary. Then $R' \to R' \otimes_R S$ is étale.*

Corollary 3.3. *Let $R \to S$ and $R \to S'$ be étale. Then $R \to S \otimes_R S'$ is étale.*

The following proposition has a more involved proof.

Proposition 3.4. *Let R be a ring, $S = R[x_1, \dots, x_n]_g/(f_1, \dots, f_n)$ for $g \in R[x_1, \dots, x_n]$ and $f_1, \dots, f_n \in R[x_1, \dots, x_n]_g$. If the image of the Jacobian determinant $\det(\frac{\partial f_j}{\partial x_i})_{1 \le i,j \le n}$ is invertible in S, then S is étale over R.*
Conversely, if $R \to S$ is étale, then there exists a presentation $S = R[x_1, \dots, x_n]/(f_1, \dots, f_n)$ such that the image of $\det(\frac{\partial f_j}{\partial x_i})_{1 \le i,j \le n}$ is invertible in S.

For the proof we refer to standard literature [Ray70], [Mil80, Corollary 3.16], to well-written lecture notes [Mil13], [Hoc17] and to the Stacks Project [Sta20, Section 00U0].

Definition. A finitely presented R-algebra S is called *standard étale* if it is of the form $S = R[t]_g/(f)$ for some polynomials $f, g \in R[t]$, such that f is monic and its derivative f' is invertible in S.

Note that by Proposition 3.4, it follows that a standard étale algebra is indeed étale.

There exists a structure theorem of étale algebras, making sure that any étale algebra is *locally* standard étale. In [Gro67, p. 120] Grothendieck attributes this fact to Chevalley and so shall we.

Theorem 3.5 (Chevalley)**.** *Let S be a finitely presented R-algebra. Then S is étale over R if and only if for every prime ideal $\mathfrak{q}$ of S with contraction $\mathfrak{p}$ to R there exist $b \in S \setminus \mathfrak{q}$ and $a \in R \setminus \mathfrak{p}$ such that S_b is isomorphic to a standard étale algebra over R_a.*

The proof is an application of Zariski's main theorem, a form of which we already mentioned in Lemma 2.5. Also Nakayama's lemma and the primitive element theorem for separable field extensions play a role in the proof. In his lecture notes [Hoc17] Hochster points out that "additional trickery" is required as well. Therefore the proof is lengthy and technical and shall not be provided here. We refer to [Ray70, pp. 51], [Ive73, pp. 63] [Mil80, Theorem 3.14] as well as [Sta20, Tag 00UE], [Gro67, pp. 120] and [Hoc17, pp. 27].

3.3 Construction of the Henselization

We want to construct the Henselization of a local ring $(R, \mathfrak{m}, K)$ and consequently prove its existence and some desirable properties. First, we define the notion of étale neighborhoods like Milne in [Mil80]:

Definition. Let $(R, \mathfrak{m}, K)$ be local. A pair $(S, \mathfrak{q})$ is called an *étale neighborhood* of R if S is an étale R-algebra and $\mathfrak{q}$ is a prime of S lying over $\mathfrak{m}$, such that the induced map between the residue fields $K = R/\mathfrak{m} \to S_\mathfrak{q}/\mathfrak{q}S_\mathfrak{q}$ is an isomorphism.

In order to save notation in our setting, it is more useful to work *locally* and to use the notion of pointed étale extensions, as does Hochster in his lecture notes [Hoc17]:

Definition. A local ring T is called *pointed étale extension* of $(R, \mathfrak{m}, K)$ if $T = S_\mathfrak{q}$ for some étale neighborhood $(S, \mathfrak{q})$.

Before stating and proving a theorem which connects étale ring maps and Henselian rings, we need to state the following lemma.

Lemma 3.6. *Assume T and T' are pointed étale extensions of R. Then there is at most one local R-algebra homomorphism from T to T'.*

The proof of this lemma requires the study the multiplication map, given by the linear extension of $\mu : S \otimes_R S \twoheadrightarrow S$ sending $s \otimes s' \mapsto ss'$, and its kernel $\mathfrak{a} := \ker(\mu)$. We omit the details and refer to [Hoc17, pp. 45], [Ive73, p. 71], [Mil80, p. 36] and [Mil13, Section 4]. Now we are ready for the central theorem of this section. Its statement and proof can be found in the references just mentioned, however we shall reprove it again following the notes of Hochster.

Theorem 3.7. *Let $(R, \mathfrak{m}, K)$ a be local ring. The following conditions are equivalent:*

(1) R is Henselian.

(2) If $f \in R[t]$ is a monic polynomial whose reduction mod $\mathfrak{m}$, *$\bar{f} \in K[t]$, has a simple root $\lambda \in K$, then there exists an element $r \in R$ such that $r \equiv \lambda \mod \mathfrak{m}$ and $f(r) = 0$.*

(3) If $R \to T$ is a pointed étale extension, then $R \cong T$.

(4) If $f_1, \ldots, f_n \in R[x_1, \ldots, x_n]$ are n polynomials in n variables whose images $\overline{f_j}$ mod $\mathfrak{m}$ *vanish simultaneously at $(\lambda_1, \ldots, \lambda_n) \in K^n$ and the Jacobian determinant* $\det(\frac{\partial f_j}{\partial x_i})$ *does not vanish* mod $\mathfrak{m}$ *at $x_1 = \lambda_1, \ldots, x_n = \lambda_n$, then there are unique elements $r_1, \ldots, r_n \in R$ such that for all i, we have $r_i \equiv \lambda_i \mod \mathfrak{m}$ and $f_j(r_1, \ldots, r_n) = 0, 1 \leq j \leq n$.*

This theorem gives a deep insight into Henselian rings. In particular, the equivalence of conditions (1) and (2) implies that it suffices to lift only simple roots in order to be able to lift coprime factorizations. Applying this for the ring of algebraic power series and Theorem 1.7 we obtain a proof for Theorem 1.8. We see that Henselian rings are connected to the theory of étale ring maps via condition (3). Moreover, (4) is a multidimensional version of Hensel's lemma for n polynomials and n variables; if the f_i's were also allowed to be power series, one would recognize the implicit function theorem. The equivalence (1) $\Leftrightarrow$ (4) states that a ring is Henselian if and only if the algebraic version of this analytic theorem holds in this ring.

Proof. We will show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2): Suppose R is Henselian and we have a monic $f \in R[t]$ such that $\bar{f}$ has a simple root $\lambda \in K$. We may factor $\bar{f}(t) = (t - \lambda)\bar{g}(t)$ for some $\bar{g} \in K[t]$ with $\bar{g}(\lambda) \neq 0$. The polynomials $t - \lambda$ and $\bar{g}(t)$ are relatively prime. Using the assumption we find a lifting of the factorization to $f(t) = (t - r)g(t)$ for some $r \equiv \lambda \mod \mathfrak{m}$ and $g \in R[t]$. Clearly $f(r) = 0$.

(2) $\Rightarrow$ (3): Let $\phi : R \to T$ be a pointed étale extension, so a localization of an étale neighborhood. By Theorem 3.5 it follows that the étale neighborhood is locally standard étale, hence we may write $T \cong (R[t]_g/(f))_{\mathfrak{q}}$ for a prime ideal $\mathfrak{q} \subseteq R[t]_g/(f)$ lying over $\mathfrak{m}$ and $g, f \in R[t]$ such that f is monic and f' is invertible in T. Denoting by λ the image of $t \in T$ in K, it follows that $\bar{f}(\lambda) = 0$. Moreover, because f' is invertible in T, we must have that $\bar{f}'(\lambda) \neq 0$, hence λ is a simple root of $\bar{f}$. Using (2), we can find an $r \in R$ for

which $f(r) = 0$. Therefore there exists an $h \in R[t]$ such that $f(t) = (t-r)h(t)$ and h is invertible in T, because λ is a simple root of $\bar{f}$. It follows that

$$T \cong (R[t]_g/(f))_{\mathfrak{q}} \cong \big(R[t]_g/((t-r)h(t))\big)_{\mathfrak{q}} \cong (R[t]_g/(t-r))_{\mathfrak{q}} \cong R_{\phi^{-1}(\mathfrak{q})}.$$

However, since ϕ and R are local, we have that $T \cong R_{\phi^{-1}(\mathfrak{q})} \cong R$, what was to be shown.

(3) $\Rightarrow$ (4): Assume we have a system of equations $f_1, \ldots, f_n \in R[x_1, \ldots, x_n]$ like in (4) with $(\lambda_1, \ldots, \lambda_n) \in K^n$ solution of $(\bar{f}_1, \ldots, \bar{f}_n) = 0$ and suppose that (3) holds. Let Q be the kernel of $\pi' : R[x_1, \ldots, x_n] \to K$, where we choose π' such that $\pi'(x_i) = \lambda_i$. By Proposition 3.4 and the assumption on the Jacobian of the $f_1, \ldots, f_n$ in (4), we have that $T \coloneqq R[x_1, \ldots, x_n]_Q/(f_1, \ldots, f_n) \cong (R[x_1, \ldots, x_n]/(f_1, \ldots, f_n))_{\bar{Q}}$ is a pointed étale extension of R. Because of (3) we must have that $R \cong T$. However, solving the equations $f_1, \ldots, f_n$ and lifting the λ_i's is equivalent to giving an R-algebra map $R[x_1, \ldots, x_n]/(f_1, \ldots, f_n) \to R$ such that under the composite $R[x_1, \ldots, x_n]/(f_1, \ldots, f_n) \to R \twoheadrightarrow K$ the elements x_i map to λ_i. This is in turn equivalent to giving a map that sends Q to $\mathfrak{m}$, hence giving a local R-algebra map $T \to R$. But we have that $R \cong T$, hence the local map exists and is unique by Lemma 3.6. It provides us with a unique solution to the equations.

(4) $\Rightarrow$ (1): Let $f = t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0 \in R[t]$ be a monic polynomial of degree n and suppose that we have a factorization $\bar{f} = \bar{g}\bar{h}$ for some monic coprime polynomials $\bar{g}, \bar{h} \in K[t]$ of degrees d and e respectively. Let $\bar{g} = \sum_{i=0}^{d} \alpha_i t^i$ and $\bar{h} = \sum_{i=0}^{e} \beta_i t^i$ for some $\alpha_i, \beta_i \in K$ and $\alpha_d = \beta_e = 1$. We seek a lifting of the factorization to $f = gh$ for monic polynomials $g, h \in R[t]$. Let the coefficients of g and h be unknowns $y_0, \ldots, y_{d-1}$ and $z_0, \ldots, z_{e-1}$, henceforth we want to solve the equation

$$t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0 = (t^d + y_{d-1}t^{d-1} + \cdots + y_1 t + y_0)(t^e + z_{e-1}t^{e-1} + \cdots + z_1 t + z_0),$$

for the unknowns over R such that the residue classes of the polynomials g and h agree with $\bar{g}$ and $\bar{h}$. Comparing coefficients leads to a system of $n = d + e$ polynomial equations in as many variables:

$$\begin{cases} y_0 z_0 & = c_0, \\ y_0 z_1 + y_1 z_0 & = c_1, \\ \vdots & \\ y_{d-1} z_e + y_d z_{e-1} & = c_{n-1}. \end{cases}$$

This system has a solution mod $\mathfrak{m}$ coming from the factorization $\bar{f} = \bar{g}\bar{h}$ given by $\alpha_0, \ldots, \alpha_{d-1}, \beta_0, \ldots, \beta_{e-1} =: (\alpha, \beta)$. In order to use (4) and to lift this solution to R we have to verify that the Jacobian determinant of this system of equations does not vanish,

i.e. that the matrix

$$J(y,z) := \begin{pmatrix} z_0 & z_1 & z_2 & \cdots & z_{e-1} & 1 & 0 & \cdots & 0 \\ 0 & z_0 & z_1 & \cdots & z_{e-2} & z_{e-1} & 1 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & & \vdots \\ 0 & \cdots & 0 & z_0 & z_1 & \cdots & z_{e-2} & z_{e-1} & 1 \\ y_0 & y_1 & y_2 & \cdots & y_{d-1} & 1 & 0 & \cdots & 0 \\ 0 & y_0 & y_1 & \cdots & y_{d-2} & y_{d-1} & 1 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & & \vdots \\ 0 & \cdots & 0 & y_0 & y_1 & \cdots & y_{d-2} & y_{d-1} & 1 \end{pmatrix}$$

is invertible at $(y,z) = (\alpha,\beta)$. However, $J(\alpha,\beta)$ is the (transpose of the) Sylvester matrix of the polynomials $\bar{g}$ and $\bar{h}$. Since the polynomials are relatively prime by assumption, we obtain that $J(\alpha,\beta)$ is invertible. This shows that the assumptions of (4) are satisfied and hence we find a unique solution for the unknowns $y_0,\ldots,y_{d-1},z_0,\ldots,z_{e-1}$. This gives the unique factorization $f = gh$ we were looking for. □

Having in mind that (1) ⇔ (3) in this theorem, we come back to our goal of constructing the Henselization. We see that it may be a good idea to combine all possible pointed étale extensions of R into one large ring. If we can do this rigorously, then we might argue that this ring does not have any proper pointed étale extensions anymore, which will mean that it will be Henselian. Finally, we might be able to verify the universal property of the Henselization and conclude that we indeed found the correct object. Let us start executing this plan.

Given a local ring R, we wish to define a *set* of pointed étale algebras of R, say $\mathcal{R}$, that contains exactly one representative from each isomorphism class of pointed étale extensions. It is not trivial that $\mathcal{R}$ is a set, since it might turn out "too large". However, the following result bounds the cardinality of a pointed étale extension from above and allows us to define $\mathcal{R}$ properly.

Lemma 3.8. *Let R be a local ring and T a pointed étale extension. Then T is finite if R is finite. In the other case, the cardinalities of R and T agree.*

Proof. By definition, $T = S_{\mathfrak{q}}$ for some prime $\mathfrak{q} \subseteq S$ and an étale R-algebra S. Since S is finitely presented over R, we have $|S| \leq |R|^n$ for some $n \in \mathbb{N}$, where $|\cdot|$ denotes cardinality. The localization is parametrized by pairs in $(S \setminus \mathfrak{q}) \times S$ and therefore $|S_{\mathfrak{q}}| \leq |S|^2$. We have

$$|R| \leq |T| = |S_{\mathfrak{q}}| \leq |R|^{2n},$$

proving the assertion. □

Now, from the axiom of choice, it follows that the *set* $\mathcal{R}$ exists, since it is a subset of the *set* of all ring structures on a set with similar cardinality as R. Let $\mathcal{A}$ be an index set of $\mathcal{R}$, whereby *index set* means that each $i \in \mathcal{A}$ corresponds bijectively to a $T_i \in \mathcal{R}$ and we can write therefore $\mathcal{R} = (T_i)_{i\in\mathcal{A}}$.

Proposition 3.9. *For $i, j \in \mathcal{A}$ define $i \leq j$ if and only if there exists a local R-algebra map $\phi_{i,j} : T_i \to T_j$. Then $(\mathcal{A}, \leq)$ is a directed set.*

Proof. Obviously, $\mathcal{A}$ is not empty since $\mathcal{R}$ contains R. Clearly, $\leq$ is reflexive, as one always has the identity map $\mathrm{id} : T_i \to T_i$ for all i. Moreover, if we have $\phi : T_i \to T_j$ and $\psi : T_j \to T_k$ both local R-algebra maps then $\psi \circ \phi : T_i \to T_k$ is a local R-algebra map. This implies that $\leq$ is transitive. Finally, we have to prove that for any two $T_i, T_j \in \mathcal{R}$, there exist $T_k \in \mathcal{R}$ and two local R-algebra maps $T_i \to T_k$ and $T_j \to T_k$. As T_i, T_j are pointed étale, they are localizations of some étale R-algebras S_i, S_j. By Corollary 3.3 we immediately have that $R \to S_i \otimes_R S_j$ is étale. Consider the composite map

$$R \to S_i \otimes_R S_j \twoheadrightarrow K \otimes_K K \xrightarrow{\cong} K,$$

which sends $r \mapsto r \cdot (1_{S_i} \otimes 1_{S_j}) \mapsto \bar{r} \cdot (1_K \otimes 1_K) \mapsto \bar{r}$ and is thus precisely the quotient map $R \twoheadrightarrow R/\mathfrak{m} \cong K$. It follows that by letting Q be the kernel of the map $S_i \otimes_R S_j \twoheadrightarrow K \otimes_K K$, we must have that $R \to (S_i \otimes_R S_j)_Q$ is local. The residue class field of $(S_i \otimes_R S_j)_Q$ is K. Set $T_k = (S_i \otimes_R S_j)_Q$ which is now by definition a pointed étale extension of R and we have maps $T_i \to T_k$ and $T_j \to T_k$. This shows the existence of a $k \in \mathcal{A}$ for given $i, j \in \mathcal{A}$ such that $i, j \leq k$ and finishes the proof. □

This proposition shows that $(\mathcal{R}, \{\phi_{i,j} : T_i \to T_j\}_{i,j \in \mathcal{A}, i \leq j})$ forms a direct system of rings. Note that because of Lemma 3.6, we know that the $\phi_{i,j}$'s are actually unique, justifying that the construction is canonical. The fact that $\mathcal{R}$ together with these maps forms a direct system of rings allows us to define the direct limit:

Definition. For a local ring $(R, \mathfrak{m}, K)$ we denote $R^{\mathrm{e}} := \varinjlim_{T \in \mathcal{R}} T$.

Given a local ring R, we combine all pointed étale extensions of it to the ring R^{e} in a rigorous way using the direct limit in the definition above. Therefore, it is natural to expect that R^{e} does not have any proper pointed étale extensions anymore, which means that R^{e} is Henselian by Theorem 3.7. It is also intuitively clear that R^{e} the "smallest" extension of R that admits this property. We prove both statements below using ideas from [Ive73] and [Hoc17].

Lemma 3.10. *Let $(R, \mathfrak{m}, K)$ be a local ring. Then R^{e} is local with maximal ideal $\mathfrak{m}R$ and residue field K. Moreover, R^{e} is Henselian.*

Proof. Locality, the statement about the maximal ideal and the condition on the residue field follow by construction, since every pointed étale R-algebra T is local with maximal ideal $\mathfrak{m}T$ and residue field K.

By Theorem 3.7 we only have to check the lifting of simple roots in order to verify the Henselian property. Let $f \in R^{\mathrm{e}}[t]$ be monic and $\lambda \in K$ a simple root of $\bar{f} \in K[t]$. Since $R^{\mathrm{e}} = \varinjlim_{T \in \mathcal{R}} T$, there exists some pointed étale R-algebra T such that all coefficients of f lie in T. We define $T' := (T[t]/(f))_{\mathfrak{q}}$, where $\mathfrak{q} := (\bar{t} - \lambda)$. The residue field of T' is K and because λ is a simple root, it follows that f' is invertible in T' and therefore T' is a pointed étale extension of R by Lemma 3.1 and Proposition 3.4. However, f has a root in T' and it lifts λ. This gives rise to an element $r \in R^{\mathrm{e}}$ such that $f(r) = 0$ and $\bar{r} = \lambda$. □

Theorem 3.11. *Let $(R, \mathfrak{m}, K)$ be a local ring. The Henselization of R is given by the direct limit as in Definition 3.3: $R^{\mathrm{h}} = R^{\mathrm{e}}$.*

Proof. We will verify the universal property. From the lemma above we already have that R^{e} is local and Henselian. Let $\psi : R \to H$ be a local map from R to a Henselian ring $(H, \mathfrak{m}_H, L)$. To show that this map factors uniquely through R^{e}, it suffices to show that it factors uniquely through every $(T, \mathfrak{q}T, K)$, where $T = S_{\mathfrak{q}}$ is a pointed étale extension of R. Consider the commutative diagram of the base change:

$$\begin{tikzcd} R \arrow[r, "\text{étale}"] \arrow[d, "\psi"] & S \arrow[d] \\ H \arrow[r] & S \otimes_R H \end{tikzcd}$$

Since $R \to S$ is étale, we obtain by Lemma 3.2 that $H \to S \otimes_R H$ is also étale. Moreover, there exists a canonical map $S \otimes_R H \to K \otimes_K L \cong L$. Denote its kernel by Q. It follows that $H \to (S \otimes_R H)_Q$ is a localization of an étale extension. Since $L \cong K \otimes_K L$, we obtain that the residue fields agree and hence this extension is pointed étale. But H is Henselian, hence $H \cong (S \otimes_R H)_Q$ by (1) $\Rightarrow$ (3) of Theorem 3.7 and therefore we found a local map $\phi : S \to (S \otimes_R H)_Q \cong H$, the map we were looking for:

$$\begin{tikzcd} R \arrow[r, "\text{étale}"] \arrow[d, "\psi"] & S \arrow[d] \\ H \arrow[r, "\text{étale}"] & S \otimes_R H \arrow[d] \\ & (S \otimes_R H)_Q \arrow[ul, "\cong"] \end{tikzcd}$$

Finally, because H is pointed étale over itself as well as over $(S \otimes_R H)_Q$, we obtain that this map is unique by Lemma 3.6. $\square$

The characterization of the Henselization as a direct limit of pointed étale extensions not only proves its existence, but also led to remarkable mathematical discoveries in this area in the second half of the last century. The theory of approximation rings and consequently the algebraic version of Artin's Approximation [Art69] use exactly this fact (amongst other). This and other related results are contained in the recent survey [Hau17] by Hauser. The Henselization of non-local rings with respect to ideals is investigated in [Gre69]. An exposition of various versions of the Henselian property can be found in [Rib85]. The connection of Henselian rings to rings satisfying Weierstrass preparation theorem was first established by Lafon in 1967 [Laf67]. Probably the most explicit application of the Theorems 3.5 and 3.11 was found by Denef and Lipshitz in 1985 and we shall explain their ideas in the next section.

4 Explicit Implications

4.1 Proof of Theorem 1.1

Theorem 4.1 (Denef & Lipshitz). *Let $f \in K\langle x\rangle$ be an algebraic power series. Then there exist an étale-algebraic power series h and polynomials $a_i, b_j \in K[x]$ for $0 \le i \le r$, $0 \le j \le s$, $r, s \in \mathbb{N}$, where $b_0(0) \neq 0$, such that*

$$f = \frac{a_0 + a_1 h + \cdots + a_r h^r}{b_0 + b_1 h + \cdots + b_s h^s}. \tag{5}$$

Proof. Set $R := K[x]_{(x)}$. We have seen that $K\langle x\rangle = R^{\mathrm{h}} = \varinjlim_{T \in \mathcal{R}} T$, where the limit is taken over all pointed étale extensions up to isomorphism. It follows that there exists a ring $T \subseteq K\langle x\rangle$ which is a pointed étale extension of R and which contains f. Hence, $T = S_{\mathfrak{q}}$ for an étale R-algebra S and a prime ideal $\mathfrak{q} \subseteq S$ lying over $\mathfrak{m} \subseteq R$. We know furthermore by Theorem 3.5 that S is locally standard étale over R; since R is local, this means that we have an isomorphism

$$\alpha : S_b \xrightarrow{\cong} R[t]_g/(p)$$

for some $b \in S \setminus \mathfrak{q}$, $g \in R[t]$ and $p \in R[t]$ monic such that its derivative p' is invertible in S_b. Localizing in $\mathfrak{q}$ and $\alpha(\mathfrak{q})$, respectively, yields $T \cong \Big(R[t]/(\tilde{P})\Big)_{\alpha(\mathfrak{q})}$ for some $\tilde{P} \in R[t]$ such that $\tilde{P}' \notin \alpha(\mathfrak{q})$. We can rephrase the isomorphism above as $T \cong (R[\tilde{h}])_{\alpha(\mathfrak{q})}$, where $\tilde{h} \in \widehat{R} = K[\![x]\!]$ is an algebraic element over R whose minimal polynomial is exactly $\tilde{P}$. Because $\tilde{P}' \notin \tilde{\alpha}(\mathfrak{q})$, we have $\partial_t \tilde{P}(0, \tilde{h}(0)) \neq 0$. Now, any element $f \in (R[\tilde{h}])_{\alpha(\mathfrak{q})} \cong T$ is of the form a/b, for $a, b \in R[\tilde{h}]$ and $b \notin \tilde{\alpha}(\mathfrak{q})$, hence we have

$$f(x) = \frac{\tilde{a}(x, \tilde{h}(x))}{\tilde{b}(x, \tilde{h}(x))},$$

for $\tilde{a}, \tilde{b} \in K[x]_{(x)}[t]$ such that $\tilde{b}(0, \tilde{h}(0)) \neq 0$. Finally, to achieve the condition $h(0) = 0$ as in the definition of étale-algebraic, we define $h(x) = \tilde{h}(x) - \tilde{h}(0)$. It is easy to verify that the derivative of the minimal polynomial $P(x, t)$ of h does not vanish at the origin, $\partial_t P(0, 0) = \partial_t \tilde{P}(0, \tilde{h}(0)) \neq 0$, and that we have again

$$f = \frac{a_0 + a_1 h + \cdots + a_r h^r}{b_0 + b_1 h + \cdots + b_s h^s},$$

for polynomials $a_i, b_j \in K[x]$ such that $b_0(0) = \tilde{b}(0, \tilde{h}(0)) \neq 0$. □

Now we can finally prove Theorem 1.1.

Proof of Theorem 1.1. Using the theorem above it follows that there exist $r, s \in \mathbb{N}$ and $a_i(x), b_j(x) \in K[x]$ for $0 \le i \le r$, $0 \le j \le s$ with $b_0(0) \neq 0$ such that

$$f(x) = \frac{a_0(x) + a_1(x)h(x) + \cdots + a_r(x)h(x)^r}{b_0(x) + b_1(x)h(x) + \cdots + b_s(x)h(x)^s}, \tag{6}$$

where $h(x) \in K\langle x\rangle$ is étale-algebraic. Define

$$W(x,t) := \frac{a_0(x) + a_1(x)t + \cdots + a_r(x)t^r}{b_0(x) + b_1(x)t + \cdots + b_s(x)t^s} \in K[x,t]_{(x,t)},$$

and let

$$R(x,t) := W(xt,t)t\frac{\partial_t P(xt,t)}{P(xt,t)}.$$

Using Lemma 1.2 and the same computation as in equation (3) we verify that we found the correct rational function:

$$\mathcal{D}(R(x,t)) = W(x,h(x)) = h(x). \qquad \square$$

4.2 Codes of Algebraic Power Series

Finally, we introduce a new result which can be seen as a corollary of Theorem 4.1. First, we remark that the following fact was explained in [AM65, pp. 88] and became later known under the name Artin-Mazur lemma, see [BCR98, AMR92]. In [Ron18, Proposition 9.3] a more general version of the statement, allowing for K to be any complete normal local domain (with appropriate changes to the assumptions), is presented.

Theorem 4.2 (Artin & Mazur)**.** *Let $f \in K\langle x_1,\dots,x_n\rangle = K\langle x\rangle$ be an algebraic power series with $f(0) = 0$. Then there exist $k \in \mathbb{N}$ and a vector of k polynomials $P(x,y_1,\dots,y_k) \in K[x][y_1,\dots,y_k]^k$ with the following properties:*

(1) $P(x,f,h_2,\dots,h_k) = 0$ for algebraic power series $h_2,\dots,h_k \in K\langle x\rangle$ with $h_i(0) = 0$ for $i = 2,\dots,k$.

(2) The Jacobian matrix $J_P(x,y_1,\dots,y_k)$ of $P(x,y_1,\dots,y_n)$ with respect to the variables $y_1,\dots,y_k$ at $x = y = 0$ is invertible: $J_P(0,0) \in \mathrm{GL}_k(K)$.

In other words, given $f \in K\langle x\rangle$, one can find $k-1$ algebraic power series $h_2,\dots,h_k \in K\langle x\rangle$ and a k-dimensional vector of polynomials $P(x,y_1,\dots,y_k) \in K[x,y]^k$, such that $P(x,f(x),h_2(x),\dots,h_k(x)) = 0$ and the Jacobian of $P(x,y)$ with respect to y at $x = y = 0$ is invertible. Similarly to Theorem 4.1, this implies that one can repair the problem of an algebraic power series of not being étale-algebraic, now by appending $k-1$ new power series and considering the k-dimensional analogue of the definition of étale-algebraicity. This polynomial vector $P(x,y) \in K[x,y]^k$ is referred to as *a (mother) code of the algebraic series f* in [ACJH18, Hau17, AMR92]. The authors Alonso, Castro-Jimenez and Hauser of the first reference point out that "The advantage of this code in comparison with taking the minimal polynomial lies in the fact that the latter determines the algebraic series only up to conjugation, so that extra information is necessary to specify the series, typically a sufficiently high truncation of the Taylor expansion. In contrast, the polynomial code determines the series completely and is easy to handle algebraically".

With the help of the theorem of Denef and Lipshitz we can improve on the Artin-Mazur lemma, proving that it is always possible to choose $k = 2$. Note that since

Theorem 1.1 is known to hold in more generality, it is also natural that also the general version by Rond can be covered and improved by our approach.

Theorem 4.3. *Let $f \in K\langle x_1, \dots, x_n\rangle = K\langle x\rangle$ be an algebraic power series with $f(0) = 0$. Then there exists a vector of two polynomials $P(x, y_1, y_2) \in K[x][y_1, y_2]^2$ with the following properties:*

(1) $P(x, f, h) = 0$ for some étale-algebraic power series $h \in K\langle x\rangle$.

(2) The Jacobian matrix $J_P(x, y_1, y_2)$ of $P(x, y_1, y_2)$ with respect to y_1 and y_2 at 0 is invertible: $J_P(0, 0, 0) \in \mathrm{GL}_2(K)$.

Note that in the two-dimensional square matrix $J_P(0, 0, 0)$, the first 0 means setting the variables $x_1, \dots, x_n$ all to 0 in $J_P(x, y_1, y_2)$, whereas the other two zeros are both one-dimensional and advert to y_1 and y_2.

Proof. Let $Q(x, y_1)$ be the minimal polynomial of f. If $\partial_{y_1} Q(0, 0) \neq 0$ then we can simply choose $P(x, y_1, y_2) = (Q(x, y_1), y_2)$ and the assertion follows in this case.

We are left with the more challenging case $\partial_{y_1} Q(0, 0) = 0$. By Theorem 4.1, we may write for some étale-algebraic power series $h \in K\langle x\rangle$

$$f = \frac{a_0 + a_1 h + \cdots + a_r h^r}{b_0 + b_1 h + \cdots + b_s h^s}, \tag{7}$$

for $r, s \in \mathbb{N}$ and $a_i(x), b_j(x) \in K[x]$ with $0 \leq i \leq r$, $0 \leq j \leq s$ and $b_0(0) \neq 0$. Define the polynomials

$$\begin{aligned} T_1(x, y_2) &\coloneqq a_0(x) + a_1(x) y_2 + \cdots + a_r(x) y_2^r, \\ T_2(x, y_2) &\coloneqq b_0(x) + b_1(x) y_2 + \cdots + b_s(x) y_2^s, \end{aligned}$$

and get the relationship $T_1(x, h(x)) = f(x) T_2(x, h(x))$ from identity (7). Let $S(x, y_2)$ be the minimal polynomial of the étale-algebraic $h(x)$, so that $\partial_{y_2} S(0, 0) \neq 0$. Now we put

$$P(x, y_1, y_2) \coloneqq \begin{pmatrix} y_1 T_2(x, y_2) - T_1(x, y_2) \\ S(x, y_2) \end{pmatrix}.$$

A simple computation confirms that this choice of P satisfies all required properties:

$$P(x, f(x), h(x)) = 0 \quad \text{and}$$

$$J_P(0, 0, 0) = \begin{pmatrix} T_2(x, y_2) & * \\ 0 & \partial_{y_2} S(x, y_2) \end{pmatrix}\Bigg|_{(0,0,0)} = \begin{pmatrix} T_2(0, 0) & * \\ 0 & \partial_{y_2} S(0, 0) \end{pmatrix}.$$

Clearly, $\det(J_P(0, 0, 0)) = T_2(0, 0) \partial_{y_2} S(0, 0) \neq 0$, because both factors are different from 0. □

Acknowledgments

First of all, the author wants to thank Herwig Hauser for the supervision and correction of the master's thesis version of this work. The author is also grateful to Christoper Chiu and Giancarlo Castellano for patiently explaining to him central concepts related to this work, reading its early versions and suggesting improvements. Moreover, we thank the anonymous referee for helpful comments and finally Alin Bostan and Kilian Raschel for organizing the wonderful conference "Transient Transcendence In Transylvania" in 2019.

References

[AB13] B. Adamczewski and J. P. Bell. Diagonalization and rationalization of algebraic Laurent series. *Annales scientifiques de l'École Normale Supérieure*, Ser. 4, 46(6):963–1004, 2013.

[ABD19] B. Adamczewski, J. P. Bell, and E. Delaygue. Algebraic independence of G-functions and congruences "à la Lucas". *Ann. Sci. Éc. Norm. Supér. (4)*, 52(3):515–559, 2019.

[ACJH18] M. E. Alonso, F. J. Castro-Jiménez, and H. Hauser. Encoding algebraic power series. *Found. Comput. Math.*, 18(3):789–833, 2018.

[AM65] M. Artin and B. Mazur. On periodic points. *Ann. of Math. (2)*, 81:82–99, 1965.

[AMR92] M. E. Alonso, T. Mora, and M. Raimondo. A computational model for algebraic power series. *J. Pure Appl. Algebra*, 77(1):1–38, 1992.

[Art69] M. Artin. Algebraic approximation of structures over complete local rings. *Inst. Hautes Études Sci. Publ. Math.*, (36):23–58, 1969.

[Azu51] G. Azumaya. On maximally central algebras. *Nagoya Math. J.*, 2:119–150, 1951.

[BCR98] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.

[BDS17] A. Bostan, L. Dumont, and B. Salvy. Algebraic diagonals and walks: algorithms, bounds, complexity. *J. Symbolic Comput.*, 83:68–92, 2017.

[BLS17] A. Bostan, P. Lairez, and B. Salvy. Multiple binomial sums. *Journal of Symbolic Computation*, 80(2):351–386, 2017.

[Chr15] G. Christol. Diagonals of rational fractions. *Eur. Math. Soc. Newsl.*, (97):37–43, 2015.

[Del84] P. Deligne. Intégration sur un cycle évanescent. *Invent. Math.*, 76(1):129–143, 1984.

[DL87] J. Denef and L. Lipshitz. Algebraic power series and diagonals. *J. Number Theory*, 26(1):46–67, 1987.

[Dum16] L. Dumont. *Algorithmes rapides pour le calcul symbolique de certaines intégrales de contour à paramètre*. Theses, Université Paris-Saclay, December 2016.

[Eis95] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[Fur67] H. Furstenberg. Algebraic functions over finite fields. *J. Algebra*, 7:271–277, 1967.

[Gre69] S. Greco. Henselization of a ring with respect to an ideal. *Trans. Amer. Math. Soc.*, 144:43–65, 1969.

[Gro67] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[Har88] T. Harase. Algebraic elements in formal power series rings. *Israel J. Math.*, 63(3):281–288, 1988.

[Hau17] H. Hauser. The classical Artin approximation theorems. *Bull. Amer. Math. Soc. (N.S.)*, 54(4):595–633, 2017.

[Hoc17] M. Hochster. Math 615 Lecture Notes, 2017. Available at http://www.math.lsa.umich.edu/~hochster/615W17/615.pdf.

[Ive73] B. Iversen. *Generic local structure of the morphisms in commutative algebra*. Lecture Notes in Mathematics, Vol. 310. Springer-Verlag, Berlin-New York, 1973.

[KPR75] H. Kurke, G. Pfister, and M. Roczen. *Henselsche Ringe und algebraische Geometrie*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1975. Mathematische Monographien, Band II.

[Laf65] J.-P. Lafon. Séries formelles algébriques. *C. R. Acad. Sci. Paris*, 260:3238–3241, 1965.

[Laf67] J.-P. Lafon. Anneaux henséliens et théorème de préparation. *C. R. Acad. Sci. Paris Sér. A-B*, 264:A1161–A1162, 1967.

[Lan84] S. Lang. *Algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, second edition, 1984.

[LT70] F. Lazzeri and A. Tognoli. Alcune proprietà degli spazi algebrici. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (3)*, 24:597–632, 1970.

[Mat80] H. Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[Mil80] J. S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[Mil13] J. S. Milne. Lectures on Etale Cohomology (v2.21), 2013. Available at www.jmilne.org/math/.

[Nag53] M. Nagata. On the theory of Henselian rings. *Nagoya Math. J.*, 5:45–57, 1953.

[Nag54] M. Nagata. On the theory of Henselian rings. II. *Nagoya Math. J.*, 7:1–19, 1954.

[Nag59] M. Nagata. On the theory of Henselian rings. III. *Mem. Coll. Sci. Univ. Kyoto Ser. A. Math.*, 32:93–101, 1959.

[Nag62] M. Nagata. *Local rings*. Interscience Tracts in Pure and Applied Mathematics, No. 13. Interscience Publishers a division of John Wiley & Sons New York-London, 1962.

[Pó22] G. Pólya. Sur les séries entières, dont la somme est une fonction algébrique. *L'Enseign. Math.*, pages 38–47, 1921–1922.

[Ray70] M. Raynaud. *Anneaux locaux henséliens*. Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, Berlin-New York, 1970.

[Rib85] P. Ribenboim. Equivalent forms of Hensel's lemma. *Exposition. Math.*, 3(1):3–24, 1985.

[Ron18] G. Rond. Artin Approximation. *Journal of Singularities*, 17:108–192, 2018. 108 pages.

[Rui93] J. M. Ruiz. *The basic theory of power series*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1993.

[Saf87] K. V. Safonov. On conditions for the sum of a power series to be algebraic and rational. *Mat. Zametki*, 41(3):325–332, 457, 1987.

[Sta20] T. Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2020.

[Str14] A. Straub. Multivariate Apéry numbers and supercongruences of rational functions. *Algebra Number Theory*, 8(8):1985–2007, 2014.

[SW88] H. Sharif and C. F. Woodcock. Algebraic functions over a field of positive characteristic and Hadamard products. *J. London Math. Soc. (2)*, 37(3):395–403, 1988.