MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

"Algebraic Power Series"

verfasst von / submitted by

Sergey Yurkevich, BSc

angestrebter akademischer Grad / in partial fulfillment of the requirements for the degree of

Master of Science (MSc)

Wien, 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 821
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Mathematik
Betreut von / Supervisor:	Univ.-Prof. Mag. Dr. Herwig Hauser

"Unmindful of the proud world's pleasure,
But friendship's claim alone in view,
I wish I could have brought a treasure
Far worthier to pledge to you:
Fit for a soul of beauty tender,
By sacred visitations taught
To blend in rhyme of vivid splendor
Simplicity and lofty thought;
Instead—to your kind hands I render
The motley chapters gathered here,
At times amusing, often doleful,
Blending the rustic and the soulful,
Chance harvest of my pastimes dear,
Of sleepless moods, light inspirations,
Fruit of my green, my withered years,
The mind's dispassionate notations,
The heart's asides, inscribed in tears."

Alexander Pushkin, *Eugene Onegin*, dedication.
Translation by Walter Arndt.

"Nicht, um die Welt zu amüsieren,
Nein, weil mir Freundschaft teuer ward,
Wünscht' ich Dir hier zu präsentieren
Ein Pfand von würdigerer Art,
Der schönen Seele wert vor allem,
Die heilig träumend sich erfreut
An dichterischen Widerhallen
Und hochgesinnter Einfachheit;
Statt dessen muß Dir nun gefallen
Dieser Kapitel Bunterlei,
Die, halb zum Lachen, halb zum Weinen,
Volkston und Ideal vereinen,
Sorglose Frucht von Spielerei,
Schlaflosen Nächten, Inspirierung,
Unreifer, welker Jahre Sinn,
Verstandes kalter Registrierung
Und Herzens schmerzlichem Gewinn."

Alexander Puschkin, *Eugen Onegin*, Widmung.
Übersetung von Rolf-Dietrich Keil.

"Не мысля гордый свет забавить,
Вниманье дружбы возлюбя,
Хотел бы я тебе представить
Залог достойнее тебя,
Достойнее души прекрасной,
Святой исполненной мечты,
Поэзии живой и ясной,
Высоких дум и простоты;
Но так и быть — рукой пристрастной
Прими собранье пестрых глав,
Полусмешных, полупечальных,
Простонародных, идеальных,
Небрежный плод моих забав,
Бессонниц, легких вдохновений,
Незрелых и увядших лет,
Ума холодных наблюдений
И сердца горестных замет."

Александр Сергеевич Пушкин, *Евгений Онегин*, Вступление.

Acknowledgements

First of all, I am indebted to my supervisor Herwig Hauser. Primarily, I want to thank him for his supportive comments, suggestions and corrections regarding the thesis, but also for his understanding and patient manner. He has encouraged me throughout the last two years, offering many opportunities to learn and grow. His remarkable ability to spot or discover someone's interest for a topic and then gently push this person into the correct direction, enabled me not only to find my perfect topic for this master thesis but also finish the work with pleasure. Only due to Herwig's support I was able to visit conferences connected to this thesis, meet new wonderful people and learn from them. Finally, I appreciate his gracious financial support.

I am also grateful to all the teachers and professors I encountered in my academic career so far and from whom I could learn. These are teachers who were coaching me in my school years for the Mathematical Olympiad and thereby awakening in me the love for mathematics, professors and tutors in the University of Vienna and the Economical University of Vienna (WU) who taught me conceptual mathematics and corrected my mistakes, and also professors from distant universities I had the pleasure of listening to during their talks and getting inspired by their research. In this spirit, a big "thank you" to Gerd Baron, Gerhard Kirchner, Clemens Heuberger, Leonhard Summerer, Gerald Teschl, Kurt Hornik, Alin Bostan and Dorin Popescu. Additionally, I want to express my gratitude to Christian Krattenthaler, who, being professor and dean at the University of Vienna, not only taught wonderful lectures but also yearly supported me and many others morally and financially for attending various mathematical competitions.

I want to thank my friends and family for their support and help. Without their assistance and care my studies would be impossible and this work would have never seen the light of day. There are too many to mention by name here – I will just say that I'm very happy to have known each and every one. I also want to thank all my colleges, who over the months and years became friends and who can and should be mentioned by name: Christopher Chiu, Hana Melánová, Jakob Steininger, Levi Haunschmid, Chiara Novarini, Markus Reibnegger, David Stinner and Johannes Droschl. A special "grazie" deserves Giancarlo "John" Castellano who was always there for me, advising and helping in every possible way and to whom I could never express enough gratitude.

Finally, dear parents, thank you for everything!

Contents

Abstract

An algebraic power series is a formal power series $f(x)$ for which a non-zero polynomial $P(x,t)$ exists, such that $P(x,f(x))=0$ holds. These elements play a significant role in various fields of mathematics and are applied and studied in algebraic geometry and combinatorics. In recent decades, many new fascinating properties of this ring of algebraic power series have been found, proven and conjectured. Very deep algebraic techniques are often used to tackle these explicit functions and outstanding aptitude is required not only for the specialized implementations of difficult theorems, but also for ability to go back to the concrete and particular. In the beginning, this thesis provides an explicit introduction to the ring of algebraic power series $K\langle x\rangle$ as an extension of the polynomials and a subring of formal power series. Thereafter a completely different view is revealed to the protagonist: algebraic power series can be viewed as the Henselization of the localization of the polynomial ring. The assembly of the Henselization as a direct limit of so-called pointed étale extensions then yields a new construction of $K\langle x\rangle$. We will use this known construction to explain the famous proof of Denef and Lipshitz regarding the presentation of algebraic power series as diagonals of rational series on the one hand and introduce a new theorem on the other.

Zusammenfassung

Algebraische Potenzreihen sind formale Potenzreihen $f(x)$, für die ein nicht triviales Polynom $P(x,t)$ existiert, sodass $P(x,f(x))=0$ gilt. Diese Reihen spielen fürwahr eine solide Rolle in unterschiedlichen Gebieten der Mathematik und finden ihre größte Bedeutung und ihr Studium in der algebraischen Geometrie und der Kombinatorik. In den letzten Jahrzehnten wurden ständig neue faszinierende Eigenschaften des Ringes der algebraischen Potenzreihen $K\langle x\rangle$ gefunden, bewiesen und vermutet. Um diese expliziten Akteure in Griff zu bekommen, wird teilweise auf sehr tiefliegende Techniken der Algebra zurückgegriffen. Die Kunst besteht sodann nicht nur in der gezielten Anwendung schwieriger Theorie, sondern auch in der Fähigkeit, zurück an die Oberfläche des Handfesten und Expliziten zu kommen. Diese Arbeit bietet zuerst eine konkrete Einführung in den Ring der algebraischen Potenzreihen als Oberring der Polynome und Unterring der formalen Potenzreihen, dann wird jedoch eine ganz andere Sichtweise auf den Protagonisten offenbart: Algebraische Potenzreihen können nämlich auch als die Henselisierung der Lokalisierung des Polynomringes betrachtet werden. Nachdem wir die Henselisierung auch als einen direkten Limes von bestimmten Ringerweiterungen ansehen können, liefert uns das eine neue Konstruktion für $K\langle x\rangle$. Schließlich wollen wir diese Konstruktion benutzen, um einerseits den berühmten Beweis von Denef und Lipshitz über die Darstellung von algebraischen Potenzreihen als Diagonalen von rationalen Reihen zu erklären, und andererseits ein neues Korollar vorstellen.

Chapter 1

Introduction

"Daß ich nicht mehr mit saurem Schweiß
Zu sagen brauche, was ich nicht weiß;
Daß ich erkenne, was die Welt
Im Innersten zusammenhält"
Johann Wolfgang von Goethe, *Faust - Der Tragödie erster Teil*, Nacht.

While giving a presentation at the University of Vienna in spring 2019, the famous French-Vietnamese mathematician Ngô Bảo Châu said:

> *"Mathematics can be described as the study of specific functions: Set theory is examining all functions, topology deals with continuous functions, analysis is about differential functions, etc. Then algebraic geometry is the study of polynomial functions."*

Indeed, like a doctor tries to understand the human, an algebraic geometer attempts to master the polynomial. The definition of such a function is quite painless: for some variables $x_1, \dots, x_n$ it is a finite sum of the form

$$\sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n}, \tag{1.1}$$

where the $a_{i_1,\dots,i_n}$'s are fixed elements in a fixed set R. Interesting questions arise when considering the zero-set of such a function or systems of polynomials. The study of elliptic curves and the corresponding cryptography started with the polynomial equation $y^2 = x^3 + ax + b$, the last theorem of Fermat is about the zero-set of a polynomial function or the still unsolved Jacobian conjecture: these are just some examples of the richness and mysteriousness of the world that algebraic geometry has to offer. Of course, numerous approaches were developed throughout many decades and centuries for dealing with these objects. Like a medic or biologist, when trying to examine a person, will compare his or her symptoms to other human beings, a mathematician will consider the set of all polynomials $R[x_1, \dots, x_n]$ when developing theorems about them. However, medicine would still be in the medieval period if the comparison stopped here: a very powerful idea is to enlarge the collection of patients, to contrast humans not only with other humans but, for example, with other mammals. While studying the much bigger group of these animals, the scientist can get a better understanding of the *Homo sapiens* by fathoming out the similarities as well as the differences between them. Transferring this idea to the world of mathematics, one asks the natural question: to which superset of $R[x_1, \dots, x_n]$ should

we expand, in order to understand it better? One intuitive and also mathematically justified answer is to take *all* sums like in (1.1) and not only the finite ones. This set is known under the name formal power series and is denoted by $R[\![x_1, \ldots, x_n]\!]$. Indeed, it has amazing properties which help understanding the polynomials, and we will define these objects properly and work with them in this chapter.

However, there is an immense drawback of this approach and answer to the natural question of how to enlarge $R[x_1, \ldots, x_n]$: the set of formal power series is too immense. To develop the analogy to other sciences further, it is as if we have taken all the possible living beings in consideration in order to study the human. Of course, this is convenient in the sense that one does not have to bother with the definition of mammals, the group that would most often fit best for scientific purposes: in this view it is easier to just consider all animals. On the other hand, this is of course not the correct approach in the long run as this huge superset is just too broad and we are not capable of understanding it at once. We need another, more manageable, extension of our set of patients $R[x_1, \ldots, x_n]$ in order to study it properly. This is where the set of algebraic power series, denoted by $R\langle x_1, \ldots, x_n\rangle$, comes into play: it consists *by definition* exactly of those elements of $R[\![x_1, \ldots, x_n]\!]$ which satisfy an algebraic property and we also have the required

$$R[x_1, \ldots, x_n] \subseteq R\langle x_1, \ldots, x_n\rangle \subseteq R[\![x_1, \ldots, x_n]\!].$$

The purpose of this thesis is to define this set of algebraic power series properly and to work with it, proving theorems and discovering other viewpoints.

In the first chapter we will define the objects mentioned above and prove fundamental results about them. After demonstrating the Weierstrass theorems, we will see that both, the formal and algebraic power series, satisfy the so-called Henselian property. To conclude this chapter, we open a short discussion about the importance of this property, indicating that there is more to it than just a fact about lifting certain factorizations.

The second chapter is dedicated to the study of Henselian rings. Using some facts from Nagata's book "Local Rings" we will be able to prove that under some assumptions a Henselian ring is algebraically closed in its completion. This is the exact same property by which algebraic power series are defined. This will bring us to the topic of Henselization, that we shall define and study. By employing the first part of this chapter we will conclude that under the hypothesis that the Henselization of the localization of the polynomial ring exists, it must be equal to the ring of algebraic power series. This gives a completely different viewpoint on our protagonist.

Chapter III is not only intended to close the gap about the existence in the previous chapter by providing an explicit construction of the Henselization, but it also deals with the shape of this construction. Citing a famous structure theorem, we will see that the Henselization of a ring is given by a direct limit of so-called pointed étale extensions. This gives an algebraically simple description of the ring of algebraic power series.

Found ourselves in a very deep algebraic environment, we want to take a step back to use the fourth chapter and the gathered theory, theorems and knowledge to provide explicit results about algebraic power series. Denef and Lipshitz used the construction of the Henselization as a direct limit of pointed étale extensions to prove an influential result about the representation of algebraic power series as diagonals of rational power series. Beside explaining this proof, we will use their ideas to improve

on the so-called Artin-Mazur lemma.

Finally, since some definitions and results were rather technical or lengthy, they were deported to the appendix, in order to not disturb the flow of reading. The interested reader will find there the definitions of the direct and inverse limits together with the explanation of the concept of completion. A short passage about the resultant and a few of its properties may also be found there.

1.1 Notation

In order to create a homogeneous work, we will try to stick to a non-changing notation over the whole thesis which we shall briefly explain now. 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. 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, the variable t is always one-dimensional and when we write xt, we mean $(x_1 t, \ldots, x_n t)$. For an n-dimensional index $\alpha \in \mathbb{N}^n$ we have the natural $|\alpha| \coloneqq \alpha_1 + \cdots + \alpha_n$ and $x^\alpha \coloneqq x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

When talking about fields, we will normally use the letters K and L and always mean fields of characteristic 0, whereas rings are usually denoted by R, S or T. A ring is always commutative with 1 and a ring homomorphism is always unital; isomorphisms are indicated with $\cong$. For ideals of rings the letters $\mathfrak{a}$, $\mathfrak{m}$, $\mathfrak{n}$, $\mathfrak{p}$ and $\mathfrak{q}$ are reserved and whenever R is a ring, the set R^* denotes the units of R. The arrows $\twoheadrightarrow$ and $\hookrightarrow$ indicate surjective and injective maps respectively. Finally, when talking about index sets we will use $\mathcal{I}$, $\mathcal{J}$ or even $\mathcal{A}$.

1.2 The Ring of Formal Power Series

Let $x = (x_1, \ldots, x_n)$ and set $R = K[x]_{(x)}$, the ring given by be the localization of the polynomial ring at the maximal ideal $(x) = \langle x_1, \ldots, x_n \rangle$. The resulting ring is local with maximal ideal $\mathfrak{m} = (x)R$. It is usually called the *ring of rational power series*. Define the *ring of formal power series* to be the $\mathfrak{m}$-adic completion of R: $K[\![x]\!] \coloneqq \widehat{R}$. The meaning of completion, its construction as an inverse limit and the most important of its properties are explained in Appendix A.1. This algebraic definition implies many facts about formal power series immediately.

Recall that one may as well construct the ring $K[\![x_1, \ldots, x_n]\!]$ by first prescribing the *set* and then providing a ring structure for it. An element $f(x) \in R[\![x]\!]$ can be then identified with a formal sum of the form

$$f(x) = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha,$$

where $c_\alpha \in K$ for each $\alpha \in \mathbb{N}^n$. The constant coefficient $c_{0,\ldots,0}$ of a formal power series $f(x)$ as above often plays an important role and is denoted by $f(0)$. Multiplication and addition are naturally inherited from the polynomial world and it is easy to see that $f(x)$ is invertible if and only if $f(0) \neq 0$. Note that for an element $f(x) \in K[\![x]\!]$ we will sometimes drop the argument and write $f \in K[\![x]\!]$ in order to simplify notation.

As already explained in the introduction, the ring defined above is a central object in algebra. However, it turns out that in many applications one has to work in a subring of the formal power series. In analysis one is mostly interested in $K\{x\}$, the ring of convergent power series, and in algebraic geometry the natural object to consider is the so-called ring of algebraic power series $K\langle x\rangle$. The goal of the next section is to define this ring properly.

1.3 The Ring of Algebraic Power Series

Definition. Let K be a field and $x = (x_1, \ldots, x_n)$. A formal power series $h(x)$ is called algebraic if there exists a non-zero polynomial $P(x,t) \in K[x,t]$ such that $P(x, h(x)) = 0$. The set of algebraic power series is denoted by $K\langle x\rangle$.

Let us consider some examples in order to get a feeling for algebraic power series:

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

Example 2: Let $x = x_1$ and recall that $\mathrm{char}(K) = 0$. Then the power series given by

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

for some rational number $r \in \mathbb{Q}$ is algebraic. 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: Again let $x = x_1$, assume $K = \mathbb{Q}$ and consider the exponential function:

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

We claim that this power series cannot be algebraic: assume it is, then we would have a non-zero polynomial $P(x,t) = p_0(x) + \cdots + p_m(x)t^m$ with $P(x, \exp(x)) = 0$. Note that without loss of generality we may choose $P(x,t)$ irreducible. Plugging in $x = 1$ gives

$$p_0(1) + \cdots + p_m(1)e^m = 0,$$

for some constants $p_i(1) \in \mathbb{Q}$ for $i = 0, \ldots, m$. Note that we cannot have that $p_i(1) = 0$ for all i, because then the irreducible $P(x,t)$ would be divisible by $x - 1$. This means that we found a non-zero polynomial in $\mathbb{Q}[t]$ annihilating e, which is a contradiction to the transcendence of this number.

Example 4: Let $K = \mathbb{C}$ and $x = x_1$. The function $f(x) = \sqrt{x}$ is not an algebraic power series, because it is not a formal power series.

Example 5: Let again $x = x_1$ and K any field of characteristic 0. Set $f(x) = \sqrt{x+1}$ and $g(x) = \sqrt[3]{x+1}$; we already saw in Example 2 that both $f(x), g(x) \in K\langle x\rangle$. One

can convince oneself that $f(x)+g(x)=\sqrt{x+1}+\sqrt[3]{x+1}$ is algebraic as well: the polynomial

$$\begin{aligned}P(x,t) = &-x^3-2x^2-x+t^6-3xt^4-3t^4-2xt^3-2t^3\\ &+3x^2t^2-2t^3+3x^2t^2+6xt^2+3t^2-6x^2t-12xt-6t\end{aligned}$$

indeed satisfies $P(x, f(x)+g(x))=0$. However, we see that finding $P(x,t)$ is not straightforward and may require some work.

As we saw in the last example, it is not clear from the definition that $K\langle x\rangle$ is a ring, but it is very natural to conjecture it. In fact, we will have to work a little bit to see this:

Proposition 1.3.1. *The set $K\langle x\rangle$ of algebraic power series is a subring of $K[\![x]\!]$.*

There are two approaches to prove the above proposition. Either one constructs for given algebraic power series $f(x)$ and $g(x)$ polynomials $P(x,t)$ and $Q(x,t)$ such that $P(x, f(x)+g(x))=Q(x, f(x)g(x))=0$, or one proves that $K\langle x\rangle$ is given by the intersection of two rings, hence again a ring. Even though the first approach is constructive, in the sense that one has a formula for $P(x,t)$ and $Q(x,t)$, we will follow the second path, as it is more conceptual and explains the proposition in a more general way.

Definition. Given any extension of domains $R\subseteq S$, define $\mathrm{Alg}_R(S)\subseteq S$ to be the set of elements of S that are algebraic over R, i.e. those elements $s\in S$, for which there exists a non-zero polynomial $P(t)\in R[t]$ with $P(s)=0$.
If $\mathrm{Alg}_R(S)=S$ we will say that S is algebraic over R or that $R\subseteq S$ is an algebraic extension.

Given an $s\in S$ which is algebraic over R, there exists a unique (up to R-constant multiplication) non-zero polynomial $P(t)\in R[t]$ of minimal degree that satisfies $P(s)=0$. We call it the *minimal polynomial* of s. Recall that given a field extension $K\subseteq L$, one may consider L as a vector space over K. The dimension of this vector space is denoted by $[L:K]$ and is called the *degree of the field extension.* If $[L:K]<\infty$, we say that the field extension is finite. Finally, recall that for some $a\in L$, one writes $K(a)$ for the smallest subfield of L, containing K and a, whereas $K[a]$ denotes the smallest *subring* of L containing those two. It turns out that all these terms are interacting with each other, as the following well-known lemma tells us:

Lemma 1.3.2. *Let $K\subseteq L$ be a field extension and $a\in L$ be algebraic over K. Then it holds that*

(1) $K[a]=K(a)$.

(2) $K\subseteq K(a)$ is a finite extension. In fact, $[K(a):K]=d$, where d is the degree of the minimal polynomial of a.

Proof. Let $p(t)\in K[t]$ be the minimal polynomial of a. Take some $f(t)\in K[t]$, such that $f(a)\neq 0$. To prove (1) it suffices to argue that $f(a)$ is invertible, since then any non-zero element in $K[a]$ will be, which will prove that it must be a field. Note that

$p(t)$ does not divide $f(t)$ and is irreducible. Hence, these polynomials are coprime and we may find $g(t), h(t) \in K[t]$ such that:

$$g(t)p(t) + h(t)f(t) = 1.$$

Plugging in a into this equation yields $h(a)f(a) = 1$, thus we found an inverse to $f(a)$ proving (1).

Now let $d = \deg(p(t))$ and consider the elements

$$1, a, \dots, a^{d-1}.$$

They are clearly linearly independent, since if we had some relation, then we would have found a polynomial of smaller degree than $p(t)$ also killing a, contradicting the minimality of $p(t)$. Finally, to see that the elements above generate $K[a]$, assume we are given some $f(a) \in K[a]$. Then dividing $f(t)$ by $p(t)$ with the division algorithm, yields polynomials $q(t), r(t) \in K[t]$ such that $\deg(r(t)) < d$ and

$$f(t) = q(t)p(t) + r(t).$$

Again after plugging in a, we see that $f(a) = r(a)$ is generated by $1, a, \dots, a^{d-1}$, justifying also the second part of the lemma. □

Now we prove the following statement of commutative algebra, explaining the interplay between our terms even more. The first two parts are very well-known results and the third part is the one we are mainly interested in.

Lemma 1.3.3. *Let $K \subseteq L$ be an extension of fields and $R \subseteq S$ be an extension of integral domains. Then:*

(1) If $[L : K] < \infty$, then this extension is algebraic.

(2) $\mathrm{Alg}_K(L)$ is a subfield of L.

(3) $\mathrm{Alg}_R(S)$ is a subring of S.

Proof. (1) If for some field extension $[L : K] < \infty$, then L is finite-dimensional as a vector space over K. Take some $a \in L$. If a was not algebraic over K, then $\{1, a, a^2, \dots\} \subseteq L$ would be an infinite K-linear independent set, but this is impossible.

(2) To show that $\mathrm{Alg}_K(L)$ is a field, it suffices to show for any $a, b \in \mathrm{Alg}_K(L)$, $b \neq 0$, that $a - b$ and a/b are both in $\mathrm{Alg}_K(L)$. Consider $K \subseteq K(a, b) \subseteq L$. Since a is algebraic, $[K(a) : K]$ is finite by the previous lemma. Also $[K(a, b) : K(a)] < \infty$ and it follows from the tower law that:

$$[K(a, b) : K] = [K(a, b) : K(a)] \cdot [K(a) : K] < \infty,$$

hence this extension is algebraic by (1). As $a - b$ and a/b are both in $K(a, b)$, which is algebraic over K, we have proven that $a - b$ and a/b are algebraic elements over K.

(3) Now let $R \subseteq S$ be an extension of integral domains and let K, L be the corresponding fields of fractions:

$$\begin{array}{ccccc} K & \hookrightarrow & \mathrm{Alg}_K(L) & \hookrightarrow & L \\ \uparrow & & \uparrow & & \uparrow \\ R & \hookrightarrow & \mathrm{Alg}_R(S) & \hookrightarrow & S \end{array}$$

We claim that $\mathrm{Alg}_R(S) = S \cap \mathrm{Alg}_K(L)$. Then we have expressed $\mathrm{Alg}_R(S)$ as the intersection of a subring and a subfield of L, so it will be a ring.
One inclusion is straightforward: take $s \in \mathrm{Alg}_R(S)$, then s is algebraic over R and so clearly also algebraic over K. Hence, $s \in S \cap \mathrm{Alg}_K(L)$ and so $\mathrm{Alg}_R(S) \subseteq S \cap \mathrm{Alg}_K(L)$. Conversely, take any $s \in S \cap \mathrm{Alg}_K(L)$. As s is algebraic over K, there exist an $n > 0$ and for $0 \leq i \leq n$ elements $a_i \in R$, not all zero, and $b_i \in R \setminus \{0\}$ with:

$$\sum_{k=0}^{n} \frac{a_k}{b_k} s^k = 0.$$

Multiplying with $b = \prod_{k=0}^{n} b_k \neq 0$ gives:

$$\sum_{k=0}^{n} (a_k \widehat{b_k}) s^k = 0,$$

where $\widehat{b_k} := b/b_k \in R$. This proves that s is algebraic over R and consequently $s \in \mathrm{Alg}_R(S)$. □

Applying the third part of this lemma to $R = K[x]$ and $S = K[\![x]\!]$ for some field K and $x = (x_1, \ldots, x_n)$, we see that the set of algebraic power series $\mathrm{Alg}_R(S) = K\langle x \rangle$ is indeed a subring of $K[\![x]\!]$. This proves Proposition 1.3.1.

Analysing the proof of (3) in the Lemma above yields another non-trivial fact about algebraic power series:

Corollary 1.3.4. *Let $f(x), g(x) \in K\langle x \rangle$ be two algebraic power series such that $f(x)/g(x) \in K[\![x]\!]$ is a formal power series. Then $f(x)/g(x) \in K\langle x \rangle$ is again an algebraic power series.*

Proof. We showed in the proof of (3) that if $R \subseteq S$ is an extension of integral domains then $\mathrm{Alg}_R(S) = S \cap \mathrm{Alg}_{K'}(L')$, where K' and L' are the quotient fields of R and S respectively. Applying this to $R = K[x]$ and $S = K[\![x]\!]$, we have by construction $f(x)/g(x) \in K' \subseteq \mathrm{Alg}_{K'}(L')$ and by assumption $f(x)/g(x) \in S$. Therefore, $f(x)/g(x)$ is in $\mathrm{Alg}_R(S)$: it is an algebraic power series. □

Finally, at some point, we will need the notion of integral extensions together with a simple fact connecting them to algebraic ones. Given an extension of rings $R \subseteq S$, we call an element $s \in S$ *integral over* R if there exists a *monic* polynomial $P(t) \in R[t]$ with $P(s) = 0$. We say that the extension is integral if this holds for any $s \in S$. The only difference to the notion of algebraic is that we require the polynomial to be monic in the integral case. Naturally, we have the following lemma connecting these notions:

Lemma 1.3.5. *Let $R \subseteq S$ be an extension of rings and $a \in S$ algebraic over R. Then there exists a non-zero $b \in R$ such that $c := ab$ is integral over S.*

Proof. Let $P(t) = p_n t^n + \cdots + p_0 \in R[t]$ be a minimal polynomial of a of degree $n \geq 1$. Take $b = p_n$ and consider

$$Q(t) = t^n + p_{n-1} t^{n-1} + p_n p_{n-2} t^{n-2} + \cdots + p_n^{n-2} p_1 t + p_n^{n-1} p_0.$$

We clearly have that $Q(t)$ is monic and

$$\begin{aligned} Q(c) = Q(ap_n) &= p_n^n a^n + p_n^{n-1} a^{n-1} p_{n-1} + p_n^{n-1} a^{n-2} p_{n-2} + \cdots p_n^{n-1} p_1 a + p_n^{n-1} p_0 \\ &= p_n^{n-1} P(a) = 0, \end{aligned}$$

since $P(t)$ annihilates a. Therefore, we found a monic polynomial that kills $c = ab$ and proved the lemma. □

1.4 Weierstrass Theorems

The Weierstrass division theorem (WPT) and the preparation theorem (WPT) are important fundamental results about the ring of formal power series. WDT is a form of the Euclidean division algorithm, but requires an extra property on the divisor. Recalling how many applications and implications the division algorithm has for the polynomial ring, we can only imagine at this point how meaningful the Weierstrass division theorem will be for $K[\![x]\!]$. For example, it implies directly that the ring of formal power series is Noetherian, Henselian and a unique factorization domain (UFD). However, our main interest lies in the fact that both WDT and WPT hold true for algebraic power series with the same implications for this ring. In order to prove this fact, we will first have to justify the validity of these theorems for formal series and then argue that their legitimacy is inherited.

Recall that $x = (x_1, \ldots, x_n)$ and $x' = (x_1, \ldots, x_{n-1})$, therefore we may identify $K[\![x]\!] = K[\![x']\!][\![x_n]\!]$. Moreover, K is, as always, a field of characteristic 0.

Before starting with the actual theorems of Weierstrass, we state a theorem about formal power series that follows from their definition of being the completion of $K[x]_{(x)}$. The following theorem does not only have a similar flavour as the statements of Weierstrass, but it will also accompany us along the whole thesis:

Theorem 1.4.1 (Hensel's Lemma)**.** *Let $f(x,t) \in K[\![x]\!][t]$ be a monic polynomial in the variable t over the ring of formal power series. Assume $f(0,t) = \bar{p}(t)\bar{q}(t)$ factors into two monic coprime polynomials. Then there exist two unique monic polynomials $p(x,t), q(x,t) \in K[\![x]\!][t]$ with $p(0,t) = \bar{p}(t)$, $q(0,t) = \bar{q}(t)$ and $f(x,t) = q(x,t)p(x,t)$.*

Proof. In the appendix we prove a more general statement: any complete local ring satisfies Hensel's lemma (Theorem A.1.3). To see that the statement above follows from the general one, note that setting $x = 0$ in a polynomial $f(x,t) \in K[\![x]\!][t]$ over the ring of formal power series is equivalent to considering $f(x,t)$ mod $\mathfrak{m}K[\![x]\!][t]$, where of course $\mathfrak{m} = (x_1, \ldots, x_n)$. Moreover, the ring of formal power series is indeed complete with respect to the $\mathfrak{m}$-adic topology, as it is the completion of the Noetherian ring $K[x]_{(x)}$. □

Now we will dive into the world of the theorems of Weierstrass, but first we need the notions of order, x_n-regularity and distinguished polynomials:

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 $\operatorname{ord}(f)$, 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 $\operatorname{ord}(f) = +\infty$.

(2) A power series $g(x) \in K[\![x]\!]$ is called x_n-regular of order d if $g(0,\dots,0,x_n) = x_n^d f(x_n)$ 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 $i = 0,\dots,d-1$.

Theorem 1.4.2 (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 $r \in K[\![x']\!][x_n]_{<d}$ which is a distinguished polynomial in x_n of degree less than d with coefficients given by power series in x', such that $f = qg + r$.*

There are several different known ways to prove this theorem. The probably most famous proof is in the book "The Basic Theory of Power Series" by J. M. Ruiz [Rui93], a more recent and very short one can be found in [Hau17]. We follow the approach of S. Lang [Lan05] since it is very explicit:

Proof. First, let us define α, τ to be the projections on the beginning and tail end of a series viewed as an element in $K[\![x']\!][\![x_n]\!]$, given by:

$$\begin{aligned} \alpha : K[\![x]\!] &\to K[\![x]\!] \\ \sum_{i\geq 0} b_i(x')x_n^i &\mapsto \sum_{i=0}^{d-1} b_i(x')x_n^i = b_0(x') + b_1(x')x_n + \cdots + b_{d-1}(x')x_n^{d-1}, \end{aligned}$$

and

$$\begin{aligned} \tau : K[\![x]\!] &\to K[\![x]\!] \\ \sum_{i\geq 0} b_i(x')x_n^i &\mapsto \sum_{i=d}^{\infty} b_i(x')x_n^{i-d} = b_d(x') + b_{d+1}(x')x_n + b_{d+2}(x')x_n^2 + \cdots . \end{aligned}$$

Immediately we see that $\tau(hx_n^d) = h$ for any $h \in K[\![x]\!]$ and also $\alpha(h) + \tau(h)x_n^d = h$. Moreover, it holds that h is a polynomial in x_n of degree less than d if and only if $\tau(h) = 0$. Because of the last fact, the existence of q and r in the statement of the theorem is equivalent to the existence of q such that

$$\tau(f) = \tau(qg).$$

In order to solve this equation and prove the uniqueness of the solution, we rewrite it first. Since τ is obviously linear and because of the facts above, this equality is equivalent to

$$\tau(f) = \tau\big(q\alpha(g) + q\tau(g)x_n^d\big) = \tau\big(q\alpha(g)\big) + q\tau(g).$$

Now, because g is x_n-regular of order d, we must have that $\tau(g)$ is invertible. Finding q is therefore equivalent to finding the formal power series $q\tau(g) =: \tilde{q}$. After rewriting the equation above once again, we end up with

$$\tau(f) = \tau\Big(\tilde{q}\frac{\alpha(g)}{\tau(g)}\Big) + \tilde{q} = \Big(\mathrm{Id}_{K[\![x]\!]} + \tau \circ \frac{\alpha(g)}{\tau(g)}\Big) \circ \tilde{q},$$

where $\mathrm{Id}_{K[\![x]\!]}$ is the identity operator on $K[\![x]\!]$ and

$$\phi \coloneqq \tau \circ \frac{\alpha(g(x))}{\tau(g(x))} : K[\![x]\!] \to K[\![x]\!]$$
$$h(x) \mapsto \tau\Big(h(x)\frac{\alpha(g(x))}{\tau(g(x))}\Big).$$

However, $\alpha(g)/\tau(g) \in (x') = (x_1, \dots, x_{n-1})$, the ideal generated by $x_1, \dots, x_{n-1}$, because $\alpha(g(0, \dots, 0, x_n)) = 0$, so we get that ϕ maps any $h \in K[\![x]\!]$ to $\phi(h) \in (x')K[\![x]\!]$. Moreover, it is also clear that for $k \geq 0$ if $h \in (x')^k$, then $\phi(h) \in (x')^{k+1}$. It follows by induction that $\phi^k(h) \in (x')^k$ for any $h \in K[\![x]\!]$. Therefore, we see that the formal inverse of the operator $\mathrm{Id}_{K[\![x]\!]} + \phi$, which is given by

$$(\mathrm{Id}_{K[\![x]\!]} + \phi)^{-1} = \sum_{i \geq 0} (-1)^i \phi^i,$$

is well-defined, as $K[\![x]\!]$ is complete in the (x)-adic topology and $(x') \subseteq (x)$. Hence, we can find $\tilde{q}$ in a unique way:

$$\tilde{q} = \big(\mathrm{Id}_{K[\![x]\!]} + \phi\big)^{-1} \circ \tau(f).$$

Then also $q = \tilde{q}/\tau(g)$ and $r = f - qg$ are obtained uniquely and the proof is finished. □

Theorem 1.4.3 (WPT)**.** *Let $g \in K[\![x]\!]$ be an x_n-regular power series of order d. Then there exist a unique $p \in K[\![x']\!][x_n]_{=d}$ which is a distinguished polynomial in x_n of degree d with coefficients given by power series in x' and a unique unit $u \in K[\![x]\!]^*$, such that $g = up$.*

Proof. The idea here is to use the previous theorem and to divide the power series $f = x_n^d$ by g, which is x_n-regular by assumption:

$$x_n^d = \tilde{u}g + \tilde{p},$$

for unique formal power series $\tilde{u}$ and $\tilde{p} = p_0(x') + p_1(x')x_n + \cdots + p_{d-1}(x')x_n^{d-1} \in K[\![x']\!][x_n]_{<d}$. Now, plugging in $(0, \dots, 0, x_n)$ yields

$$x_n^d = \tilde{u}(0, \dots, 0, x_n)g(0, \dots, 0, x_n) + p_0(0) + p_1(0)x_n + \cdots + p_{d-1}(0)x_n^{d-1}.$$

However, since $g(0, \dots, 0, x_n) = x_n^d v(x_n)$ for some $v(x_n) \in K[\![x_n]\!]$ with $v(0) \neq 0$, we see by comparing coefficients of x_n that $p_0(0) = \cdots = p_{d-1}(0) = 0$ and that $\tilde{u}(0, \dots, 0, 0) \neq 0$. Therefore, $\tilde{u}(x)$ is a unit in $K[\![x]\!]$ and also the polynomial $p \coloneqq x_n^d - \tilde{p}$ is distinguished. Finally, setting $u \coloneqq \tilde{u}^{-1} \in K[\![x]\!]$ and rearranging gives

$$g(x) = u(x)p(x),$$

as requested. Note that uniqueness follows easily from the uniqueness of $\tilde{u}(x)$ and $\tilde{p}(x)$. □

Having proved WDT and WPT for formal power series, we now want to address the ring $K\langle x \rangle$ and we will see that analogous statements hold. We start by proving the algebraic version of the Weierstrass preparation theorem as it is done in [LT70]:

Theorem 1.4.4 (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 $p \in K\langle x'\rangle[x_n]_{=d}$ 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. We note immediately that uniqueness is guaranteed by uniqueness of Weierstrass formal preparation. Moreover, assume that the statement of the theorem holds for $g_1, g_2 \in K\langle x\rangle$, both algebraic and x_n-regular of order d_1 and d_2 respectively. Then we have $g_1 = u_1 p_1$ and $g_2 = u_2 p_2$ for $u_1, u_2 \in K\langle x\rangle^*$ and polynomials $p_1, p_2 \in K\langle x'\rangle[x_n]$ of degrees d_1 and d_2 respectively. We obtain

$$g \coloneqq g_1 g_2 = u_1 u_2 p_1 p_2.$$

Of course, $u_1 u_2$ is again a unit and an algebraic power series, and $d_1 + d_2$ is both the degree of $p_1 p_2 \in K\langle x'\rangle[x_n]$ and the order of g. This shows that we may assume that g is irreducible as a power series.
We apply the formal version of Weierstrass preparation to get

$$g = up,$$

with $u \in K[\![x]\!]^*$ and $p \in K[\![x']\!][x]$ a distinguished polynomial of degree d. We need to show that both are algebraic power series. As we assumed that g is irreducible as a series, it follows that p is also irreducible as a polynomial in $K[\![x']\!][x_n]$. Therefore, and because zero characteristic of K implies separability, 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 $\alpha_1, \ldots, \alpha_d$. Hence:

$$g(x) = u \prod_{j=1}^{d} (x_n - \alpha_j).$$

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 the 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 the fact that $g(x', \alpha_i) = 0$, we obtain for every of those i's:

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

As $0 \not\equiv G_0(x', t) \in K[x', t] \subseteq K(x', t)$ 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, using Corollary 1.3.4, the same holds for $u = g/p$. □

Now we can use this theorem and the formal Weierstrass division to prove WDT for algebraic power series:

Theorem 1.4.5 (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 $r \in K\langle x'\rangle[x_n]_{<d}$ 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, uniqueness is clear by the formal WDT and we want to argue that one may assume that g is irreducible. However, now the argument requires a little bit more work:

First note that by the algebraic Weierstrass preparation theorem, we may assume without loss of generality that $g \in K\langle x' \rangle[x_n]$ is a distinguished polynomial of degree d. This is because we can write $g = up$ as in the theorem above. Then, if we are able to divide by distinguished polynomials, we will arrive at

$$f = q_p p + r = \frac{q_p}{u} g + r,$$

and as we wanted $r \in K\langle x' \rangle[x_n]$ is a distinguished polynomial of degree less than d and $q \coloneqq q_p/u$ is an algebraic power series. Assume therefore that g is a distinguished polynomial.

Now we will show that one may also assume that g is irreducible. Suppose that the statement of the theorem holds for some $g_1, g_2 \in K\langle x' \rangle[x_n]$ with degrees d_1 and d_2 respectively. We want to show the division theorem for $g = g_1 g_2 \in K\langle x' \rangle[x_n]$, a distinguished polynomial of degree $d_1 + d_2$. We divide f by g_1 to get $f = q_1 g_1 + r_1$, where $r_1 \in K\langle x' \rangle[x_n]$ of degree less than d_1 and $q_1 \in K\langle x \rangle$. Then divide q_1 by g_2 to obtain $q_1 = q_2 g_2 + r_2$, with $q_2 \in K\langle x \rangle$ and $r_2 \in K\langle x' \rangle[x_n]$ of degree less than d_2. Combining these equations yields

$$\begin{aligned} f &= q_2 g_1 g_2 + g_1 r_2 + r_1 \\ &= q_2 g + g_1 r_2 + r_1. \end{aligned}$$

Now, because g_1 is a distinguished polynomial of degree d_1, it follows that $g_1 r_2$ is a polynomial in x_n of degree less than $d_1 + d_2$. Hence, $g_1 r_2 + r_1 \in K\langle x' \rangle[x_n]$ is also of degree less than $d_1 + d_2$. Therefore, we may indeed assume that $g(x)$ is irreducible.

Given an irreducible algebraic distinguished polynomial $g \in K\langle x' \rangle[x_n]$ of degree d and an algebraic f, we can divide formally:

$$f = qg + r = qg + \sum_{j=0}^{d-1} b_j(x') x_n^j, \tag{1.2}$$

for $q \in K[\![x]\!]$ and $b_0(x'), b_1(x'), \ldots, b_{d-1}(x') \in K[\![x']\!]$ formal power series. We need to show that all of these are algebraic power series.

Because g is a distinguished polynomial, we may write

$$g = \sum_{j=0}^{d} c_j(x') x_n^j$$

for some $c_0(x'), c_1(x'), \ldots, c_d(x') \in K\langle x' \rangle$ algebraic power series. As we assumed that g is irreducible, it follows that it is also irreducible as a polynomial in $K[\![x']\!][x_n]$. Similarly to the argumentation in the algebraic WPT we get that g has d distinct roots in $\Omega = \overline{\mathrm{Frac}(K[\![x']\!])}$, say $\alpha_1, \ldots, \alpha_d$. From (1.2), 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:

$$\begin{pmatrix} f(x', \alpha_1) \\ \vdots \\ f(x', \alpha_d) \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} b_1(x') \\ \vdots \\ b_d(x') \end{pmatrix}.$$

Now note that the matrix above is the Vandermonde matrix and since the α_i's are pairwise different, we know that it is invertible. Therefore, each $b_i(x')$ is uniquely given by some polynomial expression in the $f(x', \alpha_j)$'s and α_k's for $j, k \in \{1, \ldots, d\}$. We want to make sure that each $b_i(x')$ is an algebraic power series in x'.
By the same argument as in the proof of the algebraic WPT, we obtain that each α_i is algebraic over $K(x')$. Moreover, by assumption $f = f(x', x_n)$ is algebraic over $K(x', x_n)$. By applying Lemma 1.3.2 twice, 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 by the first part of Lemma 1.3.3, we see that $f(x', \alpha_i)$ is algebraic over $K(x')$. As this holds for every $i = 1, \ldots, d$, it follows that also any polynomial 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, using Corollary 1.3.4, the same holds for $q = (f - r)/g$. □

We will encounter the situation where f in the theorem above is a distinguished polynomial itself. For this case we have a somewhat stronger version of the WDT:

Lemma 1.4.6. *Let $g \in K\langle x' \rangle[x_n]$ be a distinguished polynomial of degree d. For any $f \in K\langle x' \rangle[x_n]$ there exist uniquely an algebraic power series $q \in K\langle x' \rangle[x_n]$ which is a polynomial in x_n and $r \in K\langle x' \rangle[x_n]_{<d}$ which is a distinguished polynomial in x_n of degree less than d with coefficients given by algebraic power series in x', such that $f = qg + r$.*

In other words, if g in the Weierstrass division theorem is distinguished and f a polynomial in x_n, then q must also be a polynomial in x_n. The proof is an easy combination of WDT and the polynomial division over the ring $K\langle x' \rangle$:

Proof. Dividing $f \in K\langle x' \rangle[x_n]$ by $g \in K\langle x' \rangle[x_n]$ as polynomials in the ring $K\langle x' \rangle$ gives

$$f = \tilde{q}g + \tilde{r},$$

with $\tilde{q}, \tilde{r} \in K\langle x' \rangle[x_n]$ and $\tilde{r}$ of degree less than d in x_n.
However, similarly dividing f by g with the algebraic WDT yields:

$$f = qg + r.$$

for some algebraic power series q and $r \in K\langle x' \rangle[x_n]$ of degree less than d. By uniqueness of the Weierstrass division, it follows that $\tilde{q} = q$ and $\tilde{r} = r$, hence $q \in K\langle x' \rangle[x_n]$. □

Now, the following lemma implies that the condition on x_n-regularity in all theorems above is in praxis not too restrictive, since we can make any non-zero power series x_n-regular by a certain linear transformation of the variables. More precisely, we have the following lemma from [Rui93]:

Lemma 1.4.7. *Let $f(x) \in K\langle x\rangle$ be an algebraic power series of order $d < \infty$. Then there exist $c_1, \ldots, c_{n-1} \in K$ such that the algebraic power series*

$$g(x) \coloneqq f(x_1 + c_1 x_n, \ldots, x_{n-1} + c_{n-1} x_n, x_n)$$

is x_n-regular of order d.

Proof. We have $f(x) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$, so set

$$f_d(x) \coloneqq \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| = d}} a_\alpha x^\alpha,$$

the homogeneous part of $f(x)$ of degree d. There exist $c_1, \ldots, c_{n-1} \in K$ with $c \coloneqq f_d(c_1, \ldots, c_{n-1}, 1) \neq 0$, because otherwise the homogeneous polynomial $f_d(x)$ would be divisible by $x_n - 1$. Now deploying these c_i's, we have that

$$g(0, \ldots, 0, x_n) = f(c_1 x_n, \ldots, c_{n-1} x_n, x_n) = c x_n^d + \text{ higher order terms},$$

exactly what we wanted. Note that the linear coordinate change of course preserves algebraicity of the power series. □

Note that the this proof uses the fact that the characteristic of K is zero, as this implies that K must have infinite cardinality. There is a trick by which one can avoid this assumption, however then one cannot assume a linear transformation any more.

Corollary 1.4.8. *The ring of algebraic power series over a field of zero characteristic is Noetherian.*

Proof. We argue by induction on n, the number of variables. If $n = 0$, the result is trivial, so let $n > 0$ and assume that $K\langle x_1, \ldots, x_{n-1}\rangle = K\langle x'\rangle$ is Noetherian. Given a non-zero ideal $\mathfrak{n} \subseteq K\langle x\rangle$, we want to find finitely many generators of it. Take $g \in \mathfrak{n}, g \neq 0$. According to the lemma above, we may assume that g is x_n-regular of order, say d. By the algebraic Weierstrass division theorem, it follows that the ring $K\langle x\rangle/(g)$ is generated by $1, x_n, \ldots, x_n^{d-1}$ as a $K\langle x'\rangle$-module. However, $K\langle x'\rangle$ is Noetherian by the induction hypothesis, hence $K\langle x\rangle/(g)$ is a Noetherian $K\langle x'\rangle$-module. It follows that $\mathfrak{n}/(g)$ is finitely generated as a $K\langle x'\rangle$-module, say by the classes of $f_1, \ldots, f_s \in \mathfrak{n}$. Then $f_1, \ldots, f_s, g$ generate $\mathfrak{n}$. □

Corollary 1.4.9. *The ring of algebraic power series over a field of zero characteristic is factorial.*

Proof. Let $g \in K\langle x\rangle$ be a non-zero algebraic power series, which we want to factor uniquely into irreducible components up to a unit. The existence of a factorization is easy: every time one has $h = h_1 h_2$ for some reducible h and $h_1, h_2 \in K\langle x\rangle$ non-units, one must have that $\operatorname{ord}(h_1) < \operatorname{ord}(h)$ and $\operatorname{ord}(h_2) < \operatorname{ord}(h)$. Since the order of g is finite, we must arrive at some finite factorization into irreducible factors.

To prove uniqueness, we proceed again by induction on n, where the case $n = 0$ is obvious and we can assume that $K\langle x_1, \ldots, x_{n-1}\rangle = K\langle x'\rangle$ is factorial. Once again, by Lemma 1.4.7, we may assume that g is x_n-regular. Then, by the algebraic Weierstrass preparation theorem, we may write $g = up$ for some unit $u \in K\langle x\rangle^*$ and a polynomial $p \in K\langle x'\rangle[x_n]$. Now, because $K\langle x'\rangle$ is factorial by induction hypothesis, we have that $K\langle x'\rangle[x_n]$ is also a factorial ring [Lang, 2.3]. Hence, we can write p uniquely up to units as a product of irreducible elements $p_1, \ldots, p_s \in K\langle x'\rangle[x_n]$. This gives the unique factorization:

$$g(x) = p_1(x) \cdots p_s(x)u(x). \qquad \square$$

Now we will prove a version of Hensel's lemma for algebraic power series, following [Rui93].

Theorem 1.4.10 (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 $t' = t - \alpha$, we may assume that $\alpha = 0$ and, since α is a d-th 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

$$f(x,t) = u(x,t)p(x,t), \tag{1.3}$$

where $p(x,t) \in K\langle x\rangle[t]$ is a distinguished polynomial in t of degree d and $u(x,t) \in K\langle x,t\rangle^*$ 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 $p(0,t) = t^d = (t-\alpha)^d$. To see that $u(x,t)$ is a polynomial in t we apply Lemma 1.4.6. Uniqueness follows from the uniqueness of the algebraic Weierstrass division theorem and concludes the proof. $\square$

The statement above ensures that a root $\alpha \in K$ of $f(0,t)$ gives rise to a factorization $f(x,t) = u(x,t)p(x,t)$. One calls this factorization the *lifting* of α. We can prove a different and seemingly stronger version of Hensel's lemma, which states that we can lift coprime factorizations and not only d-th roots. In Chapter III we will see that these two versions of Hensel's lemma are equivalent in a very general ring-theoretic setting.

Theorem 1.4.11 (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 $f = qp$.*

Proof. First we prove the existence of the factorization in the ring $\overline{K}\langle x\rangle[t]$, where $\overline{K}$ is the algebraic closure of K. As $\bar{p}(t), \bar{q}(t) \in \overline{K}[t]$, we may write

$$\begin{aligned} f(0,t) = \bar{p}(t)\bar{q}(t) &= \prod_{j=1}^{d_1}(t-\alpha_j)^{P_j}\prod_{j=1}^{d_2}(t-\beta_j)^{Q_j} \\ &= (t-\alpha_1)^{P_1}\prod_{j=2}^{d_1}(t-\alpha_j)^{P_j}\prod_{j=1}^{d_2}(t-\beta_j)^{Q_j}, \end{aligned}$$

for $\alpha_1, \ldots, \alpha_{d_1}, \beta_1, \ldots, \beta_{d_2} \in \overline{K}$ pairwise different and $P_1, \ldots, P_{d_1}, Q_1, \ldots, Q_{d_2} \in \mathbb{N}$. By the previous theorem we can lift the root α_1 to get $f = p_1 q_1$, where $p_1, q_1 \in \overline{K}\langle x \rangle[t]$ and $p(0,t) = (t-\alpha_1)^{\bar{p}_1}$. Considering then just $q_1(x,t)$, we can do the same:

$$\begin{aligned} q_1(0,t) &= \prod_{j=2}^{d_1} (t-\alpha_j)^{P_j} \prod_{j=1}^{d_2} (t-\beta_j)^{Q_j} \\ &= (t-\alpha_2)^{P_2} \prod_{j=3}^{d_1} (t-\alpha_j)^{P_j} \prod_{j=1}^{d_2} (t-\beta_j)^{Q_j}. \end{aligned}$$

Lifting α_2 gives a factorization $q_2 = p_2 q_2$ with $p_2(0,t) = (t-\alpha_2)^{\bar{p}_2}$, which we can use to write $f = p_1 p_2 q_2$. After repeating this process in total d_1 times, we will arrive at $f = p_1 \cdots p_{d_1} q_{d_1} =: pq$. Of course $p, q \in \overline{K}\langle x \rangle[t]$ and clearly $p(0,t) = \prod_{j=1}^{d_1} (t-\alpha_j)^{P_j} = \bar{p}(t)$ and similarly $q(0,t) = \bar{q}(t)$. Hence, we found a factorization when working with the algebraically closed $\overline{K}$ and we wish to show that both p and q lie in $K\langle x \rangle[t]$. However, this follows from the uniqueness in Hensel's lemma for the formal case (Theorem 1.4.1): the formal liftings of $\bar{p}$ and $\bar{q}$ in $K[\![x]\!][t]$ and $\overline{K}[\![x]\!][t]$ have to agree, and because a lifting in $K\langle x \rangle[t]$ is also a formal lifting, it is the same again by uniqueness. We obtain that $p, q \in \overline{K}\langle x \rangle[t] \cap K[\![x]\!][t] = K\langle x \rangle[t]$. This concludes the proof. □

The theorem above is crucial for this work, as it does not only present an important fact about the ring of algebraic power series, it also motivates us to define an interesting class of rings: we will call a ring Henselian if it satisfies Hensel's lemma. Before we make this idea precise, we shall give an explanation why the property of lifting factorizations is of immense importance for algebraic geometry [Eis95].

1.5 The Importance of Hensel's Lemma

Consider the nodal plane cubic curve over a field K (of zero characteristic as always) given by the equation $t^2 - x^2(1+x) = 0$ for $x = x_1$:

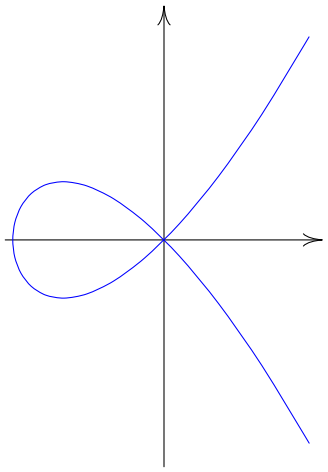


Figure 1.1: The node: $\mathbb{R}[x,t]/(t^2 - x^2(1+x))$.

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 1.1), 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 neighbourhood of 0 of the node is irreducible. The reason is that over the complex numbers a neighbourhood of 0 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 neighbourhood" 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 that 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, considering the polynomial $f(x,t) = t^2 - (1+x)$ we see that $f(0,t) = (t-1)(t+1) = \bar{p}(t)\bar{q}(t)$ 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.

Chapter 2

Algebraic Power Series and Henselization

"One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them"
J.R.R.Tolkien, *The Lord of the Rings*, Book I, Chapter 2.

2.1 Henselian Rings

In this chapter 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 $\phi^{-1}(\mathfrak{n}) = \mathfrak{m}$. This notion is very natural, since it describes those maps between local rings, which are continuous with respect to the induced topologies, explained in the appendix A.1. As always, we require every field to have zero characteristic. Note that both, the rings of formal and algebraic power series, are local with maximal ideal $\mathfrak{m} = (x) = (x_1, \ldots, x_n)$, because $K[\![x]\!]^* = K[\![x]\!] \setminus (x)$ and similarly $K\langle x\rangle^* = K\langle x\rangle \setminus (x)$. We also see immediately that $K[\![x]\!]/(x) \cong K\langle x\rangle/(x) \cong K$. Given a $p(t) \in R[t]$, we will denote by $\bar{p}(t) \in K[t]$ the reduction of $p(t)$ mod $\mathfrak{m}R[t]$, given by reducing all coefficients of $p(t)$ mod $\mathfrak{m}$.

In the spirit of the last Theorems (1.4.10 and 1.4.11), we introduce the notion of Henselian rings:

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 property above is usually referred to as "Hensel's lemma" even though is actually 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 theorem:

Theorem 2.1.1 (Hensel's lemma for complete rings)**.** *Let $(R, \mathfrak{m}, K)$ be a complete local ring. Then R is Henselian.*

The proof of this statement can be found in the appendix, Theorem A.1.3. Note also, that we already used this fact when proving Theorem 1.4.1.

For the purpose of this work, a very significant fact is that Theorem 1.4.11 implies the following:

Theorem 2.1.2. *The ring of algebraic power series $K\langle x\rangle$ is Henselian.*

Proof. Note that since $\mathfrak{m} = (x_1, \ldots, x_n)$, it follows that considering some $f(x, t)$ mod $\mathfrak{m}K\langle x\rangle[t]$ in $K\langle x\rangle[t]$ means setting $x = 0$. Then, the statement of Theorem 1.4.11 becomes Hensel's property. □

A rather useful implication of Hensel's property is the following lemma, which states that any integral extension of a Henselian ring must be local. Its statement and proof appear in [Nag75] and give an introductory flavour of the next section:

Lemma 2.1.3. *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 $\mathfrak{m}'_2$. Since $a \in R'$ and R' is an integral extension, we have an irreducible monic polynomial

$$f(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0,$$

which has a as root and $c_i \in R$ for $0 \leq i \leq n-1$. 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

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

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

Our next step is to study Henselian rings in a purely algebraic way, like M. Nagata already did in the middle of the last century.

2.2 Henselian Characterization of Algebraic Power Series

The main goal of this chapter is stressing the connection between the property of being Henselian and the algebraic closure in the completion. 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 hold that $a \in R$. These conditions may appear technical at first sight, however they have the purpose of excluding pathologies while still allowing for a large class of rings. First, recall the notions of analytically irreducible and analytically normal:

Definition. A local ring R is called analytically irreducible if its completion $\widehat{R}$ is a domain. R is called analytically normal if $\widehat{R}$ is normal.

Recall that a normal ring is a domain R that is integrally closed in its field of fractions, which we will denote by $\mathrm{Frac}(R)$. It is a fact that a ring is a domain (respectively normal), if it is analytically irreducible (respectively analytically normal). Moreover, it is clear that our main object of interest, $K[x]_{(x)}$, is analytically normal, as its completion $K[\![x]\!]$ is factorial and therefore normal. In this section we heavily follow the approach of M. Nagata [Nag75] and therefore we need the notion of a Nagata ring[1] for which we first define Japanese rings:

Definition. Let R be an integral domain with quotient field L. R is called Japanese[2] 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.

Now we can define Nagata rings:

Definition. A ring R is called Nagata (or pseudo-geometric) if R is Noetherian and for every prime ideal $\mathfrak{p} \subseteq R$, the ring $R/\mathfrak{p}$ is Japanese.

The category of Nagata rings is reasonably large and closed under many operations. In order to justify this, we present some statements from M. Nagata's "Local Rings" [Nag75], H. Matsumura's "Commutative Algebra" [Mat80] and the Stacks Project [Stacks]:

Proposition 2.2.1. *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.*

This is statement (36.1) in [Nag75].

Proposition 2.2.2. *If R is a Nagata ring, then any localization of R is also Nagata.*

The proof can be found in [Stacks, Tag 032U].

Proposition 2.2.3 (Nagata)**.** *If R is a Nagata ring, then any finitely generated R-algebra is Nagata.*

For a proof of this proposition see [Nag75, (36.5)], or [Stacks, Tag 0334].

Note that obviously any field is Nagata, therefore by the proposition above $K[x_1, \ldots, x_n]$ is also a Nagata ring. Then $K[x]_{(x)}$ is again Nagata, since it is just a localization.

For our purposes we will also need the following version of Zariski main theorem, which can be found in [Nag75] as Theorem 37.8.

Lemma 2.2.4. *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.*

[1] This notion first appeared in Nagata's book "Local Rings" in the year 1962 under the name "pseudo-geometric".

[2] According to [Stacks] this name was first used by Grothendieck in EGA [DG67] in order to contribute to Nakayama, Takagi, Nagata and many others.

We are ready to prove one central theorem of this chapter, connecting the Henselian rings with the property of being algebraically closed in the completion. This theorem explains why the study of algebraic power series essentially comes down to studying Henselian rings.

Theorem 2.2.5. *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, by Lemma 1.3.5, we can find $b \neq 0$ in R such that the element $ab = c$ is integral over R. We want to prove that $R[c] = R$, because then we will be able to conclude that also $a \in R$. Assume otherwise and let $f(t) \in R[t]$ 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.

$$\begin{array}{ccccccc} L & \hookrightarrow & L[c] & \xrightarrow{=} & L[c] & \hookrightarrow & \widehat{L} \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ R & \hookrightarrow & R[c] & \hookrightarrow & R' & \hookrightarrow & \widehat{R} \end{array}$$

We claim that R' is also the integral closure of R in $L[c]$, which we denote by R''. Obviously, $R'' \subseteq R'$ and to see the other inclusion take an $r \in R'$; then $r \in L[c]$ and is integral over $R[c]$, but since $R[c]$ is an integral extension of R, we must have that r is integral also over R as well. Hence we obtain $R' \subseteq R''$, proving equality.

Now, 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 by Lemma 1.3.2 that $L[c]$ is a finite extension of L and therefore R' is a finitely generated R-module.

Furthermore, R', being finitely generated of a Nagata ring, is still Nagata by Proposition 2.2.1 and also R' is indeed local by Lemma 2.1.3 (this is where we use the Henselian assumption), hence we may apply Lemma 2.2.4 to get that R' is analytically irreducible. However, we have that $\widehat{R'} = R' \otimes_R \widehat{R}$ by Lemma A.1.5 and this must be a domain because of the consideration before. Now look at the completion of $R[c]$, which is again given by $R[c] \otimes_R \widehat{R}$, also by Lemma A.1.5. Because $R \to \widehat{R}$ is flat, we have the inclusion $R[c] \otimes_R \widehat{R} \subseteq R' \otimes_R \widehat{R}$ and hence $\widehat{R[c]}$ must also be a domain. On the other hand, we have $\widehat{R[c]} = R[c] \otimes_R \widehat{R} = \widehat{R}[t]/(f(t))$, identifying $f(t)$ with its image in $\widehat{R}[t]$. However, since $c \in \widehat{R}$ annihilates $f(t)$, we get that $f(t) = (t-c)g(t)$ for some non-zero $g(t) \in \widehat{R}[t]$. Hence, $\widehat{R}[t]/(f(t))$ can not be a domain, which is a contradiction. So we get $c \in R$ and hence $a \in \mathrm{Frac}(R)$. Because $R = \mathrm{Frac}(R) \cap \widehat{R}$ by Lemma A.1.6 and since a is in both rings, we get that $a \in R$ as wanted. □

We see 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 view point on our main ring of interest.

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:

$$\begin{array}{ccc} R & \xrightarrow{\ i\ } & R^{\mathrm{h}} \\ {\scriptstyle\psi}\downarrow & \swarrow_{\phi} & \\ H & & \end{array}$$

Note that from the definition it follows that if R^{h} exists, then it must be unique up to isomorphism. For: Assume $R^{\mathrm{h}'}$ is another Henselization of R. Then, by definition, we have that the map $R \to R^{\mathrm{h}'}$ factors uniquely as $R \to R^{\mathrm{h}} \to R^{\mathrm{h}'}$. Similarly, $R \to R^{\mathrm{h}}$ factors as $R \to R^{\mathrm{h}'} \to R^{\mathrm{h}}$. It follows that we can compose the maps $R^{\mathrm{h}} \to R^{\mathrm{h}'}$ and $R^{\mathrm{h}'} \to R^{\mathrm{h}}$ and get the identity on R^{h} and $R^{\mathrm{h}'}$ respectively because of the uniqueness of ϕ in the definition. Hence, $R^{\mathrm{h}} \cong R^{\mathrm{h}'}$ and we obtain that the Henselization is indeed unique up to isomorphism.

Even though we have not proven anything about the Henselization of a ring (in fact up to now it is even not clear that it exists), we can already formulate the goal of this chapter:

Theorem 2.2.6. *Let $R = K[x]_{(x)}$ be the localization of $K[x]$ at the maximal ideal (x). Assume that the Henselization of R exists. Then it is given by the ring of algebraic power series: $R^{\mathrm{h}} = K\langle x \rangle$.*

In the next chapter we will construct the Henselization of R as a direct limit of certain extensions of R, proving existence. However, before doing so, we first explain what results one may extract directly from the definition of R^{h}.

Lemma 2.2.7. *Let R^{h} together with $i : R \to R^{\mathrm{h}}$ be the Henselization of a Noetherian local ring R. Then i is injective.*

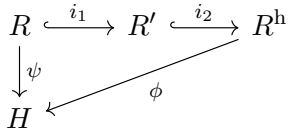
Proof. We choose in the universal property of the Henselization $H = \widehat{R}$, which is Henselian by Lemma A.1.3. Then $\psi : R \hookrightarrow \widehat{R}$ is injective (since R is required to be Noetherian) and local. As we have a map $\phi : R^{\mathrm{h}} \to \widehat{R}$ with $\psi = \phi \circ i$, we must have that $i : R \hookrightarrow R^{\mathrm{h}}$ is injective. □

Note that it is not clear that $\phi : R^{\mathrm{h}} \to \widehat{R}$ is injective, in fact it is quite hard to prove that R^{h} is a subring of the completion. However, this fact becomes evident in the next chapter.

Lemma 2.2.8. *Let R^{h} be the Henselization of a local ring R and assume the existence of a Henselian ring R' such that $R \subseteq R' \subseteq R^{\mathrm{h}}$. Then $R' = R^{\mathrm{h}}$.*

In other words, there cannot be any Henselian ring between R and R^{h}: A property one would expect from the "smallest" Henselian extension of R.

Proof. The universal property of R^{h} gives for any Henselian ring H and any local ψ:

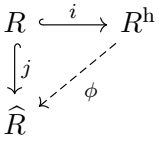


Where ϕ is the unique local map $R^{\mathrm{h}} \to H$ such that $\psi = \phi \circ i_2 \circ i_1$. As i_2 is just an inclusion, we may consider $\phi|_{R'} : R' \to H$, the unique local factorization of ψ through R'. This means, R' also satisfies the universal property of the Henselization of R. Because the Henselization is unique we must have $R' = R^{\mathrm{h}}$. □

Lemma 2.2.9. *Let R^{h} be the Henselization of a Noetherian local ring R. Then $\widehat{R} \subseteq \widehat{R^{\mathrm{h}}}$.*

It is a fact that the completions of any local Noetherian R and its Henselization R^{h} agree. However to see this, one needs the construction we will give in the next chapter. Up to now, the fact above is enough to prove the main theorem of this chapter.

Proof. From the universal property we have the factorization of the injective map $j : R \hookrightarrow \widehat{R}$ as follows:



Because ϕ is local, we have for every $n \in \mathbb{N}$ that $(\mathfrak{m}^{\mathrm{h}})^n \subseteq \phi^{-1}(\widehat{\mathfrak{m}}^n)$, where $\mathfrak{m}^{\mathrm{h}}$ is the (unique) maximal ideal of R^{h} and $\widehat{\mathfrak{m}}$ is the maximal ideal of $\widehat{R}$. Similarly, one has $\mathfrak{m}^n \subseteq i^{-1}((\mathfrak{m}^{\mathrm{h}})^n)$. This gives us maps

$$R/\mathfrak{m}^n \to R^{\mathrm{h}}/(\mathfrak{m}^{\mathrm{h}})^n \to \widehat{R}/\widehat{\mathfrak{m}}^n.$$

Now note that the composition of the maps above is the canonical isomorphism $R/\mathfrak{m}^n \to \widehat{R}/\widehat{\mathfrak{m}}^n$. In particular it is injective, therefore the first map must be injective as well. Hence, $R/\mathfrak{m}^n \hookrightarrow R^{\mathrm{h}}/(\mathfrak{m}^{\mathrm{h}})^n$ for every n. We can apply Lemma A.1.2 from the appendix to obtain $\widehat{R} \cong \varprojlim R/\mathfrak{m}^n \hookrightarrow \varprojlim R^{\mathrm{h}}/(\mathfrak{m}^{\mathrm{h}})^n \cong \widehat{R^{\mathrm{h}}}$. This proves the assertion. □

Lemma 2.2.10. *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 [Nag75, (44.2, 44.3)].

Hence, assuming $K[x]^{\mathrm{h}}_{(x)}$ exists, then it is both, analytically normal and Nagata. Now we are able to prove the following result, which is the main step on the way of proving Theorem 2.2.6:

Proposition 2.2.11. *Let $R = K[x]_{(x)}$ be the localization of $K[x]$. Then, if the Henselization of R exists, it contains the ring of algebraic power series: $R^{\mathrm{h}} \supseteq K\langle x\rangle$.*

Proof. Let $f(x) \in K\langle x \rangle$ be a formal power series, which is algebraic over $R = K[x]_{(x)}$. We want to show that $f(x) \in R^{\mathrm{h}}$. By the Theorem 2.2.5 and because R^{h} is Henselian, Nagata and analytically normal (by definition and by the lemma above), it suffices to prove:

a) $f(x)$ is algebraic over R^{h},

b) $f(x) \in \widehat{R^{\mathrm{h}}}$.

Now, *a)* holds true, because from $f(x)$ algebraic over R it follows that $f(x)$ is algebraic over R^{h}, since $R \subseteq R^{\mathrm{h}}$. And *b)* holds true, because $f(x) \in K[\![x]\!] = \widehat{K[x]_{(x)}} \subseteq \widehat{K[x]^{\mathrm{h}}_{(x)}}$ by Lemma 2.2.9. □

For $R = K[x]_{(x)}$, we have shown $K\langle x \rangle \subseteq R^{\mathrm{h}}$. Using the fact that $K\langle x \rangle$ is Henselian (Theorem 2.1.2) and applying Lemma 2.2.8, we obtain that $K\langle x \rangle = R^{\mathrm{h}}$, which finally proves Theorem 2.2.6.

In order to prove existence and some important results about the Henselization, we will have to construct it. For that we need the notion and some theory of étale maps, which brings us to the next chapter.

Chapter 3

Étale Ring Maps and Henselization

"La mer était étale, mais le reflux commençait à se faire sentir;"
Victor Hugo, *Les Travailleurs de la mer*, Deuxième partie, Livre II [1]

3.1 Motivation for Étale Ring Maps

Before giving the rigorous definition of an étale map $R \to S$ for rings R, S, we will try to explain the motivation behind it. J.S. 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."*

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 these analogues and we will try to motivate the one that comes most from geometry and is 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

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

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

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

$$\begin{array}{ccc} S = K[X] & \longrightarrow & K \\ \uparrow{\scriptstyle \phi} & \nearrow & \\ R = K[Y] & & \end{array}$$

[1] *"The sea, indeed, was calm, but the ebb had begun."*, Victor Hugo, *Toilers of the Sea*, Part II, Book II.

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 $a \coloneqq (a_1, \ldots, a_n) \in K^n$ with the condition that each $f_j(a_1, \ldots, a_n) = 0$, $1 \leq j \leq r$, hence, by definition, $a \in X$. Similarly, $K[Y] \to K$ is a K-point, say $b = (b_1, \ldots, b_m) \in Y$, because $g_j(b_1, \ldots, b_m) = 0$ for $j = 1, \ldots, s$. The commutativity of the diagram means that sending $(y_1, \ldots, y_m) \mapsto (b_1, \ldots, b_m)$ by the diagonal map is the same as sending $(y_1 \ldots, y_m) \mapsto (\phi_1(x_1, \ldots, x_n), \ldots, \phi_m(x_1, \ldots, x_n)) \mapsto (\phi_1(a), \ldots, \phi_m(a))$: K-points are sent to K-points.

Now we want to describe the behaviour 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:

$$\begin{array}{ccc} S = K[X] & \longrightarrow & K \\ {\scriptstyle\phi}\uparrow & & \uparrow \\ R = K[Y] & \longrightarrow & K[\varepsilon]/(\varepsilon^2) \end{array}$$

Since

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

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

$$\begin{aligned} K[Y] = K[y_1, \ldots, y_m]/(g_1, \ldots, g_s) &\to K[\varepsilon]/(\varepsilon^2) \\ y_i &\mapsto b_i + \varepsilon c_i, \quad 1 \leq i \leq m, \end{aligned}$$

for some $b \coloneqq (b_1, \ldots, b_m) \in K^m$ and $c \coloneqq (c_1, \ldots, c_m) \in K^m$. Then it must hold that $g_j(b_1 + \varepsilon c_1, \ldots, b_m + \varepsilon c_m) = 0$ for $1 \leq j \leq s$. 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

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

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 even 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: we

require additionally the existence and uniqueness of the diagonal arrow, preserving commutativity:

$$\begin{array}{ccc} S = K[X] & \longrightarrow & K \\ \phi\uparrow & \nearrow & \uparrow \\ R = K[Y] & \longrightarrow & K[\varepsilon]/(\varepsilon^2) \end{array}$$

By the same argument as above, we can easily convince ourselves that this diagonal map $K[X] \to K[\varepsilon]/(\varepsilon^2) : x_i \mapsto a_i + \varepsilon d_i$ for $i = 1, \ldots, n$ and some $d \coloneqq (d_1, \ldots, d_n)$ 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 $y_j \mapsto b_j + \varepsilon c_j$, $1 \leq j \leq m$ 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

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

To put these m equations into one, we define the Jacobian matrix

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

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

Definition. Let S be an R-algebra. For any pair $(T, \mathfrak{n})$ of an R-algebra T and an ideal $\mathfrak{n} \subseteq T$ such that $\mathfrak{n}^2 = 0$ consider the map

$$\begin{aligned} \Theta_{T,\mathfrak{n}} : \mathrm{Hom}_R(S, T) &\to \mathrm{Hom}_R(S, T/\mathfrak{n}) \\ f : S \to T &\mapsto \pi \circ f : S \to T/\mathfrak{n}, \end{aligned}$$

where $\pi : T \to T/\mathfrak{n}$ is the natural surjection. We say the R-algebra S is formally smooth if $\Theta_{T,\mathfrak{n}}$ is surjective for all pairs $(T, \mathfrak{n})$. S is a formally unramified R-algebra if $\Theta_{T,\mathfrak{n}}$ is injective for all $(T, \mathfrak{n})$. Finally by a formally étale R-algebra we mean an R-algebra S for which $\Theta_{T,\mathfrak{n}}$ is bijective for all T and $\mathfrak{n}$.

Hence, given an R-algebra map $S \to T/\mathfrak{n}$ with $\mathfrak{n}^2 = 0$, if S is formally smooth, there is a lifting to an R-algebra map $S \to T$. If S is formally unramified, there is at most one lifting and if S is formally étale, there is a unique lifting. Some authors call a formally smooth (respectively unramified, étale) R-algebra an "extension" of R, however this is badly justified since $\phi : R \to S$ does not have to be injective.

Note that usually, when dealing with a formally smooth (respectively unramified, étale) S, we will call the map $\phi : R \to S$ formally smooth (respectively unramified, étale) rather than the R-algebra itself.

Rephrasing this definition, we can find the motivation explained in the section above: given an R-algebra S with the homomorphism $\phi : R \to S$, we call S (or the map ϕ) formally smooth/formally unramified/formally étale if the following condition is satisfied:

Suppose that T is an R-algebra, $\mathfrak{n} \subseteq T$ an ideal with $\mathfrak{n}^2 = 0$ and the following diagram of R-algebra maps commutes:

$$\begin{array}{ccc} S & \xrightarrow{\bar{u}} & T/\mathfrak{n} \\ {\scriptstyle\phi}\uparrow & & \uparrow{\scriptstyle\pi} \\ R & \longrightarrow & T \end{array}$$

Then there is at least/at most/precisely one R-algebra morphism $u : S \to T$, which lifts $\bar{u}$, i.e. the following diagram also commutes:

$$\begin{array}{ccc} S & \xrightarrow{\bar{u}} & T/\mathfrak{n} \\ {\scriptstyle\phi}\uparrow & \overset{u}{\searrow} & \uparrow{\scriptstyle\pi} \\ R & \longrightarrow & T \end{array}$$

This property is known under the name infinitesimal lifting. As we saw in the previous section, it reflects the definition of a submersion, immersion and local diffeomorphism inside of algebraic geometry.

To go from *formally* smooth (respectively unramified, étale) to smooth (respectively unramified, étale) ring map, 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

$$S \cong R[x_1, \ldots, x_n]/(f_1, \ldots, f_m),$$

for $f_i \in R[x_1, \ldots, x_n]$, $i = 1, \ldots, m$.

Naturally, we have the following fact about transitivity immediately:

Lemma 3.2.1. *If S if finitely presented over R and T is finitely presented over S, then T is finitely presented over R.*

Proof. We have

$$S \cong R[x_1, \dots, x_n]/(f_1, \dots, f_m) \text{ and } T \cong S[y_1, \dots, y_k]/(g_1, \dots, g_s).$$

Consider $R[x_1, \dots, x_n, y_1, \dots y_k]$. Each $g_j \in S[y_1, \dots, y_k]$ can be lifted to some $h_j \in R[x_1, \dots, x_n, y_1, \dots y_k]$. Then clearly

$$T \cong R[x_1, \dots, x_n, y_1, \dots y_k]/(f_1, \dots, f_m, h_1, \dots, h_s),$$

as required. □

Note that a localization of R at one element, say $a \in R$, is finitely presented: $R_a \cong R[t]/(at - 1)$. It follows therefore directly that a localization at finitely many elements is still finitely presented. This does not have to be true for any multiplicative system.

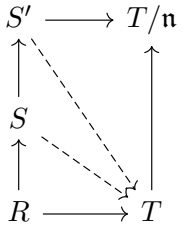
Now we can define what we mean by a smooth, unramified and étale ring map:

Definition. Let S be an R-algebra. S is called smooth (respectively unramified, étale) if it is formally smooth (respectively unramified, étale) and finitely presented.

This concludes the definitions connected to the notions of smooth, unramified and étale and brings us to the section where we prove and mention the most important consequences of these definitions. Note that we will present the most results with the focus on étale ring maps, rather than on smooth or unramified ones, since the étale algebras are the ones we are mostly interested in. We start with a natural property:

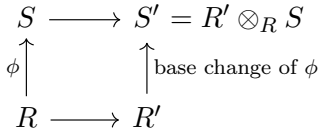
Lemma 3.2.2. *Let S be an R-algebra and S' an S-algebra. Assume that $R \to S$ and $S \to S'$ are (formally) étale, then the induced map $R \to S'$ is also (formally) étale.*

Proof. Note first that S' is indeed finitely presented over R if S is, by Lemma 3.2.1. Hence, we only need to justify the universal property in the definition of formally étale. However, this is straightforward: consider an R-algebra T and $\mathfrak{n} \subseteq T$ with $\mathfrak{n}^2 = 0$ and the commutative diagram



Since $R \to S$ is étale, we find a unique $S \to T$. Then, since $S \to S'$ is étale, we find a unique $S' \to T$. □

Another important fact 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 $R' \to R' \otimes_R S =: S'$.



To understand this notion, we note that the explicit description of a base change is very natural when a presentation is given: we already saw that since S is an R-algebra, it 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 [Stacks, Tag 05G3] this fact is described as "the key to understanding base change". Now let us state the lemma and its proof:

Lemma 3.2.3. *Let $R \to S$ be étale and $R \to R'$ be arbitrary. Then $R' \to R' \otimes_R S$ is étale.*

Proof. The proof is straightforward: By the consideration above, we see that $R' \otimes_R S$ is finitely presented over R since S is. Hence, we just have to justify formally étale. We have the following commutative diagram for an R-algebra T and an ideal $\mathfrak{n} \subseteq T$ with $\mathfrak{n}^2 = 0$:

$$\begin{array}{ccccc} S & \longrightarrow & R' \otimes_R S & \longrightarrow & T/\mathfrak{n} \\ \uparrow & & \uparrow & \nearrow & \uparrow \\ R & \longrightarrow & R' & \longrightarrow & T \end{array}$$

The goal is to find a unique map $R' \otimes_R S \to T$ preserving the commutativity of the diagram. Since $R \to S$ is étale and the horizontal maps above create a commutative square as in the definition, we have a unique $u : S \to T$ preserving commutativity. But then, having fixed $R' \to T$ and found a unique $S \to T$, we will have of course a unique map $R' \otimes_R S \to T$ by the property of the tensor product. □

Corollary 3.2.4. *Let $R \to S$ and $R \to S'$ be étale. Then $R \to S \otimes_R S'$ is étale.*

Proof. By the previous lemma it follows that $S' \to S \otimes_R S'$ is étale. Then we conclude by Lemma 3.2.2. □

One can use the next result to produce formally smooth, unramified and étale R-algebras easily. The proof shows that applying the somewhat involved definition of these terms correctly, can yield many facts about them in a direct fashion.

Proposition 3.2.5. *Let S be an R-algebra with $\phi : R \to S$. Then:*

(1) Let S be a polynomial ring over R in arbitrary many indeterminates, i.e. $S = R[x_i : i \in \mathcal{I}]$. Then S is formally smooth over R. If in this case $|\mathcal{I}| < \infty$, then S is smooth over R.

(2) Let $W \subseteq R$ be a multiplicative system and $S = W^{-1}R$. Then $R \to S$ is formally étale.

(3) If $\mathfrak{a} \subseteq R$ is an ideal and $S = R/\mathfrak{a}$, then S is formally unramified over R.

Proof. To justify (1), consider the commutative diagram

$$\begin{array}{ccc} R[x_i] & \xrightarrow{\bar{u}} & T/\mathfrak{n} \\ \uparrow & & \uparrow \\ R & \longrightarrow & T \end{array}$$

For any $\bar{t_i} \coloneqq \bar{u}(x_i) \in T/\mathfrak{n}$, we choose some representative $t_i \in T$. Consequently, the map $R[x_i] \to T$ sending x_i to t_i clearly lifts $\bar{u}$ and preserves commutativity. Note that we did not even use $\mathfrak{n}^2 = 0$ here.

In (2) we have to prove existence and uniqueness of the dashed map:

$$\begin{array}{ccc} W^{-1}R & \xrightarrow{\bar{u}} & T/\mathfrak{n} \\ {\scriptstyle i}\uparrow & \nearrow & \uparrow{\scriptstyle \pi} \\ R & \xrightarrow[g]{} & T \end{array}$$

Consider $g : R \to T$. There is a lifting through $W^{-1}R$ if and only if g maps $W \subseteq R$ to units of T. However, since $W^{-1}R \to T/\mathfrak{n}$ must map $i(W)$ to units and projecting nilpotents with π does not affect invertibility, we see that this condition on g must hold. Therefore we can find the sought map. It is clearly unique by the universal property of $W^{-1}R$.

Finally for part (3): assume that $R/\mathfrak{a} \to T/\mathfrak{n}$ has two different liftings to $R/\mathfrak{a} \to T$. Then we may compose $R \twoheadrightarrow R/\mathfrak{a} \to T$ and get two different maps $R \to T$, contradiction. □

Proposition 3.2.6. *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.*

In particular, setting $n = 1$, it follows that $R \to R[t]_g/(f)$ is étale for some $f, g \in R[t]$, if f', the derivative of f, is invertible in $R[t]_g/(f)$.

Proof. First note that

$$S = R[x_1, \dots, x_n]_g/(f_1, \dots, f_n) \cong R[x_1, \dots, x_n, x_{n+1}]/(f_1, \dots, f_n, x_{n+1}g - 1),$$

and after setting $f_{n+1} = x_{n+1}g - 1$, one has $\det(\frac{\partial f_j}{\partial x_i})_{1 \le i,j \le n+1} = \pm g \det(\frac{\partial f_j}{\partial x_i})_{1 \le i,j \le n}$. Since g is a unit in S, this is invertible if and only if $\det(\frac{\partial f_j}{\partial x_i})_{i,j=1}^{n}$ is. Therefore, we can assume that $S = R[x_1, \dots, x_n]/(f_1, \dots, f_n)$.
Now suppose we are given a pair $(T, \mathfrak{n})$ with $\mathfrak{n}^2 = 0$ together with the commutative diagram:

$$\begin{array}{ccc} S = \frac{R[x_1,\dots,x_n]}{(f_1,\dots,f_n)} & \xrightarrow{\bar{u}} & T/\mathfrak{n} \\ {\scriptstyle \phi}\uparrow & & \uparrow{\scriptstyle \pi} \\ R & \longrightarrow & T \end{array}$$

We seek to find the lifting $u : S \to T$ preserving the commutativity of the diagram. Let $\bar{x} = (\bar{x}_1, \dots, \bar{x}_n)$ be the image of $x = (x_1, \dots, x_n)$ in S. Taking some representatives $y_1, \dots, y_n \in T$ of $\bar{u}(\bar{x}_1), \dots, \bar{u}(\bar{x}_n)$, we have $y_i \equiv \bar{u}(\bar{x}_i) \bmod \mathfrak{n}$ for

all $i = 1, \ldots, n$. It follows that $f_j(y_1, \ldots, y_n) \in \mathfrak{n}$ for all $j = 1, \ldots, n$. In order to construct a factorization map $u : S \to T$ we need to have $f_j(y_1, \ldots, y_n) = 0$ for all $j = 1, \ldots, n$. Of course, we cannot take any $y_1, \ldots, y_n$ which lift $\bar{u}(\bar{x}_1), \ldots, \bar{u}(\bar{x}_n)$, in fact we want to assure that the choice is unique. The existence and uniqueness of such y_i's are justified with an ansatz: We prove that there are unique $\delta_1, \ldots, \delta_n \in \mathfrak{n}$ such that $f_j(y_1 + \delta_1, \ldots, y_n + \delta_n) = 0$ for all $j = 1, \ldots, n$. After applying Taylor's formula and using the fact that $\mathfrak{n}^2 = 0$, we see that this condition is equivalent to the system of equations:

$$f_j(y_1, \ldots, y_n) + \sum_{i=1}^{n} \delta_i \cdot \frac{\partial f_j}{\partial x_i}(y_1, \ldots, y_n) = 0. \tag{3.1}$$

Let $J = \left(\frac{\partial f_j}{\partial x_i}\big|_{x=y}\right)_{1 \leq i,j \leq n} \in M_n(T)$ be the $n \times n$ Jacobian matrix at $x_1 = y_1, \ldots, x_n = y_n$. The determinant of J is a unit mod $\mathfrak{n}$, hence it is also a unit in T. It follows that J is an invertible matrix. Rewriting eq. (3.1) in terms of J yields

$$F + J\Delta = 0,$$

where $F = (f_1(y_1, \ldots, y_n), \ldots, f_n(y_1, \ldots, y_n))^t$ and similarly $\Delta = (\delta_1, \ldots, \delta_n)^t$. Evidently , this equation has a unique solution for Δ given by $\Delta = -J^{-1}F$. Moreover, the entries of Δ are indeed in $\mathfrak{n}$ because all entries of F are. This proves the existence and uniqueness of $\delta_1, \ldots, \delta_n$. □

We have as an immediate consequence that localizations at elements are necessary étale. Of course, this also follows from Proposition 3.2.5, but here we see a nice way of using the statement above.

Corollary 3.2.7. *Let $a \in R$ be a non-nilpotent element. Then the canonical map $R \to R_a$ is étale.*

Proof. Note that $R_a \cong R[t]/(at - 1)$ and the derivative of $f(t) = at - 1$ is given by $f'(t) = a$. It is clearly invertible in R_a, hence $R \to R_a$ is étale. □

When working over fields, the primitive element theorem implies:

Corollary 3.2.8. *A finite separable algebraic extension L of a field K is étale over K.*

Proof. By the primitive element theorem, it follows that $L = K[\theta]$ for an algebraic element θ. The minimal polynomial $f(t)$ of θ is separable over K and therefore the image of $f'(t)$ in L does not vanish. Hence, we have $L \cong K[t]/(f(t))$ where $f'(t)$ is invertible in L. This is étale by the proposition above. □

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

Note that again by Proposition 3.2.6, 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 [DG67, (IV), p. 120] A. Grothendieck attributes this fact to C. Chevalley and so shall we.

Theorem 3.2.9 (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 2.2.4. Also Nakayama's lemma and the primitive element theorem for separable field extensions, which we already used in Corollary 3.2.8, play a role in the proof. In his lecture notes [Hoc17] M. Hochster points out that "additional trickery" is required as well. Therefore the proof is very lengthy and technical and shall not be provided in this work. We refer to [Hoc17, pp. 27] as well as [Stacks, Tag 00UE], [DG67, (IV), pp. 120] or [Mil80, pp. 26].

This structure theorem concretely describes étale algebras locally. Thus, it has many applications, for example using it, we can easily prove a non-trivial fact that an étale R-algebra S is necessarily flat over R. Recall that an R-algebra S is called *flat*, if tensoring any short exact sequence $0 \to T_1 \to T_2 \to T_3 \to 0$ of R-modules with S preserves exactness, in the sense that $0 \to S \otimes_R T_1 \to S \otimes_R T_2 \to S \otimes_R T_3 \to 0$ is still exact. S is called *faithfully flat*, if taking the tensor product with a sequence produces an exact sequence if *and only if* the original sequence is exact.

Corollary 3.2.10. *Let $R \to S$ be étale. Then $R \to S$ is a flat ring map.*

Proof. First, we prove that $R \to T$ for a standard étale R-algebra is flat. This is easy, since $T \cong (R[t]/(f))_g$ for $f \in R[t]$ monic, say of degree d, such that f' is invertible in T and $g \in R[t]/(f)$. Then we have

$$R \to R[t]/(f) \cong R \oplus Rx \oplus \cdots \oplus Rx^{d-1} \to (R[t]/(f))_g.$$

Both maps are flat and therefore also their composition is. Now, it also follows that $R \to S$ for S any étale R-algebra is flat, because flatness is a local property on the one hand and because of the structure theorem above on the other [Stacks, Tag 00H9]. □

3.3 Construction of the Henselization

We want to construct the Henselization of a local ring $(R, \mathfrak{m}, K)$ and prove existence and some desirable properties of it. For that we define the notion of étale neighbourhoods like Milne in his book "Étale Cohomology" [Mil80]:

Definition. Let $(R, \mathfrak{m}, K)$ be local. A pair $(S, \mathfrak{q})$ is called an étale neighbourhood 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 neighbourhood $(S, \mathfrak{q})$.

By Proposition 3.2.5 we immediately see that $R \to S_{\mathfrak{q}} = T$ is formally étale, however it is not étale in general since $S_{\mathfrak{q}}$ does not have to be finitely presented over R. Moreover, it follows from Corollary 3.2.10 that S is flat over R. Localization preserves flatness, therefore also $R \to S_{\mathfrak{q}} = T$ is flat. Since R and $S_{\mathfrak{q}} = T$ are local and the map between them is local as well, we see that it must be faithfully flat and in particular injective. This justifies the word "extension" when talking about pointed étale R-algebras. Moreover, it follows directly from the definition of étale neighbourhoods that $S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{p}} \cong K$, therefore the residue field of a pointed étale algebra T of $(R, \mathfrak{m}, K)$ is isomorphic to K.

The property of being Henselian can be expressed in terms of pointed étale extensions. More precisely, we will see soon that a ring R is Henselian if and only if it does not have any proper pointed étale extension. However, first we have to prove that there is at most one local R-algebra map between two pointed étale R-algebras: a fact we will use several times. For that purpose, for a given R-algebra S, we want to study the multiplication map, given by the linear extension of

$$\begin{aligned} \mu : S \otimes_R S &\twoheadrightarrow S \\ s \otimes s' &\mapsto ss', \end{aligned}$$

and its kernel $\mathfrak{a} \coloneqq \ker(\mu)$. The following proposition is the starting point of our study.

Proposition 3.3.1. *Let S be an R-algebra and $\mathfrak{a} = \ker(S \otimes_R S \twoheadrightarrow S)$. Then $\mathfrak{a}$ is generated by the elements $s \otimes 1 - 1 \otimes s$ for $s \in S$.*

Proof. Call $\mu : S \otimes_R S \twoheadrightarrow S$ and let $\mathfrak{a}' = \langle s \otimes 1 - 1 \otimes s : s \in S \rangle \subseteq S \otimes_R S$, the ideal generated by all elements $s \otimes 1 - 1 \otimes s$. The goal is to prove that $\mathfrak{a}' = \mathfrak{a}$. Since $\mu(s \otimes 1 - 1 \otimes s) = s - s = 0$, we have that $\mathfrak{a}' \subseteq \mathfrak{a}$. To see the other inclusion, consider an element $a \in \mathfrak{a}$; it is a finite sum of the form

$$a = \sum_{i=1}^{n} r_i s_i \otimes s_i',$$

for some $r_i \in R$ and $s_i, s_i' \in S$ for $1 \leq i \leq n$, such that $\mu(a) = 0$. This condition is clearly equivalent to

$$\sum_{i=1}^{n} r_i s_i s_i' = 0.$$

We want to see that $a \in \mathfrak{a}'$. An explicit trick solves this problem very fast:

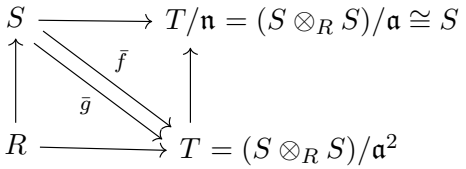
$$\begin{aligned} \sum_{i=1}^{n} r_i (s_i \otimes 1)(1 \otimes s_i' - s_i' \otimes 1) &= \sum_{i=1}^{n} r_i (s_i \otimes s_i' - s_i s_i' \otimes 1) \\ &= \sum_{i=1}^{n} r_i s_i \otimes s_i' - \sum_{i=1}^{n} r_i s_i s_i' \otimes 1 \\ &= \sum_{i=1}^{n} r_i s_i \otimes s_i' - \Bigg(\underbrace{\sum_{i=1}^{n} r_i s_i s_i'}_{0} \Bigg) \otimes 1 \\ &= \sum_{i=1}^{n} r_i s_i \otimes s_i' = a. \end{aligned}$$

Since the left-hand side is obviously in $\mathfrak{a}'$, we are done. □

Theorem 3.3.2. *Let S be a formally unramified R-algebra and denote by $\mathfrak{a} = \ker(S \otimes_R S \twoheadrightarrow S)$. Then $\mathfrak{a} = \mathfrak{a}^2$.*

In [Hoc17] it is proven that this implication is in fact an equivalence, however here we only explain the direction we are interested in.

Proof. Obviously $\mathfrak{a}^2 \subseteq \mathfrak{a}$ and we have to justify the other inclusion. Consider the universal property of formally unramified, set $T = (S \otimes_R S)/\mathfrak{a}^2$ and $\mathfrak{n} = \mathfrak{a}/\mathfrak{a}^2 \subseteq T$. We have two maps $S \to S \otimes_R S$ given by $f : s \mapsto s \otimes 1$ and $g : s \mapsto 1 \otimes s$, hence we have also two maps $\bar{f}, \bar{g} : S \to T$, which, of course, agree on $T/\mathfrak{n} \cong S$:



Since $R \to S$ is formally unramified, we have that $\bar{g} = \bar{f}$. This means that $s \otimes 1 - 1 \otimes s$ vanishes in $T = (S \otimes_R S)/\mathfrak{a}^2$ for any $s \in S$, i.e. $s \otimes 1 - 1 \otimes s \in \mathfrak{a}^2$. But these elements generate $\mathfrak{a}$ by the previous proposition, therefore we obtain that $\mathfrak{a} \subseteq \mathfrak{a}^2$. □

For the next theorem we have to state Nakayama's lemma first. It is a standard algebra tool, obtained from the theorem of Cayley-Hamilton and has many different versions and numerous applications. In his book "Commutative Algebra" [Mat80] H. Matsumura wrote "This simple but important lemma is due to T. Nakayama, G. Azumaya and W. Krull" describing this theorem. For the proof we refer to [AM69, pp. 21], [Mat80, p. 11] or [Stacks, Tag 00DV].

Lemma 3.3.3 (Nakayama)**.** *Let M be a finitely generated module over a local ring R. If $\mathfrak{m}M = M$ for the unique maximal ideal $\mathfrak{m} \subseteq R$, then $M = 0$.*

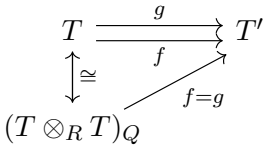
Theorem 3.3.4. *Let $(R, \mathfrak{m}, K)$ be a local ring and T a pointed étale extension. Denote $Q = \ker(T \otimes_R T \twoheadrightarrow K \otimes_K K \cong K)$. Then $(T \otimes_R T)_Q \cong T$ via the obvious map $(t \otimes t')/1 \mapsto tt'$.*

Moreover, assume T' is another pointed étale extensions of R. Then there is at most one local R-algebra homomorphism from T to T'.

Proof. It is clear that the map $\mu : T \otimes_R T \twoheadrightarrow T$ sends Q onto the maximal ideal of T. By the previous theorem, we see that for $\mathfrak{a} = \ker(T \otimes_R T \to T)$ we have $\mathfrak{a} = \mathfrak{a}^2$, since T is formally étale. Moreover, note that $\mathfrak{a}$ is finitely generated, since T is a localization of a finitely presented R-algebra. Let $\mathfrak{A} \coloneqq \mathfrak{a}(T \otimes_R T)_Q$ be the kernel of the map $(T \otimes_R T)_Q \twoheadrightarrow T$. Then $\mathfrak{A}$ is finitely generated (since $\mathfrak{a}$ is), contained in the maximal ideal (since $(T \otimes_R T)_Q$ is local) and $\mathfrak{A}^2 = \mathfrak{A}$. By Nakayama's lemma, for $M = \mathfrak{A}$, we obtain that $\mathfrak{A} = 0$ and therefore $(T \otimes_R T)_Q \cong T$. This verifies the first claim.

For the second part, suppose there are two local R-algebra maps $f, g : T \to T'$. Then there is an R-algebra homomorphism $T \otimes_R T \to T'$ that sends $t \otimes t' \mapsto f(t)g(t')$ and carries Q into the maximal ideal of T. Hence we have a local map $\psi : (T \otimes T)_Q \to T'$. Now the image of $t \otimes 1/1$ under ψ is given by $f(t)$ and the image of $1 \otimes t/1$ is of

course $g(t)$. However, we saw that $(T \otimes_R T)_Q \cong T$ and this isomorphism identifies $t \otimes 1/1 = t = 1 \otimes t/1$:



Hence $f(t) = g(t)$, and since this holds for any $t \in T$, we are done. □

Note that a simple corollary arises from this lemma, namely the fact that for some pointed étale T, the identity id: $T \to T$ is the only local R-algebra homomorphism from T to itself.

Now we are ready to state and prove a powerful theorem, connecting étale extensions and Henselian rings. Its statement and proof can be found in [Mil13] and [Hoc17]. We note that both use Theorem 3.2.9 and that we will follow the second reference.

Theorem 3.3.5. *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 $(\lambda_1, \ldots, \lambda) \in K^n$ 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, $r_i \equiv \lambda_i \mod \mathfrak{m}$ 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. In the special case of the ring of algebraic power series we have proved this fact in the first chapter when we derived Theorem 1.4.11 from Theorem 1.4.10. Now we will see that this equivalence holds in a more general setting. A common theme in the literature is to define Henselian rings with the condition (2) as above. However, it turns out that there is no known easy way to see the equivalence of (1) and (2): we will have to prove (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1) and use Theorem 3.2.9 on the way to establish it. Since (1) $\Rightarrow$ (2) is very simple, the reader-friendly approach is to do it like in this thesis.

Moreover, condition (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 this algebraic version of the this analytic theorem holds over this ring. For example, applying this equivalence for the ring of convergent power series yields that this ring is Henselian.

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 the image $\bar{f}$ mod $\mathfrak{m}$ has a simple root $\lambda \in K$. We may factor $\bar{f}(t) = (t-\lambda)\bar{g}(t)$. Since λ is a simple root, it follows that $\bar{g}(\lambda) \neq 0$ and therefore we obtain that the polynomials $t - \lambda$ and $\bar{g}(t)$ are relatively prime. Using that R is Henselian we find a lifting of the factorization to $f(t) = (t - r)g(t)$ for $r \equiv \lambda \mod \mathfrak{m}$. It follows that $f(r) = 0$, which shows (2).

(2) $\Rightarrow$ (3): Let $\phi : R \to T$ be a pointed étale extension, so a localization of an étale neighbourhood. By Theorem 3.2.9 it follows that the étale neighbourhood 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 invertible in T. We have the following commutative diagram:

$$\begin{array}{ccccccc} R & \hookrightarrow & R[t] & \longrightarrow & R[t]_g/(f) & \hookrightarrow & (R[t]_g/(f))_{\mathfrak{q}} \cong T \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ K & \hookrightarrow & K[t] & \longrightarrow & K[t]_{\bar{g}}/(\bar{f}) & \longrightarrow & K \end{array}$$

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 $h(t) \in R[t]$ such that $f(t) = (t - r)h(t)$ and $h(t)$ 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 all $\bar{f}_1, \ldots, \bar{f}_n$ and suppose that (3) holds. We want to lift the λ_i's and may use the fact R has no proper pointed étale extension. Let Q be the kernel of $\pi' : R[x_1, \ldots, x_n] \to K$, where we choose π' such that $\pi'(x_i) = \lambda_i$. We have the commutative diagram

$$\begin{array}{ccc} R & \hookrightarrow & R[x_1, \ldots, x_n] \\ & {\scriptstyle \pi} \searrow \quad \swarrow {\scriptstyle \pi'} & \\ & K & \end{array}$$

By Proposition 3.2.6 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. We can apply (3) to obtain that we must have that $R \cong T$.

Now, 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 maps 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 Theorem 3.3.4. 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 $g = \sum_{i=0}^{d} \alpha_i t^i$ and $h = \sum_{i=0}^{e} \beta_i t^i$ 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 $\bar{h}$, as explained in Appendix B. Since the polynomials are relatively prime by assumption, we obtain by the theory briefly discussed there 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 a unique factorization $f = gh$ we were looking for. $\square$

Having in mind that (1) $\Leftrightarrow$ (3) in the previous theorem, we come back to our goal of constructing the Henselization. We see that it may be a good idea to try to combine all possible pointed étale extensions of R into one bigger ring. If we can do this rigorously, then we might argue that this ring does not have any proper pointed étale extensions any more, 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, we have the following result bounds the cardinality of a pointed étale extension from above and allows us to define $\mathcal{R}$ properly.

Lemma 3.3.6. *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. Moreover, 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 $\mathcal{R} = (T_i)_{i \in \mathcal{A}}$.

Our goal is to define a suitable preorder $\leq$ on $\mathcal{A}$ and then prove that $\mathcal{R}$ together with some maps $\phi : T_i \to T_j$, $i, j \in \mathcal{A}$ fulfils all necessary properties in order to form a direct limit, see Appendix A.2. We will then call this limit R^{e} and prove that it is the Henselization of R. First we introduce and prove a proposition which assures the validity of the claims above.

Proposition 3.3.7. *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 3.2.4 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 and of course 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. □

Following the notions of Appendix A.2, 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 Theorem 3.3.4, we even 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 $R^{\mathrm{e}} \coloneqq \varinjlim_{T \in \mathcal{R}} T$.

Recall that in Theorem 3.3.5 we showed that a local ring is Henselian if and only if it has no proper pointed étale extensions. Now, 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 that R^{e} is Henselian and also the "smallest" extension of R that admits this property. We prove both statements below using ideas from [Ive73] and [Hoc17].

Lemma 3.3.8. *Let $(R, \mathfrak{m}, K)$ be a local ring. Then R^{e} is local with maximal ideal $\mathfrak{m}R$ and residue field is 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, see Lemma A.2.2 and [stacks?, Iversen].

By Theorem 3.3.5 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 $T' \coloneqq (T[t]/(f))_{\mathfrak{q}}$, 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 3.2.2 and Proposition 3.2.6. However, f has clearly 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 3.3.9. *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, by the property of the direct limit. Now, consider the commutative diagram of the base change:

$$\begin{array}{ccc} R & \xrightarrow{\text{étale}} & S \\ \downarrow{\scriptstyle \psi} & & \downarrow \\ H & \longrightarrow & S \otimes_R H \end{array}$$

Since $R \to S$ is étale, we obtain by Lemma 3.2.3 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) ⇒ (3) of Theorem 3.3.5 and therefore we found a local map $\phi : S \to (S \otimes_R H)_Q \cong H$, the map we were looking for:

$$\begin{array}{ccc} R & \xrightarrow{\text{étale}} & S \\ \downarrow{\scriptstyle \psi} & & \downarrow \\ H & \xrightarrow{\text{étale}} & S \otimes_R H \\ & \overset{\cong}{\searrow} & \downarrow \\ & & (S \otimes_R H)_Q \end{array}$$

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 Theorem 3.3.4. $\square$

This theorem does not only ensure that the Henselization of a local ring exists, but shows that it comes with a construction as a direct limit of pointed étale extensions of the ring. This fact concludes the chapter on étale algebras and brings us to the next section where we shall exploit it extensively.

Chapter 4

Explicit Implications

"The museum is always big, and you are always small, an art historian told me."
Nora Schultz, *Proposal*, Secession, Vienna, 2019

In this chapter we will study explicit facts about the ring of algebraic power series by applying the theorems we proved. The ring $R = K[x]_{(x)}$ is now fixed, where $x = (x_1, \ldots, x_n)$ and K a field of characteristic zero.

We have seen in Theorem 2.2.6 that if the Henselization of R exists, then it must be equal to $K\langle x\rangle$. In the previous chapter, we constructed R^{h} and not only proved its existence, but also the fact that it is given as the direct limit of pointed étale extensions of R (Theorem 3.3.9). Now we will be able to apply this fact, proving a theorem of Denef and Lipshitz from 1987 in [DL87]. Then we will use it in two ways: on the one hand, we present a new result, Theorem 4.1.2, improving the so-called Artin-Mazur lemma and on the other hand, explain another theorem by Denef and Lipshitz about the representation of algebraic power series as diagonals of rational series.

Definition. An algebraic power series $h(x) \in K\langle x_1, \ldots, x_n\rangle = K\langle x\rangle$ with minimal polynomial $P(x,t) \in K[x,t]$ is called étale-algebraic if $h(0) = 0$ and $\partial_t P(0,0) \neq 0$.

Theorem 4.0.1 (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 $0 \leq i \leq r$, $0 \leq j \leq s$, $r, s \in \mathbb{N}$, where $b_0(0) \neq 0$, such that*

$$f = \frac{a_0 + a_1 h + \cdots + a_r h^r}{b_0 + b_1 h + \cdots + b_s h^s}. \tag{4.1}$$

Proof. 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 $R = K[x]_{(x)}$ 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 3.2.9 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. Writing the right hand side differently, gives the isomorphism

$$\tilde{\alpha} : S_b \xrightarrow{\cong} \left(R[t]/(\tilde{P})\right)_{\tilde{g}},$$

for some $\tilde{P} \in R[t]$ such that $\tilde{P}' \notin \tilde{\alpha}(\mathfrak{q})$ and $\tilde{g} \in R[t]/(\tilde{P})$ with $\tilde{g} \notin \alpha(\mathfrak{q})$ Furthermore, localizing in $\mathfrak{q}$ and $\tilde{\alpha}(\mathfrak{q})$, respectively, yields

$$T \cong \left(R[t]/(\tilde{P})\right)_{\tilde{\alpha}(\mathfrak{q})}.$$

Finally, we can rephrase the isomorphism above as

$$T \cong \left(R[\tilde{h}]\right)_{\tilde{\alpha}(\mathfrak{q})},$$

where $\tilde{h} \in \widehat{R} = K[\![x]\!]$ is an algebraic element over R whose minimal polynomial is exactly $\tilde{P}$. In fact, it has to hold $\tilde{P}' \notin \tilde{\alpha}(\mathfrak{q})$ and therefore $\partial_t \tilde{P}(0, \tilde{h}(0)) \neq 0$. Now, any element $f \in T \cong \left(R[\tilde{h}]\right)_{\tilde{\alpha}(\mathfrak{q})}$ is of the form a/b, for $a, b \in R[\tilde{h}]$ and $b \notin \tilde{\alpha}(\mathfrak{q})$, hence we have

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

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

4.1 Codes of Algebraic Power Series

The following fact was explained in [AM65, pp. 88] and became later known under the name Artin-Mazur lemma (see for example [BCR98] or [AMR92]).

Theorem 4.1.1 (Artin & Mazur)**.** *Let $f \in K\langle x_1, \ldots, x_n\rangle = K\langle x\rangle$ be an algebraic power series with $f(0) = 0$. Then there exists an $k \in \mathbb{N}$ and a vector of k polynomials $P(x, y_1, \ldots, y_k) \in K[x][y_1, \ldots, y_k]^k$ with the following properties:*

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

(2) The Jacobian matrix $J_P(x, y_1, \ldots, y_k)$ of $P(x, y_1, \ldots, y_n)$ with respect to the variables $y_1, \ldots, y_k$ at $x = y = 0$ is invertible: $J_P(0,0) \in GL_k(K)$.

In other words, given $f(x) \in K\langle x\rangle$, one can find $k-1$ algebraic power series $h_2, \ldots, h_k \in K\langle x\rangle$ and a k-dimensional vector of polynomials $P(x, y_1, \ldots, y_k) \in K[x, y]^k$, such that $P(x, f(x), h_2(x), \ldots, h_k(x)) = 0$ and the Jacobian of $P(x, y)$ with respect to y at $x = y = 0$ is invertible. Similarly to the previous theorem, this implies that one can repair the problem of an algebraic power series of not being étale-algebraic, now by appending $k-1$ other 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 *the (mother) code of the algebraic series* $f(x)$ in [ACH14],[Hau17] and [AMR92]. The authors M.E. Alonso, F.J. Castro-Jimenez and H. 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 the Artin-Mazur lemma, proving that it is always possible to choose $k = 2$:

Theorem 4.1.2. *Let $f \in K\langle x_1, \ldots, x_n\rangle = K\langle x\rangle$ 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: $J_P(0, 0, 0) \in GL_2(K)$.

Note that in the two-dimensional square matrix $J_P(0, 0, 0)$, the first 0 means setting the variables $x_1, \ldots, x_n$ 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 $P(x, y_1, y_2) = (Q(x, y_1), y_2)$ to get $P(x, f(x), 0) = 0$ and, of course,

$$J_P(0, 0, 0) = \begin{pmatrix} \partial_{y_1} Q(0, 0) & 0 \\ 0 & 1 \end{pmatrix}$$

has $\det(J_P(0, 0, 0)) = \partial_{y_1} Q(0, 0) \neq 0$. Hence, we are done in this case.

We are left with the more challenging case $\partial_{y_1} Q(0, 0) = 0$. By the previous Theorem 4.0.1, we may write for some étale-algebraic power series $h \in K\langle x\rangle$

$$f = \frac{a_0 + a_1 h + \cdots + a_r h^r}{b_0 + b_1 h + \cdots + b_s h^s}, \tag{4.2}$$

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

$$T_1(x, y_2) \coloneqq a_0(x) + a_1(x) y_2 + \cdots + a_r(x) y_2^r,$$
$$T_2(x, y_2) \coloneqq b_0(x) + b_1(x) y_2 + \cdots + b_s(x) y_2^s,$$

to get the relationship $T_1(x, h(x)) = f(x)T_2(x, h(x))$ from identity (4.2). Let also $S(x, y_2)$ be the minimal polynomial of the étale-algebraic $h(x)$, so $\partial_{y_2} S(0, 0) \neq 0$. 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 and so we are done. □

4.2 Representation of Algebraic Power Series as Diagonals

Recall that if not indicated otherwise, $x = (x_1, \ldots, x_n)$ is a vector of n variables and $t = t$ is a single variable. We define the diagonal of a power series as follows:

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

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

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

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

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

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

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-dimensional and $f(x, t) = 1/(1 - x - t)$. Then

$$\mathcal{D}(f(x,t))(x) = \mathcal{D}\Big(\frac{1}{1-x-t}\Big)(x) = \mathcal{D}\left(\sum_{k\geq 0}(x+t)^k\right)(x)$$
$$= \sum_{k\geq 0} \mathcal{D}\left((x+t)^k\right)(x) = \sum_{k\geq 0}\sum_{j\geq 0} \binom{k}{j} \mathcal{D}\left(x^j t^{k-j}\right)(x).$$

However, in order to have $\mathcal{D}(x^j t^{k-j})(x) \neq 0$, we must have $j = k - j$, i.e. $j = k/2$, and in particular k must be even, say $k = 2n$. In this case, $\mathcal{D}(x^j t^{k-j})(x) = x^{k/2}$ and we obtain:

$$\mathcal{D}(f(x,t))(x) = \sum_{n \geq 0} \binom{2n}{n} x^n = \frac{1}{\sqrt{1-4x}}.$$

This function is an algebraic power series with minimal polynomial

$$P(x,t) = t^2 - 4xt^2 - 1.$$

Example 2: Recall that $xt \coloneqq (x_1 t, \ldots, x_n t)$. For any $f(x) = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha \in K[\![x]\!] \subseteq K[\![x,t]\!]$ it holds that

$$\begin{aligned}
\mathcal{D}\left(f(xt)\right)(x) &= \sum_{\alpha \in \mathbb{N}^n} c_\alpha \mathcal{D}\left((x_1 t)^{\alpha_1} \cdots (x_n t)^{\alpha_n}\right)(x) \\
&= \sum_{\alpha \in \mathbb{N}^n} c_\alpha \mathcal{D}\left(x^\alpha t^{\alpha_1 + \cdots + \alpha_n}\right)(x) \\
&= \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha = f(x).
\end{aligned}$$

Hence we may represent $f(x)$ as the diagonal of $f(xt)$.

Example 3: Define the Hadamard product of two power series $f(x) = \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha$ and $g(x) = \sum_{\alpha \in \mathbb{N}^n} g_\alpha x^\alpha$ as the series

$$(f * g)(x) = \sum_{\alpha \in \mathbb{N}} f_\alpha g_\alpha x^\alpha.$$

Let $x = x_1$ be one-dimensional and $f(x,t) = \sum_{i,j \geq 0} c_{i,j} x^i t^j$. Define $D \coloneqq \{(i,j) \in \mathbb{N}^2 : i = j\}$ and its indicator function $\mathbb{1}_D : \mathbb{N}^2 \to \{0,1\}$, then we obtain:

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

the diagonal of $f(x,t)$, where one substituted xt into x. This gives another view point on the diagonal operator. There is a generalization of this idea to a multidimensional x, but we shall not examine it here.

Example 4: [1] Consider the well-known transcendental G-function

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

[1] This example is taken from [AB13].

This series appears in Apéry's proof of the irrationality of $\zeta(3)$. It also known to satisfy a Picard-Fuchs differential equation. Furthermore, a lengthy but simple computation shows that $f(t)$ is the small diagonal of the rational power series

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

There are many theorems in the literature connecting algebraic power series and diagonals. For example, in 1922 Pólya proved that the diagonal of any rational power series in two variables is necessarily algebraic. Fürstenberg proved in 1967 that if $f(x)$ is an algebraic power series and $x = x_1$ one-dimensional, then there exists a rational power series $R(x,t)$ with $\mathcal{D}(R(x,t)) = f(x)$ [Fur67]. In the same paper, he proved that a small diagonal of any rational power series over a finite field is algebraic. In 1984, Deligne improved the second result: the small diagonal of any *algebraic* power series over a finite field is algebraic [Del84]. Note that for fields of characteristic 0 neither Deligne's nor Fürstenberg's statements hold, as it is evident from example 4 above. Denef and Lipshitz gave a simpler proof for the last statement in 1987 and generalized the first theorem of Fürstenberg to several variables in [DL87]. This generalization uses the fact that $K\langle x\rangle$ is given by a direct limit of pointed étale extensions of $K[x]_{(x)}$ and we will present its proof now. However, we need the following technical lemma first:

Lemma 4.2.1. *Let $h(x)\in K\langle x\rangle$ be étale-algebraic with minimal polynomial $P(x,t)\in K[x,t]$. Then it holds that:*

(1) The following rational function is a power series:

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

(2) If $i\in\mathbb{N}^n$ and $j\in\mathbb{N}$, then

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

(3) More generally, if $W(x,t)\in K[\![x,t]\!]$ is a power series, then

$$\mathcal{D}\Big(W(xt,t)t\frac{\partial_t P(xt,t)}{P(xt,t)}\Big)=W(x,h(x)).$$

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

$$\partial_t P(x,t)=Q(x,t)+(t-h(x))\partial_t Q(x,t), \tag{4.3}$$

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

$$t\frac{\partial_t P(x,t)}{P(x,t)}=\frac{t}{t-h(x)}+t\frac{\partial_t Q(x,t)}{Q(x,t)}. \tag{4.4}$$

Plugging $(0,0)$ into (4.3) and using the assumptions on $P(x,t)$ and $h(x)$, we get that $Q(0,0) \neq 0$, therefore $Q(x,t)$ is a unit in $K[\![x,t]\!]$ and so the second summand in the equation above is a power series. Furthermore, we have

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

We conclude the proof of (1) by putting together:

$$t\frac{\partial_t P(xt,t)}{P(x,t)} = \underbrace{\frac{t}{t-h(xt)}}_{\in K[\![x,t]\!]} + t\,\underbrace{\frac{\partial_t Q(xt,t)}{Q(xt,t)}}_{\in K[\![x,t]\!]}.$$

For (2) we use that $\mathcal{D}$ is linear and (4.4) to arrive at

$$\begin{aligned}\mathcal{D}\Big((xt)^i t^{j+1}\frac{\partial_t P(xt,t)}{P(xt,t)}\Big) &= \mathcal{D}\Big(\frac{(xt)^i t^{j+1}}{t-h(xt)} + (xt)^i t^{j+1}\frac{\partial_t Q(xt,t)}{Q(xt,t)}\Big)\\ &= \mathcal{D}\Big(\frac{(xt)^i t^{j+1}}{t-h(xt)}\Big) + \mathcal{D}\Big((xt)^i t^{j+1}\frac{\partial_t Q(xt,t)}{Q(xt,t)}\Big).\end{aligned}$$

The second summand is equal to 0, since the degree of t is always strictly larger then the sum of the corresponding degrees of the x_i's. Thus, it remains to compute

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

This proves also the second part of the lemma.
For (3) let $W(x,t) = \sum_{i,j\in\mathbb{N}^n\times\mathbb{N}} a_{i,j}x^i t^j$. A simple computation using (2) yields:

$$\begin{aligned}\mathcal{D}\Big(W(xt,t)t\frac{\partial_t P(xt,t)}{P(xt,t)}\Big) &= \mathcal{D}\Big(\sum_{i,j\in\mathbb{N}^n\times\mathbb{N}} a_{i,j}(xt)^i t^j t\frac{\partial_t P(xt,t)}{P(xt,t)}\Big)\\ &= \sum_{i,j\in\mathbb{N}^n\times\mathbb{N}} a_{i,j}\mathcal{D}\Big((xt)^i t^{j+1}\frac{\partial_t P(xt,t)}{P(xt,t)}\Big)\\ &= \sum_{i,j\in\mathbb{N}^n\times\mathbb{N}} a_{i,j}x^i h(x)^j\\ &= W(x,h(x)).\end{aligned}$$

□

Now we are ready to prove the theorem of Denef and Lipshitz:

Theorem 4.2.2. *Let $f(x) \in K\langle x\rangle$ be an algebraic power series, $x = (x_1,\ldots,x_n)$ and K a field of characteristic 0. Then there exists a rational power series in $n+1$ variables $R(x,t) \in K[x,t]_{(x,t)}$ such that*

$$f(x) = \mathcal{D}(R(x,t)).$$

Proof. Using Theorem 4.0.1, it follows that there exist $r, s \in \mathbb{N}$ and $a_i(x), b_j(x) \in K[x]$ for $0 \leq i \leq r$, $0 \leq j \leq s$ with $b_0(0) \neq 0$ such that

$$f(x) = \frac{a_0(x) + a_1(x)h(x) + \cdots + a_r(x)h(x)^r}{b_0(x) + b_1(x)h(x) + \cdots + b_s(x)h(x)^s}, \tag{4.5}$$

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

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

and let

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

From part (1) in the previous lemma, we know that $R(x,t)$ is a rational power series. Therefore, $R(x,t) \in K[x,t]_{(x,t)}$ and we conclude using part (3) from that lemma:

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

This is exactly what we wanted. □

Appendix A

Direct and Inverse Limits

"No one is ever satisfied where he is."
Antoine de Saint-Exupéry, *The Little Prince*, Chapter 22

The direct and the inverse limits are important algebraic tools that can be used for creating new algebraic structures such as groups, rings or modules from a collection of existing ones. To form these objects, we will need the definition of a directed set:

Definition. A directed set is a non-empty set $\mathcal{A}$ together with a reflexive and transitive binary relation $\leq$, with the additional property that every pair of elements has a common upper bound.

Recall that $\leq$ is reflexive if $i \leq i$ for all $i \in \mathcal{A}$, it is transitive if $i \leq j$ and $j \leq k$ for some $i, j, k \in \mathcal{A}$ implies that $i \leq k$. Finally, the condition on the upper bound means that for any pair $i, j \in \mathcal{A}$ there exists a $k \in \mathcal{A}$ such that $i \leq k$ and $j \leq k$.

A.1 Inverse Limit and the Completion

Definition. Let $(\mathcal{A}, \leq)$ be a directed set. By an inverse system of rings over $(\mathcal{A}, \leq)$ we mean a pair

$$(\{R_i\}_{i\in\mathcal{A}}, \{f_{i,j} : R_j \to R_i\}_{i,j\in\mathcal{A}, i\leq j}),$$

where each R_i is a ring and the $f_{i,j}$ are ring homomorphisms satisfying $f_{i,i} = \mathrm{id}_{R_i}$ and $f_{i,k} = f_{i,j} \circ f_{j,k}$ for all $i, j, k \in \mathcal{A}$ with $i \leq j \leq k$.

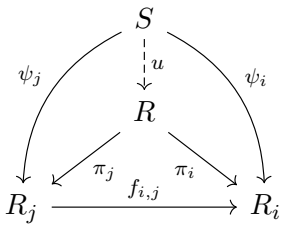
Now we are ready to define the inverse limit:

Definition. Given a directed set $(\mathcal{A}, \leq)$ and an inverse system of rings like above, we define the inverse limit of this system to be the pair

$$(R, \{\pi_i : R \to R_i\}_{i\in\mathcal{A}}),$$

where R is a ring and the π_i are homomorphisms satisfying $f_{i,j} \circ \pi_j = \pi_i$ for all $i \leq j$. Moreover, we require the pair $(R, \{\pi_i\}_{i\in\mathcal{A}})$ to be universal in the sense that for any other pair $(S, \{\psi_i\}_{i\in\mathcal{A}})$ satisfying all above, there exists a unique morphism $u : S \to R$ such that $\pi_i \circ u = \psi_i$ for all $i \in \mathcal{A}$.

The universal condition above implies the existence of a unique $u : S \to R$ such that the following diagram commutes:



Of course, the universal property also implies uniqueness of the inverse limit. The inverse limit is often denoted by $\varprojlim R_i$ with the underlying inverse system $(\{R_i\}, \{f_{i,j}\})$ being understood. For the existence and the explicit description we have the following theorem identifying $\varprojlim R_i$ with a subring of $\prod_{i\in\mathcal{A}} R_i$, see [Bou89, pp. 118]:

Theorem A.1.1. *Let $(\{R_i\}, \{f_{i,j}\})$ be an inverse system of rings. Then*

$$R = \varprojlim R_i = \Big\{ a \in \prod_{i\in\mathcal{A}} R_i \,\Big|\, a_i = f_{i,j}(a_j) \text{ for all } i, j \in \mathcal{A} \text{ and } i \leq j \Big\}.$$

The maps $\pi_i : R \to R_i$ are the natural projections which pick the i-th component of the direct product for each $i \in \mathcal{A}$.

The following fact is easy to prove and we use it at some point. It gives a good flavour of the work style with inverse systems and limits.

Lemma A.1.2. *Assume $\{A_n\}_{n\geq 1}$ and $\{B_n\}_{n\geq 1}$ are inverse systems of rings and $A_n \subseteq B_n$ for every n. Then $\varprojlim A_n =: A \subseteq B := \varprojlim B_n$.*

Proof. For every n we have an injective map $A_n \hookrightarrow B_n$ describing the inclusion, hence we have a natural map $A \to B$ and we want it to be injective as well. Consider the commutative diagram which exists for every n:

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A_n & \hookrightarrow & B_n \end{array}$$

Take $f \in \ker(A \to B)$. Then f maps to 0 in B, which then projects to 0 in every B_n. Call f_n the image of f in A_n. As $A_n \hookrightarrow B_n$ maps f_n to 0 and is injective we obtain that $f_n = 0$ for every n. But then $f = 0$, because $A = \varprojlim A_n$. This shows that $A \hookrightarrow B$ is injective and proves the claim. □

We use the notion of the inverse limit mostly for defining the $\mathfrak{m}$-adic completion of a local ring R at the maximal ideal $\mathfrak{m} \subseteq R$ and we will follow [Eis95]. In order to define the completion, we take the directed set $(\mathbb{N}, \leq)$ with the usual $\leq$. Then, after defining $R_i := R/\mathfrak{m}^i$, we see that one has obvious projections

$$f_{i,j} : R/\mathfrak{m}^j \to R/\mathfrak{m}^i, \text{ for } j \geq i,$$

because $\mathfrak{m}^j \subseteq \mathfrak{m}^i$ for a pair i, j like above. Since the $f_{i,j}$'s are projections, it follows that $(\{R_i\}_{i\in\mathbb{N}}, \{f_{i,j} : R_j \to R_i\}_{i,j\in\mathbb{N}, i\leq j})$ is an inverse system of rings and we may

form an inverse limit. Then, we set $\widehat{R} \coloneqq \varprojlim R_i = \varprojlim R/\mathfrak{m}^i$. This object is called the $\mathfrak{m}$-*adic completion of* R.
From Theorem A.1.1 we immediately get the description of $\widehat{R}$ in terms of sequences:

$$\widehat{R} = \{a = (a_1, a_2, \dots) \in \prod_{i \geq 1} R/\mathfrak{m}^i : a_i \equiv a_j \mod \mathfrak{m}^i, \text{ for all } j > i\}.$$

Defining

$$\widehat{\mathfrak{m}^i} = \{a = (a_1, a_2, \dots) \in \widehat{R} : a_j = 0 \text{ for all } j \leq i\},$$

it follows from the definition that $\widehat{R}/\widehat{\mathfrak{m}^i} \cong R/\mathfrak{m}^i$. We claim that $\widehat{R}$ is local with maximal ideal $\widehat{\mathfrak{m}} \coloneqq \widehat{\mathfrak{m}^1}$: If $a = (a_1, a_2, \dots) \in \widehat{R} \setminus \widehat{\mathfrak{m}}$, it follows easily that $b = (a_1^{-1}, a_2^{-1}, \dots)$ exists and is the inverse of a, proving the claim. To explain the term "complete" we need to talk a little bit topology: we say that a sequence of elements $a_1, a_2, \dots \in \widehat{R}$ converges to an $a \in \widehat{R}$ if for every integer n there is an integer $i(n)$ so that $a - a_{i(n)} \in \widehat{\mathfrak{m}^n}$. It follows that a sequence $(a_i)_{i \geq 1}$ of elements of $\widehat{R}$ converges if and only if it is a Cauchy sequence, in the sense that for every integer n there is an integer $i(n)$ such that

$$a_i - a_j \in \widehat{\mathfrak{m}^n} \text{ for all } i, j \geq i(n).$$

The limit of a convergent sequence $(a_i)_{i \geq 1}$ is given by the element $a \in \prod_i R/\mathfrak{m}^i = \widehat{R}$ whose n-th component is the same as that of $a_{i(n)}$. Then we write $a = \lim_i a_i$. Because the $\widehat{\mathfrak{m}^i}$ are ideals, it follows that addition and multiplication are continuous in $\widehat{R}$, in the sense that if $a = \lim a_i$ and $b = \lim b_i$ then both $a_i + b_i$ and $a_i b_i$ are convergent sequences, which converge to $a + b$ and ab respectively.

We say a local ring R with maximal ideal $\mathfrak{m}$ is complete if the natural map $R \to \widehat{R}$ is an isomorphism. Note that $\cap_i \mathfrak{m}^i$ goes to zero under this mapping, therefore completeness implies $\cap_i \mathfrak{m}^i = 0$. Because of Krull's intersection theorem, we see that the completion of a Noetherian ring is indeed complete.

Finally we note that all these definitions and results are very natural: taking for an element $a \in \widehat{R}$ the sets $(a + \widehat{m^i})_{i \geq 1}$ to be the base of open neighbourhoods of a, one arrives at the so-called Krull topology, in which our definition of Cauchy sequences agrees with the usual one.

The following facts about the completion of rings are of importance for this work and also interesting on their own. First we give a detailed proof of Hensel's lemma:

Theorem A.1.3 (Hensel's lemma)**.** *Let $(R, \mathfrak{m}, K)$ be a complete local ring and $f(t) \in R[t]$ a monic polynomial of degree $n \geq 1$. Denote $\bar{f}(t) \in K[t]$ to be the reduction of $f(t) \mod \mathfrak{m}R[t]$ and suppose there exist monic coprime polynomials $G(t), H(t) \in K[t]$ of degrees $d, e \geq 0$ respectively such that*

$$\bar{f}(t) = G(t)H(t).$$

Then there exist unique monic polynomials $g(t), h(t) \in R[t]$ of degrees e and d such that $g(t) \equiv G(t) \mod \mathfrak{m}R[t]$, $h(t) \equiv H(t) \mod \mathfrak{m}R[t]$ and $f(t) = g(t)h(t)$.

Proof. In order to simplify notation in this proof, we will drop the variable t, when referring to $f, g, h \in R[t]$, $G, H \in K[t]$ and other polynomials still to appear. Moreover, we denote $\mathfrak{m}^i[t] \coloneqq \mathfrak{m}^i R[t]$.

The idea of the proof is to construct by induction unique monic polynomials $g_i, h_i \in R[t]$ such that $f \equiv g_i h_i \mod \mathfrak{m}^i[t]$ for all $i \geq 1$, such that $g_i \equiv G \mod \mathfrak{m}[t]$

and $h_i \equiv H \bmod \mathfrak{m}[t]$. Then, we will prove that $\lim_i g_i =: g$ and $\lim_i h_i =: h$ satisfy the requested properties and are unique.

The induction basis is done immediately by the hypothesis of the theorem: we can choose $g_1 = G$ and $h_1 = H$, then obviously $g_1 \equiv G \bmod \mathfrak{m}[t]$, $h_1 \equiv H \bmod \mathfrak{m}[t]$ and $f \equiv g_1 h_1 \bmod \mathfrak{m}[t]$. Note that this choice is of course unique and the degrees of these polynomials are d and e.

Now assume that g_k and h_k have been constructed and shown to be unique for some $k \geq 1$. We must construct g_{k+1} and h_{k+1} and prove their uniqueness. We will do this by finding $\gamma, \eta \in \mathfrak{m}^k[t]$ of degrees less than d and e such that $g_{k+1} \coloneqq g_k + \gamma$ and $h_{k+1} \coloneqq h_k + \eta$ satisfy the necessary properties. Since G, H are coprime, they generate the unit ideal in $K[t]$. Therefore, there exist polynomials $\tilde{\gamma}, \tilde{\eta} \in K[t]$ with

$$1 = \tilde{\eta} G + \tilde{\gamma} H \equiv \tilde{\eta} g_k + \tilde{\gamma} h_k \mod \mathfrak{m}[t].$$

By the induction hypothesis, we have $\Delta \coloneqq f - g_k h_k \in \mathfrak{m}^k[t]$. Multiplying the equation above with Δ yields $\Delta \equiv \Delta\tilde{\eta} g_k + \Delta\tilde{\gamma} h_k \bmod \mathfrak{m}^{k+1}[t]$. Now we are nearly done, however $\Delta\tilde{\eta}$ and $\Delta\tilde{\gamma}$ may have incorrect degrees. Therefore, we apply the division algorithm dividing $\Delta\tilde{\eta} \in \mathfrak{m}^k[t]$ by $h_k \in R[t]$ which is monic by assumption. This gives us $\alpha, \eta \in R[t]$ with $\deg(\eta) < e$ and $\Delta\tilde{\eta} = \alpha h_k + \eta$. We claim that $\alpha, \eta \in \mathfrak{m}^k[t]$. To see this note that we must have $0 \equiv \alpha h_k + \eta \bmod \mathfrak{m}^k[t]$ since $\Delta\tilde{\eta} \in \mathfrak{m}^k[t]$. Moreover, $h_k \in (R/\mathfrak{m}^k)[t]$ is monic of degree e, therefore by uniqueness of the division algorithm in $(R/\mathfrak{m}^k)[t]$ we obtain the validity of the claim. Now, we are ready to set $\gamma = \alpha g_k + \Delta\tilde{\gamma} \in \mathfrak{m}^k[t]$ and to obtain

$$\eta g_k + \gamma h_k = (\Delta\tilde{\eta} - \alpha h_k) g_k + (\alpha g_k + \Delta\tilde{\gamma}) h_k = \Delta\tilde{\eta} g_k + \Delta\tilde{\gamma} h_k \equiv \Delta \mod \mathfrak{m}^{k+1}[t].$$

Since $\deg(\Delta) < n$ and $\deg(\eta g_k) < n$, it follows that the degree of γ is smaller than d. Finally, setting $g_{k+1} = g_k + \gamma$, $h_{k+1} = h_k + \eta$, we convince ourselves that $g_{k+1} \equiv G \bmod \mathfrak{m}[t]$, $h_{k+1} \equiv H \bmod \mathfrak{m}[t]$ and calculate $\bmod \mathfrak{m}^{k+1}[t]$:

$$\begin{aligned} g_{k+1} h_{k+1} &\equiv g_k h_k + h_k \gamma + g_k \eta + \gamma\eta \\ &\equiv g_k h_k + \Delta \\ &\equiv f. \end{aligned}$$

This proves the existence of $g_i, h_i \in R[t]$ for all $i \geq 0$ with the wanted properties. To see uniqueness, we again argue by induction. For $k = 1$, we have already seen that g_1, h_1 are unique. Assume the obtained g_i, h_i are unique up to some $k \geq 1$ and let $g', h' \in R[t]$ be monic polynomials of degrees d, e such that $g' \equiv G \bmod \mathfrak{m}[t]$, $h' \equiv H \bmod \mathfrak{m}[t]$ and $f \equiv g'h' \bmod \mathfrak{m}^{k+1}[t]$. Define $\gamma' = g' - g_k$ and $\eta' = h' - h_k$. By the induction hypothesis we get that $\gamma', \eta' \in \mathfrak{m}^k[t]$. Then it follows easily that we must have

$$\eta' g_k + \gamma' h_k \equiv \Delta \mod \mathfrak{m}^{k+1}[t].$$

Now set $\hat{\gamma} = \gamma - \gamma' = g_{k+1} - g'$ and $\hat{\eta} = \eta - \eta' = h_{k+1} - h'$. It follows that $0 \equiv \hat{\eta} g_k + \hat{\gamma} h_k \bmod \mathfrak{m}^{k+1}[t]$. Multiplying by $\tilde{\gamma}$ and using the fact that $\tilde{\gamma} g_k + \tilde{\gamma} h_k - 1 =: m \in \mathfrak{m}[t]$, we have

$$\hat{\eta} \equiv (\hat{\eta}\tilde{\eta} - \tilde{\gamma}\hat{\gamma}) h_k - \hat{\eta} m \mod \mathfrak{m}^{k+1}[t].$$

However, $\hat{\eta} \in \mathfrak{m}^k[t]$ and $m \in \mathfrak{m}[t]$, therefore $\hat{\eta}$ must be a multiple of h_k in $(R/\mathfrak{m}^{k+1})[t]$. But $\deg(\hat{\eta}) < e$ and $\deg(h_k) = e$, hence $\hat{\eta} \equiv 0 \bmod \mathfrak{m}^{k+1}[t]$ and similarly $\hat{\gamma} \in \mathfrak{m}^{k+1}[t]$.

It follows that

$$h' \equiv h_{k+1} \mod \mathfrak{m}^{k+1},$$
$$g' \equiv g_{k+1} \mod \mathfrak{m}^{k+1},$$

which concludes the proof of uniqueness of g_i, h_i for every $i \geq 1$.

Now, if $1 \leq i < j$ then $f - g_j h_j \in \mathfrak{m}^j[t] \subseteq \mathfrak{m}^i[t]$, so $f \equiv g_j h_j \mod \mathfrak{m}^i[t]$. By uniqueness, it follows that $g_i \equiv g_j \mod \mathfrak{m}^i[x]$ and $h_i \equiv h_j \mod \mathfrak{m}^i[x]$. Looking at the coefficients of the polynomials, this implies that the sequences of those are Cauchy and therefore converge in R, because it is a complete ring by assumption. Set

$$g \coloneqq \lim_{i\geq 1} g_i = \lim_{i\geq 1} a_0^{(i)} + a_1^{(i)} t + \cdots + a_{d-1}^{(i)} t^{d-1} + t^d =: a_0 + a_1 + \cdots + a_{d-1} t^{d-1} + t^d,$$
$$h \coloneqq \lim_{i\geq 1} h_i = \lim_{i\geq 1} b_0^{(i)} + b_1^{(i)} t + \cdots + b_{d-1}^{(i)} t^{e-1} + t^e =: b_0 + b_1 + \cdots + b_{d-1} t^{e-1} + t^e.$$

It is easy to see that $g \equiv G \mod \mathfrak{m}[t]$ and $h \equiv H \mod \mathfrak{m}[t]$. A small straightforward computation also verifies that $(g_i h_i)_j \to (gh)_j$ for every $0 \leq j \leq n-1$ as $i \to \infty$. However

$$f_j - (gh)_j = f_j - (g_i h_i)_j + (g_i h_i)_j - (gh)_j,$$

and $f_j - (g_i h_i)_j \in \mathfrak{m}^i$ by construction. It follows that $f_j - (gh)_j \in \cap_k \mathfrak{m}^k = 0$, by the considerations about complete rings. We see that all coefficients of f and gh agree and conclude that the polynomials are equal. □

Lemma A.1.4. *Let R be a Noetherian local ring. Then $\widehat{R}$ is also Noetherian.*

See [Eis95, p. 185] for a proof.

Lemma A.1.5. *Let R be a local Noetherian ring and M a ring that is a finite R-module. Then the completion of M is given by $M \otimes_R \widehat{R}$.*

The proof can be found in [Nag75] or [Stacks, Tag 00MA]

Lemma A.1.6. *Let R be a local Noetherian ring and $\widehat{R}$ its completion. Then the map $R \to \widehat{R}$ is flat. If R is a domain then $\mathrm{Frac}(R) \cap \widehat{R} = R$.*

For the first statement see [Stacks, Tag 00MB]. The second one follows from [Nag75, (18.4)].

A.2 Direct Limit

Definition. Let $(\mathcal{A}, \leq)$ be a directed set. By a direct system of rings over $(\mathcal{A}, \leq)$ we mean a pair

$$(\{R_i\}_{i\in\mathcal{A}}, \{f_{i,j} : R_i \to R_j\}_{i,j\in\mathcal{A}, i\leq j}),$$

where each R_i is a ring and the $f_{i,j}$ are ring homomorphisms satisfying $f_{i,i} = \mathrm{id}_{R_i}$ and $f_{i,k} = f_{j,k} \circ f_{i,j}$ for all $i, j, k \in \mathcal{A}$ with $i \leq j \leq k$.

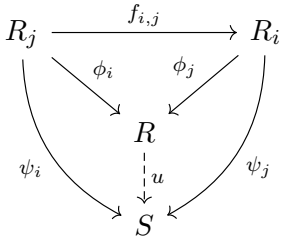
Now we are ready to define the direct limit:

Definition. Given a directed set $(\mathcal{A}, \leq)$ and a direct system of rings like above, we define the direct limit of this system to be the pair

$$(R, \{\phi_i : R_i \to R\}_{i \in \mathcal{A}}),$$

where R is a ring and the ϕ_i are homomorphisms satisfying $\phi_j \circ f_{i,j} = \phi_i$ for all $i \leq j$. Moreover, we require the pair $(R, \{\phi_i\}_{i \in \mathcal{A}})$ to be universal in the sense that for any other pair $(S, \{\psi_i\}_{i \in \mathcal{A}})$ satisfying all above, there exists a unique morphism $u : R \to S$ such that $u \circ \phi_i = \psi_i$ for all $i \in \mathcal{A}$.

The universal condition above implies the existence of a unique $u : R \to S$ such that the following diagram commutes:



Note that this is the same commutative diagram as for the inverse limit, but with all arrows reversed. Of course, the universal property again also implies uniqueness of the direct limit. The direct limit is often denoted by $\varinjlim R_i$ with the underlying direct system $(\{R_i\}, \{f_{i,j}\})$ being understood. For the existence and the explicit description we have the following theorem identifying $\varinjlim R_i$ with the disjoint union $\bigsqcup_{i \in \mathcal{A}} R_i$ modulo an equivalence relation, see [Bou89, pp. 120]:

Theorem A.2.1. *Let $(\{R_i\}, \{f_{i,j}\})$ be a direct system of rings. Then*

$$R = \varinjlim R_i = \bigsqcup_{i \in \mathcal{A}} R_i \Big/ \sim,$$

where for $x_i \in R_i$ and $x_j \in R_j$ we say $x_i \sim x_j$ if and only if there exists some $k \in \mathcal{A}$ with $i \leq k$ and $j \leq k$ and $f_{i,k}(x_i) = f_{j,k}(x_j)$. The maps $\phi_i : R_i \to R$ are obtained canonically by sending each element to its equivalence class.

In other words, an element is equivalent to all its images under the maps of the direct system, i.e. $x_i \sim f_{ij}(x_i)$ whenever $i \leq j$.

When talking about the direct limit of pointed étale extensions, while constructing the Henselization, we use the following lemma. Its proof is a good example on how one deals with the defined object.

Lemma A.2.2. *Let $\{R_i\}_{i \in \mathcal{A}}$ be a directed system of local rings and set $R \coloneqq \varinjlim R_i$. Then R is also local.*

Proof. Consider $\mathfrak{m} \coloneqq R \setminus R^*$ the subset of non-units. We will show that $\mathfrak{m}$ is an ideal proving that it must be the unique maximal ideal of R.

First note that if $x, y \in \mathfrak{m}$ then by definition of the direct limit for some large enough $i \in \mathcal{A}$ there is a homomorphism $\phi_i : R_i \to R$ and elements $\bar{x}, \bar{y} \in R_i$ such that $\phi_i(\bar{x}) = x$ and $\phi_i(\bar{y}) = y$. Since $x, y \notin R^*$ we must have that $\bar{x}$ and $\bar{y}$ are also non-units in R_i. As R_i is local, it follows that $\bar{x}, \bar{y} \in \mathfrak{m}_i$, where $\mathfrak{m}_i$ is the unique maximal ideal of R_i.

We claim that $x-y \in \mathfrak{m}$ and we prove this by contradiction: assume the contrary, then $x-y \in R^*$ and there is an inverse $z \in R$. It follows for a possibly even bigger $i \in \mathcal{A}$ that $1 = z(x-y) = \phi_i(\bar{z}(\bar{x}-\bar{y}))$. But then, for an even larger $i \in \mathcal{A}$, we must have $\bar{z}(\bar{x}-\bar{y}) = 1$, hence $\bar{x}-\bar{y}$ is invertible. However, $\bar{x}-\bar{y} \in \mathfrak{m}_i$, a contradiction.

Finally, take some $r \in R$ and $x \in \mathfrak{m}$. Considering their preimages in R_i for sufficiently large $i \in \mathcal{A}$, gives $\bar{r}\bar{x} \in \mathfrak{m}_i$ which, by a similar argument to the above, yields $\phi_i(\bar{r}\bar{x}) = rx \in \mathfrak{m}$.

We have proven that $\mathfrak{m}$ is an ideal; since it is the set of non-units it follows that R must be local. $\square$

Appendix B

The Resultant

"Curiouser and curiouser!"
Lewis Carroll, *Alice's Adventures in Wonderland*, Chapter II

The mathematical theory connected to the resultant is very broad; however we want to state just the most important facts about it, as just a very small piece of information is needed for our purposes. For defining the resultant we work over a field K and with univariate polynomials, but note that one may also consider all appearing objects over some ring and allow for several variables. Some similar results hold true in this case, however some others fail [GKZ08].

We start by defining $\mathcal{P}_n$ for $n \in \mathbb{N}$ to be the set of all polynomials over some fixed field K of degree less than n. It is obvious that $\mathcal{P}_n$ is a vector space over K of dimension n. Now let $p(t) = p_0 + \cdots + p_d t^d$ and $q(t) = q_0 + \cdots + q_e t^e$ be two coprime monic polynomials of degrees d and e respectively. Note that $p(t) \notin \mathcal{P}_d$ and $q(t) \notin \mathcal{P}_e$, because their degrees are too large, nevertheless we may define the linear map

$$\begin{aligned} \Phi : \mathcal{P}_e \times \mathcal{P}_d &\to \mathcal{P}_{d+e} \\ (a(t), b(t)) &\mapsto p(t)a(t) + q(t)b(t). \end{aligned}$$

Clearly, the dimensions of $\mathcal{P}_e \times \mathcal{P}_d$ and $\mathcal{P}_{d+e}$ agree. Moreover, take some $(a(t), b(t)) \in \ker(\Phi)$, then $p(t)a(t) + q(t)b(t) = 0$. Because $p(t)$ and $q(t)$ are relatively prime, we must have that $q(t)$ divides $a(t)$ and $p(t)$ divides $b(t)$. However, since the degrees of $a(t)$ and $b(t)$ are smaller than e and d this is only possible if $a(t) = b(t) = 0$. Therefore we see that Φ is injective and since it is a linear map between two vector spaces of equal dimension, it must be surjective as well and hence it is invertible.

Furthermore, we know that Φ, being a linear map between vector spaces, is representable as a matrix. It is clear that over the basis of $\mathcal{P}_e \times \mathcal{P}_d$ given by $\mathcal{B} = \{(1,0), \ldots, (t^{e-1}, 0), (0,1), \ldots, (0, t^{d-1})\}$, the map Φ is given by the $(d+e) \times (d+e)$

matrix

$$\begin{pmatrix} p_0 & 0 & \cdots & 0 & q_0 & 0 & \cdots & 0 \\ p_1 & p_0 & \cdots & 0 & q_1 & q_0 & \cdots & 0 \\ p_2 & p_1 & \ddots & 0 & q_2 & q_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & p_0 & \vdots & \vdots & \ddots & q_0 \\ p_d & p_{d-1} & \cdots & \vdots & q_e & q_{e-1} & \cdots & \vdots \\ 0 & p_d & \ddots & \vdots & 0 & q_e & \ddots & \vdots \\ \vdots & \vdots & \ddots & p_{d-1} & \vdots & \vdots & \ddots & q_{e-1} \\ 0 & 0 & \cdots & p_d & 0 & 0 & \cdots & q_e \end{pmatrix}$$

This matrix (or sometimes its transpose) is called the *Sylvester matrix* of the polynomials $p(t) = p_0 + \cdots + p_d t^d$ and $q(t) = q_0 + \cdots + q_e t^e$ and is usually denoted by $S_{p(t),q(t)}$. The determinant of this matrix, which of course does not depend on whether we use the form above or the transposed one, is called the *resultant of* $p(t)$ *and* $q(t)$ and is often denoted by $\operatorname{res}(p(t), q(t))$. By the discussion above, we convinced ourselves that $S_{p(t),q(t)}$ is invertible if $p(t)$ and $q(t)$ are relatively prime. Of course we have that $\operatorname{res}(p(t), q(t)) \neq 0$ in this case.

Bibliography

[DG67] J. Dieudonné and A. Grothendieck. "Éléments de géométrie algébrique". In: *Inst. Hautes Études Sci. Publ. Math.* 4, 8, 11, 17, 20, 24, 28, 32 (1961–1967).

[AM65] M. Artin and B. Mazur. "On Periodic Points". In: *Annals of Mathematics* 81.1 (1965), pp. 82–99. ISSN: 0003486X. URL: http://www.jstor.org/stable/1970384.

[Fur67] H. Furstenberg. "Algebraic functions over finite fields". In: *Journal of Algebra* 7.2 (1967), pp. 271–277. ISSN: 0021-8693. DOI: https://doi.org/10.1016/0021-8693(67)90061-0. URL: http://www.sciencedirect.com/science/article/pii/0021869367900610.

[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969, pp. I–IX, 1–128. ISBN: 978-0-201-40751-8.

[LT70] F. Lazzeri and A. Tognoli. "Alcune proprietà degli spazi algebrici". it. In: *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze* Ser. 3, 24.4 (1970), pp. 597–632. URL: http://www.numdam.org/item/ASNSP_1970_3_24_4_597_0.

[Ive73] B. Iversen. *Generic Local Structure of the Morphisms in Commutative Algebra.* Lecture Notes in Mathematics. Springer Berlin Heidelberg, 1973. ISBN: 9783540383383.

[Nag75] M. Nagata. *Local Rings.* R.E. Krieger Publishing Company, 1975.

[Mat80] H. Matsumura. *Commutative Algebra.* Math Lecture Notes Series. Benjamin/Cummings Publishing Company, 1980. ISBN: 9780805370263.

[Mil80] J. S. Milne. *Etale Cohomology (PMS-33).* Princeton Legacy Library. Princeton University Press, 1980. ISBN: 9780691082387.

[Del84] P. Deligne. "Intégration sur un cycle évanescent." In: *Inventiones mathematicae* 76 (1984), pp. 129–144. URL: http://eudml.org/doc/143120.

[DL87] J. Denef and L. Lipshitz. "Algebraic power series and diagonals". In: *Journal of Number Theory* 26.1 (1987), pp. 46–67. ISSN: 0022-314X. DOI: https://doi.org/10.1016/0022-314X(87)90095-3. URL: http://www.sciencedirect.com/science/article/pii/0022314X87900953.

[Bou89] N. Bourbaki. *Algebra I: chapters 1-3.* Elements of mathematics. Springer-Verlag, 1989. ISBN: 9783540193739.

[AMR92] M. E. Alonso, T. Mora, and M. Raimondo. "A computational model for algebraic power series". In: *Journal of Pure and Applied Algebra* 77.1 (1992), pp. 1–38. ISSN: 0022-4049. DOI: https://doi.org/10.1016/0022-4049(92)90029-F. URL: http://www.sciencedirect.com/science/article/pii/002240499290029F.

[Rui93] J.M. Ruiz. *The Basic Theory of Power Series*. Advanced Lectures in Mathematics. Vieweg+Teubner Verlag, 1993. ISBN: 9783528065256.

[Eis95] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995. ISBN: 9780387942698.

[BCR98] J. Bochnak, M. Coste, and M.F. Roy. *Real Algebraic Geometry*. Springer Berlin Heidelberg, 1998. ISBN: 9783662037188.

[Lan05] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005. ISBN: 9780387953854.

[GKZ08] I.M. Gelfand, M. Kapranov, and A. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Modern Birkhäuser Classics. Birkhäuser Boston, 2008. ISBN: 9780817647704.

[AB13] B. Adamczewski and J. P. Bell. "Diagonalization and rationalization of algebraic Laurent series". en. In: *Annales scientifiques de l'École Normale Supérieure* Ser. 4, 46.6 (2013), pp. 963–1004. DOI: 10.24033/asens.2207. URL: http://www.numdam.org/item/ASENS_2013_4_46_6_963_0.

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

[ACH14] M. E. Alonso, Francisco Jesus Castro-Jiménez, and H. Hauser. "Encoding Algebraic Power Series". In: *Foundations of Computational Mathematics* 18 (2014), pp. 789–833.

[Hau17] H. Hauser. "The classical Artin approximation theorems". In: *Bulletin of the American Mathematical Society* 54 (Jan. 2017), p. 1. DOI: 10.1090/bull/1579.

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

[Stacks] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu. 2020.