ulm university universität
uulm

Models of Curves and Valuations

Julian Peter Rüth

Dissertation zur Erlangung des Doktorgrades Dr. rer. nat. der Fakultät für Mathematik und Wirtschaftswissenschaften der Universität Ulm.

Vorgelegt von Julian Peter Rüth aus Würzburg im Jahr 2014.

Diese Dissertation wurde gefördert vom DFG Schwerpunktprogramm SPP 1489 *Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory.*

Tag der Prüfung:
30.4.2015

Gutachter:
Prof. Dr. Stefan Wewers
Prof. Dr. Irene Bouw

Amtierender Dekan:
Prof. Dr. Dieter Rautenbach

Abstract

The Semistable Reduction Theorem by Deligne and Mumford [10] states that any absolutely irreducible smooth projective curve over a field with a discrete valuation has a semistable model, at least if one admits a finite separable extension of the base field. The original proof does not provide a construction which can in practice be exploited to compute semistable models of curves. A recent proof of the Semistable Reduction Theorem by Arzdorf and Wewers [2] uses techniques which are more accessible to algorithmic constructions. For their proof they consider a curve as a cover $Y \to X = \mathbb{P}^1$ of the projective line. To any semistable model of the projective line they consider its normalization in Y, a normal model of Y. They show that, starting from any model of X, one can find a blowup of the model such that the singularities of the special fibers of the normalizations have *improved*. The improvement is measured by numeric invariants which are attached to the singularities and which show that the process terminates after finitely many steps with a semistable model of Y.

The present work makes several aspects of their approach explicit and realizes them in a computer algebra system. We represent models as finite sets of discrete valuations which correspond to the irreducible components of the special fiber. A theory by Mac Lane [24, 25] provides a compact representation of such valuations which is well suited for algorithmic considerations. In particular, it allows us to efficiently compute the normalization of a model of X in Y, i.e., the valuations which correspond to the normalization. From this we can also immediately deduce whether a model has reduced special fiber or not, a necessary condition for a model to be semistable.

If the special fiber of a model is not reduced, then a theorem of Epp [11] guarantees that there is a finite extension of the base field which makes it reduced. As Epp's method is not fully constructive, we discuss alternatives to his approach. Using the theory of Mac Lane valuations, we provide a new algorithm to construct such an extension of the base field when working in mixed characteristic $(0, p)$. Our algorithm is provably correct if p^2 does not divide the degree of $Y \to X$.

Assuming that the special fiber is reduced, we provide a new algorithm to compute equations for certain affine patches of the special fiber. Finally, we illustrate all the techniques developed in this work by computing semistable models in several examples.

Zusammenfassung

Der Satz von der semistabilen Reduktion von Deligne und Mumford [10] besagt, dass eine absolut-irreduzible glatte projektive Kurve über einem diskret bewerteten Körper ein semistabiles Modell besitzt, wenn man eine endliche separable Erweiterung des Grundkörpers zulässt. Der ursprüngliche Beweis liefert keine Konstruktion, die die Berechnung solcher semstabilen Modelle in der Praxis erlaubt. Ein Beweis dieses Satzes von Arzdorf und Wewers [2] basiert auf Techniken, die zugänglicher für die algorithmische Umsetzung sind. In ihrem Beweis wird die Kurve als eine Überlagerung $Y \to X = \mathbb{P}^1$ der projektiven Geraden aufgefasst. Zu jedem semistabilen Modell der projektiven Geraden betrachten sie nun dessen Normalisierung in Y, ein normales Modell von Y. Sie zeigen, dass man, beginnend mit einem semistabilen Modell von X, eine Aufblasung finden kann, sodass sich die Singularitäten auf der speziellen Faser der Normalisierung *verbessern*. Diese Verbesserung wird durch numerische Invarianten der Singularitäten gemessen, welche dann zeigen, dass der Prozess nach endlich vielen Schritten mit einem semistabilen Modell von Y endet.

Die vorliegende Arbeit konkretisiert verschiedene Aspekte dieses Ansatzes und setzt diese in einem Computeralgebrasystem um. Hierzu stellen wir Modelle als endliche Mengen von Bewertungen dar, die zu den irreduziblen Komponenten der speziellen Faser korrespondieren. Eine Theorie, die auf Mac Lane zurückgeht [24, 25], liefert eine kompakte Darstellung solcher Bewertungen, die außerdem gut für algorithmische Überlegungen geeignet ist. Insbesondere erlaubt es diese Theorie die Normalisierung eines Modells von X in Y, also die zugehörigen Bewertungen, effizient zu berechnen Von diesen Bewertungen lässt sich unmittelbar ablesen, ob die spezielle Faser eines Modells reduziert ist, eine notwendige Bedingung für Semistabilität.

Ist die spezielle Faser nicht reduziert, so garantiert ein Theorem von Epp [11] die Existenz einer endlichen Erweiterung des Grundkörpers über dem die spezielle Faser reduziert ist. Wir diskutieren Alternativen zur Methode von Epp, da diese nicht vollständig konstruktiv ist. In gemischter Charakteristik $(0, p)$ gelangen wir, ausgehend von der Theorie der Mac Lane Bewertungen, zu einem neuen Algorithmus, um eine solche Erweiterung zu konstruieren. Falls p^2 nicht den Grad von $Y \to X$ teilt, können wir zeigen, dass der Algorithmus korrekt ist.

Für Modelle mit reduzierter spezieller Faser geben wir einen neuen Algorithmus an, um gewisse affine Karten der speziellen Faser zu berechnen. Zuletzt illustrieren wir die Techniken, die in dieser Arbeit entwickelt wurden, indem wir semistabile Modelle für einige Beispiele berechnen.

Contents

Chapter 1

Introduction

In arithmetic geometry one often wants to study models of curves with respect to a valuation of the base field. For us a model is an integral, proper, and flat scheme over a discrete valuation ring which has the curve in question as its generic fiber. A particularly nice model of a curve is a semistable model. A semistable model of an (absolutely) irreducible smooth projective curve is a model whose special fiber is reduced and has only ordinary double points as singularities. The Semistable Reduction Theorem by Deligne and Mumford [10] shows that such a model always exists after a finite separable extension of the base field. Although the proof provides a construction, the steps that are performed (making torsion points of the Jacobian rational and computing a minimal regular model) can in practice not be performed for interesting examples. Several alternative proofs of this theorem have been given in the past (see [23, Remark 10.4.4] for a brief overview,) most recently by Arzdorf and Wewers in [1].

The idea of their proof is as follows. Let Y be an absolutely irreducible smooth projective curve over a valued field K and consider Y as a cover of $X = \mathbb{P}^1_K$, i.e., let $\phi\colon Y \to X$ be a non-constant finite separable morphism. Let $\mathcal{X}$ be a semistable model of X, e.g., a projective line over the ring of integers of K, and write $\mathcal{Y}$ for the normalization of $\mathcal{X}$ in Y. Then $\mathcal{Y}$ is a normal model of Y. If $\mathcal{Y}$ is semistable, then we have found a semistable model of Y. If this is not the case, then it might be that the special fiber $\mathcal{Y}_s$ of $\mathcal{Y}$ is not reduced. There is, however, a finite extension of the base field K over which the special fiber of $\mathcal{Y}$ is reduced. The existence of such an extension is guaranteed by a (non-constructive) theorem of Epp [11]. If $\mathcal{Y}_s$ is reduced, then $\mathcal{Y}$ can only fail to be semistable because there are singularities on the special fiber which are not ordinary double points. Let $y \in \mathcal{Y}_s$ be such a singularity. The idea is now to *modify* $\mathcal{X}$ by a suitable blowup with center in x, the image of y on $\mathcal{X}$. This provides a new semistable model $\mathcal{X}' \to \mathcal{X}$ whose normalization in Y gives a normal model $\mathcal{Y}' \to \mathcal{Y}$. One can use the multiplicity m_y and the δ-invariant δ_y of a singularity [23, Definition 7.5.13] to measure how far it is from being a smooth point or an ordinary double point. With their construction, a point y' in the fiber of y satisfies

$$\delta_{y'} < \delta_y \quad \text{or} \quad \delta_{y'} = \delta_y \text{ and } m_{y'} > m_y.$$

Repeating the above construction for $\mathcal{Y}' \to \mathcal{X}'$, this process must terminate after finitely many steps since $\delta_y \geq m_y - 1$ always holds. The above modification

$\mathcal{X}' \to \mathcal{X}$ is obtained individually from local information of the singularities on the special fiber of $\mathcal{Y}$, i.e., by considering the completions in each of the singular points. Expressed in rigid analytic language, these modifications correspond to closed subdisks of the open unit disk and can therefore be described by determining their center and radius. For an important class of special cases, namely prime-cyclic Galois covers, this construction has already been made explicit and turned into an algorithm by Arzdorf in [2].

The present work builds a framework under which the above construction can be realized algorithmically. A general problem when dealing with models of a curve X is to find good representations for such models. Of course one could just write down affine patches but this is clearly inefficient, and since we do not want to use the global geometry of models, this approach does not seem appropriate. However, we only have to deal with *normal* models X. Such models can be represented by finite sets of discrete valuations on $K(X)$, the function field of X (Propositions 3.4.) These valuations on $K(X)$ extend the valuation on K and are such that their residue field is transcendental over the residue field of K. In fact, if K is Henselian, then the finite non-empty sets of such valuations and the normal models of X are in bijection (Corollary 3.18, cf. [17]) This reduces the problem of representing normal models to that of representing valuations on $K(X)$.

Let v be a discrete valuation on $K(X)$ which extends the valuation on K and is such that its residue field is transcendental over the residue field of K. If $X = \mathbb{P}^1$, then $K(X)$ is a rational function field $K(x)$. For an element $f/g \in K(x)$ we have $v(f/g) = v(f) - v(g)$. To describe such valuations on $K(x)$ it therefore suffices to describe discrete valuation on $K[x]$ with the above properties. These discrete valuations are equipped with a partial order $w \geq v$ if $v(f) \geq v(f)$ for all $f \in K[x]$. It suffices to describe all valuations $v \geq v_0$ where v_0 is the *Gauss valuation*. A complete description of such valuations has been given by Mac Lane in [24], and was apparently rediscovered by Montes in [27]. This description is particularly well suited for algorithmic considerations, in particular it allows us to efficiently compute valuations and reductions of elements. The idea is that a discrete valuation v can be *augmented* with a *key polynomial* $\phi \in K[x]$ and a value $\lambda \in \mathbb{Q}$ to a valuation $w = [v, w(\phi) = \lambda]$ which satisfies $w \geq v$. Conversely, if $w \geq v$, then w can be approximated by augmenting v (Proposition 4.35.) This is used to show that all such discrete valuations on $K[x]$ are *inductive*, i.e., they can be obtained by finitely many augmentations of the Gauss valuation (Theorem 4.31.)

An equivalent description of such valuations on $K[x]$ can be given using the language of rigid diskoids (Theorem 4.56.) This connection, which has apparently not been noticed before, leads to a novel statement on the uniqueness of the presentation of inductive valuations (Theorem 4.57) which extends the original statement by Mac Lane (Theorem 4.33.) Another useful tool to study such valuations is the graded algebra of a valuation as introduced in that context by Vaquié [39]. We give a simple proof for the structure of this algebra (Theorem 4.61) which has originally been described in [12].

The theory developed up to this point allows us to describe normal models of $\mathbb{P}^1$. To extend this to normal models of general curves, we consider a curve as a cover $Y \to X := \mathbb{P}^1$. The function field $K(Y)$ is then a finite separable extension of a rational function field $L_0 := K(X)$. A discrete valuation w on $K(Y)$ (which extends the valuation on K and whose residue field is transcendental over that

of K) restricts to a discrete valuation v on L_0. If we write $K(Y) = L_0[t]/(G)$, we can interpret w as a discrete pseudo-valuation on $L_0[t]$ which is such that precisely the ideal (G) is sent to infinity. Fortunately, the theory developed by Mac Lane also covers this case and gives a complete description of such valuations (Theorem 4.65.) Mac Lane also provides algorithms to compute such pseudo-valuations in [25]. We illustrate these algorithms in two applications: polynomial factorization (as is done by Montes in [27]) and determination of the configuration of roots of a polynomial. The latter appears to be a novel application of these techniques.

Now that we have a general framework to describe normal models of curves in place, we can discuss the algorithmic tasks that have to be solved to construct semistable models. Let $Y \to X = \mathbb{P}^1$ be a cover of curves and let $\mathcal{X}$ be a semistable model of X. The normalization $\mathcal{Y}$ of $\mathcal{X}$ in Y can now be easily computed on the level of valuations (Proposition 5.2.) The nature of the singularities of $\mathcal{Y}_s$ can however not be immediately seen from the valuations which describe $\mathcal{Y}$. If $\mathcal{Y}_s$ is reduced, then we provide a new algorithm (Subsection 5.1.3) which can be used to compute affine equations for $\mathcal{Y}_s$, or at least for the parts of it which are important for the semistable reduction algorithm. If $\mathcal{Y}_s$ is not reduced, then its failure of being reduced is encoded in the ramification of the valuations describing $\mathcal{Y}$ over the valuation of the base field (Proposition 5.4,) namely, the special fiber is reduced if and only if the valuations are weakly unramified over the valuation of the base field. It is therefore natural to consider the following problem: Given such a discrete valuation w on $K(Y)$, construct a finite extension K'/K which is such that the extensions of w to $K'K(Y)$ are weakly unramified over their extension to K'.

A theorem of Epp (Section 6.2) guarantees that such a finite extension always exists. The arguments which Epp uses do, however, not lead to a construction of this extension which is applicable in practice. As we have already discussed, a valuation w on $K(Y)$ extends $v \coloneqq w\big|_{K(x)}$. This allows us to split the problem of eliminating ramification into two parts: eliminating the ramification of v over the base field and eliminating the ramification of w over v.

The first part is easier (we restrict our attention to the case of mixed characteristic.) If the ramification index of v is prime to the residue field characteristic $p > 0$, then a variant of Abhyankar's Lemma constructs a totally ramified extension which eliminates the ramification (Proposition 6.12.) In general, we can write v as an inductive valuation. Using the language of rigid diskoids which we developed earlier this lets us easily construct an extension of the base field which eliminates the ramification (Proposition 6.16.)

In any case, we may assume that v is weakly unramified over the valuation of the base field. The more difficult part is the elimination of the ramification of w over v. Again, Abhyankar's Lemma can be used to eliminate ramification which is prime to p (Corollary 6.6.) Using the language of Mac Lane we can write w as an *inductive pseudo-valuation*. More careful analysis shows that we can assume that w is the unique extension of v to $K(Y)$, so w is in fact an *infinite inductive valuation*. We provide a new algorithm which eliminates ramification in that setting. The proof of the correctness of this algorithm is, however, incomplete. Currently, it requires a few technical conditions on the minimal polynomial of a generator. These conditions are trivially satisfied if the ramification index is not divisible by p^2.

The current work does not discuss at all the problem of finding centers and radii which lead to a semistable model. Both problems have been discussed by Arzdorf in [1]. For the problem of finding suitable centers we also refer to an article which we are working on with Wewers [32] which generalizes the work by Lehr and Matignon [22]. Provided that the correct center is already known, the correct radius can often be guessed or read off the Mac Lane valuations which describe the model (we discuss this briefly in Chapter 7.)

A large part of this thesis has been devoted to the implementation of algorithms and tools which are necessary to compute semistable reduction in practice. We believe that it is important to not only develop these as a *proof-of-concept* but to provide a robust implementation which is integrated into some major computer algebra system. Since, in the authors opinion, research mathematics should not be realized in closed source software, we chose for this the free computer algebra system Sage [35]. Consequently, many of the algorithms described here have been implemented as modifications to the Sage library. Essentially everything described up to and including Chapter 5 has been implemented and is in the process of being incorporated into the stable distribution of Sage.[1] The algorithms and tools described in Chapter 6 and 7 have been implemented to a large part, however they are certainly not as robust and well tested. To make such an implementation possible a substantial amount of basic functionality had to be added to Sage, including function fields (which were not present at all when this project started,) general extensions of p-adic fields, and squarefree-decomposition algorithms, to name just a few.

Acknowledgments

First and foremost I would like to thank Stefan Wewers for his support throughout the past years. Without his guidance this thesis would certainly not have been possible. My colleagues always provided inspiring discussions, especially the members of the Zalando Club and its predecessors. I also learned a lot from the people of the Sage community, in particular from David Roe who guided me through the p-adics code in Sage. Moritz Gerlach (without him I would not have studied Mathematics in the first place,) Carlos Prieto, and Uwe Schöning inspired me to write a thesis, and I am grateful they did. My work was supported during the first three years by the DFG Priority Program *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory.*

I feel very privileged for the friends I have here in Ulm. You made my unexpected return to this city so much more pleasant than I could have imagined. Finally, I would not be writing the last line of my thesis now if it was not for Tine, who always cheered me up and took me through times of doubt.

Conventions and Standing Assumptions

We usually use K to denote our base field, a non-archimedean field with a discrete valuation v_K. We denote the residue field of v_K by k and, unless otherwise noted, we do not assume our base fields to be complete or k to be perfect. If we do not discuss extensions of valued fields, then all valuations are normalized

[1] The current state of these modifications which has been used to compute the examples given in the text, can be found at `https://github.com/saraedum/sage-renamed/tree/experimental`.

such that a uniformizer $\pi \in K$ has valuation $v_K(\pi) = 1$. We only use discrete valuations on fields, and never the induced absolute value. In particular we say that $x, y \in K$ have distance δ if $v_K(x - y) = \delta$, i.e., a large value δ means that the two elements are close to each other. This work was written with application to fields K of mixed characteristic in mind, however, most results do not need this assumption; if it is needed, it is explicitly mentioned at the beginning of a section.

Chapter 2

Outline of the Semistable Reduction Algorithm

We give a brief outline of our algorithm to compute the semistable reduction of curves. We will fill in more details in later chapters and in particular in Chapter 7. Let us fix some notation first. For the remainder of this chapter let K be a field with a discrete valuation $v\colon K^\times \to \mathbb{Q}$, $\mathcal{O}_K$ the ring of integers of K, and k its residue field. If X is an irreducible smooth projective curve over K, then a model of X is an integral, proper, and flat $\mathcal{O}_K$-scheme $\mathcal{X}$ with an isomorphism from its generic fiber $\mathcal{X}_g$ to X. A normal model of X is called semistable if its special fiber $\mathcal{X}_s$ is reduced and all singularities of $\mathcal{X}_s$ are ordinary double points.

Let Y be a smooth projective curve over K which is absolutely irreducible. We consider Y as a finite cover of $X \coloneqq \mathbb{P}^1_K$, the projective line over K, so let $\phi : Y \to X$ be a nonconstant separable finite morphism. To compute a semistable model of Y, we start with any semistable model $\mathcal{X}$ of X and repeatedly modify $\mathcal{X}$ as follows.

We compute the normalization of $\mathcal{X}$ in Y, a normal model of Y, which we want to denote by $\mathcal{Y}$. If $\mathcal{Y}$ is semistable, then we have computed a semistable model of Y. If the special fiber of $\mathcal{Y}$ is not reduced, then there is a finite extension K'/K which makes the special fiber reduced, i.e., if we compute the normalization again with the base change of $\mathcal{X}$ to the ring of integers of K' then $\mathcal{Y}$ will have reduced special fiber. Let $y \in \mathcal{Y}_s$ be a singularity which is not an ordinary double point. We denote the image of y under the induced map $\phi_{\mathcal{O}_K} : \mathcal{Y} \to \mathcal{X}$ by x. We modify $\mathcal{X}$ by an appropriate blowup with center x and restart the process. One can show that suitable blowups improve the singularities over x so that the whole procedure terminates after finitely many iterations with a semistable model of Y.

2.1 A First Example

To illustrate the previous outline, we walk the reader through the computation of a semistable model. Here, we only list the right steps one needs to perform without justifying our choices further. For details, the footnotes refer to later chapters.

Let us consider the smooth projective curve Y over $K \coloneqq \mathbb{Q}_3$ given by the affine equation[1]

$$y^3 = 1 + 3x^3 + 3x^5.$$

We consider Y as a cover of $X \coloneqq \mathbb{P}^1_K$ of degree 3:

$$\phi : Y \to X.$$

To compute a semistable model of Y, we determine a semistable model $\mathcal{X}$ of X whose normalization in Y is semistable. We start with $\mathcal{X} \coloneqq \mathbb{P}^1_R$ with $R \coloneqq \mathbb{Z}_3$. To compute the corresponding model of Y, i.e., the normalization of $\mathcal{X}$ in Y, we take affine patches of $\mathcal{X}$ and compute their integral closure in $K(Y)$. (In the following we will always limit our attention to one affine patch of $\mathcal{X}$, namely the patch where something *interesting* happens.) One such patch is $\operatorname{Spec} A$ with $A = R[x]$ whose integral closure is $B \coloneqq A[y]$. The special fiber of $\operatorname{Spec} B$, i.e., the reduction of B modulo (3), is $\operatorname{Spec} \mathbb{F}_3[x,y]/(y^3-1)$ which is not reduced[2]. Since a semistable model has reduced special fiber, our model is not yet semistable.

We need to modify $\mathcal{X}$. We take $K \coloneqq \mathbb{Q}_3(\pi)$, where π is a third root of 3, and base change[3], i.e., we let $\mathcal{X} = \mathbb{P}^1_R$ with $R \coloneqq \mathbb{Z}_3[\pi]$. Again, we consider the open affine $\operatorname{Spec} A$ with $A = R[x]$ and compute its normalization[4] $\operatorname{Spec} B$ in Y. We obtain $B = A[w]$ where $w = (y-1)/\pi$. The special fiber of $\operatorname{Spec} B$, i.e., the reduction of B modulo (π), is

$$\bar{Y} \coloneqq \operatorname{Spec} \mathbb{F}_3[x,w]\big/(w^3 - x^3 - x^5),$$

a reduced scheme.

The Jacobi criterion shows that $\bar{Y}$ has a singularity at $x = 0, w = 0$. This singularity is not an ordinary double point so $\mathcal{Y}$ is not semistable. The image of the singular point under ϕ_R is the point on $\mathcal{X}_s$ with coordinate $x = 0$.

We modify $\mathcal{X}$ by performing a blowup which has this point as a center. We perform the blowup which corresponds to a closed disk with center ζ and radius $1/12$ where ζ is a root of

$$m(T) = 145T^{12} + 342T^{10} + 189T^8 + 180T^7 + 198T^5 + 18T^3 + 30T^2 + 3.$$

We note that the twelve conjugate roots of m are contained in a disk of radius $1/12$ which also contains zero[5], so we could have equally taken zero as a center. We replace our ground field with $K' \coloneqq K(\zeta)$ which also provides us with an element of valuation $1/12$. We consider the model $\mathcal{X} = \mathbb{P}^1_R$ where R is the ring of integers $R \coloneqq \mathbb{Z}_3[\zeta]$ and let $\mathcal{X}'$ be the blowup of $\mathcal{X}$ which corresponds to the aforementioned disk. The normalization $\mathcal{Y}'$ of $\mathcal{X}'$ in Y is not reduced, so we have to enlarge the base field K'.

[1] This is an example in Chapter 3 of [1].

[2] Section 5.2 describes an algorithm which determines whether a model has reduced special fiber without computing that fiber explicitly.

[3] Chapter 6 discusses various algorithms which can be used to find a field extension over which the special fiber of a model is reduced.

[4] Section 5.1 describes an algorithm which determines the normalization assuming that its special fiber is reduced.

[5] Section 4.8 describes an algorithm which can be used to determine the configuration of such polynomials.

Any totally ramified extension of degree 3 makes $\mathcal{Y}'$ reduced, so we adjoin an element $\pi'^3 = \zeta$. The interesting affine patch of $\mathcal{Y}'_s$ is

$$\bar{Y}' \coloneqq \operatorname{Spec} \mathbb{F}_3[u,v]/(u^5 - u^3 + u - v^3)$$

where the variables are the reductions of

$$u \coloneqq \frac{y-1}{\pi'^{15}} \quad \text{and} \quad v \coloneqq \frac{y-1}{\pi'^{17}} + \frac{x}{\pi'^5}.$$

The curve $\bar{Y}$ is not smooth. Over $\mathbb{F}_9 \coloneqq \mathbb{F}_3[a]/(a^2 - a - 1)$ the curve has four singular points with coordinates

$$(-1,-1),\ (1,1),\ (-a-1,0),\ \text{and}\ (a+1,0).$$

It turns out that we did not choose the right radius yet. We should have chosen $1/8$. Since we will not need the element π' anymore, we work again over the field $K' = K(\zeta)$. In K' there is no element of valuation $1/8$, so we pass to the field $K'' = K'(\sqrt{\zeta})$. Let $\mathcal{X}''$ be the model of $\mathcal{X}'$ obtained by performing the blowup which corresponds to the closed disk with center ζ and radius $1/8$. The normalization $\mathcal{Y}''$ of $\mathcal{X}''$ in Y is not reduced, so we have to enlarge the base field K''.

To make the special fiber reduced we adjoin to K'' an element ψ which satisfies

$$\psi^3 + 2\zeta^{12}\psi + \zeta^{17} = 0.$$

The relevant affine patch of the special fiber of $\mathcal{Y}''$ is

$$\bar{Y}'' \coloneqq \operatorname{Spec} \mathbb{F}_3[u,v]/(v^3 - v + u^2),$$

a smooth curve of genus 1.

It is now easy to see that the corresponding blowup in the other three singularities from above produces the same kind of curve. Since the curve Y has genus 4 and we found 4 components of genus 1, this determines a semistable model of Y.

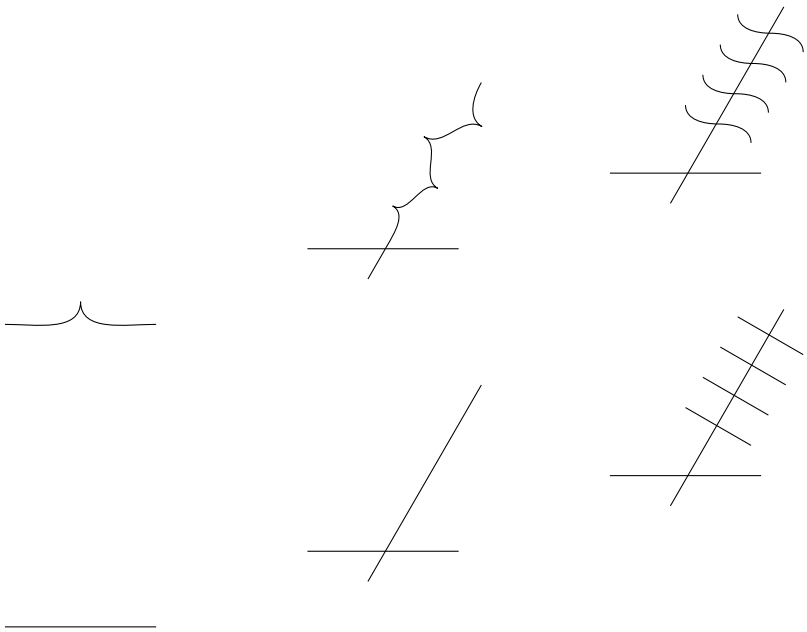


Figure 2.1: The models of X (bottom) and Y (top) which occur during the computation.

Chapter 3

Normal Models of Curves

For the remainder of this chapter let K be a field with a discrete valuation $v_K \colon K^\times \to \mathbb{Q}$, $\mathcal{O}_K$ the ring of integers of K, and k its residue field. Furthermore let X be an irreducible smooth projective curve over K.

Definition 3.1 A *model* of X is an integral, proper, and flat $\mathcal{O}_K$-scheme $\mathcal{X}$ equipped with an isomorphism from its generic fiber to X. We denote the generic fiber of $\mathcal{X}$ by $\mathcal{X}_g$, the special fiber by $\mathcal{X}_s$.

We will be mainly interested in normal models of X.

Example 3.2 Let $\mathcal{O}_K \coloneqq \mathbb{Z}_p$, $K \coloneqq \mathbb{Q}_p$, and $X \coloneqq \mathbb{P}^1_K$. A normal model of X is given by $\mathcal{X} \coloneqq \mathbb{P}^1_{\mathcal{O}_K}$ with the evident isomorphism from the generic fiber $\mathcal{X}_g = \mathcal{X}_K$ to $\mathbb{P}^1_K$. The special fiber $\mathcal{X}_s$ has one irreducible component which is isomorphic to $\mathbb{P}^1_k$

Remark 3.3 We could omit *integral* from our definition of a model since it is implied by flatness of the model and integrality of X [23, Proposition 4.3.8]. Furthermore, we note that a point $x \in \mathcal{X}$ of codimension one which is regular is normal. Conversely, a normal point of codimension one is regular by Serre's criterion [23, Lemma 8.2.21].

By a *modification* of normal models of X we mean a morphism of $\mathcal{O}_K$-schemes $\mathcal{X}' \to \mathcal{X}$ which induces the identity on the generic fiber. As our models are proper, a modification is a proper morphism. Since a modification is dominant it is also surjective. Note that by Zariski's Connectedness Principle, a modification has connected fibers [16, Corollaire 4.3.2].

The goal of this chapter is to establish a bijection between the normal models of X and certain sets of valuations on $K(X)$, the function field of X. This will be a bijection up to isomorphism of models of X; we say that two models $\mathcal{X}, \mathcal{X}'$ of X are isomorphic if there is a modification $\mathcal{X}' \to \mathcal{X}$ and a modification $\mathcal{X} \to \mathcal{X}'$. To be able to state the central proposition of this chapter, we denote by $V(X)$ the set of discrete valuations $v \colon K(X)^\times \to \mathbb{Q}$ which satisfy

(a) $v\big|_K = v_K$, and

(b) the residue field of v is of transcendence degree one over k.

Proposition 3.4 *There is a map from the isomorphism classes of normal models of X to the finite non-empty subsets of $V(X)$.*

Proof Let $\mathcal{X}$ be a normal model of X. We associate to each generic point of the special fiber of $\mathcal{X}$ a valuation in $V(X)$: A generic point ξ is a point of codimension one in $\mathcal{X}$, i.e., the local ring $\mathcal{O}_{\mathcal{X},\xi}$ is a discrete valuation ring since it is a Noetherian ring which is one-dimensional and normal. It gives rise to a discrete valuation v on $\mathrm{Frac}(\mathcal{O}_{\mathcal{X},\xi}) = K(X)$. Since $\mathcal{X}$ is a flat $\mathcal{O}_K$-scheme, $\mathcal{O}_{\mathcal{X},\xi}$ dominates $\mathcal{O}_K$, and we may scale v such that the restriction of v to K is v_K. If we denote the irreducible component of the special fiber which contains ξ by Z, then $Z \hookrightarrow \mathcal{X}$ is a closed immersion and so $\mathcal{O}_{\mathcal{X},\xi} \to \mathcal{O}_{Z,\xi}$ is onto. Therefore, the residue field of v is an extension of transcendence degree one over the residue field of v_K. This shows that $v \in V(X)$. Clearly, isomorphic models induce the same set of valuations, so we get a map from isomorphism classes of normal models of X to finite non-empty subsets of $V(X)$. ∎

We will see later in this chapter that this map is injective and that it preserves the partial orders given by modifications and inclusion of sets, respectively (Corollary 3.18); if K is Henselian, then this map is a bijection. In the following we write $V(\mathcal{X}) \subseteq V(X)$ to denote the image of a normal model $\mathcal{X}$ under the above map.

Example 3.5 The model $\mathcal{X} \coloneqq \mathbb{P}^1_{\mathbb{Z}_p}$ (Example 3.2) induces $V(\mathcal{X}) = \{v\}$ where v is the valuation corresponding to the valuation ring $(\mathbb{Z}_p[t])_{(p)}$. In the language of Chapter 4, $v = v_0$.

3.1 Morphisms and Valuations

In this section we want to discuss how the sets of valuations of a normal model relate to morphisms of normal models and in particular to modifications of normal models.

Lemma 3.6 *Let $\mathcal{X}$ be a normal model of X, let $\mathcal{X}'$ be a normal model of another irreducible smooth projective curve X', and let $\varphi\colon \mathcal{X}' \to \mathcal{X}$ be a morphism of $\mathcal{O}_K$-schemes which induces a cover $X' \to X$ on the generic fiber. Let η be a generic point on the special fiber of $\mathcal{X}$. Then the preimage of η under φ is non-empty and consists of generic points on the special fiber of $\mathcal{X}'$. If φ is birational, then that preimage consists of exactly one generic point.*

Proof Let Z be the irreducible component of the special fiber of $\mathcal{X}$ which contains η. Since φ is surjective (our models are assumed to be proper and φ is dominant), there is a point η' on an irreducible component Z' of the special fiber of $\mathcal{X}'$ which is mapped to η. Since φ is dominant, the ring homomorphism $\mathcal{O}_{\mathcal{X},\eta} \to \mathcal{O}_{\mathcal{X}',\eta'}$ is injective. This is an extension of discrete valuation rings. Therefore $\eta' \in Z'$ must be generic. In particular, if φ is birational, then both rings are integrally closed in the same field of fractions which makes them equal. Therefore η' must be unique since $\mathcal{X}'$ is separated (see also Lemma 3.10). ∎

Combining Proposition 3.4 and Lemma 3.6, we get the following result.

Lemma 3.7 *Let $\varphi : \mathcal{X}' \to \mathcal{X}$ be a modification of normal models of X. Then $V(\mathcal{X}) \subseteq V(\mathcal{X}')$.* ∎

This shows that the map constructed in Proposition 3.4 turns the partial order on normal models of X, given by $\mathcal{X} \leq \mathcal{X}'$ if there is a morphism $\mathcal{X}' \to \mathcal{X}$, into the partial order on finite subsets of $V(X)$, given by inclusion of sets (cf. Corollary 3.18). The converse of this holds as well.

Lemma 3.8 [23, Theorem 8.3.20] *Let $\mathcal{X}$, $\mathcal{X}'$ be normal models of X with $V(\mathcal{X}) \subseteq V(\mathcal{X}')$. Then there is a modification $\mathcal{X}' \to \mathcal{X}$.* ∎

Note that unlike Lemma 3.6, this does not generalize to covers of curves: If $X' \to X$ is a cover of smooth irreducible curves with normal models $\mathcal{X}'$, $\mathcal{X}$ which satisfy

$$V(\mathcal{X}) = \{\, v\big|_{K(X)} : v \in V(\mathcal{X}') \,\}$$

there may not be a morphism of $\mathcal{O}_K$-schemes $\mathcal{X}' \to \mathcal{X}$.

We use Lemma 3.8 to show that the map constructed in Proposition 3.4 is injective.

Proposition 3.9 [23, Corollary 8.3.23] *Let $\mathcal{X}$, $\mathcal{X}'$ be normal models of X. Then $\mathcal{X}$, $\mathcal{X}'$ are isomorphic as normal models of X if and only if $V(\mathcal{X}) = V(\mathcal{X}')$.*

Proof Suppose that $V(\mathcal{X}) = V(\mathcal{X}')$. Then there are morphisms of normal models $\mathcal{X} \to \mathcal{X}'$ and $\mathcal{X}' \to \mathcal{X}$. The statement follows since the composition of these morphisms is in the equivalence class of the identity when considered as a rational map. ∎

3.2 Constructing Models from Valuations

In this section we want to show that, given a finite non-empty set of valuations in $V(X)$, we can construct a model which induces exactly these valuations, at least if we assume K to be Henselian. First, we need a few technical lemmata which help us to detect whether a normal model induces a given valuation.

Lemma 3.10 [23, Definition 8.3.17] *Let $\mathcal{X}$ be a normal model of X and let $v \in V(X)$. Then v has a unique center $x \in \mathcal{X}$, i.e., a point x on the special fiber which is such that for $\mathcal{O}_v \subseteq K(X)$, the valuation ring of v, there is a morphism $f : \operatorname{Spec} \mathcal{O}_v \to \mathcal{X}$ which maps the closed point to x and which makes the following diagram commutative:*

$$\begin{array}{ccc} \operatorname{Spec} \mathcal{O}_v & \xrightarrow{\quad f \quad} & \mathcal{X} \\ \uparrow & & \uparrow \\ \operatorname{Spec} \operatorname{Frac} \mathcal{O}_v & = & \operatorname{Spec} K(X) \end{array}$$

Proof By the valuative criterion of properness such a center exists and the morphism f is unique. The center is unique since two morphisms $\operatorname{Spec} \mathcal{O}_v \to \mathcal{O}_{\mathcal{X},x} \to \mathcal{X}$ (with possibly different centers x) coincide on a dense open subset of $\operatorname{Spec} \mathcal{O}_v$ and are therefore equal, in particular they map the closed point to the same closed point of $\mathcal{X}$. ∎

Example 3.11 Let $\mathcal{X}$ be a normal model of X. By definition, $v \in V(\mathcal{X})$ is induced by a generic point on the special fiber $\eta \in \mathcal{X}_s$. This point is the center of v. Conversely, take a $v \in V(X)$ which admits a center $x \in \mathcal{X}$ of codimension one. The defining diagram of the center shows that the map $\operatorname{Spec} \mathcal{O}_v \to \mathcal{X}$ factors through $\operatorname{Spec} \mathcal{O}_v \to \operatorname{Spec} \mathcal{O}_{\mathcal{X},x}$, i.e., $\mathcal{O}_v$ extends $\mathcal{O}_{\mathcal{X},x}$. Since $\mathcal{O}_{\mathcal{X},x}$ is integrally closed in its field of fractions, these discrete valuation rings are equal, which shows that $v \in V(\mathcal{X})$.

Lemma 3.12 *Let $\mathcal{X}$ be a normal model of X and let $v \in V(X)$ with center $x \in \mathcal{X}$. Let $f \in \mathcal{O}_{\mathcal{X},x}$ be such that $v(f) = 0$ and the image of f in the residue field of v is transcendental over k. Then $v \in V(\mathcal{X})$.*

Proof As outlined in the previous example, it suffices to show that x is a point of codimension one. By assumption there is an affine open set $\operatorname{Spec} A = U \subseteq \mathcal{X}$ such that $x \in U$ and $f \in A$. Let $\mathfrak{p}$ be the prime ideal of A corresponding to x. Since x is a point on the special fiber, its codimension is at least one. Its codimension is at most one if the dimension of $A/\mathfrak{p}$ is at least one, i.e., if $A/\mathfrak{p}$ is not a field. If it was a field, then it would be a finite extension of k but this is not the case since $f \in A$ remains transcendental over k when reduced mod $\mathfrak{p}$.∎

Lemma 3.13 *Let $\mathcal{X}$ be a normal model of X and let $v \in V(X)$. Let $f \in K(X)$ be such that $v(f) = 0$ and the image of f in the residue field of v is transcendental over k. Assume further that the rational map $\mathcal{X} \dashrightarrow \mathbb{P}^1$ induced by f is defined at the center of v. Then $v \in V(\mathcal{X})$.*

Proof Let $x \in \mathcal{X}$ be the center of v. With the previous lemma, it suffices to show that $f \in \mathcal{O}_{\mathcal{X},x}$. By assumption there are affine open sets $x \in U \subseteq \mathcal{X}$, $V \subseteq \mathbb{P}^1$ such that $f\colon K(t) \coloneqq K(\mathbb{P}^1) \to K(\mathcal{X})$, $t \mapsto f$ restricts to $\mathcal{O}_{\mathbb{P}^1}(V) \to \mathcal{O}_{\mathcal{X}}(U)$. Since V is affine, t or t^{-1} is contained in $\mathcal{O}_{\mathbb{P}^1}(V)$, and so f or f^{-1} is contained in $\mathcal{O}_{\mathcal{X}}(U)$ and therefore also in $\mathcal{O}_{\mathcal{X},x}$. We are done if $f \in \mathcal{O}_{\mathcal{X}}(U) \subseteq \mathcal{O}_{\mathcal{X},x}$. Suppose that $f^{-1} \in \mathcal{O}_{\mathcal{X},x}$. The image of f^{-1} under the local ring homomorphism $\mathcal{O}_{\mathcal{X},x} \to \mathcal{O}_v$ is a unit and therefore f^{-1} is a unit in $\mathcal{O}_{\mathcal{X},x}$. ∎

We use Lemma 3.13 to show that for any valuation we can find a model which induces it. The proof given here is not constructive; a slightly more constructive proof will be given afterwards.

Proposition 3.14 *Let $v \in V(X)$ and let $\mathcal{X}$ be a normal model of X. Then there is a modification $\varphi : \mathcal{X}' \to \mathcal{X}$ such that $v \in V(\mathcal{X}')$.*

Proof Let $f \in K(X)$ be such that $v(f) = 0$ and the image of f in the residue field of v is transcendental over k. Consider the rational map which f induces $\mathcal{X} \dashrightarrow \mathbb{P}^1$, let us also call this map f, and let $U \subseteq \mathcal{X}$ be its domain of definition. Let $\Gamma_f \subseteq \mathcal{X} \times \mathbb{P}^1$ be the graph of f, i.e., take the graph of $f\big|_U$ in $U \times \mathbb{P}^1$ and form its closure in $\mathcal{X} \times \mathbb{P}^1$. This is a model of X. The first projection $\mathcal{X} \times \mathbb{P}^1 \to \mathcal{X}$ induces a birational morphism $\Gamma_f \to \mathcal{X}$. The second projection induces a morphism $\Gamma_f \to \mathbb{P}^1$ which extends the rational map $f : \Gamma_f \dashrightarrow \mathbb{P}^1$. If $\mathcal{X}' \to \Gamma_f$ denotes the normalization of Γ_f, then this gives a normal model of X for which $f : \mathcal{X}' \to \mathbb{P}^1$ is a morphism; by Lemma 3.13, this implies that $v \in V(\mathcal{X}')$. ∎

Proposition *Let $X = \mathbb{P}^1_K$. Let $v \in V(X)$ and let $\mathcal{X}$ be a normal model of X. Then there is a modification $\varphi : \mathcal{X}' \to \mathcal{X}$ such that $v \in V(\mathcal{X}')$.*

Proof Let $x \in \mathcal{X}_s$ be the center of v. If x is a generic point of the special fiber, then there is nothing to do. Choose a parameter t to write $K(X)$ as a rational function field over K in t with $v(t) > 0$. In the notation of Chapter 4, let us write $v = [v_0, \ldots, v(\phi) = \lambda]$ for a key polynomial $\phi \in K[t]$ and a positive $\lambda = a/b \in \mathbb{Q}$. Since x is the center of v, we have $\phi \in \mathcal{O}_{\mathcal{X},x}$. Consider the ideal $I \coloneqq \left(\phi^b, \pi^a\right) \subseteq \mathcal{O}_{\mathcal{X},x}$ with π a uniformizer in K. As ϕ^b and π^a have positive valuation, they are in the maximal ideal of $\mathcal{O}_{\mathcal{X},x}$ and therefore I is a proper ideal. The ideal I induces an ideal sheaf $\mathcal{I}$ on $\mathcal{X}$. Let $\psi\colon \mathcal{X}' \to \mathcal{X}$ be the blowup of $\mathcal{X}$ with center $\mathcal{I}$. Let $\psi'\colon \mathcal{X}'' \to \mathcal{X}'$ be the normalization. This defines a normal model of X. The element $f \coloneqq \phi^b/\pi^a \in K(X)$ is a unit with respect to v and its reduction to the residue field of v remains transcendental over k. (That it remains transcendental can be seen from the reduction algorithm in Subsection 4.1.3.) The same holds for f^{-1}. Write x'' for the center of v in $\mathcal{X}''$. With Lemma 3.12 it suffices to show that f or its inverse is contained in $\mathcal{O}_{\mathcal{X}'',x''}$. Note that $\psi \circ \psi'(x'')$ is a center for v in $\mathcal{X}$; as the center is unique, $x' \coloneqq \psi'(x'')$ is in the fiber of x. Consider an affine patch of $U = \operatorname{Spec} A \subseteq \mathcal{X}$ which contains x and on which ϕ^b and π^a are regular. The blowing-up of A along (ϕ^b, π^a) is covered by the affine open schemes $\operatorname{Spec} A[f]$ and $\operatorname{Spec} A[f^{-1}]$ [23, Lemma 8.1.4]. Therefore, the local rings at all points of $\mathcal{X}'$ above x (in particular x') contain at least one of f, f^{-1}. This completes the proof since the local ring at x' injects into the local ring at x''. ∎

Example 3.15 Consider the model $\mathcal{X} \coloneqq \mathbb{P}^1_{\mathbb{Z}_p}$ (Example 3.2) and a valuation v on $K(X)$ which is given, in the language of Chapter 4, as $v = [v_0, v(t) = 1]$. Let $U \coloneqq \operatorname{Spec} \mathbb{Z}_p[t]$ be an affine open subset of $\mathcal{X}$. Consider the blowup $\mathcal{X}' \to \mathcal{X}$ with center (t, p). On U one patch of the blowup is given as $U' \coloneqq \operatorname{Spec} \mathbb{Z}_p[t, u]/(tu - p)$. Since p is invertible in $\mathbb{Q}_p$, the generic fiber of U' is $\mathbb{A}^1$ without one point. The special fiber is of the form $\operatorname{Spec} \mathbb{F}_p[t, u]/(tu)$, two affine lines meeting in a single point. In particular the special fiber is reduced. Therefore $\mathcal{X}'$ is a normal model of X[23, Lemma 4.1.18]. For the line $u = 0$, the local ring at its generic point $\mathcal{O}_{\mathcal{X},\eta}$ induces the Gauss valuation v_0. For the line $t = 0$ a direct calculation shows that the local ring at its generic point induces the valuation v.

Inductively this shows that for any finite set of valuations we can find a model which induces all these valuations. However this process might introduce additional undesired valuations. To eliminate those, we use the following proposition.

Proposition 3.16 *Let K be Henselian, let $\mathcal{X}$ be a normal model of X, and let $V \subseteq V(\mathcal{X})$ be non-empty. Then there is a normal model $\mathcal{X}'$ of X with $V(\mathcal{X}') = V$ and a modification $\mathcal{X} \to \mathcal{X}'$.*

Proof [23, Theorem 8.3.36] ∎

Remark 3.17 Note that complete fields are Henselian, so the proposition holds in particular for local fields. The proposition is wrong without the Henselian hypothesis. A counterexample is given in [4, Section 6.7]. For a more general statement see [17, Theorem 1].

Combining the statements of this section, we see that the map constructed in Proposition 3.4 is surjective. We collect the results we obtained until now in the following corollary.

Corollary 3.18 *Over a Henselian field there is an isomorphism of partially ordered sets between the finite non-empty subsets of $V(X)$ (ordered by inclusion) and the isomorphism classes of normal models of X (ordered by morphisms of normal models.)* ■

Chapter 4

Mac Lane Valuations

Let K be a field with a discrete valuation v_K and residue field k. Let X be an irreducible smooth projective curve over K. We have seen in Chapter 3 how normal models of X relate to certain discrete valuations on $K(X)$, the function field field of X. These valuations have the following two properties:

(a) $v\big|_K = v_K$, and

(b) the residue field of v is of transcendence degree one over k.

Example 4.1 For $K = \mathbb{Q}_p$ and $X = \mathbb{P}^1_K$, an example of such a valuation is the valuation which corresponds to the discrete valuation ring $(\mathbb{Z}_p[t])_{(p)} \subseteq \mathbb{Q}_p(t) = K(X)$. The valuation of a point, e.g., the one corresponding to the valuation ring $(\mathbb{Q}_p[t])_{(t)}$, would be a non-example since it does not extend the p-adic valuation on $\mathbb{Q}_p$.

In general, a curve X can be considered as a finite cover of $\mathbb{P}^1$. In this case, $K(X)$ is a finite separable extension of the function field of the projective line. The latter is of the form $K(t)$ for a transcendental variable t.

We begin this chapter recalling the theory developed in [24] and [12] to describe discrete valuations on $K(t)$ (Section 4.1.) Using that theory, one can classify the valuations on $K(t)$ which additionally satisfy (a) and (b) (Section 4.2.) We then discuss to what extent we can find a unique representation of such valuations (Section 4.3.) Using the language of rigid analytic geometry, we obtain another classification of such valuations which also strengthens some uniqueness results (Section 4.4.) After a brief excursion to the graded algebra of such valuations (Section 4.5,) we follow the exposition in [25] to get a description of discrete valuations on function fields of curves and show how this description can be computed in practice (Section 4.6.) Finally, we illustrate the theory with two applications, namely a factorization algorithm over the completion of K (Section 4.7) and an algorithm which determines the configuration of the roots of a polynomial (Section 4.8.)

4.1 Valuations on Rational Function Fields

Throughout this section let K be a field with a discrete valuation $v_K \colon K \to \mathbb{Q} \cup \{\infty\}$. Let v be a discrete valuation on the rational function field $K(t)$ which

extends v_K. An element in $K(t)$ is of the form f/g with $f, g \in K[t]$ and satisfies $v(f/g) = v(f) - v(g)$. To describe the valuation v it is therefore sufficient to describe the valuation $v\big|_{K[t]}$. We will now recall the theory developed in [24] and [12] to describe such valuations.

4.1.1 Inductive Valuations on Polynomial Rings

Let $V(K[t])$ denote the set of discrete valuations on $K[t]$ which extend v_K and satisfy $v(t) \geq 0$. (This condition comes at no loss of generality since eventually we want to describe valuations on the rational function field $K(t)$. If $v(t) < 0$, we can work over the rational function field $K(s)$ with $s = 1/t$.) For the valuations in $V(K[t])$ there is a partial order: we say that $v \leq v'$ if $v(f) \leq v'(f)$ for all polynomials f.

Example 4.2 The *Gauss valuation*, i.e., the valuation

$$v_0\Big(\sum a_i t^i\Big) \coloneqq \min_i\{v_K(a_i)\},$$

is minimal with respect to that order.

For most discrete valuations $v \in V(K[t])$, the ring

$$\mathcal{O}_v \coloneqq \{f \in K[t] : v(f) \geq 0\}$$

modulo its elements of positive valuation

$$\mathcal{O}_v^+ \coloneqq \{f \in K[t] : v(f) > 0\}$$

will not be a field but only an integral domain. We will therefore call this ring the *residue ring* of v and its field of fractions the *residue field* of v (which can be identified with the residue field of $K(t)$.)

Example 4.3 For the Gauss valuation v_0, the residue ring

$$\{f \in K[t] : v_0(f) \geq 0\}/\{f \in K[t] : v_0(f) > 0\}$$

is not a field but an integral domain isomorphic to $k[t]$ where k is the residue field of v_K. As we have discussed earlier, the Gauss valuation induces a valuation on $K(t)$. There,

$$\{f \in K(t) : v_0(f) \geq 0\}/\{f \in K(t) : v_0(f) > 0\}$$

is a field isomorphic to $k(t)$ which is isomorphic to the field of fractions of the former residue ring.

Suppose that we are given two discrete valuations $v' \geq v$ on $K[t]$. If the value group of v is contained in the value group of v', we call the index of the subgroup the *index* of v' over v and denote this number by $e(v' \mid v)$.

We now come back to the aim of this section, describing the elements of $V(K[t])$. Let $v \in V(K[t])$, $\phi \in K[t]$ monic, and $\lambda \in \mathbb{Q}$. Define $w\colon K[t] \to \mathbb{Q} \cup \{\infty\}$ as follows. Write $f \in K[t]$ in its *ϕ-adic expansion*, i.e., write $f = \sum_i a_i \phi^i$ such that all $a_i \in K[t]$ satisfy $\deg a_i < \deg \phi$. Such an expansion can be computed using division with remainder, which also shows that it is unique. Associate to f

a generalized *Newton polygon*, the lower convex hull of the points $(i, v(a_i) + i\lambda)$. Set $w(f)$ to be the smallest ordinate of that polygon, i.e.,

$$w(f) \coloneqq \min_i \{v(a_i) + i\lambda\}.$$

To determine when such w defines a discrete valuation on $K[t]$, we need the following notions which generalize equivalence modulo v in $K[t]$.[1]

Definition 4.4 Let v be a discrete valuation in $V(K[t])$, and let $f, g \in K[t]$. We say that

(a) f and g are *v-equivalent* if $v(f-g) > v(f)$ or $f = g = 0$. We denote this equivalence relation by
$$f \sim_v g.$$

(b) f is *v-divisible* by g if there is a $c \in K[t]$ such that $gc \sim_v f$. We denote this by
$$g \mid_v f.$$

(c) f is *v-irreducible* if whenever a product of elements in $K[t]$ is v-divisible by f, then one of its factors is.

(d) f is *v-minimal* if it is not constant and any nonzero element $h \in K[t]$ which is v-divisible by f has $\deg h \geq \deg f$.

Example 4.5 Take $K = \mathbb{Q}_p$ with v_K the p-adic valuation. Let v_0 be the Gauss valuation on $K[t]$. Then $\sim_{v_0}$ is a natural generalization of the equivalence relation given by reduction mod p. For example we have $1 \sim_v pt + 1$ and $p \sim_v p + p^2$ but we also get $p \nsim_v p^2$. An example of a polynomial which is v_0-irreducible and v_0-minimal is $\phi = t^2 + t + 1$ over $\mathbb{Q}_2$.

Some basic properties of equivalence and divisibility are collected in the following lemma.

Lemma 4.6 *Let v be a discrete valuation in $V(K[t])$ and let f, f', g, $g' \in K[t]$. Then the following statements hold:*

(a) If $f \sim_v f'$ and $g \sim_v g'$, then $fg \sim_v f'g'$.

(b) If $f \sim_v f'$, $g \sim_v g'$, and $g \mid_v f$, then $g' \mid_v f'$.

(c) If $f \sim_v f'$, $0 \neq f$, and $fg \sim_v f'g'$, then $g \sim_v g'$.

(d) If $ff' \sim_v 1$, then $g \mid_v g'$ if and only if $g \mid_v fg'$.

(e) If $ff' \sim_v 1$, then $g \mid_v g'$ if and only if $fg \mid_v g'$.

(f) If $v(f) = v(g) = 0$, then $f \mid_v g$ if and only if f divides g in the residue ring of v.

Proof The proofs are simple applications of the strict triangle inequality for discrete valuations:

[1] In [39], equivalent definitions are given starting from the graded algebra of v. Some readers might find those more appealing. Since we do not need the graded algebra for most of our considerations we chose to postpone those until Section 4.5.

(a) Since $v(f-f') > v(f) = v(f')$ and $v(g-g') > v(g) = v(g')$, we have $v(fg - f'g') = v((f-f')g + f'(g-g')) > v(fg) = v(f'g')$.

(b) Let c be such that $v(f-cg) > v(f) = v(cg)$. Then $v(f'-cg') = v((f'-f) - c(g'-g) + f - cg) > v(f)$.

(c) Suppose that $v(g-g') = v(g)$. Since $v(f-f') > v(f) = v(f')$, we have $v((f-f')g) > v(fg)$. At the same time $v(f'(g-g')) = v(f'g) = v(fg)$. Therefore $v(fg - f'g) = v((f-f')g + f'(g-g')) = v(fg)$, a contradiction.

(d) If $g|_v g'$, then there is a c such that $cg \sim_v g'$, and so $cfg \sim_v fg'$. Conversely if $g \mid_v fg'$, then there is a c such that $cg \sim_v fg'$. Therefore $cf'g \sim_v ff'g'$ which, by the previous statement implies that $cf'g \sim_v g'$ as required.

(e) Suppose that $g \mid_v g'$. Then there is a c such that $cg \sim_v g'$. Therefore $cfg \sim_v fg'$, and so $fg \mid_v fg'$. With the previous statement we get $fg \mid_v g'$. The other direction is trivial.

(f) This is immediate by definition. ∎

Definition 4.7 [24, Definition 4.1] Let v be a discrete valuation in $V(K[t])$. A monic polynomial $\phi \in K[t]$ which is v-irreducible and v-minimal is called a *key polynomial* over v.

We classify the key polynomials over v_0 in the following lemma.

Lemma 4.8 *Let $\phi = \sum_{i=0}^{m} a_i t^i \in K[t]$ be a monic polynomial positive degree. Then ϕ is a key polynomial over v_0 if and only if*

(a) $v_0(\phi) = 0$, and

(b) the reduction of ϕ modulo v_0 is irreducible in the residue ring of v_0.

Proof Suppose that ϕ satisfies the conditions. To see that ϕ is v_0-irreducible, let $f, g \in K[t]$ be such that $\phi \mid_{v_0} fg$. After multiplication with a power of the uniformizer in K, we may assume that $v(f) = v(g) = 0$ (Lemma 4.6 (d).) The v-irreducibility follows immediately from Lemma 4.6 (f).

To prove v_0-minimality, let $g \in K[t] \setminus \{0\}$ be such that $\phi \mid_{v_0} g$. Again, we may assume that $v_0(g) = 0$. Since the reduction of ϕ has the same degree as ϕ, the reduction of g must have at least that degree.

For the converse, let ϕ be a key polynomial over v_0. Suppose that $v_0(\phi) < 0$. Let $k \in \{0, \dots, m-1\}$ be the largest index such that $v_K(a_k)$ is minimal. Then $g \coloneqq \sum_{i=0}^{k} a_i t^i$ is v_0-divisible by ϕ but has lower degree than ϕ, contradicting its minimality.

If the reduction of ϕ is not irreducible in the residue ring, say it factors as fg, these factors lift to $K[t]$ contradicting the v_0-irreducibility. ∎

Definition 4.9 Let $v \in V(K[t])$, $\phi \in K[t]$ a key polynomial over v, and $\lambda \in \mathbb{Q}$. The function

$$\begin{aligned} w\colon \qquad & K[t] \to \mathbb{Q} \cup \{\infty\}, \\ & \sum_i a_i \phi^i \mapsto \min_i (v(a_i) + i\lambda) \end{aligned}$$

is called an *augmented valuation* if $w > v$. We write $w = [v, w(\phi) = \lambda]$.

It might appear difficult to check whether $w \geq v$. Lemma 4.17 shows that this is actually trivial for the valuations which we are studying.

Example 4.10 Let $K = \mathbb{Q}_2$ and let $v := v_0$ be the Gauss valuation on $K[t]$ over the 2-adic valuation. Let $\phi := t^2 + t + 1 \in K[t]$, a key polynomial over v_0. Then

$$w = [v_0, w(\phi) = 1/2]$$

is an augmented valuation.

Lemma 4.11 [24, Theorem 4.2] *Let $v \in V(K[t])$ and let $w = [v, w(\phi) = \lambda]$ be an augmented valuation. Then w is a discrete valuation on $K[t]$.* ∎

The proof of the above lemma and many other basic results on augmented valuations rely on the following lemma.

Lemma 4.12 [24, Lemma 4.3] *Let $v \in V(K[t])$, $\phi \in K[t]$ a key polynomial over v. Let $f \in K[t] \setminus \{0\}$ and write $f = q\phi + r$ for the quotient with remainder. Then $v(r) \geq v(f)$ and $v(q\phi) \geq v(f)$. The first inequality is strict, i.e., $v(r) > v(f)$, if and only if $\phi \mid_v f$.* ∎

Note that the lemma allows us to decide whether $\phi \mid_v f$ from the ϕ-adic expansion. For an augmented valuation, this fact can be phrased as follows.

Lemma 4.13 [24, Theorem 5.1] *Let $w = [v, w(\phi) = \lambda]$ be an augmented valuation on $K[t]$ and let $f \in K[t]$. Then $w(f) > v(f)$ if and only if $\phi \mid_v f$.* ∎

As an application of these lemmata, we get the following statement about divisibility of key polynomials.

Lemma 4.14 *Let v be a discrete valuation in $V(K[t])$. Let ϕ, $\phi' \in K[t]$ be key polynomials over v. Then $\phi' \mid_v \phi$ if and only if $\phi' \sim_v \phi$.*

Proof That equivalence implies divisibility is clear from the definition. Let us therefore assume that $\phi' \mid_v \phi$. Write the quotient with remainder $\phi = q\phi' + r$. By Lemma 4.12, $v(r) > v(\phi)$, i.e., $\phi \sim_v q\phi'$. As ϕ is v-irreducible q or ϕ' are v-divisible by ϕ. If $\phi \mid_v q$, then this would contradict the minimality of ϕ. Therefore $\phi \mid_v \phi'$, and $\deg \phi = \deg \phi'$. Hence $\phi - \phi' = r$ with $v(r) > v(\phi)$ which proves v-equivalence. ∎

Remark 4.15 Let $w = [v, w(\phi) = \lambda]$ and $w' = [v, w'(\phi') = \lambda]$ be two augmented valuations. Note that w and w' may be different even though ϕ and ϕ' are v-equivalent. As an example of this, let $v := v_0$ be the Gauss valuation on $\mathbb{Q}[t]$ induced by the 2-adic valuation on $\mathbb{Q}$. Let $\phi = t$ and $\phi' = t + 2$, two v-equivalent polynomials. Then $w = [v, w(\phi) = 2]$ and $w' = [v, w(\phi') = 2]$ are different. Indeed, $w(t + 2) = 1 \neq 2 = w'(t + 2)$. However, if we had chosen $w = [v, w(\phi) = 1]$ and $w' = [v, w'(\phi') = 1]$, then the valuations would be equal. (See Theorem 4.33 for a more detailed discussion.)

The procedure of augmenting valuations can be used to augment the Gauss valuation v_0 to a discrete valuation $v_1 := [v_0, v_1(\phi_1) = \lambda_1]$. Augmenting again, we inductively get valuations of the form

$$v_n = [v_0, v_1(\phi_1) = \lambda_1, v_2(\phi_2) = \lambda_2, \ldots, v_n(\phi_n) = \lambda_n].$$

We call a valuation of this kind *inductive* over v_K if it additionally satisfies

(i) $\deg \phi_{i+1} \geq \deg \phi_i$, and

(ii) $\phi_i \nsim_{v_i} \phi_{i+1}$ for all $i \in \{1, \ldots, n-1\}$.

It turns out that all discrete valuations which are relevant to our theory, i.e., they extend v_K and their residue field is of transcendence degree one, are inductive (Theorem 4.31.)

Remark 4.16 The two conditions come with no loss of generality. If any of the conditions is not satisfied, then ϕ_{i+1} is a key polynomial over v_{i-1} and v_{i+1} coincides with $w \coloneqq [v_{i-1}, w(\phi_{i+1}) = \lambda_{i+1}]$. With the same argument, the first condition could even be strengthened further, requiring the degrees of key polynomials to be strictly increasing.

The following lemma shows that the increasing degrees of the key polynomials are enough to guarantee that inductive valuations are actually augmented valuations.

Lemma 4.17 [24, Theorem 5.1, Lemma 6.3] *Let $v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$ be an inductive valuation over v_K, let $\phi_{n+1} \in K[t]$ be a key polynomial over v_n with $\deg \phi_{n+1} \geq \deg \phi_n$, and let $\lambda_{n+1} > v_n(\phi_{n+1})$. Then*

$$v_{n+1} = [v_n, v_{n+1}(\phi_{n+1}) = \lambda_{n+1}]$$

is an augmented valuation, i.e., $v_{n+1} \geq v_n$. ∎

Example 4.18 Consider again the example $v_1 = [v_0, v_1(t^2 + t + 1) = 1/2]$ over $\mathbb{Q}_2$. This inductive valuation has index two over v_0. The residue field of v_1 is generated over $\mathbb{F}_2$ by the reduction of t (which in reduction satisfies the equation $t^2 + t + 1 = 0$) and the reduction of

$$\frac{(t^2 + t + 1)^2}{2}$$

which remains transcendental over the residue field of v_K.

For an inductive valuation the following lemma, which complements Lemma 4.8, is useful to check whether a polynomial is a key polynomial.

Lemma 4.19 [24, Theorem 9.4] *Let $v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$ with $n \geq 1$ be an inductive valuation over v_K. Let $\phi \in K[t]$ be a polynomial with $\deg \phi \geq \deg \phi_n$ which is not v_n-equivalent[2] to ϕ_n and whose ϕ_n-adic expansion is*

$$\phi = \sum_{i=0}^{m} a_i \phi_n^i.$$

Then ϕ is a key polynomial over v_n if and only if

(i) $a_m = 1$,

(ii) $v_n(a_0) = v_n(\phi)$,

[2]This condition is missing in the statement of [24, Theorem 9.4]; it is, however, used in the proof. It is necessary: the key polynomial $\phi = \phi_n$ does not satisfy (ii).

(iii) $v_n(\phi_n^m) = v_n(\phi)$,

(iv) $e(v_n \mid v_{n-1})$ *divides* m, *and*

(v) ϕ *is* v_n*-irreducible.*

Remark 4.20 This Lemma makes it easy to decide whether a polynomial ϕ is a key polynomial. The validity of the first three conditions of the Lemma can be read off the ϕ_n-adic expansion of ϕ which can be computed through polynomial quotient with remainder. The size of the value groups of the v_i are essentially given by the denominators of the λ_i, verifying the condition on the index is therefore easy (this is made explicit in Corollary 4.30.) It is slightly more difficult to decide whether ϕ is v_n-irreducible. We will see in Lemma 4.27 how this can be reduced to a problem of irreducibility of a polynomial in the residue ring of v_n.

As a consequence of Lemma 4.19 we see that the sequence of λ_n must be increasing in an inductive valuation.

Lemma 4.21 [24, Lemma 6.3] *Let* $v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$ *be an inductive valuation over* v_K*. Then*

$$\lambda_n > \lambda_{n-1} > \cdots > \lambda_1 > 0.$$

Proof It suffices to show that $\lambda_n > \lambda_{n-1}$. Let

$$\phi_n = \sum_{i=0}^{m} a_i \phi_{n-1}^i$$

be the ϕ_{n-1}-adic expansion of ϕ_n. Then

$$\begin{aligned} \lambda_n &= v_n(\phi_n) \\ &> v_{n-1}(\phi_n) && \text{by definition of an augmented valuation} \\ &= v_{n-1}(\phi_{n-1}^m) && \text{by Lemma 4.19} \\ &= m\lambda_{n-1}. \end{aligned}$$

■

Lemma 4.22 [24, Theorem 6.4] *Let* $v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$ *be an inductive valuation over* v_K*. Then*

$$v_n(\phi_k) = \lambda_k$$

for all $k \in \{1, \ldots, n\}$.

Proof We prove this for $k = n - 1$. (The general case is an easy extension of the argument.) If $\deg \phi_{n-1} < \deg \phi_n$, then there is nothing to prove, so let us assume that the degrees are equal. By the assumptions on inductive valuations, ϕ_n is not v_{n-1}-equivalent to ϕ_{n-1}, i.e.,

$$v_{n-1}(\phi_n - \phi_{n-1}) = v_{n-1}(\phi_{n-1}) = \lambda_{n-1}.$$

As the degree of $\phi_n - \phi_{n-1}$ is lower than the degree of ϕ_n,

$$v_n(\phi_n - \phi_{n-1}) = v_{n-1}(\phi_n - \phi_{n-1}).$$

With Lemma 4.21 this gives

$$v_n(\phi_{n-1}) = v_n(\phi_n - (\phi_n - \phi_{n-1})) = \min\{\lambda_n, \lambda_{n-1}\} = \lambda_{n-1}.$$

■

4.1.2 Computational Tools

We are going to collect some constructive results on inductive valuations which are the base for our algorithmic considerations. As before, K is a field with a discrete valuation v_K, and v_0 denotes the Gauss valuation on $K[t]$.

Lemma 4.23 [24, Theorem 9.3] *Let $v_n = [v_0, \dots, v_n(\phi_n) = \lambda_n]$ be an inductive valuation over v_K and let $\lambda \in \mathbb{Q}$ be an element of the value group of v_n. Then there is a polynomial $S_\lambda \in K[t]$ such that $v_n(S_\lambda) = \lambda$ and $v(S_\lambda) = \lambda$ for any inductive valuation obtained by augmenting v_n.*

Proof There are natural numbers m_i such that the valuation of $\phi_1^{m_1} \cdots \phi_n^{m_n}$ differs from λ by an integer. Multiplying by a power of the uniformizer of K yields a polynomial S_λ with $v_n(S_\lambda) = \lambda$. For augmented valuations, $v(S_\lambda) = \lambda$ by Lemma 4.22. ∎

The following lemma shows that we can essentially treat certain polynomial as if they were units.

Lemma 4.24 [24, Lemma 9.1] *Let $v_n = [v_0, \dots, v_n(\phi_n) = \lambda_n]$ be an inductive valuation over v_K with $n \geq 1$. Let $f \in K[t]$ be such that $v_n(f) = v_{n-1}(f)$. Then there is a v_n-reciprocal $f' \in K[t]$, i.e., f' satisfies $v_{n-1}(f') = v_n(f') = -v_n(f)$ and $f'f$ is v_n-equivalent to 1.*

Proof By Lemma 4.13 the polynomial f is not v_{n-1}-divisible by ϕ_n. In particular ϕ_n does not divide f in $K[t]$. Since ϕ_n is irreducible (in the classical sense,) f and ϕ_n are coprime and there are polynomials such that $f'f + h\phi_n = 1$. Then $v_{n-1}(f') = v_n(f')$ because $\deg f' < \deg \phi_n$, We have

$$\begin{aligned} v_n(f'f - 1) &= v_n(h\phi_n) \\ &> v_{n-1}(h\phi_n) && \text{by Lemma 4.13} \\ &= v_{n-1}(f'f - 1) \\ &\geq \min\{v_{n-1}(f'f), v_{n-1}(1)\} \end{aligned}$$

but as neither the valuation of $f'f$ nor the valuation of 1 changes when going from v_{n-1} to v_n, we have $v_n(f'f) = v_n(1)$ and $v_{n-1}(f'f) = v_{n-1}(1)$. Therefore $f'f$ is v_n-equivalent to 1. ∎

Example 4.25 Let $K = \mathbb{Q}_2$ and $v_1 = [v_0, v_1(t^2+t+1) = 1/2]$. The construction from the proof shows that for $f = t^2$ we get $f' = t$ and indeed

$$v_1(t^3 - 1) = v_1((t-1)\phi_1) = 1/2 > 0 = v_1(t^3) = v_1(1).$$

The previous two lemmata allow us to shift certain polynomials to valuation zero and decide their irreducibility and minimality after reduction to the residue ring. The following two lemmata can be seen as a generalization of Lemma 4.8 which uses the same idea in the proof.

Lemma 4.26 [24, Lemma 11.1] *Let $v_n = [v_0, \dots, v_n(\phi_n) = \lambda_n]$ be an inductive valuation over v_K with $n \geq 1$. Let $f \in K[t]$ be such that $v_n(f)$ is in the value group of v_{n-1},[3] and let S be a polynomial with $v_{n-1}(S) = v_n(S) = -v_n(f)$*

[3] [24, Lemma 11.1] mistakenly requires $v_n(f) = v_{n-1}(f)$ instead. This would make the statement trivial, since such $f \neq 0$ divides any element. The proof loc. cit. only uses that $v_n(f)$ is in the value group of v_{n-1}.

(e.g., as constructed in Lemma 4.23.) Then a polynomial h with $v_n(h) = 0$ is v_n-divisible by f if and only if Sf divides h in the residue ring of v_n.

Proof By Lemma 4.6 (e), $f \mid_{v_n} h$ if and only if $Sf \mid_{v_n} h$, which by Lemma 4.6 (f) happens if and only if Sf divides h in the residue ring. ∎

Lemma 4.27 [24, Lemma 11.2] *Let $v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$ be an inductive valuation over v_K with $n \geq 1$. Let $f \in K[t]$ be such that $v_n(f)$ is in the value group of v_{n-1}, and let S be a polynomial with $v_{n-1}(S) = v_n(S) = -v_n(f)$ (e.g., as constructed in Lemma 4.23.) Then f is v_n-irreducible if and only if Sf is prime in the residue ring of v_n.* ∎

4.1.3 Algorithmic Reduction

Deciding whether a polynomial is a key polynomial over an inductive valuation is an essential step in the construction of inductive valuations. The preceding lemmata show that this can be reduced to determining the ϕ-adic expansion of the polynomial, computing reductions to the residue ring, and deciding irreducibility there. We now present an efficient way to compute that reduction following the exposition in [24, Theorems 10.2 and 12.1]. The approach is inductive: the reduction maps for $v_0, \ldots, v_n$ will be used to define the reduction map for v_{n+1}.

It is clear how to compute reductions for the Gauss valuation v_0: Let $\mathbb{F}_0[y_0]$ be the residue ring of v_0, i.e., let $\mathbb{F}_0$ be the residue field of v_K and define the reduction of a polynomial $f \in K[t]$ with integral coefficients by reducing the coefficients to the residue field of v_K and mapping $t \mapsto y_0$. Let us denote this reduction map by H_0.[4]

Let $v_1 = [v_0, v_1(\phi_1) = \lambda_1]$ be an inductive valuation. As ϕ_1 is a key polynomial, $v_0(\phi_1) = 0$ and $\lambda_1 > 0$. Let ψ_1 be the reduction of ϕ_1 to the residue ring of v_0, an irreducible element by Lemma 4.8. Set

$$\mathbb{F}_1 \coloneqq \mathbb{F}_0[y_0]/(\psi_1(y_0)).$$

We want to show that the residue ring of v_1 is isomorphic to $\mathbb{F}_1[y_1]$. Define a reduction map $H_1 \colon \mathcal{O}_{v_1} \to \mathbb{F}_1[y_1]$ as follows. Polynomials with positive valuation are mapped to zero; for a polynomial f of valuation zero, let

$$f = \sum_{i=0}^{m} a_i \phi_1^i$$

be its ϕ_1-adic expansion. Since any terms with $v_0(a_i\phi_1^i) > 0$ do not affect the reduction, we may assume that all terms have valuation zero or vanish. For the terms that do not vanish we have $v_0(a_i) = -i\lambda_1$, in particular i must be a multiple of the index $e \coloneqq e(v_1 \mid v_0)$. Let $S \coloneqq \pi$ be a uniformizer in K and let $\ell = e\lambda_1$. We may then write

$$f = \sum_{j=0}^{m/e} a_{ej} S^{\ell j} S^{-\ell j} \phi_1^{ej}$$

[4] In the following $\mathbb{F}_i$ will be used to denote a certain subfield of the residue ring of v_i. In examples we will also use $\mathbb{F}_i$ to denote a finite field with i elements. It will always be clear from the context which of the two should be considered.

and set

$$H_1(f) \coloneqq \sum_{j=0}^{m/e} H_0\big(a_{ej} S^{\ell j}\big) y_1^j.$$

It is clear from the construction that H_1 is a surjective homomorphism of rings whose kernel is $\mathcal{O}_{v_1}^+$. Note that polynomials with $v_0(f) \geq 0$ must have $H_1(f) = H_1(a_0)$ and are thus mapped to the subring $\mathbb{F}_1 \subseteq \mathbb{F}_1[y_1]$.

Example 4.28 Let $K = \mathbb{Q}_2$ and $v_1 = [v_0, v_1(t^2 + t + 1) = 1/2]$. We compute the reduction of

$$f \coloneqq \frac{t^4 + 2t^3 + 5t^2 + 4t + 5}{2}.$$

The ϕ_1-adic expansion of f is

$$f \coloneqq \frac{1}{2}\phi_1^2 + \phi_1 + 1.$$

The linear term does not affect the reduction so we may rewrite this as

$$f \equiv \frac{1}{2}\phi_1^2 + 1 = \frac{1}{2} S \cdot S^{-1} \phi_1^2 + 1$$

with $S = 2$. Hence $H_1(f) = y_1 + 1$.

The general inductive construction is very similar to the one described in the previous paragraph, we only have to replace S^ℓ and $S^{-\ell}$ appropriately. Let an inductive valuation $v_{n+1} = [v_0, \ldots, v_{n+1}(\phi_{n+1}) = \lambda_{n+1}]$ be given. Without loss of generality we may assume that $\deg \phi_{i+1} > \deg \phi_i$ (one may safely drop all ϕ_i for which this is not the case without changing the valuation.) Suppose that a residue ring of the form $\mathbb{F}_n[y_n]$ and a reduction map H_n have been constructed for v_n. By Lemma 4.19, $v_n(\phi_{n+1})$ must be in the value group of v_{n-1}. We can use Lemma 4.23 to construct an element $S \in K[t]$ which is uniformizing for v_{n-1} and satisfies $v_{n-1}(S) = v_n(S)$; let S' be its v_n-reciprocal (Lemma 4.24). Let R be a power of S' such that $v_n(R\phi_{n+1}) = 0$ and define $\psi \coloneqq H_n(R\phi_{n+1})$, an irreducible polynomial by Lemma 4.27. Let $\mathbb{F}_{n+1} \coloneqq \mathbb{F}_n[y_n]/(\psi(y_n))$. We show in Lemma 4.29 that the residue ring of v_{n+1} is isomorphic to $\mathbb{F}_{n+1}[y_{n+1}]$. Assuming that this is the case, let us define a map H_{n+1} which maps polynomials f with $v_{n+1}(f) \geq 0$ to that ring.

A polynomial f with $v_{n+1}(f) > 0$ is mapped to zero. For a polynomial with $v_{n+1}(f) = 0$, write down its ϕ_{n+1}-adic expansion,

$$f = \sum_{i=0}^{m} a_i \phi_{n+1}^i.$$

Terms with $v_{n+1}(a_i \phi_{n+1}^i) > 0$ have no influence on the reduction, so we may assume that for such terms $a_i = 0$. For other terms, $v_n(a_i) = v_{n+1}(a_i) = -v_{n+1}(\phi_{n+1}^i) = -i\lambda_{n+1}$. Since $v_n(a_i)$ is in the value group of v_n, i must be a multiple of the index $e \coloneqq e(v_{n+1} \mid v_n)$. Let S be a uniformizing element for v_n and S' its v_{n+1}-reciprocal. Pick a positive integer ℓ such that $v_n(S^\ell) = e\lambda_{n+1}$. We may now write

$$f = \sum_{j=0}^{m/e} \big(a_{ej} S^{\ell j}\big) \big(S'^{\ell} \phi_{n+1}^e\big)^j,$$

and set

$$H_{n+1}(f) \coloneqq \sum_{j=0}^{m/e} H_n\big(a_{ej}S^{\ell j}\big) \cdot y_{n+1}^j \in \mathbb{F}_{n+1}[y_{n+1}].$$

Lemma 4.29 [24, Theorem 12.1] *Let $v_{n+1} = [v_0, \ldots, v_{n+1}(\phi_{n+1}) = \lambda_{n+1}]$ be an inductive valuation over v_K. Then H_{n+1} as defined above is the reduction map to the residue ring, i.e., $H_{n+1}\colon \mathcal{O}_{v_{n+1}} \to \mathbb{F}_{n+1}[y_{n+1}]$ is a surjective homomorphism of rings with kernel $\mathcal{O}^+_{v_{n+1}}$.*

Proof We proceed by induction on n. Let us therefore assume that H_n is the reduction map for v_n. (The cases $n = 0$, 1 have already been treated above.) In the following we use the same notation for H_{n+1} as we used in the paragraph preceding this lemma. That H_{n+1} is a homomorphism of rings follows readily from the construction. To see for example that it respects sums, take two polynomials f and g of valuation zero with respective ϕ_{n+1}-adic expansions (dropping irrelevant terms)

$$f = \sum_i a_{ei}\phi_{n+1}^{ei},$$
$$g = \sum_i b_{ei}\phi_{n+1}^{ei}.$$

Then the ϕ_{n+1}-adic expansion of $f + g$ is

$$\sum_i (a_{ei} + b_{ei})\phi_{n+1}^{ei},$$

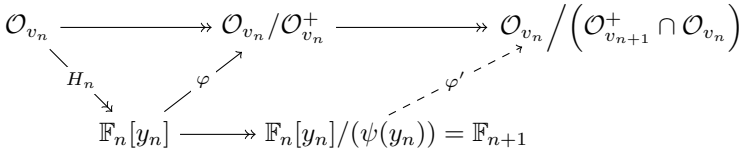
and so

$$H_{n+1}(f+g) = \sum_{j=0}^{m/e} H_n(a_{ej}S^{\ell j} + b_{ej}S^{\ell j}) \cdot y_{n+1}^j.$$

This is $H_{n+1}(f) + H_{n+1}(g)$ because H_n respects sums. Similarly, one shows that H_{n+1} respects products.

By construction $\mathcal{O}^+_{v_{n+1}}$ is contained in the kernel of H_{n+1}. A "monomial" $f \coloneqq a\phi_{n+1}^{ej}$ with $v_{n+1}(f) \geq 0$ and $\deg a < \deg \phi_{n+1}$ is in the kernel of H_{n+1} if and only if $H_n(aS^{\ell j})$ is zero. From the inductive hypothesis we know that this can only happen if $aS^{\ell j} \in \mathcal{O}^+_{v_n}$, but then $f \in \mathcal{O}^+_{v_{n+1}}$. Since H_{n+1} respects sums, this shows that the latter is the kernel of H_{n+1}.

As y_{n+1} is the image of $S'^{\ell}\phi_{n+1}^e$ and H_{n+1} respects products and sums, it remains to show that $\mathbb{F}_{n+1}$ is in the image of H_{n+1} to see that this map is onto. Consider the following diagram where φ is the isomorphism which exists by the inductive hypothesis.



We claim that there is an isomorphism φ', in other words, that the kernel of

$$\mathbb{F}_n[y_n] \to \mathcal{O}_{v_n}/\mathcal{O}_{v_n}^+ \twoheadrightarrow \mathcal{O}_{v_n}\Big/\Big(\mathcal{O}_{v_{n+1}}^+ \cap \mathcal{O}_{v_n}\Big)$$

is generated by $\psi(y_n)$. This is equivalent to: An element $f \in \mathcal{O}_{v_n}$ with $v_n(f) = 0$ has $v_{n+1}(f) > 0$ if and only if $H_n(f)$ is divisible by $\psi(y_n)$, the statement of Lemma 4.26. ∎

As a corollary to this construction we get explicit formulas for the ramification index and residual degree of an inductive valuation.

Corollary 4.30 [24, Theorem 12.1] *Let $v_n = [v_0, \ldots, v_n(\phi_n) = a_n/b_n]$ be an inductive valuation over v_K with $\deg \phi_{i+1} > \deg \phi_i$. Then for $1 \leq m \leq n$ the following equalities hold:*

$$e(v_m \mid v_{m-1}) = \frac{b_m}{\gcd\Big(\prod_{j=1}^{m-1} e(v_j \mid v_{j-1}), b_m\Big)}$$
$$[\mathbb{F}_m : \mathbb{F}_{m-1}] = \frac{\deg \phi_m}{e(v_m \mid v_{m-1}) \cdot \deg \phi_{m-1}}.$$

In particular, the ramification index of v_n over v_K is the least common multiple of the b_i. ∎

4.2 Valuations of Transcendence Degree One

Recall from the beginning of this chapter that we aim to describe valuations whose residue field is an extension of transcendence degree one over k, the residue field of v_K. The construction of the preceding pages shows that inductive valuations have such a residue field. The following theorem shows that these are the only discrete valuations with this property. Let us denote by $V_1(K[t]) \subseteq V(K[t])$ the set of discrete valuations whose residue field has transcendence degree one over k.

Theorem 4.31 [12, Corollary 7.6][24, Theorem 8.1] *Let $v \in V(K[t])$. Then $v \in V_1(K[t])$ if and only v is inductive over v_K.*

For the proof we introduce the notion of an *approximant*, an inductive valuation which approximates v from below.

Definition 4.32 Let $v \in V_1(K[t])$. An inductive valuation

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

on $K[t]$ is called an *approximant* for v if the following conditions hold:

$$v(f) \geq v_n(f), \qquad \text{for all } f \in K[t] \tag{1}$$
$$v(f) = v_n(f), \qquad \text{for all } f \in K[t] \text{ with } \deg(f) < \deg \phi_n \tag{2}$$
$$v(\phi_i) = v_n(\phi_i), \qquad \text{for all } i \in \{1, \ldots, n\} \tag{3}$$

Proof One direction of the theorem follows immediately from the construction of the previous section. For the other direction, let $v \in V_1(K[t])$. We are going to approximate v from below with approximants. Clearly, v_0 is an approximant for v. Suppose that for $n \geq 1$, an approximant

$$v_{n-1} = [v_0, \ldots, v_{n-1}(\phi_{n-1}) = \lambda_{n-1}]$$

has been constructed. If $v \neq v_{n-1}$, then, among the monic polynomials with $v(f) > v_{n-1}(f)$, consider the set of those which have minimal degree. The polynomials in this set are key polynomials over v_{n-1} [24, p.378, equations (5) and (6)]. Let ϕ_n be one of these polynomials and let $\lambda_n := v(\phi_n)$. Set $v_n := [v_{n-1}, v_n(\phi_n) = \lambda_n]$. By Lemma 4.13, $\phi_n \nmid_{v_{n-1}} \phi_{n-1}$, and so $\phi_n \nsim_{v_{n-1}} \phi_{n-1}$ (Lemma 4.14.) As $\deg \phi_n \geq \deg \phi_{n-1}$, v_n is inductive. Furthermore this valuation satisfies the conditions of an approximant:
(1) For a polynomial in its ϕ_n-adic expansion $f = \sum_i a_i \phi_n^i$, we get

$$v(f) \geq \min\{v(a_i) + i\lambda_n\} = v_n(f).$$

(2) Let $f \in K[t]$ with $\deg f < \deg \phi_n$. After multiplication by a constant, this is a monic polynomial. Because of the minimality of the degree of ϕ_n, $v(f) = v_{n-1}(f) = v_n(f)$.
(3) Let $k \in \{1, \ldots, n-1\}$. We have

$$\begin{aligned} \lambda_k &= v(\phi_k) \\ &\geq v_n(\phi_k) && \text{by Condition (1)} \\ &\geq v_{n-1}(\phi_k) && \text{by Lemma 4.13} \\ &= \lambda_k && \text{by Lemma 4.22} \end{aligned}$$

This shows that we can continue the inductive construction as long as we can find a polynomial f which satisfies $v(f) > v_n(f)$. If this is at some point not the case, then $v = v_n$, and we are done. Otherwise we get an infinite sequence of inductive valuations. We want to show that this can not happen under our assumptions.

Suppose for contradiction that the degrees of the ϕ_n increase indefinitely. An element $f \in K[t]$ with $v(f) = 0$ must satisfy $v_n(f) = 0$ for all n with $\deg \phi_n > \deg f$ (otherwise a multiple of f would have been chosen as a key polynomial earlier). In terms of the reduction described earlier, this implies that f reduces to an element of $\mathbb{F}_n$. As $\mathbb{F}_n$ is an algebraic extension of k, there is an $F \in K[T]$ such that $v_0(F(t)) \geq 0$ and $v_n(F(f)) > 0$. Since $v(F(f)) \geq v_n(F(f))$, this is a contradiction since we assumed that there is an $f \in K[t]$ which remains transcendental over k.

We may now assume that there is some N such that the degrees of ϕ_n are equal for all $n \geq N$. Recall from the explicit construction of residue fields above that the residue field of v_{n+1} is of the form $\mathbb{F}_{n+1}[y_{n+1}]$ with $\mathbb{F}_{n+1} = \mathbb{F}_n[y_n]/(\psi_{n+1})$ and $\mathbb{F}_0 = k$. In particular $\mathbb{F}_n$ is finite over $\mathbb{F}_0$. Let $f \in K[t]$ again be an element with $v(f) = 0$. We claim that $v_n(f) = 0$ for some $n \geq N$. Suppose for contradiction that $v(f) > v_n(f)$ for all n. Let $n \geq N$ and write $f = q\phi_{n+1} + r$

for the quotient with remainder when dividing f by ϕ_{n+1}. Then $\phi_{n+1} \mid_{v_n} f$ since

$$\begin{aligned} v_n(q\phi_{n+1} - f) &= v(q\phi_{n+1} - f) && \text{as } \deg r < \deg \phi_n \\ &\geq \min\{v(q\phi_{n+1}), v(f)\} \\ &> \min\{v_n(q\phi_{n+1}), v_n(f)\}. \end{aligned}$$

By Lemma 4.13, $v_{n+1}(f) > v_n(f)$, i.e., $v_n(f)$ is monotonically increasing. Since all $v_n(f)$ are in the discrete value group of v,

$$v(f) > \lim_{n\to\infty} v_n(f) = \infty,$$

a contradiction, and so $v_n(f) = v(f) = 0$ for some $n \geq N$. As in the last paragraph this shows that f is algebraic over k which is a contradiction to the assumption that there is an $f \in K[t]$ which remains transcendental. ∎

4.3 Uniqueness of Inductive Valuations

Any $v \in V_1(K[t])$ can be written as an inductive valuation $v = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$. The proof of this statement, Theorem 4.31, essentially gave an algorithm to compute such an inductive valuation; but to which extent is this presentation unique?

The presentation of an inductive valuation fails to be unique in two rather trivial ways. Clearly,

$$v = [v_0, v(t + \pi) = 2] = [v_0, w(t) = 1, w(t + \pi) = 2] = w$$

with $\pi \in K$ uniformizing. So if we want any kind of uniqueness, we should at least demand the degrees of the key polynomials to be strictly increasing. But even then,

$$v = [v_0, v(t) = 1] = [v_0, w(t + \pi) = 1] = w.$$

More generally, if ϕ_{n+1} and ψ_{n+1} are v_n-equivalent with $v_n(\phi_{n+1} - \psi_{n+1}) \geq \lambda_{n+1}$, then

$$\begin{aligned} v_{n+1} &\coloneqq [v_n, v_{n+1}(\phi_{n+1}) = \lambda_{n+1}] \\ &= [v_n, w_{n+1}(\psi_{n+1}) = \lambda_{n+1}] =: w_{n+1}. \end{aligned}$$

Indeed,

$$\begin{aligned} v_{n+1}\Big(\sum a_i \psi_{n+1}^i\Big) &\geq \min\{v_n(a_i) + i v_{n+1}(\psi_{n+1})\} \\ &= \min\{v_n(a_i) + i\lambda_{n+1}\} \\ &= w_{n+1}\Big(\sum a_i \psi_{n+1}^i\Big) \end{aligned}$$

and vice versa. It turns out that these are the only ways in which the presentation of an inductive valuation can vary.

Theorem 4.33 [12, Proposition 3.7; 24, Theorem 15.3] *Let K be a field with a discrete valuation v_K. Let*

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n] \quad \textit{and} \quad w_m = [v_0, \ldots, w_m(\psi_m) = \mu_m]$$

be inductive valuations[5] *over* v_K *with key polynomials of strictly increasing degree. Then* $v_n = w_m$ *if and only if* $m = n$ *and the following hold for all* $1 \leq i \leq n$,

(a) $\lambda_i = \mu_i$,

(b) $\deg \phi_i = \deg \psi_i$, *and*

(c) $v_{i-1}(\phi_i - \psi_i) \geq \lambda_i$. ∎

This can be generalized to a criterion to check whether two inductive valuations are equal, see Theorem 4.57. The following lemma gives an easy condition to check whether inductive valuations are incomparable.

Lemma 4.34 *Let* K *be a field with a discrete valuation* v_K. *Let*

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n] \quad \textit{and} \quad w_m = [v_0, \ldots, w_m(\psi_m) = \mu_m]$$

be inductive valuations over v_K *with key polynomials of strictly increasing degree. Suppose that there is a minimal* $i < m, n$ *such that* $v_i = w_i$ *but* ϕ_{i+1} *is not* v_i*-equivalent to* ψ_{i+1}. *Then* v_n *and* w_m *are incomparable, i.e., neither* $v_n \geq w_m$ *nor* $v_n \leq w_m$ *holds.*

Proof By Lemma 4.14, ϕ_{i+1} is not v_i-divisible by ψ_{i+1}. By Lemma 4.13,

$$w_{i+1}(\phi_{i+1}) = w_i(\phi_{i+1}) = v_i(\phi_{i+1}) < v_{i+1}(\phi_{i+1}).$$

Exchanging the roles of ϕ_{i+1} and ψ_{i+1}, it follows that w_{i+1} and v_{i+1} are incomparable. This implies that v_n and w_m are incomparable since the valuations of ϕ_{i+1} and ψ_{i+1} do not change as the degrees of the key polynomials are strictly increasing. ∎

As a consequence of the construction of Theorem 4.31, we deduce the following result on comparability of inductive valuations.

Proposition 4.35 *Let* K *be a field with a discrete valuation* v_K. *Let* v *and* w *be inductive valuations over* v_K *such that* $w \geq v$. *Then* v *and* w *can be written as*

$$v = v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

and

$$\begin{aligned} w = w_m = [v_0, \ldots, v_{n-1}, w_n(\phi_n) = \mu_n, \\ w_{n+1}(\psi_{n+1}) = \mu_{n+1}, \ldots, w_m(\psi_m) = \mu_m] \end{aligned}$$

with $\mu_n \geq \lambda_n$ *and* $m \geq n$.

Proof The idea of the proof is to construct approximants for w which are approximants for v as well and to see that if such an approximant v_n can not be augmented to an approximant for v anymore, then $v = v_n$. The proof uses the following inductive construction. Let v_0 be the Gauss valuation on $K[t]$. Then $w \geq v \geq v_0$ and v_0 is an approximant for v and for w. Suppose now that for

[5] This statement also holds for infinite inductive valuations as defined in Subsection 4.6.1.

$n \geq 0$ an inductive valuation v_n has been constructed which is an approximant for v and for w and which satisfies $w \geq v \geq v_n$. If $v = v_n$, then we know from the proof of Theorem 4.31 that w can be obtained by augmenting v finitely many times. Let us therefore assume that $v > v_n$. Since $v > v_n$, there are polynomials f such that $v(f) > v_n(f)$. Let $\mathcal{V}$ be the set of monic polynomials with this property. Let $\mathcal{W} \supseteq \mathcal{V}$ be the set of monic polynomials which satisfy $w(f) > v_n(f)$. Let $\phi \coloneqq \phi_{n+1} \in \mathcal{V}$ be an element of minimal degree and suppose that it is such that if we write $v_{n+1} = [v_n, v_{n+1}(\phi) = v(\phi)]$, then $v = v_{n+1}$ or a next approximant for v which augments v_{n+1} uses a key polynomial of strictly larger degree.

We claim that ϕ has minimal degree in $\mathcal{W}$ as well. Suppose that this is not the case and let $\psi \in \mathcal{W}$ have minimal degree and suppose that it has been chosen such that $w_{n+1} = [w_n, w_{n+1}(\psi) = w(\psi)]$ satisfies $w = w_{n+1}$ or a next approximant for w which augments w_{n+1} uses a key polynomial of strictly larger degree. Both ϕ and ψ are key polynomials over v_n. They can not be v_n-equivalent, because if they were, they would have the same degree because of their v_n-minimality. By Lemma 4.34, w and v would be incomparable, which is not the case. Therefore, ϕ has minimal degree in $\mathcal{W}$.

We form the augmented valuation $v_{n+1} = [v_n, v_{n+1}(\phi) = v(\phi)]$. If v_{n+1} is an approximant for w, i.e., if $v(\phi) = w(\phi)$, then we can continue the induction. After finitely many steps either v_{n+1} is not an approximant for w anymore or it is but $v_{n+1} = v$ (a case we already discussed earlier.)

Suppose that v_{n+1} is not an approximant for w anymore, i.e., $w(\phi) > v(\phi)$. We claim that in this case $v_{n+1} = v$. Let ϕ_{n+2} be a key polynomial over v_{n+1}. We are done if we can show that $v_{n+1}(\phi_{n+2}) = v(\phi_{n+2})$. Consider the ϕ-adic expansion

$$\phi_{n+2} = \sum_{k=0}^{m} a_i \phi^i.$$

Since ϕ_{n+2} is a key polynomial over v_{n+1}, it follows from Lemma 4.19 that

$$v_{n+1}(\phi_{n+2}) = v_{n+1}(a_0) = v_n(a_0) \leq v_n(a_k \phi^k) \text{ for all } k \in \{1, \ldots, m\}.$$

If we set $w_{n+1} = [v_n, w_{n+1}(\phi) = w(\phi)]$, this shows that $v_n(a_0) < w_{n+1}(a_k \phi^k)$ for $k \in \{1, \ldots, m\}$ and so

$$w_{n+1}(\phi_{n+2}) = v_n(a_0).$$

By Lemma 4.22 and the strong triangle inequality we get

$$\begin{aligned} w(\phi_{n+2}) &= \min\{\, w(a_k \phi^k) \colon k \in \{0, \ldots, m\} \,\} \\ &= w(a_0) \\ &= v_n(a_0) \\ &= v_{n+1}(\phi_{n+2}) \\ &\leq v(\phi_{n+2}) \\ &\leq w(\phi_{n+2}) \end{aligned}$$

This shows that $v(\phi_{n+2}) = v_{n+1}(\phi_{n+2})$ for all key polynomials over v_{n+1}. Hence $v = v_{n+1}$. ∎

Remark 4.36 Essentially the proposition says that w can be written as an inductive valuation which augments $v = v_n$, i.e.,

$$w = [v_0, \dots, v_n, w_n(\phi_n) = \mu_n, w_{n+1}(\psi_{n+1}) = \mu_{n+1}, \dots, w_m(\psi_m) = \mu_m].$$

However, this would formally not be correct since we did not allow equal key polynomials following directly after another in our definition of an inductive valuation. This is the reason why we have to augment v_{n-1} and not v_n in the statement.

We deduce the following criterion for incomparability of inductive valuations.

Corollary 4.37 *Let K be a field with a discrete valuation v_K. Let*

$$v_n = [v_0, \dots, v_n(\phi_n) = \lambda_n] \quad \text{and} \quad w_m = [v_0, \dots, w_m(\psi_m) = \mu_m]$$

be inductive valuations over v_K with key polynomials of strictly increasing degree. Suppose that there is some $i < m, n$ such that $v_i \neq w_i$. Then v_n and w_m are incomparable, i.e., neither $v_n \geq v_m$ nor $v_n \leq v_m$ holds. ∎

4.4 Rigid Diskoids and Inductive Valuations

Again, let K be a field equipped with a discrete valuation v_K and residue field k. Let K_v be the completion of K with respect to v_K, and let K_v^{ac} be an algebraic closure. Let us also denote by v_K the unique extension of v_K to K_v^{ac}.

The theory developed up to this point, allows us to write down a discrete valuation v on $K(t)$ whose residue field has transcendence degree one over k as an inductive valuation, i.e., in the form $v = [v_0, \dots, v_n(\phi_n) = \lambda_n]$. This description is well suited for algorithms but tends to be cumbersome for some theoretical considerations. A more concise description can be obtained using the language of rigid analytic geometry. For this we need a few basic notions which we introduce first.

4.4.1 Rigid Disks and Diskoids

Definition 4.38 Let $\alpha \in K_v^{\mathrm{ac}}$ and let $\lambda \in \mathbb{Q} \cup \{\infty\}$. Then

$$D(\alpha, \lambda) \coloneqq \{\, x \in K_v^{\mathrm{ac}} \colon v_K(x - \alpha) \geq \lambda \,\}$$

is the *(closed) disk* with center α and radius λ.

Remark 4.39 Usually, one defines the closed disk with center α and radius $p^{-\lambda}$ as the set of points which satisfy $|x - \alpha| \leq p^{-\lambda}$ where $|\cdot|$ is the absolute value associated to v_K, i.e., $p^{-v_K(\cdot)}$. We found it confusing to mix the notions of *absolute value* and *valuation* of K and decided to only use the latter. Admittedly, this can be confusing at first: Disks with *large* radius r are smaller than those with *small* radius. In particular, the disk with center $0 \in K$ and radius 0 is not empty, but rather large (it consists of all integral elements.)

More generally, we define a *diskoid*, a union of conjugate disks, as follows.

Definition 4.40 Let $\phi \in K_v[t]$ be a monic irreducible polynomial and let $\lambda \in \mathbb{Q} \cup \{\infty\}$. The set

$$D(\phi, \lambda) \coloneqq \{\, x \in K_v^{\mathrm{ac}} \colon v_K(\phi(x)) \geq \lambda \,\}$$

is called the *diskoid* with center ϕ and radius λ.

Remark 4.41 Any disk with center in K_v is a diskoid. Conversely, if $\phi = t - \alpha$, then $D(\phi, \lambda)$ coincides with the disk $D(\alpha, \lambda)$. More generally, a diskoid $D(\phi, \lambda)$ is a union of disjoint disks of equal radius which are centered at the roots of ϕ (see the following Lemma.) However, those disks typically have a radius which is strictly smaller than λ.

Example 4.42 Consider the diskoid with center $t^2 + 4t + 16 \in \mathbb{Q}_2[t]$ and radius 5, i.e., the set

$$D(t^2 + 4t + 16, 5) \coloneqq \{\, x \in \mathbb{Q}_2^{\mathrm{ac}} \colon v(x^2 + 4x + 16) \geq 5 \,\}.$$

This is the disjoint union

$$D(t - 4a, 3) \cup D(t + 4a + 4, 3)$$

where a satisfies $a^2 + a + 1 = 0$. It is elementary to see that this is the case. Take for example

$$x \in D(t^2 + 4t + 16, 5) \setminus D(t - 4a, 3),$$

then

$$v(x + 4a + 4) = v(x^2 + 4x + 16) - v(x - 4a) > 5 - 3 = 2;$$

but since

$$v(x - 4a) = v((x + 4 + 4a) - (8a + 4)) = 2,$$

we have $v(x + 4a + 4) \geq 3$.

Lemma 4.43 *Let $D \coloneqq D(\phi, \lambda)$ be a diskoid. Then D is the union of $\deg \phi$ disks (which may not be pairwise distinct) of equal radius centered at the roots of ϕ. Furthermore, the K_v-automorphisms of K_v^{ac} act transitively on these disks.*

Proof Let $\alpha_1, \ldots, \alpha_n \in K_v^{\mathrm{ac}}$ be the roots of ϕ with multiplicities ϵ_i. Let $\mu_1, \ldots, \mu_n$ be minimal such that $D(\alpha_i, \mu_i) \subseteq D$. To see that $D \subseteq \bigcup D(\alpha_i, \mu_i)$, let $\alpha \in D$. Then

$$\lambda \leq v(\phi(\alpha)) = \sum_{i=1}^{n} \epsilon_i v(\alpha - \alpha_i).$$

Without loss of generality, we may assume that

$$v(\alpha - \alpha_1) \geq \cdots \geq v(\alpha - \alpha_n).$$

Let $\beta \in D(\alpha_1, v(\alpha - \alpha_1))$. Then

$$\begin{aligned} v(\phi(\beta)) &= \epsilon_1 v(\beta - \alpha_1) + \cdots + \epsilon_n v(\beta - \alpha_n) \\ &\geq \epsilon_1 v(\alpha - \alpha_1) \\ &\quad + \epsilon_2 v(\beta - \alpha_1 + \alpha_1 - \alpha + \alpha - \alpha_2) + \cdots + \epsilon_n v(\beta - \alpha_1 + \alpha_1 - \alpha + \alpha - \alpha_n) \\ &\geq \epsilon_1 v(\alpha - \alpha_1) + \cdots + \epsilon_n v(\alpha - \alpha_n) \\ &\geq \lambda \end{aligned}$$

whence $\beta \in D$. Since β was arbitrary, $v(\alpha - \alpha_1) \geq \mu_1$, i.e., $\alpha \in D(\alpha_1, \mu_1)$.

To see that all the μ_i are equal, reorder the disks so that the μ_i are increasing. Let $\alpha \in D(\alpha_n, \mu_1)$. Let σ be an K_v-automorphism of K_v^{ac} which maps $\alpha_n \mapsto \alpha_1$. Since K_v is complete, $v = v \circ \sigma$ [28, II.§6.2] and therefore

$$v(\sigma(\alpha) - \alpha_1) = v(\sigma(\alpha - \alpha_n)) = v(\alpha - \alpha_n) \geq \mu_1.$$

Hence $\sigma(\alpha) \in D(\alpha_1, \mu_1)$ and so $v(\phi(\alpha)) = v(\phi(\sigma(\alpha))) \geq \lambda$. Since α has been chosen arbitrarily, $D(\alpha_n, \mu_1) \subseteq D(\phi, \lambda)$ and $\mu_n \leq \mu_1$. ∎

Due to the nature of non-archimedean geometry, two closed disks can either be contained in each other or disjoint. The same is true for diskoids.

Lemma 4.44 *Let $D \coloneqq D(\phi, \lambda)$, $D' \coloneqq D(\phi', \lambda')$ be two diskoids with $D \cap D' \neq \emptyset$. Then $D \subseteq D'$ or $D' \subseteq D$.*

Proof We know from the previous lemma that we may write

$$D = \bigcup D(\alpha_i, \mu) \text{ and } D' = \bigcup D(\alpha_i', \mu')$$

where the α_i, α_i' are the roots of ϕ and ϕ', respectively. Let us assume that $\mu \geq \mu'$ and that there is $x \in D(\alpha_1, \mu) \cap D(\alpha_1', \mu')$. Then $D(\alpha_1, \mu) \subseteq D(\alpha_1', \mu') \subseteq D'$. As the K_v-automorphisms of K_v^{ac} act transitively on the α_i, it follows that $D(\alpha_i, \mu) \subseteq D'$ for all i. ∎

Lemma 4.45 *Let $D \coloneqq D(\phi, \lambda)$ be a diskoid. If D is not a disk, then $D \cap K$ is empty.*

Proof D splits over K_v^{ac} into disks centered at the α_i, the roots of ϕ. Suppose that there is an $x \in D \cap K$. If D is not a disk but a disjoint union of disks, not all of the α_i are at the same distance to x. Therefore, the Newton polygon of $\phi(t - x)$ has different slopes and f factors over K_v, in contradiction to the assumed irreducibility of ϕ. ∎

4.4.2 Correspondence with Inductive Valuations

We show in this subsection that there is a correspondence between valuations in $V_1(K[t])$ and diskoids with center in $K[t]$. Since finite subsets of $V_1(K[t])$ correspond to normal models of $\mathbb{P}^1$, this implies that normal models of $\mathbb{P}^1$ correspond to finite sets of diskoids. This is similar to the fact that normal models with reduced special fiber correspond to pure affinoid coverings of $\mathbb{P}^1$ [13, Theorem 4.10.7]. Let us first introduce how we want to map valuations to diskoids and vice versa.

Definition 4.46 Let $D \subseteq K_v^{\mathrm{ac}}$. The *valuation* associated to D is

$$\begin{aligned} v_D \colon K[t] &\to \mathbb{Q} \cup \{\infty\} \\ f &\mapsto \inf\{\, \mu_x(f) \colon x \in D \,\}, \end{aligned}$$

where

$$\begin{aligned} \mu_x \colon K[t] &\to \mathbb{Q} \cup \{\infty\} \\ \phi &\mapsto v_K(\phi(x)). \end{aligned}$$

Remark 4.47 If D is a diskoid, it is a union of closed disks. Therefore, the infimum in the above definition is attained, i.e., for all $f \in K[t]$ there is an $x \in D$ such that $v_D(f) = \mu_x(f)$ [13, Example 2.2.2].

We are now going to discuss how a valuation v_D extends from $K[t]$ to $K'[t]$ for a finite normal extension K'/K. Even though the focus of this work on the case where K has characteristic zero (and K'/K is therefore a Galois extension,) we do not want to limit ourselves to that case and develop the theory for inseparable K'/K as well. Note that this complicates some of the proofs below.

The K-automorphisms of K' extend to $K[t]$-automorphisms of $K'[t]$ by acting on the coefficients. In fact, if we write $K'(t)$ and $K(t)$ for the rational function fields in the variable t, then the $K(t)$-automorphisms of $K'(t)$ are precisely the ones which are induce by K-automorphisms of K': If K'/K is a Galois extension, then this follows from the fact that $K'(t)/K(t)$ is a Galois extension of the same degree. If K'/K is normal but not separable, then one can show this by choosing a subfield L such that L/K is separable and K'/L purely inseparable. It follows that $K'(t)/L(t)$ is purely inseparable as well and that therefore K'/K and $K'(t)/K$ have the same degree of separability which shows that there are no $K(t)$-automorphisms of $K'(t)$ other than the ones induced by K'/K. In any case, the $K(t)$-automorphisms of $K'(t)$ restrict to $K[t]$-automorphisms of $K'[t]$, so it makes sense to talk about the group of $K[t]$-automorphisms of $K'[t]$. As a first statement about this group of automorphisms, we see that it acts on extensions of v_D to $K'[t]$.

Lemma 4.48 *Let v be a discrete valuation on $K[t]$ which extends v_K. Let K'/K be a finite normal extension, and let G be the group of K-automorphisms of K'. Then G, understood as the group of $K[t]$-automorphisms of $K'[t]$, acts transitively on the extensions of v to $K'[t]$.*

Proof Let $\sigma \in G$, and let w be an extension of v to $K'[t]$. It is clear that $w \circ \sigma$ also extends v to $K'[t]$ so the only non-trivial part of the statement is the transitivity. We follow the proof of [28, II.§9.1]. Let w and w' be two extensions of v to $K'[t]$. If there was no σ such that $w' = w \circ \sigma$, then the sets

$$\{\, w \circ \sigma \colon \sigma \in G \,\} \quad \text{and} \quad \{\, w' \circ \sigma \colon \sigma \in G \,\}$$

would be disjoint. Using an Approximation Theorem such as [28, II.§3.4], there is an $f \in K'[t]$ such that $(w \circ \sigma)(f) \geq 1$ and $(w' \circ \sigma)(f + 1) \geq 1$ for all $\sigma \in G$. This choice implies that $(w' \circ \sigma)(f) = 0$ for all $\sigma \in G$. For the norm of f we get

$$\alpha \coloneqq N_{K'(t)/K(t)}(f) = \prod_{\sigma \in G} \sigma(f)^q$$

where $q = 1$ if K'/K is separable, and q is a power of the characteristic otherwise. Therefore,

$$v(\alpha) = w(\alpha) = q \sum w(\sigma(f)) \geq 1$$

in contradiction to

$$v(\alpha) = w'(\alpha) = q \sum w'(\sigma(f)) = 0.$$

∎

Lemma 4.49 *Let $D \coloneqq D(\phi, \lambda)$ be a diskoid. Let K'/K be a normal extension which contains a splitting field of $\phi = \prod_{i=1}^{n}(t-\alpha_i)^{\epsilon_i}$. Write*

$$D = \bigcup_{i=1}^{n} D_i \text{ with } D_i \coloneqq D(\alpha_i, \lambda')$$

and some $\lambda' \in \mathbb{Q} \cup \{\infty\}$. Then the set of extensions of v_D to $K'[t]$ is given by

$$\{v_{D_1}, \dots, v_{D_n}\}.$$

Proof To formally make sense of the statement, we have to fix an embedding $\tau' \colon K' \to K_v^{\mathrm{ac}}$ which extends $\tau \colon K \to K_v^{\mathrm{ac}}$. This induces an isomorphism $\tau' \colon K'^{\mathrm{ac}}_v \to K_v^{\mathrm{ac}}$ which allows us to write $D = \bigcup D_i$. We will in the following silently use this isomorphism to consider elements of K'^{ac}_v as elements of K_v^{ac}. In particular, we extend v_K to K'^{ac}_v through this isomorphism. Restricting this to K' gives an extension of v_K to K' which we denote by v_K as well.

Let us first show that the v_{D_i} are extensions of v_D. It suffices to show that

$$v_{D_i}\big|_{K[t]} = v_{D_j}\big|_{K[t]}$$

for all i, j. Let $f \in K[t]$ and let $\beta_i \in D_i$ be such that $v_{D_i}(f) = v_K(f(\beta_i))$. A K_v-automorphism σ of K_v^{ac} which maps $\sigma \colon \alpha_i \mapsto \alpha_j$ then maps β_i into D_j (Lemma 4.43.) Therefore,

$$\begin{aligned} v_{D_i}(f) &= v_K(f(\beta_i)) \\ &\geq v_{D_j}(f). \end{aligned}$$

This shows that the v_{D_i} are extensions of v_D.

Since the K-automorphisms of K' act transitively on the extensions of v_D to $K'[t]$ by the previous lemma, it suffices to show that they act on the v_{D_i} to see that the v_{D_i} are the totality of extensions. Let σ be a K-automorphisms of K'. Let us also denote by σ the induced $K[t]$-automorphism of $K'[t]$. As σ extends to a K-automorphism of K'^{ac}_v, it can also be extended through τ' to a K-automorphism of K_v^{ac}, and in turn to a K_v-automorphism of K_v^{ac}. Let $i \in \{1, \dots, n\}$, and let j be such that $\sigma(\alpha_j) = \alpha_i$. We want to show that $v_{D_i} \circ \sigma = v_{D_j}$. For $f \in K'[t]$ let $\beta \in D_i$ be such that $v_{D_i}(\sigma(f)) = v_K(\sigma(f)(\beta))$. Then

$$\begin{aligned} (v_{D_i} \circ \sigma)(f) &= v_K(\sigma(f)(\beta)) \\ &= v_K(\sigma(f(\sigma^{-1}(\beta)))) \\ &= v_K(f(\sigma^{-1}(\beta))) \\ &\geq v_{D_j}(f). \end{aligned}$$

The same calculation shows that $v_{D_j}(f) = (v_{D_j} \circ \sigma \circ \sigma^{-1})(f) \geq v_{D_i} \circ \sigma(f)$. ∎

It is our aim to connect the valuations induced by diskoids with the valuations which come from normal models of curves, i.e., valuations whose residue field have transcendence degree one. The following lemma shows that valuations induced by diskoids are indeed of this kind.

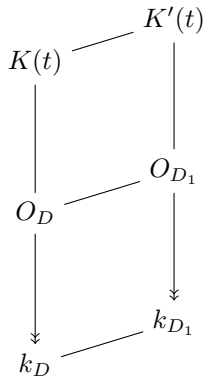
Lemma 4.50 *Let $D \coloneqq D(\phi, \lambda)$ be a diskoid. Then $v_D \in V(K[t])$. If λ is finite, then $v_D \in V_1(K[t])$*

Proof Let K'/K be a finite normal extension which contains a splitting field of ϕ. By the previous lemma,

$$v_D = v_{D_i}\big|_{K[t]}$$

for any of the disks D_i centered at the roots of $\phi = \prod_{i=1}^{n} t - \alpha_i$. The v_{D_i} are in $V(K'[t])$, and, if λ is finite, then $v_{D_i} \in V_1(K'[t])$ [13, Example 2.2.2]. This shows that $v_D \in V(K[t])$.

Let us now assume that λ is finite. We construct an element $y \in K[t]$ which remains transcendental over k, the residue field of v_K, after reduction modulo v_D. The valuation v_D extends to the rational function field $K(t)$ and the valuation v_{D_1} extends to $K'(t)$. Let $\mathcal{O}_D$ and $\mathcal{O}_{D_1}$ denote the ring of integral elements and k_D, k_{D_1} their respective residue fields.



We have seen earlier that k_{D_1} is transcendental over k. As k_{D_1}/k_D is finite, k_D is transcendental as well. Let $\bar{x} \in k_D$ be an element which is transcendental over k. Let $x = f/g \in \mathcal{O}_D$ be an element which reduces to $\bar{x}$. Let $n \in \mathbb{N}$ be such that $nv_D(f) = nv_D(g)$ is in the value group of v_K. Let π^m be such that $nv_D(f) = v_K(\pi^m)$. Then

$$f^n/\pi^m,\ g^n/\pi^m \in \mathcal{O}_D \cap K[t]$$

and both remain transcendental after reduction modulo v_D since otherwise their quotient could not have that property. This shows that $v_D \in V_1(K[t])$. ∎

Definition 4.51 Let $v \in V_1(K[t])$. Then we call

$$D_v \coloneqq \{\, x \in K_v^{\mathrm{ac}} \colon \mu_x \geq v \,\}$$

the *diskoid* associated to v.

At this point it is not clear that D_v is in fact a diskoid. This will be proved in Lemma 4.55.

Lemma 4.52 *Let $D \coloneqq D(\phi, \lambda)$ be a diskoid. Then $D = D_{v_D}$.*

Proof Let $x \in D$. Then $x \in D_{v_D}$ since

$$\mu_x(f) \geq \min_{y \in D} \mu_y(f) = v_D(f)$$

for all $f \in K[t]$. Conversely, let $x \in D_{v_D}$. Then $x \in D$ since

$$v_K(\phi(x)) = \mu_x(\phi) \geq v_D(\phi) = \min_{y \in D} \mu_y(\phi) = \min_{y \in D} v_K(\phi(y)) \geq \lambda.$$

■

Lemma 4.53 *Let*

$$v_n \coloneqq [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

be an inductive valuation over v_K. Then

$$D(\phi_n, \lambda_n) \subsetneq D(\phi_{n-1}, \lambda_{n-1}) \subsetneq \cdots \subsetneq D(\phi_1, \lambda_1) \subsetneq D(0, 0).$$

Proof It suffices to show that $D(\phi_n, \lambda_n) \subsetneq D(\phi_{n-1}, \lambda_{n-1})$. Since $\lambda_n > \lambda_{n-1}$ (Lemma 4.21) and since diskoids can not have non-trivial intersection (Lemma 4.44,) the statement holds if and only if $D(\phi_n, \infty) \subseteq D(\phi_{n-1}, \lambda_{n-1})$, i.e., if and only if the roots of ϕ_n are in $D(\phi_{n-1}, \lambda_{n-1})$. Write

$$v'_n \coloneqq [v_{n-1}, v_n(\phi_n) = \infty]$$

for the unique extension of v_K to $L \coloneqq K_v[t]/(\phi_n)$ (see Subsection 4.6.1.) Write $\alpha \in L$ for the class of t, a root of ϕ_n. We have $v'_n(\phi_{n-1}(t)) = \lambda_{n-1}$ (Lemma 4.22.) In L this becomes $v_K(\phi_{n-1}(\alpha)) = \lambda_{n-1}$ and so $\alpha \in D(\phi_{n-1}, \lambda_{n-1})$. Since ϕ_{n-1} has the same valuation when evaluated at any conjugate of α in K_v^{ac}, all roots of ϕ_n are in $D(\phi_{n-1}, \lambda_{n-1})$. ■

Lemma 4.54 *Let*

$$v \coloneqq v_n \coloneqq [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

be an inductive valuation over v_K. Then $v_{D_v} \geq v$ and $v_{D(\phi_n, \lambda_n)} \geq v$.

Proof For the first part, let $f \in K[t]$. Then

$$v_{D_v}(f) = \inf_{x \in D_v} \mu_x(f) \geq v(f)$$

and therefore $v_{D_v} \geq v$.

For the second part, write $D \coloneqq D(\phi_n, \lambda_n)$. We proceed by induction, showing that $v_D \geq v_m$ for all $m \leq n$. Let $f = \sum a_i t^i \in K[t]$, and let $x \in D$. Then

$$\begin{aligned} \mu_x(f) &\geq \min\{v_K(a_i x^i)\} \\ &\geq \min\{v_K(a_i)\} && \text{since } x \in D(0,0) \\ &= v_0(f). \end{aligned}$$

Let us now assume that $v_D \geq v_{m-1}$ for some $0 < m \leq n$. Let $f = \sum a_i \phi_m^i \in K[t]$, and let $x \in D$. Then

$$\begin{aligned} \mu_x(f) &\geq \min\{\mu_x(a_i) + i\mu_x(\phi_m)\} \\ &\geq \min\{v_{m-1}(a_i) + i\lambda_m\} && \text{by Lemma 4.53} \\ &= v_m(f). \end{aligned}$$

■

Lemma 4.55 *Let*

$$v \coloneqq v_n \coloneqq [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

be an inductive valuation over v_K. Then $D_v = D(\phi_n, \lambda_n)$.

Proof For the Gauss valuation, i.e., the case $n = 0$, this is evident. So let us assume that $n \geq 1$. Let $x \in D_v$. Then

$$\begin{aligned} v_K(\phi_n(x)) &= \mu_x(\phi_n) \\ &\geq v_n(\phi_n) \\ &= \lambda_n \end{aligned}$$

whence $x \in D(\phi_n, \lambda_n)$. Conversely, let $x \in D(\phi_n, \lambda_n)$. Let $f \in K[t]$ have ϕ_n-adic expansion

$$f = \sum a_i \phi_n^i.$$

Then

$$\begin{aligned} \mu_x(a_i) &\geq \min\{\, \mu_y(a_i) \colon y \in D(\phi_n, \lambda_n) \,\} \\ &\geq \min\{\, \mu_y(a_i) \colon y \in D(\phi_{n-1}, \lambda_{n-1}) \,\} && \text{by Lemma 4.53} \\ &= v_{D(\phi_{n-1}, \lambda_{n-1})}(a_i) \\ &\geq v_{n-1}(a_i) && \text{by Lemma 4.54} \end{aligned}$$

and therefore

$$\begin{aligned} \mu_x(f) &= \mu_x\Big(\sum a_i \phi_n^i\Big) \\ &\geq \min\{\mu_x(a_i) + i\mu_x(\phi_n)\} \\ &= \min\{\mu_x(a_i) + iv_K(\phi_n(x))\} \\ &\geq \min\{v_{n-1}(a_i) + i\lambda_n\} \\ &= v_n(f). \end{aligned}$$

Hence $x \in D_{v_n}$. ∎

Theorem 4.56 *Let $\mathcal{D}(K[t])$ be the set of diskoids with finite radius. Then the map*

$$\begin{aligned} \mathcal{D}(K[t]) &\to V_1(K[t]) \\ D &\mapsto v_D \end{aligned}$$

is a bijection with inverse

$$D(\phi_n, \lambda_n) \leftarrow\!\shortmid v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

which can equivalently be written as

$$D_v \leftarrow\!\shortmid v.$$

Furthermore, this map inverts the partial orders, i.e., for $D, D' \in \mathcal{D}(K[t])$ and $v, v' \in V_1(K[t])$

(i) $D \subseteq D' \Rightarrow v_D \geq v_{D'}$ and

(ii) $v \leq v' \Rightarrow D_v \supseteq D_{v'}$.

Proof That this map is well defined is Lemma 4.50. By Lemma 4.52 $D \mapsto v_D$ is one-to-one. By Lemma 4.55 the maps $v_n \mapsto D(\phi_n, \lambda_n)$ and $v_n \mapsto D_{v_n}$ coincide. It remains to show that the map $D \mapsto v_D$ is onto.

Let $v \in V_1(K[t])$. By Theorem 4.31, we can write v as an inductive valuation

$$v =: v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n].$$

Let $D \coloneqq D(\phi_n, \lambda_n) = D_v$. We have to show that $v_n = v_D$. By Lemma 4.54, $v_D \geq v_n$. By Proposition 4.35, v_D can be obtained augmenting v_n, i.e.,

$$v_D \coloneqq w_m = [w_0, \ldots, w_{n-1}(\phi_{n-1}) = \lambda_{n-1}, w_n(\phi_n) = \mu_n, \ldots, w_m(\phi_m) = \mu_m]$$

with $\mu_n \geq \lambda_n$. Then

$$\begin{aligned} D_{v_D} &\subseteq D(\phi_m, \mu_m) \\ &\subseteq D(\phi_n, \lambda_n) && \text{by Lemma 4.53} \\ &= D_{v_D} && \text{by Lemma 4.52.} \end{aligned}$$

Therefore, $m = n$ and $\mu_n = \lambda_n$ since this would otherwise contradict the strict inclusions in Lemma 4.53. Hence, $v_n = w_m = v_D$. ∎

4.4.3 More on Uniqueness of Inductive Valuations

Using the rigid language, we obtain the following theorem, an extension of Theorem 4.33.

Theorem 4.57 *Let*

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n], \quad w_m = [v_0, \ldots, w_m(\psi_m) = \mu_m]$$

be inductive valuations[6] *over* v_K *with* $\phi_n = \psi_m$ *and* $\lambda_n = \mu_m$ *Then* $v_n = w_m$.

Proof Since $v_n, v_m \in V_1(K[t])$, $v_n = v_U = w_m$ where U is the diskoid with center ϕ_n and radius λ_n (Theorem 4.56.) ∎

As a corollary we see that a key polynomial gets only one chance to appear in an inductive valuation.

Corollary 4.58 *Let*

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

be an inductive valuation over v_K *with key polynomials of strictly increasing degrees. Let* $\psi \in K[t]$ *be a key polynomial over* v_m *with* $m < n$. *Suppose that* $m < n - 1$ *or that* $\deg \psi > \deg \phi_n$. *Then* ψ *is not a key polynomial over* v_n.

Proof Suppose that ψ is a key polynomial over v_n. For a sufficiently large $\mu \in \mathbb{Q}$

$$v_{n+1} \coloneqq [v_n, v_{n+1}(\psi) = \mu], \quad v'_{m+1} \coloneqq [v_m, v'_{m+1}(\psi) = \mu]$$

are inductive valuations. By the previous theorem $v_{n+1} = v'_{m+1}$ in contradiction to Theorem 4.33. ∎

[6] The statement also holds for inductive pseudo-valuations (Section 4.6,) i.e., if $\lambda_n = \infty$. In that case v_n, w_m describe extensions of v_K to $L \coloneqq K[t]/(\phi_n)$ (cf. section 4.6.) Since ϕ_n is a key polynomial it is irreducible over the completion of K. By [28, II.§8.2] there is only one such extension and $v_n = v_m$.

4.5 Graded Algebras of Inductive Valuations

As before K is a field with a discrete valuation v_K. Let $\mathcal{O}_K$ be the valuation ring of K with maximal ideal $\mathfrak{m}_K$. Given an inductive valuation v over v_K, we have seen earlier how to compute the reduction of elements to the residue ring. The residue ring can explicitly be described as the elements of valuation zero modulo elements of valuation bigger than zero. This construction can be generalized to other residue rings: the elements of valuation α modulo elements of valuation bigger than α for any α in the value group of v. All these residue rings can be combined into a graded algebra which we now introduce following the exposition in [12, 39].

Definition 4.59 Let v be a discrete valuation on $K[t]$ which extends v_K. For any α in the value group $v(K[t])$ consider the $\mathcal{O}_v$-modules

$$\mathcal{O}_\alpha \coloneqq \{f \in K[t] : v(f) \geq \alpha\}$$

and

$$\mathcal{O}_\alpha^+ \coloneqq \{f \in K[t] : v(f) > \alpha\}.$$

The *graded algebra* of v is the integral domain

$$\operatorname{Gr}(v) \coloneqq \bigoplus_{\alpha \in v(K[t])} \mathcal{O}_\alpha / \mathcal{O}_\alpha^+.$$

The *residue map* of v is the map

$$H_v : K[t] \to \operatorname{Gr}(v)$$

which sends 0 to $0 \in \operatorname{Gr}(v)$ and a nonzero $g \in K[t]$ to the class of g in $\mathcal{O}_{v(g)}/\mathcal{O}_{v(g)}^+$. (Note that H_v is not a homomorphism of rings, it respects products but does in general not respect sums.)

The canonical homomorphism $\mathcal{O}_K \to \mathcal{O}_0$ induces a homomorphism $\mathcal{O}_K/\mathfrak{m}_K \to \mathcal{O}_0/\mathcal{O}_0^+$ which endows $\operatorname{Gr}(v)$ with the structure of a $\mathcal{O}_K/\mathfrak{m}_K$-algebra.

Remark 4.60 Some of the definitions introduced earlier can be restated in terms of the graded algebra and its reduction map: Two polynomials $f, g \in K[t]$ are *v-equivalent* if $H_v(f) = H_v(g)$. A polynomial $f \in K[t]$ is *v-divisible* by $g \in K[t]$ if $H_v(f)$ is divisible by $H_v(g)$ in $\operatorname{Gr}(v)$. A polynomial $f \in K[t]$ is *v-irreducible* if $H_v(f)$ generates a nonzero prime ideal in $\operatorname{Gr}(v)$.

The rest of this subsection is used to prove the following theorem which gives an easy description of $\operatorname{Gr}(v)$. Note that the proof here is different from the one in [12].

Theorem 4.61 [12, Theorem 4.13] *Let $v_n = [v_0, \dots, v_n(\phi_n) = \lambda_n]$ be an inductive valuation over v_K. Let $\mathbb{F}_n$ be the finite extension of $\mathbb{F}_0 \coloneqq \mathcal{O}_K/\mathfrak{m}_K$, the residue field of K, as constructed in Subsection 4.1.3. Then there is an isomorphism of $\mathbb{F}_0$-algebras*

$$\mathbb{F}_n[x, z, z^{-1}] \to \operatorname{Gr}(v_n).$$

Proof To simplify notation we write $v \coloneqq v_n$ and $H \coloneqq H_v$. We may assume that $\deg \phi_{i+1} > \deg \phi_i$. If $n = 0$, then the map $\mathbb{F}_0[x, z, z^{-1}] \to \mathrm{Gr}(v_0), x \mapsto t, z \mapsto \pi$ is clearly an isomorphism. We may assume in the following that $n \geq 1$. Recall that we already studied the structure of the degree zero part of $\mathrm{Gr}(v)$ in Subsection 4.1.3. We found that $\mathcal{O}_0/\mathcal{O}_0^+$ was isomorphic to a polynomial ring $\mathbb{F}_n[y_n]$ and constructed an explicit reduction map $H_n \colon \mathcal{O}_0 \to \mathbb{F}_n[y_n]$. The idea of the proof is to understand each degree of $\mathrm{Gr}(v)$, i.e., $\mathcal{O}_\alpha/\mathcal{O}_\alpha^+$, by shifting elements to valuation zero and applying the map H_n; we will see that we get a free $\mathbb{F}_n[y_n]$-module in each degree. The ring structure of $\mathrm{Gr}(v)$ will then be deduced by studying how these *shifts* relate to each other.

We first show that $\mathcal{O}_\alpha/\mathcal{O}_\alpha^+$ is a free $\mathbb{F}_n[y_n]$-module. By Lemma 4.23 there is an $S \in K[t]$ which is a uniformizer for v_{n-1} and which is such that $v_{n-1}(S) = v_n(S)$. Let S' be the v_n-reciprocal of S as constructed in Lemma 4.24. To simplify notation we agree that for a negative integer m we write S^{-m} to denote S'^m. Typically, $S^m S^{-m} \neq 1 \in K[t]$, however, by Lemma 4.24 this is true when applying H, i.e., $H(S^m)H(S^{-m}) = H(S^m S^{-m}) = 1 \in \mathrm{Gr}(v)$. More generally, as H respects products, we have $H(S^\mu)H(S^\nu) = H(S^{\mu+\nu})$ for integers μ, ν. We set $z \coloneqq H(S)$.

Let $f \in K[t]$ be an element of valuation $\alpha \coloneqq v_n(f) < \infty$. If e denotes the index $e(v_n|v_{n-1})$, then there is an integer m such that $v_n(S^m f) \in \{0, \lambda_n, \dots, (e-1)\lambda_n\}$. Let $l \coloneqq v_n(S^m f)/\lambda_n$. Consider the ϕ_n-adic expansion

$$S^m f = \sum_i a_i \phi_n^i.$$

For the reduction only the terms with $v_n(a_i\phi_n^i) = v_n(S^m f)$ matter. For those $i \equiv l \mod e$. To compute $H(S^m f)$ we may therefore assume that

$$S^m f = \sum_j a_{l+je}\phi_n^{l+je} = \phi_n^l \sum_j a_{l+je}\phi_n^{je}.$$

The sum in the last term has valuation zero so we can use H_n to compute its reduction to $\mathbb{F}_n[y_n]$. If we write x for $H(\phi_n)$, we get

$$H(f) = H(S^{-m})H(\phi_n^l)H(\sum_j a_{l+je}\phi_n^{je}) = z^{-m} \cdot x^l \cdot H_n(\sum_j a_{l+je}\phi_n^{je}).$$

It follows that $\mathcal{O}_\alpha/\mathcal{O}_\alpha^+$ is the free $\mathbb{F}_n[y_n]$ module $z^{-m}x^l\mathbb{F}_n[y_n]$.

We now show that $\mathrm{Gr}(v)$ has the structure of a ring. Consider the homomorphism of rings

$$\begin{aligned}\varphi \colon \mathbb{F}_n[x, z, z^{-1}, y_n] &\to \mathrm{Gr}(v),\\ z &\mapsto z = H(S),\\ z^{-1} &\mapsto H(S^{-1}),\\ x &\mapsto x = H(\phi_n),\\ y_n &\mapsto y_n \in \mathcal{O}_0/\mathcal{O}_0^+.\end{aligned}$$

This is a well defined map since the relation $zz^{-1} = 1$ is preserved in the image. From the discussion above we know that this map is onto. Recall that in the construction of H_n in Subsection 4.1.3 we chose y_n to be the image of $S'^m\phi_n^e$ with a positive integer m. Therefore the kernel of φ is generated by $z^{-m}x^e - y_n$ and $\mathrm{Gr}(v) \simeq \mathbb{F}_n[x, z, z^{-1}]$ as enounced. ∎

4.6 Valuations on Function Fields of Curves

We already developed a complete description for the discrete valuations on rational function fields which are relevant to our theory. Now we are going to extend this to function fields of curves, i.e., finite extensions of rational function fields. Note that a discrete valuation on a function field of a curve restricts to a discrete valuation on a rational function field. To make this explicit, let X be an irreducible smooth projective curve over a perfect field K and consider a cover $X \to \mathbb{P}^1$. This cover induces an extension of function fields $K(\mathbb{P}^1) \subseteq K(X)$. This extension is simple. (In the separable case, this is guaranteed by the Theorem of the Primitive Element, but even if this extension is inseparable in positive characteristic, it is simple since its degree of imperfection is at most one [3].) Hence, if x is a parameter for the rational function field, i.e., $K(x) \coloneqq K(\mathbb{P}^1)$, then $K(X)$ is of the form $K(x)[t]/(G)$ for a monic irreducible polynomial $G \in K(x)[t]$. Since a polynomial $f \in K(x)[t]$ represents an element of $K(X)$, a discrete valuation v on $K(X)$ defines a discrete pseudo-valuation[7]

$$\begin{aligned} K(x)[t] &\to \mathbb{Q} \cup \{\infty\} \\ f &\mapsto v(f + (G)). \end{aligned}$$

Conversely, a discrete pseudo-valuation v on $K(x)[t]$ for which the preimage of infinity is (G), defines a discrete valuation on $K(X)$.

A discrete valuation on $K(X)$ can therefore be described by

(a) a discrete valuation $v_{K(x)}$ on $K(x)$ whose residue field is transcendental over the residue field of v_K and

(b) a discrete pseudo valuation on $K(x)[t]$ which extends $v_{K(x)}$ and maps exactly the ideal (G) to infinity.

A description of the former has been developed in Section 4.1. We are now going to obtain a similar description for the latter.

4.6.1 Pseudo-Valuations on Polynomial Rings

For the rest of this section let K again be a field with a discrete valuation $v_K : K \to \mathbb{Q} \cup \{\infty\}$.

Definition 4.62 [25, Section 2]

(i) Let $v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$ be an inductive valuation over v_K and let $\phi_{n+1} \in K[t]$ be a key polynomial over v_n. We write

$$v_{n+1} = [v_0, \ldots, v_{n+1}(\phi_{n+1}) = \infty]$$

for the function

$$\begin{aligned} v_{n+1} \colon K[t] &\to \mathbb{Q} \cup \{\infty\}, \\ f &\mapsto v_n(a_0), \end{aligned}$$

[7] A discrete pseudo-valuation is a discrete valuation which may send more than just zero to infinity.

where a_0 is given by the ϕ_{n+1}-adic expansion of

$$f = \sum_i a_i \phi_{n+1}^i.$$

We call v_{n+1} an *infinite inductive valuation* if it satisfies

(i) $\deg(\phi_{n+1}) \geq \deg(\phi_n)$ and

(ii) ϕ_{n+1} is not v_n-equivalent to ϕ_n.

(ii) Let $\phi_i \in K[t]$ be a sequence of polynomials and let λ_i be a sequence of rationals with bounded denominators such that

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

is an inductive valuation for all $n \in \mathbb{N}$. We write $\lim v_n$ for the function

$$\begin{aligned} \lim v_n \colon K[t] &\to \mathbb{Q} \cup \{\infty\}, \\ f &\mapsto \lim_{n\to\infty} v_n(f) \end{aligned}$$

and say that $\lim v_n$ is a *limit valuation*.

We call a function of any of these two kinds an *inductive pseudo-valuation*.

Lemma 4.63 [24, Section 2] *Let v be an inductive pseudo-valuation on $K[t]$. Then v is a discrete pseudo-valuation on $K[t]$.* ∎

Example 4.64 Let $K = \mathbb{Q}_2$ and let v_0 be the Gauss valuation on $K[t]$. Then

$$v \coloneqq [v_0, v(t-1) = \infty]$$

is an infinite inductive valuation. As an example of a limit valuation, consider the series of valuations $v_0, v_1, \ldots$ with

$$v_{n+1} \coloneqq [v_n, v_{n+1}(t + \sum_{k=0}^{n} 2^k) = n+1]$$

which defines the limit valuation $\lim v_n$. Since

$$\begin{aligned} v_n(t-1) &= \min\{n, v_K(\sum_{k=n}^{\infty} 2^k)\} \\ &= \min\{n, n\} \to \infty \text{ (as } n \to \infty) \end{aligned}$$

the two valuations v and $\lim v_n$ are equal. Over a complete field, it is always the case that limit valuations are infinite inductive (Corollary 4.67.) For fields which are not complete, the two definitions do not coincide.

The following theorem shows that all discrete pseudo-valuations on $K[t]$ which extend v_K come from one of the inductive constructions which we introduced so far.

Theorem 4.65 [12, Corollary 7.6][24, Theorem 7.1] *Let v be a discrete pseudo-valuation on $K[t]$ with $v \geq v_0$ which extends v_K. Then exactly one of the following holds:*

(i) v is inductive. In this case, v is a discrete valuation whose residue field has transcendence degree one over the residue field of v_K.

(ii) v is an infinite inductive valuation. In this case, v is not a discrete valuation and its residue field is a finite extension of the residue field of v_K.

(iii) v is a limit valuation with key polynomials of unbounded degree. In this case, v is a discrete valuation whose residue field is an infinite algebraic extension of the residue field of v_K.

(iv) v is a limit valuation $\lim v_n$ (which is not an infinite inductive valuation) with key polynomials ϕ_n of bounded degree which form a Cauchy sequence with respect to v_N. Let N be such that the degree of the key polynomials is bounded by the degree of ϕ_N. Then exactly one of the following possibilities holds:

(iv-a) There is a nonzero $g \in K[t]$ which in $K_{v_K}[t]$ is divisible by $\lim \phi_n$. In this case, v is not a discrete valuation and the residue field of v is a finite extension of the residue field of v_K.

(iv-b) There is no such g. In this case, v is a discrete valuation and the residue field of v is a finite extension of the residue field of v_K.

Since the statement of this theorem is rather lengthy, we will give a few easy corollaries, before the actual proof. First, this generalizes Theorem 4.31, which essentially says that inductive valuations and discrete valuation with residue field of transcendence degree one are the same. The statement of the theorem is much easier if we assume that K is complete (we separate the case of valuations and pseudo-valuations in the following two corollaries):

Corollary 4.66 *Let K be a field which is complete with respect to a discrete valuation v_K and let $v \in V(K[t])$. Then exactly one of the following holds:*

(i') v is inductive and its residue field has transcendence degree one over the residue field of v_K.

(ii') v is a limit valuation with key polynomials of unbounded degree and its residue field is a infinite algebraic extension of the residue field of v_K. ■

Corollary 4.67 *Let K be a field which is complete with respect to a discrete valuation v_K. Let v be a discrete pseudo-valuation which extends v_K and is not a valuation, and assume that $v(t) \geq 0$. Then v is an infinite inductive valuation and its residue field is a finite extension of the residue field of v_K.* ■

The following notion (which generalizes Definition 4.32) will be central in the proof of the theorem.

Definition 4.68 Let v be a discrete pseudo-valuation on $K[t]$ with $v \geq v_0$ which extends v_K. An inductive pseudo-valuation

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

on $K[t]$ is called an *approximant* for v if the following conditions hold:

$$v(f) \geq v_n(f), \qquad \text{for all } f \in K[t] \tag{1}$$
$$v(f) = v_n(f), \qquad \text{for all } f \in K[t] \text{ with } \deg(f) < \deg \phi_n \tag{2}$$
$$v(\phi_i) = v_n(\phi_i), \qquad \text{for all } i \in \{1, \ldots, n\} \tag{3}$$

Proof (of Theorem 4.65) As in the proof of Theorem 4.31, we approximate v from below with approximants v_n. Clearly, the Gauss valuation v_0 is an approximant for v. Suppose that for some $n \geq 1$ an approximant

$$v_{n-1} = [v_0, \ldots, v_{n-1}(\phi_{n-1}) = \lambda_{n-1}]$$

has been constructed. If $v \neq v_{n-1}$, then, among the monic polynomials with $v(f) > v_{n-1}(f)$, consider the set of those with minimal degree. The polynomials in this set are key polynomials over v_{n-1} [24, p.378, equations (5) and (6)]. Let ϕ_n be one of these polynomials and let $\lambda_n \coloneqq v(\phi_n)$. Set

$$v_n \coloneqq [v_{n-1}, v_n(\phi_n) = \lambda_n].$$

If $\lambda_n = \infty$, then we are in case (ii); we have $v = v_n$ and it is clear that the assertions on v hold. Otherwise, v_n is inductive and satisfies conditions of an approximant, with the same proof as in Theorem 4.31. We may continue this process for as long as $v_n < v$. If this process stops, then we are either in case (i) (see Theorem 4.31) or (ii). If the process does not stop, set

$$w \coloneqq \lim_n v_n.$$

We now show that we must be in one of the cases (iii) or (iv) by showing that $v = w$.

As the λ_n are strictly increasing (Lemma 4.21) in the discrete value group of v, they tend to infinity.

(iii) Suppose that the degrees of the ϕ_n are not bounded. For a nonzero $f \in K[t]$ choose $N \in \mathbb{N}$ such that the degree of ϕ_N exceeds that of f. Then $w(f) = v_N(f) = v(f)$ This shows that v is a valuation since $w_N(f) < \infty$. We had seen in the proof of Theorem 4.31 that the residue field of v is algebraic over the residue field of v_K. To see that it is an infinite extension, note that the degree of ϕ_{n+1} can only exceed the degree of ϕ_n if the residue field of v_{n+1} is a non-trivial extension of the residue field of v_n or if the corresponding index is bigger than 1. Since v is discrete, the latter can only happen a finite number of times.

(iv) We may now suppose that the degrees of the ϕ_n are bounded, i.e., there is an $N \in \mathbb{N}$ such that $\deg \phi_n = \deg \phi_N$ for all $n \geq N$. By construction $v \geq w$. Suppose for contradiction that this inequality is strict, i.e., there is some $f \in K[t]$ such that $v(f) > w(f)$. In particular $v(f) > v_n(f)$ for all $n \geq N$. Let $f = q\phi_{n+1} + r$ be the quotient with remainder when dividing f by ϕ_{n+1}. Then f is v_n-divisible by ϕ_{n+1} since

$$\begin{aligned} v_n(q\phi_{n+1} - f) &= v(q\phi_{n+1} - f) && \text{as } \deg r < \deg \phi_n \\ &\geq \min\{v(q\phi_{n+1}), v(f)\} \\ &> \min\{v_n(q\phi_{n+1}), v_n(f)\}. \end{aligned}$$

By Lemma 4.13, $v_{n+1}(f) > v_n(f)$, i.e., $v_n(f)$ is monotonically increasing. Since all $v_n(f)$ are in the discrete value group of v,

$$v(f) > w(f) = \lim_n v_n(f) = \infty,$$

a contradiction. Hence, $v = w$.

The ϕ_n form a Cauchy sequence with respect to v_N:

$$\begin{aligned} \lambda_n = v_n(\phi_n) &= v_n(\phi_{n+1} - \phi_n) \\ &= v(\phi_{n+1} - \phi_n) && \text{by condition 2} \\ &= v_N(\phi_{n+1} - \phi_n) && \text{by condition 2} \end{aligned}$$

Let $\hat{\phi}$ be the limit of ϕ_N in $(K[t])_{v_N}$, the completion of $K[t]$ with respect to v_N. As the degrees of the ϕ_n are bounded, $\hat{\phi} \in K_{v_K}[t]$.

We have to distinguish two cases.

(iv-a) Suppose that there is a nonzero $g \in K[t] \subseteq K_{v_K}[t]$ and $h \in K_{v_K}[t]$ such that $g = h\hat{\phi}$. Let $h_n \in K[t]$ be a sequence such that $h = \lim_n h_n$ with respect to v_N. Then for $n \geq N$

$$\begin{aligned} v_n(g) &\geq \min\{v_n(h_n\phi_n), v_n(g - h_n\phi_n)\} \\ &\geq \min\{v_N(h_n) + \lambda_n, v_N(g - h_n\phi_n)\}. \end{aligned}$$

Since $\lim_n v_N(g - h_n\phi_n) = \infty$ and $\lim v_N(h_n)$ exist, this shows that $v(g) = \infty$. In particular, v is not a discrete valuation. Recall that the residue field of v_{n+1} is of the form $\mathbb{F}_{n+1}[y_{n+1}]$ with $\mathbb{F}_{n+1} = \mathbb{F}_n[y_n]/(\psi_{n+1})$ and $\mathbb{F}_0$ the residue field of v_K. In particular, $\mathbb{F}_N$ is finite over $\mathbb{F}_0$. As the degrees of the ϕ_n stagnate for $n \geq N$, the extension $\mathbb{F}_{n+1}/\mathbb{F}_n$ becomes trivial for $n \geq N$. To show that the residue field of v is finite over $\mathbb{F}_0$, take $f \in K[t]$ with $v(f) = 0$. Since $v_n(f) = 0$ for some $n \geq N$, the polynomial f is mapped to $\mathbb{F}_{n+1}$ when reducing with respect to v_{n+1}. By the above f is v-equivalent to some element of the valuation ring of v_N which reduces to $\mathbb{F}_N$. Hence the residue field of v is isomorphic to $\mathbb{F}_N$ which is finite over $\mathbb{F}_0$.

(iv-b) Suppose that there is no $g \in K[t]$ which is divisible by $\hat{\phi}$. We want to show that v is a discrete valuation. Suppose for contradiction that there is $g \in K[t]$ such that $v(g) = \infty$. For $n > N$ we form the quotient with remainder $g = h_n\phi_n + r_n$ with $h_n, r_n \in K[t]$. We have

$$\begin{aligned} v_N(g - h_n\phi_n) &= v_N(r_n) \\ &= v_{n-1}(r_n) \\ &\geq v_{n-1}(g) && \text{by Lemma 4.12.} \end{aligned}$$

Since the last term tends to infinity, $h_n\phi_n \to g$ with respect to v_N. Therefore, h_n converges to some $h \in (K[t])_{v_N}$ with $g = h\hat{\phi}$. This shows that $h \in K_{v_K}[t]$, a contradiction. The proof that the residue field is finite over the residue field of v_K is the same as in case (iv-a).

■

Example 4.69 Let $K = \mathbb{Q}_2(x)$ with the valuation induced by the Gauss valuation on $\mathbb{Q}_2[x]$. Let $G = t^2 - x^2 - 2 \in K[t]$, an irreducible polynomial. We can try to compute the extensions of v_K to $L \coloneqq K[t]/(G)$ with the method outlined in the proof. Let v be such an extension, considered as a pseudo-valuation on $K[t]$.

As a first approximant, we take the Gauss valuation v_0. To get a better approximant, we need to find a monic polynomial $\phi_1 \in K[t]$ of minimal degree with $v(\phi_1) > v_0(\phi_1)$. Making an educated guess, we take $\phi_1 = t - x$. We determine that

$$\begin{aligned} v(\phi_1^2) &= v(t^2 - 2tx + x^2) \\ &= v(G - 2tx + 2x^2 + 2) \\ &= v(2) + v(tx + x^2 + 1) \\ &= 1. \end{aligned}$$

Since ϕ_1 has minimal degree, a next approximant is

$$v_1 = [v_0, v_1(\phi_1) = 1/2].$$

To construct the next approximant we have to find another polynomial ϕ_2 with $v(\phi_2) > v_1(\phi_2)$. Suppose that there was such a monic ϕ_2 of degree one, say $\phi_2 =: t - \alpha$. Then

$$\begin{aligned} v(\phi_2) &= v(\phi_1 + x - \alpha) \\ &= \min\{v(\phi_1), v(x - \alpha)\} && \text{since } v(\alpha) \in \mathbb{Z} \\ &\in \{0, 1/2\}. \end{aligned}$$

However,

$$\begin{aligned} v_1(\phi_2) &= v_1(\phi_1 + x - \alpha) \\ &= \min\{v_1(\phi_1), v_1(x - \alpha)\} \\ &= \min\{1/2, v(x - \alpha)\} \\ &\in \{0, 1/2\}. \end{aligned}$$

Considering the possible cases, it can not happen that $v(\phi_2) > v_1(\phi_2)$. Therefore, ϕ_2 must have degree at least two. Since G is a monic polynomial of degree two with $v(G) > v_1(G)$, we have

$$v = v_2 = [v_1, v_2(G) = \infty].$$

Even though we were able to determine the extensions of v_K to L in this example, it should be clear now that such ad-hoc arguments can hardly be exploited algorithmically. A different approach is presented in the following.

4.6.2 Extending Valuations

Given a cover of irreducible smooth projective curves $X \to \mathbb{P}^1$, we observed earlier how a discrete valuation on $K(X)$ restricts to a discrete valuation on the function field of the projective line. This brings up a natural question: Given a discrete valuation on the function field of $\mathbb{P}^1$, can we compute all extensions

to the function field of X? We will see in Section 5.1 how the solution to this problem can be used to describe normal models of curves.

Let us consider a slightly more general problem. Let K be a field with a discrete valuation v_K and let $G \in K[t]$ be a monic integral polynomial. Let $G = \prod \hat{G}_i^{\hat{e}_i}$ be a factorization of G over K_v, the completion of K with respect to v_K, into coprime irreducible factors. Our aim is to describe the extensions of v_K to $K_v[t]/(\hat{G}_i)$ for all i. Let us denote the set of these extensions by $\hat{V}(G)$.

Remark 4.70 If G is irreducible, then the elements of $\hat{V}(G)$ correspond to the extensions of v_K to $K[t]/(G)$ [28, II.§8.2].

Remark 4.71 If $X \to \mathbb{P}^1$ is a cover of irreducible smooth projective curves, and if we let $K \coloneqq K(\mathbb{P}^1)$, then there is a monic irreducible $G \in K[t]$ such that $K(X) = K[t]/(G)$. If we consider a variable t/π^m instead of t, we can assume that G is integral.

Any $\hat{v} \in \hat{V}(G)$ can be described as an inductive pseudo valuation on $K_v[t]$ which sends precisely one of the ideals $(\hat{G}_i)$ to infinity. From an algorithmic point of view it is often desirable to work over K instead of K_v. That this is possible is a consequence of the following lemma.

Lemma 4.72 *Let $G = \prod G_i^{e_i}$ be a factorization of a monic polynomial G over K into coprime irreducible factors. Denote by $V(G)$ the set of pseudo-valuations on $K[t]$ which extend v_K and send precisely one of the ideals (G_i) to infinity. Then $\hat{V}(G)$ and $V(G)$ are in bijection.*

Proof Let $G = \prod_j \hat{G}_j^{\hat{e}_j}$ be a factorization of G over K_v into coprime irreducible factors. Every $\hat{G}_j$ is a factor of exactly one G_i. The statement then follows from the fact that $V(G_i)$ is in bijection with $\hat{V}(G_i)$ [28, II.§8.2]. ∎

To solve the original problem of this section, we need to compute the elements of $V(G)$. From Theorem 4.65 we know that each of these elements can be of two kinds. It can be an infinite inductive valuation or a limit valuation with key polynomials whose degrees stagnate. For the second kind of valuation it is not clear what we mean by *computing* them. The following lemma clarifies this.

Lemma 4.73 *Let $G \in K[t]$ be a monic irreducible polynomial, and let $v \in V(G)$. Then there is an approximant v_n for v such that*

(a) the residue fields of v_n and v are isomorphic as extensions of the residue field of v_K, and

(b) the ramification index of v and the index of v_n over v_K are equal.

Furthermore, for all $f \in K[t]$ with $v(f) = 0$, there is an approximant v_n for v such that $v_n(f) = 0$ and the reductions of f with respect to v_n and with respect to v coincide (modulo the above isomorphism of residue fields.)

Proof If v is an infinite inductive valuation then there is nothing to prove as v is its own approximant. Let us therefore suppose that v is a limit valuation

$$v = \lim v_n.$$

Write

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n].$$

We have seen in Theorem 4.65 that the degrees of ϕ_n stagnate. Let $N \in \mathbb{N}$ be such that $\deg \phi_n = \deg \phi_N$ for all $n \geq N$. Recall that we can always write the residue ring of v_n as $\mathbb{F}_n[y_n]$. We have seen in the proof of Theorem 4.65 that for $n \geq N$ the field $\mathbb{F}_{n+1} = \mathbb{F}_n[y_n]/(\psi_{n+1})$ is a trivial extension of $\mathbb{F}_n$. Furthermore, all the elements of the residue ring of v_n are mapped to $\mathbb{F}_{n+1}$ when reduced modulo v_{n+1}. This means that even elements which were transcendental in reduction modulo v_n become elements of $\mathbb{F}_{n+1} \simeq \mathbb{F}_N$ after reduction modulo v_N. Since all elements with $v(f) = 0$ must have $v_n(f) = 0$ for some $n \geq N$, this shows that the residue ring and field of v are isomorphic to $\mathbb{F}_N$. This proves the first part of the statement.

For the statement about the ramification index, we note that whenever the index of v_{n+1} over v_n is not one, then the key polynomial ϕ_{n+2} must have larger degree than ϕ_{n+1}. Since the degrees of the key polynomials stagnate, the index of v_n over v_0 is constant for all $n \geq N$. Given a uniformizer $\pi \in K[t]$ for v, we have $v(\pi) = v_n(\pi)$ for some $n \geq N$. This shows that the index of v_n over v_0 and the ramification index of v are the same.

Finally, given some $f \in K[t]$ with $v(f) = 0$, there is an $n \geq N$ such that $v_n(f) = 0$. From the statement about the residue fields it follows that the reduction of f modulo v and modulo v_{n+1} coincide. ∎

Remark 4.74 For separable G there is a Fundamental Equality [25, Theorem 5.1] from which one can decide whether an approximant satisfies conditions (a) and (b) for a given v_n. Over many fields there are efficient algorithms to compute a squarefree decomposition of G [15].

In principle, the proof of Theorem 4.65 tells us how to compute $V(G)$, in the sense of the above lemma. All we have to do is compute approximants to each $v \in V(G)$. By definition, $v \in V(G)$ sends one irreducible factor of G to infinity. This definition is probably not very practical since a priori a factorization of G is not known. Of course $v \in V(G)$ also sends G to infinity. That this already characterizes the elements of $V(G)$ is the statement of the following lemma.

Lemma 4.75 *Let G be a monic polynomial over K. Let v be a pseudo-valuation on $K[t]$ which extends v_K. Then $v \in V(G)$ if and only if $v(G) = \infty$.*

Proof For the non-trivial part suppose that v satisfies $v(G) = \infty$. It follows from the definition of a pseudo-valuation that $I \coloneqq v^{-1}(\{\infty\})$ is a prime ideal of $K[t]$. Let $\phi \in K[t]$ be a monic irreducible polynomial such that $I = (\phi)$. Then $\phi \mid G$, i.e., ϕ is an irreducible factor of G over K. Therefore, $v \in V(G)$. ∎

Recall from the proof of Theorem 4.65 that to compute approximants to $v \in V(G)$, we start with v_0 and augment our approximants in each step. More precisely, given an approximant v_n for v, all we need to do is find a next key polynomial ϕ_{n+1} and its valuation λ_{n+1}, form the augmented valuation $v_{n+1} \coloneqq [v_n, v_{n+1}(\phi_{n+1}) = \lambda_{n+1}]$, and repeat this process until $\lambda_{n+1} = \infty$ or the conditions of Lemma 4.73 are met. In the end (or in the limit) we know that $v(G) = \infty$, so it is not surprising that we have to choose ϕ_{n+1} and λ_{n+1} such that $v_{n+1}(G) > v_n(G)$.

Lemma 4.76 *Let $G \in K[t]$ be a monic integral polynomial and let $v \in V(G)$. Let w, w' discrete valuations on $K[t]$ which are approximants for v and suppose that $w' > w$. Then $w'(G) > w(G)$.*

Proof Write w as an inductive valuation

$$w = [w_0, \ldots, w_n(\phi_n) = \lambda_n].$$

By Proposition 4.35,

$$w' = [w_0, \ldots, w_{n-1}, w'_n(\phi_n) = \mu_n, \ldots, w'_m(\phi_m) = \mu_m]$$

with $\mu_n \geq \lambda_n$. But since both w and w' are approximants for v,

$$\lambda_n = w(\phi_n) = v(\phi_n) = w'(\phi_n) = \mu_n.$$

Therefore $m > n$. It suffices to show that $w_{n+1}(G) > w_n(G)$.

We now proceed as in [25, Lemma 3.4]. Write

$$G = \sum a_i \phi_{n+1}^i$$

for the ϕ_{n+1}-adic expansion of G. We claim that $w_n(G) = \min\{w_n(a_i\phi_{n+1}^i)\}$. Since w_n is a discrete valuation, it suffices to show that the left hand side does not exceed the minimum. If it did, then there would be at least two indices i such that $w_n(G) = w_n(a_i\phi_{n+1}^i)$. Let j be the largest such index. Then $a_j\phi_{n+1}^j$ is w_n-equivalent to $\sum_{i=0}^{j-1} a_i\phi_{n+1}^i$, contradicting the w_n-minimality of ϕ_{n+1}^j.

By definition, $w_{n+1}(G) = \min\{w_n(a_i) + i\mu_{n+1}\}$. Among the i for which the minimum is attained, let α be the smallest and β the largest. We claim that $\beta > \alpha$. Suppose that this is not the case. As w_{n+1} is an approximant for v, $v(a_i\phi_{n+1}^i) = w_n(a_i) + i\mu_{n+1}$. This implies that $v(G) = \min\{v(a_i\phi_{n+1}^i)\} = w_{n+1}(G) < \infty$, a contradiction. In particular $\beta > 0$.

Finally, this shows

$$\begin{aligned} w_{n+1}(G) &= w_{n+1}(a_\beta \phi_{n+1}^\beta) \\ &> w_n(a_\beta \phi_{n+1}^\beta) \\ &\geq \min\{w_n(a_i\phi_{n+1}^i)\} \\ &= w_n(G). \end{aligned}$$

■

The main obstacle in the above description is in finding the next key polynomial. It seems to be difficult to follow the proof of 4.65 and find the polynomial ϕ of smallest degree such that $v(\phi) > v_n(\phi)$. However, the above lemma leads to a different characterization of approximants which we will turn into an algorithm afterwards.

Lemma 4.77 [25, Lemma 3.2] *Let $G \in K[t]$ be a monic integral polynomial and let*

$$v_{n+1} = [v_0, \ldots, v_n(\phi_{n+1}) = \lambda_{n+1}]$$

be an inductive valuation which is an approximant for some $v \in V(G)$. Let $G = \sum a_i\phi_{n+1}^i$ be the ϕ_{n+1}-adic expansion of G. Then the following hold:

(a) There is more than one index i such that $v_{n+1}(G) = v_{n+1}(a_i\phi_{n+1}^i)$, and

(b) G is v_n-divisible by ϕ_{n+1}.

Proof Suppose in contradiction to (a) that there is only one such index i. If v_{n+1} was an approximant for v then it could be augmented to an approximant v_{n+2} with $v_{n+2}(G) > v_{n+1}(G)$ by the previous lemma. Since v_{n+2} is a discrete valuation,

$$\begin{aligned} v_{n+2}(G) &\geq \min\{v_{n+2}(a_j\phi_{n+1}^j)\} \\ &= \min\{v_n(a_j) + v_{n+1}(\phi_{n+1}^j)\} = v_{n+1}(G)\}. \end{aligned}$$

With our assumption there is a unique minimum. Hence $v_{n+2}(G) = v_{n+1}(G)$, a contradiction. That (b) holds is an immediate consequence of the previous lemma and Lemma 4.13. ∎

Once we found a suitable key polynomial ϕ_{n+1}, the lemma tells us how to choose λ_{n+1} to construct an approximant.

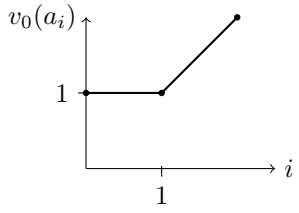
A key polynomial ϕ_{n+1} must v_n-divide G. One can show that all key polynomials over v_n which are not v_n-equivalent to ϕ_n lead to an approximant for some valuation in $v(G)$ [25, Theorem 5.1]. It follows from Lemma 4.26 and Lemma 4.27 that there are (up to v_n-equivalence) only finitely many polynomials by which G is v_n-divisible [25, Section 5]. These polynomials can be obtained with the techniques from Subsection 4.1.2. We illustrate the whole process with an example.

Example 4.78 Consider the rational function field $K = \mathbb{Q}_p(x)$ with the p-adic valuation, i.e., the valuation whose valuation ring is the localization $(\mathbb{Z}_p(x))_{(p)}$. (Equally, we could say that this is the valuation which is induced by the Gauss valuation on $\mathbb{Q}_p[x]$.) Let $L \coloneqq K[t]/(G)$ with $G = t^2 - x^2 - p$, an irreducible polynomial. Let v_0 be the Gauss valuation on $K[t]$, an approximant to any $v \in V(G)$ since G is integral. To determine all key polynomials over v_0 by which G is v_0-divisible, we apply Lemma 4.26, i.e., we factor the reduction of G modulo v_0 and lift the factors back to $K[t]$. The residue ring of $K[t]$ is $\mathbb{F}_p(x)[t]$ and the image of G is $t^2 - x^2$ which factors as $(t-x)(t+x)$. The factors lift to $t+x$, $t-x \in K[t]$, key polynomials over v_0. We can therefore construct approximants of the form $v_1 = [v_0, v_1(\phi_1) = \lambda_1]$ with $\phi_1 = t \pm x$.

To determine the value of λ_1, let us first assume that $p \neq 2$. Let $\phi \coloneqq t - x$ and consider the ϕ-adic expansion

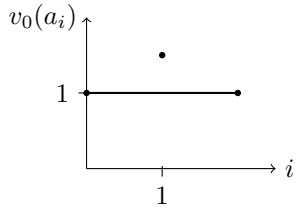
$$G = t^2 - x^2 - p = \phi^2 + 2x\phi - p.$$

By Lemma 4.77, we have to choose λ_1 such that there is no unique minimum amongst $2\lambda_1$, $1 + \lambda_1$, and 1. We can draw these values in a Newton polygon (below is the case for $\lambda = 1$). The condition is satisfied if and only if the Newton polygon has a horizontal slope.



There would also be a horizontal slope if we chose $\lambda_1 = 0$ but this does not yield an inductive valuation since λ_1 must exceed $v_0(\phi)$. The situation is similar for $\phi_1 = t + x$ where we obtain the same Newton polygon for $\lambda_1 = 1$. In total we obtained two different valuations with ramification index 1 and residual degree 1.

If $p = 2$, the situation is different. For $\phi_1 = t - x$, the only valid choice is $\lambda_1 = 1/2$ with the following Newton polygon.



For $\phi_1 = t + x$ we have to choose $\lambda_1 = 1/2$ with the same Newton polygon. Now, however, the two valuations which we obtain are actually equal. (This should come as no surprise since the ϕ_1 are just different lifts of the same factor in the residue ring.) We obtained one valuation with ramification index 2 and residual degree 1.

4.7 Polynomial Factorization

In the previous section we described an algorithm which computes all extensions of a valuation v_K on a field K to a finite extension $K[t]/(G)$. Since these extensions are in correspondence with the irreducible factors of G over the completion of K, this algorithm can be used to compute a factorization of G. The algorithm described in this section has originally been developed in [27]. A faster algorithm which is based on the same idea can be found in [18].

Throughout this section let K be a field with a discrete valuation v_K and let $G \in K[t]$ be a squarefree monic integral polynomial.[8]

Clearly, we can not expect to compute an actual factorization of G over the completion K_v, simply because we can only write down approximations of elements in K_v, e.g., as series in a uniformizer $\pi \in K$. Therefore we can only hope to be able to compute arbitrarily good approximations to factors of G.

The algorithm from the previous section lets us compute approximations to $V(G)$. Let

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

be a sequence of such approximations to a valuation $v \in V(G)$ which corresponds to an irreducible factor $\hat{G}_i$ of G over the completion K_v. The roots of $\hat{G}_i$ are contained in the diskoid D_n associated to v_n, i.e., the diskoid with center ϕ_n and radius λ_n. Since λ_n tends to infinity for large n, we may choose n sufficiently large such that $\deg \phi_n = \deg \hat{G}_i$. We have $v(\phi_n(\alpha)) = \lambda_n$ for α a root of $\hat{G}_i$. Since ϕ_n and $\hat{G}_i$ are monic polynomials of the same degree, the ϕ_n converge to $\hat{G}_i$ for large n.

[8] A simple substitution can be performed to turn G into monic integral polynomial G'. The factors of G can easily be recovered from the factors of G'.

Remark 4.79 The algorithm computes in each step an approximate factorization $G \simeq \prod G_i^{e_i}$ with coprime G_i. If G is squarefree, then eventually all $e_i = 1$ and the algorithm has found approximations to the actual factors of G_i which can then be lifted to more precision by performing additional iterations. If G is not squarefree, then the algorithm can not distinguish whether $G_i^{e_i}$ corresponds to an actual factor with multiplicity e_i or whether it will eventually turn into coprime factors of larger degree. In other words, after finitely many steps the algorithm computes approximations to the actual factors of G but it can not decide whether this is already the case. Fortunately, there are efficient algorithms to compute squarefree decompositions over many fields.[15]

In the next section we introduce an algorithm to compute the configuration of roots of ϕ_n. From this one could obtain a bound on the distance of the roots of ϕ_n to the roots of $\hat{G}_i$.

4.8 Configuration of Roots of a Polynomial

In the following let K be a field, equipped with a discrete valuation v_K. Let us fix $L \coloneqq K_v^{\mathrm{ac}}$, an algebraic closure of the completion of K and write $v \coloneqq v_L$ for the extension of v_K to this field. We may now ask how the roots of a $G \in K[t]$ are configured in L, i.e., for any pair of roots α, α' what is $v(\alpha - \alpha')$.

Assume that $G = \prod G_i$ is a factorization over K_v into coprime factors. Let $\alpha_i \in L$ be a root of G_i and write

$$H_{j,i}(t) \coloneqq G_j(t + \alpha_i) \in K_v(\alpha_i)[t].$$

If $\alpha_j' \in L$ is a root of G_j, then $\alpha_j' - \alpha_i$ is a root of $H_{j,i}$. Therefore, the distance from α_i to a root of G_j can be read off the Newton Polygon of $H_{i,j}$.[9] From this information the configuration of the roots of G can easily be determined: Let $\lambda_1 > \lambda_2 > \cdots > \lambda_n$ be the slopes of the Newton polygons. Then all roots of G lie within a disk of radius $-\lambda_1$. Any disk with larger radius does not contain all roots anymore; the roots cluster into several disks of radius $-\lambda_2$. The structure of these clusters can be read off the Newton polygons of the $H_{j,i}$; collecting all segments of the Newton polygon of $H_{j,i}$ whose slope is at most λ_2, tells us how many roots of G_j are within the conjugate disks of radius $-\lambda_2$ centered at the roots of G_i. These disks can then be split up further by looking at the segments of the Newton polygons whose slope is at most λ_3, and so on.

The above algorithm relies on a factorization of G over K_v. The method from the previous section in principle determines such a factorization. However, that *factorization* is only an approximation to the actual factors of G. We need to determine whether such approximate factors have the same configuration of the roots as the real factors of G. We will deduce a bound for this from the following lemma.

Lemma 4.80 *Let $D \coloneqq D(\phi, \lambda)$ be a diskoid with an irreducible $\phi \in K[t]$. Let $\alpha_1, \ldots, \alpha_n \in L \coloneqq K_v^{\mathrm{ac}}$ be the roots of ϕ. Then D splits into $\deg \phi$ disjoint disks*

[9] Note that the valuations of the coefficients of $H_{i,j}$ can be determined by computing norms in the extension $K_v(\alpha_i)/K_v$ [28, II.§4.8].

if and only if

$$\lambda > \max\{\, v(\alpha_i - \alpha_1) \colon i = 2, \ldots, n \,\} + \sum_{i=2}^{n} v(\alpha_i - \alpha_1).$$

Proof Suppose that D splits into $\deg \phi$ disjoint disks. Let $x \in L$ be such that $v(\phi(x)) = \lambda$. Since D splits, there is one root α such that $v(x - \alpha) > v(\alpha_i - \alpha)$ for all $\alpha_i \neq \alpha$. By the strict triangle inequality, $v(x - \alpha_i) = v(\alpha_i - \alpha)$ for all $\alpha_i \neq \alpha$. Hence

$$\begin{aligned}
\lambda = v(\phi(x)) &= \sum_{i=1}^{n} v(x - \alpha_i) \\
&= \max\{\, v(x - \alpha_i) \colon i = 1, \ldots, n \,\} + \sum_{\alpha_i \neq \alpha} v(\alpha - \alpha_i) \\
&> \max\{\, v(\alpha - \alpha_i) \colon \alpha_i \neq \alpha \,\} + \sum_{\alpha_i \neq \alpha} v(\alpha - \alpha_i) \\
&= \max\{\, v(\alpha_1 - \alpha_i) \colon \alpha_i \neq \alpha_1 \,\} + \sum_{\alpha_i \neq \alpha_1} v(\alpha_1 - \alpha_i)
\end{aligned}$$

where the last equality follows because the roots are conjugate.

Conversely suppose that D does not split. Then there is some $x \in D$ which is closest to to some root α but equally close to another root α_j, i.e.,

$$v(x - \alpha_j) = v(x - \alpha) \geq v(x - \alpha_i)$$

for all α_i. By the strict triangle inequality, $v(\alpha_i - \alpha) \geq v(x - \alpha_i)$. We may assume that α_j is a root closest to α. Then

$$\begin{aligned}
\lambda \leq v(\phi(x)) &= \sum_{i=1}^{n} v(x - \alpha_i) \\
&\leq \sum_{i=1}^{n} v(\alpha_i - \alpha) \\
&= v(\alpha_j - \alpha) + \sum_{\alpha_i \neq \alpha} v(\alpha_i - \alpha) \\
&= \max\{\, v(\alpha_i - \alpha) \colon \alpha_i \neq \alpha \,\} + \sum_{\alpha_i \neq \alpha} v(\alpha_i - \alpha) \\
&= \max\{\, v(\alpha_i - \alpha_1) \colon \alpha_i \neq \alpha_1 \,\} + \sum_{\alpha_i \neq \alpha_1} v(\alpha_i - \alpha_1)
\end{aligned}$$

where the last equality follows again because the roots are conjugate. ∎

Suppose that we computed an approximate factorization of a polynomial G, encoded as inductive pseudo-valuations $v_1, \ldots, v_m$. By Theorem 4.56 these correspond to diskoids $D_1, \ldots, D_m$. The roots of G are contained in these diskoids. Write $D_i =: D(\phi_i, \lambda_i)$. The approximation is sufficiently precise if $\bigcup D_i$ splits into $\deg G$ disjoint disks. The algorithm which we described earlier in

this section can determine the configuration of the roots of each of the ϕ_i (since these are irreducible over the completion of K.) The lemma lets us then decide whether a D_i splits into $\deg \phi_i$ disjoint disks. By Lemma 4.44 and Theorem 4.56, two diskoids are pairwise disjoint if their corresponding valuations are incomparable. Whether this is the case can easily be read off the inductive description of the valuations (see Section 4.3.)

Example 4.81 Consider the irreducible polynomial $G \in \mathbb{Q}[t]$

$$\begin{aligned} G = {} & t^{16} + 12t^{14} - 59055t^{13} + 27t^{12} - 708660t^{11} + 177138t^{10} - 1594485t^9 \\ & + 2125656t^8 + 1062990t^7 + 4782726t^6 + 12755880t^5 - 3188808t^4 \\ & + 28700730t^3 - 38265696t^2 + 3400686585. \end{aligned}$$

Over $\mathbb{Q}_3$ this polynomial factors into five coprime factors of degrees 2, 2, 3, 3, and 6. The configuration of the roots is visualized in the following figures.

In the graph to the left, the leaves are the roots. Leaves with the same color are conjugate over $\mathbb{Q}_3$, i.e., they belong to the same irreducible factor. The number in each inner node is the size of the smallest disk which contains all of the roots reachable from there.

The picture to the right visualizes the same situation as rigid diskoids. The filled circles are the roots, and circles of the same color are again conjugates. The number in each circle gives the size of the smallest disk containing all the roots.

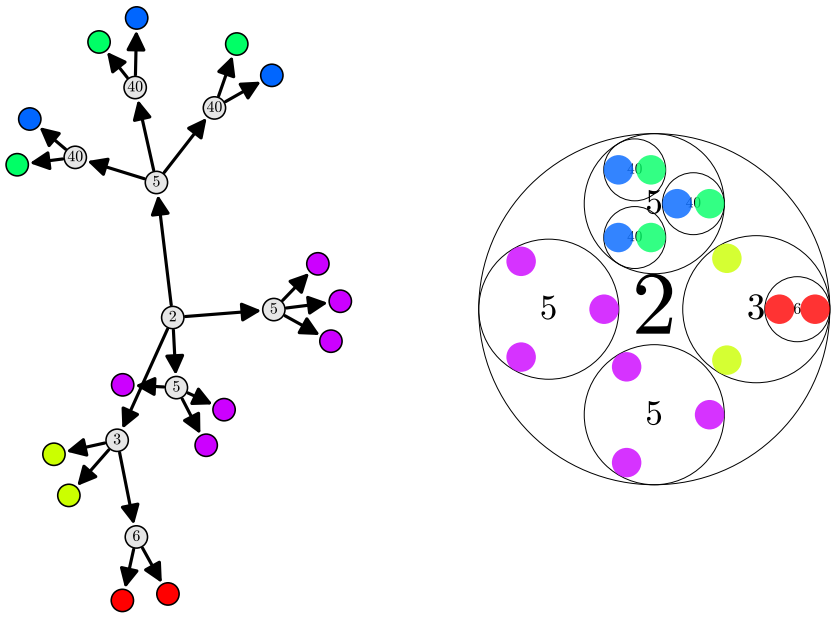


Figure 4.1: Configuration of the roots of G, normalized with $v(3) = 6$.

Chapter 5

Algorithmic Tools to Study Normal Models

Throughout this chapter let K be a field with a discrete valuation v_K, uniformizer $\pi \in K$, and residue field k.

For the computation of semistable models of curves, we want to be able to solve the following problem: Given a normal model of a curve, decide whether it is semistable; or more generally, describe (the singularities of) the special fiber. If we represent a model through explicit equations for an affine covering, it is clear how to extract that information. We chose, however, to represent models through finite sets of valuations on the function field $K(X)$ (Corollary 3.18). In this chapter we develop algorithms to extract information on a normal model from its description as such a finite set.

5.1 Normalization of Models

Our algorithm to compute a semistable model of a curve Y could roughly be described as follows (cf. Chapter 2): Consider Y as a cover of $X \coloneqq \mathbb{P}^1$. Construct a semistable model $\mathcal{X}$ of X and take its normalization $\mathcal{Y}$ in Y. If $\mathcal{Y}$ is semistable, then it is the model we were looking for, otherwise modify $\mathcal{X}$ and start over.

In this section, we want to discuss how to compute the normalization of $\mathcal{X}$ in Y. Let us first clarify the meaning of this notion.

Definition 5.1 Let $Y \to X$ be a cover of irreducible smooth projective curves and let $\mathcal{X}$ be a normal model of X. The *normalization* of X in Y is a normal model $\mathcal{Y}$ of Y together with an finite morphism $\pi : \mathcal{Y} \to \mathcal{X}$ which makes the following diagram commute:

$$\begin{array}{ccc} Y & \xrightarrow{\subseteq} & \mathcal{Y} \\ \downarrow & & \downarrow \pi \\ X & \xrightarrow{\subseteq} & \mathcal{X} \end{array}$$

5.1.1 Normalization on Affine Patches

Naïvely, normalizations can be computed by taking affine patches $\operatorname{Spec} A \subseteq \mathcal{X}$ and considering the embedding $A \subseteq K(Y)$. If B is the integral closure of A in $K(Y)$, then the model $\mathcal{Y}$ can be recovered by gluing the $\operatorname{Spec} B$ appropriately [23, Proposition 4.1.22]. There are very general algorithms to compute such integral closures (e.g. [9].) To our knowledge there is, however, no working implementation which can be used in our setting.

5.1.2 Valuation Theoretic Normalization

An entirely different approach can be obtained in light of Corollary 3.18 which says that normal models correspond to finite sets of valuations. Given a cover $Y \to X$ and a normal model $\mathcal{X}$, it suffices to determine the set of valuations which correspond to the normalization $\mathcal{Y}$ to uniquely describe the latter; recall that we denoted this set of valuations by $V(\mathcal{Y})$.

Proposition 5.2 *Let $Y \to X$ be a cover of irreducible smooth projective curves over K. Let $\mathcal{X}$ be a normal model of X, and let $\pi\colon \mathcal{Y} \to \mathcal{X}$ be the normalization of $\mathcal{X}$ in Y. Then $V(\mathcal{Y})$ is the set of the extensions of valuations in $V(\mathcal{X})$ to $K(Y)$.*

Proof Let V be the set of extensions of elements of $V(\mathcal{X})$ to $K(Y)$. We have to show that $V = V(\mathcal{Y})$. For one direction let $v \in V(\mathcal{Y})$. The valuation v corresponds to a generic point $\eta \in \mathcal{Y}_s$. Let $\eta' \coloneqq \pi(\eta)$ be the image of η on $\mathcal{X}$. Let $U \ni \eta'$ be an affine open subset with affine preimage $V \subseteq \mathcal{Y}$. Write $\operatorname{Spec} A \coloneqq U$, $\operatorname{Spec} B \coloneqq V$, where B is the integral closure of A in $K(Y)$. Suppose for contradiction that η' is a point of codimension two. Since B/A is integral, η would also be a point of codimension two by Going-Down [37, Theorem 2.2.7]. Since this is not possible, η' must be a generic point on the special fiber of $\mathcal{X}$. Therefore $\mathcal{O}_{\mathcal{X},\eta'} \to \mathcal{O}_{\mathcal{Y},\eta}$ is an extension of discrete valuation rings, and v is an extension of the valuation on $K(X)$ associated to η'. In other words, $v \in V$.

For the other direction let v be an element of $V(\mathcal{X})$, and let W be the set of valuation on $K(Y)$ which extend v. Let $\eta \in \mathcal{X}_s$ be the generic point corresponding to v. Let $\operatorname{Spec} A \subseteq \mathcal{X}$ be an open affine set which contains η and let $\mathfrak{p}$ be the prime ideal of A corresponding to η. Let B be the integral closure of A in $K(Y)$. Then $\operatorname{Spec} B$ is the preimage of $\operatorname{Spec} A$ under π. As $A \hookrightarrow B$ is a morphism of A-modules, we may consider its localization at $\mathfrak{p}$. This gives an injection $A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$. As $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ and integrally closed, $B_\mathfrak{p}$ is the integral closure of $A_\mathfrak{p}$ in $K(Y)$. Hence,

$$B_\mathfrak{p} = \bigcap_{w \in W} \mathcal{O}_w$$

where $\mathcal{O}_w \subseteq K(Y)$ is the valuation ring of w [26, Theorem 10.4]. For $w' \in W$, the map

$$A \hookrightarrow B \hookrightarrow B_\mathfrak{p} = \bigcap_{w \in W} \mathcal{O}_w \hookrightarrow \mathcal{O}_{w'}$$

shows that the maximal ideal of $\mathcal{O}_{w'}$ restricts to a prime ideal of B over $\mathfrak{p}$ which by Lemma 3.6 has height one. For any w' an Approximation Theorem such as [28, II.§3.4] shows that there is $z \in K(Y)$ with $w'(z) = 0$ and $w(z) > 0$ for all

$w \neq w'$. This shows that the $\mathcal{O}_{w'}$ induce pairwise distinct prime ideals of B. Therefore, $W \subseteq V(\mathcal{Y})$. ∎

The proposition shows that in theory to determine the normalization of $\mathcal{X}$ in Y, it suffices to compute the extensions of $V(\mathcal{X})$ to $K(Y)$. (A problem which is solved by the algorithms in Subsection 4.6.2.) In practice, however, these extensions can only be used to obtain information on the generic points of the special fiber of $\mathcal{Y}$.

5.1.3 Normalization with Reduced Fibers

Let $Y \to X := \mathbb{P}_1$ be a cover of irreducible smooth projective curves over K. Let $\mathcal{X}$ be a semistable model of X with reduced special fiber, and let $\mathcal{Y}$ be its normalization in Y. Let Z be a geometrically irreducible component of $\mathcal{X}_s$ such that there is at most one point $*$ on Z which intersects one other component of the special fiber. For our algorithm it suffices to understand the preimage of the affine line $Z \setminus \{*\}$ in $\mathcal{Y}_s$. To compute that preimage it suffices to determine the integral closure of a ring $A := \mathcal{O}_K[x]$ in a function field $L := K(x)[t]/(F)$. We collect the conditions on these rings which hold in our context (namely that F comes from a smooth curve and that our model has reduced special fiber) in the following proposition which gives a criterion to recognize the integral closure.

Proposition 5.3 [23, Lemma 4.1.18] *Let $A := \mathcal{O}_K[x]$ and $L := K(x)[t]/(F)$ where $F \in A[t]$ is a monic irreducible polynomial such that $B_K := K[x,t] \subseteq L$ determines a smooth K-curve* $\operatorname{Spec} B_K$. *Let $B \subseteq L$ be the integral closure of A in L and suppose that $\bar{B} := B/(\pi)$ is reduced. Let $B' \subseteq L$ be a finite extension of A such that $B'[\pi^{-1}] = B_K$ and such that $\bar{B}' := B'/(\pi)$ is reduced. Then $B' = B$.* ∎

The proposition lets us compute the normalization B through the following induction. We begin with $B_0 := A[t]$ which satisfies $B_0[\pi^{-1}] = B_K$. Suppose that B_i, a finite extension of A with $B_i[\pi^{-1}] = B_K$ has been chosen. If $\bar{B}_i := B_i/(\pi)$ is reduced, then it follows from the Proposition that $B_i = B$. Otherwise, let $\bar{z} \in \bar{B}_i$ be a nonzero nilpotent and let $n \in \mathbb{N}$ be such that $\bar{z}^n = 0$. Let $z \in B_i$ be a lift of $\bar{z}$ and write $w := z/\pi \in B_K$. Then $w \notin B_i$, as $\bar{z} \neq 0$. However, $w^n \in B_i$, and so we can enlarge $B_{i+1} := B_i[w] \subseteq B$. This process yields a chain of finite extensions of A

$$B_0 \subsetneq B_1 \subsetneq \cdots B.$$

Since A is Noetherian, $B = B_n$ for sufficiently large n [33, Proposition 8].

5.2 Reduced Special Fiber

The following criterion lets us decide whether a normal model has reduced special fiber, a necessary condition for a model to be semistable and a requirement for the normalization algorithm above to work.

Proposition 5.4 *Let X be an irreducible smooth projective curve over K, and let $\mathcal{X}$ be a normal model of X, represented by a finite set $V = V(\mathcal{X})$ of discrete valuations on $K(X)$. Then the special fiber of $\mathcal{X}$ is reduced if and only if all $v \in V$ are weakly unramified over v_K, i.e., $e(v \mid v_K) = 1$.*

Proof Let $v \in V$ be ramified over v_K with ramification index $e > 1$. Then there is an $f \in K(X)$ such that $e \cdot v(f) = v_K(\pi) = v(\pi)$ where $\pi \in K$ is a uniformizing parameter for v_K. Let $\xi \in \mathcal{X}_s$ be the generic point on the special fiber corresponding to v. Since the image of f in $\mathcal{O}_{\mathcal{X},\xi}/(\pi) \simeq \mathcal{O}_{\mathcal{X}_s,\xi}$ is a nonzero nilpotent, the special fiber of $\mathcal{X}$ is not reduced.

Conversely, let us suppose that the special fiber of $\mathcal{X}$ is not reduced. We claim that there is a generic point $\eta \in \mathcal{X}_s$ such that $\mathcal{O}_{\mathcal{X}_s,\eta}$ is not reduced. Suppose that this is not the case and let $x \in \mathcal{X}_s$ be a point which is not reduced. Since all generic points of $\mathcal{X}_s$ are reduced, this is also the case for all generic points of $\operatorname{Spec} \mathcal{O}_{\mathcal{X}_s,x}$. As the closed point of the latter is the only point which is not reduced, it is an embedded point of $\operatorname{Spec} \mathcal{O}_{\mathcal{X}_s,x}$ [23, Exercise 7.1.3]. Therefore $x \in \mathcal{X}_s$ is an embedded point. However, by Serre's Criterion [23, Theorem 8.2.23], the normal scheme $\mathcal{X}$ satisfies the property (S_2), i.e., the depth of $\mathcal{O}_{\mathcal{X},x}$ equals two. Therefore, $\mathcal{X}_s$ can not have any embedded points. This proves the claim.

Now let η be a generic point on the special fiber which is not reduced. There is a $g \in \mathcal{O}_{\mathcal{X},\eta} \subseteq K(X)$ and $e > 1$ such that $g^e \in (\pi)$ but $g \notin (\pi)$. Therefore, the valuation corresponding to x is not weakly unramified. ∎

Example 5.5 In Section 2.1 we considered the smooth projective curve Y given by the equation

$$y^3 = 1 + 3x^3 + 3x^5$$

as a cover of the projective line with variable x. Let us consider Y as a curve over $K \coloneqq \mathbb{Q}_3$. Write $R \coloneqq \mathbb{Z}_p$ and let $\mathcal{Y}$ be the normalization of the normal model $\mathbb{P}^1_R$ in Y. With the method described in Subsection 5.1.2, we determine that $\mathcal{Y}_s$ has a single irreducible component which is given by

$$v \coloneqq [v_0, v_1(y+2) = 1/3, v_2(y^3 - 3x^5 - 3x^3 - 1) = \infty].$$

As v is ramified over v_K with ramification index 3, the special fiber of $\mathcal{Y}$ is not reduced; this agrees with the explicit computation in Section 2.1 which came to the same result.

Remark 5.6 Let $\mathcal{X}$ be a normal model of an absolutely irreducible smooth projective curve X with a special fiber which is not reduced. By the above proposition, some of the valuations in $V(\mathcal{X})$ are not weakly unramified over v_K. In Chapter 6 we discuss algorithms which determine a finite extension K'/K such that the extensions of $v \in V(\mathcal{X})$ to $K(X \times K')$ are weakly unramified over the extension of v_K to K'. If, for an appropriate K', we let $\mathcal{X}'$ be the normal model corresponding to the set of all extensions of elements in $V(\mathcal{X})$ to $V(X \times K')$, then $\mathcal{X}'$ is a normal model of $X \times K'$ with reduced special fiber. In other words, we can get rid of a non-reduced special fiber by a finite extension of the base field K.

5.3 Irreducible Components of the Special Fiber

Let $\mathcal{X}$ be a normal model of an irreducible smooth projective curve X. If the special fiber $\mathcal{X}_s$ is reduced, we could decide whether $\mathcal{X}$ is semistable by examining the singularities on the special fiber. Sometimes it is easier to compare the genera of the irreducible components of $\mathcal{X}_s$ with the genus of X to decide whether $\mathcal{X}$ is semistable.

Proposition 5.7 *Let X be an irreducible smooth projective curve over K, and let $\mathcal{X}$ be a normal model of X with reduced special fiber. Let $\Gamma_1, \ldots, \Gamma_n$ be the irreducible components of $\mathcal{X}_s$, and suppose that they are geometrically irreducible. Denote by Γ_i' the normalization of Γ_i. Let $x_1, \ldots, x_m \in \mathcal{X}_s$ be the singularities on $\mathcal{X}_s$. Let*

$$\Delta \coloneqq 1 - n + \sum_{i=1}^{m} [k(x_i) : k] + \sum_{i=1}^{n} g(\Gamma_i').$$

Then the following hold:

(a) If $\mathcal{X}$ is semistable, then $g(X) = \Delta$.

(b) If $g(X) = \Delta$ and all x_i have at least two preimages in the normalization of $\mathcal{X}_s$, then $\mathcal{X}$ is semistable.

Proof For $x \in \mathcal{X}_s$ one defines

$$\delta_x \coloneqq ([k(x) : k])^{-1} \dim_k \mathcal{S}_x$$

with

$$\mathcal{S}_x \coloneqq \mathcal{O}'_{\mathcal{X}_s,x} / \mathcal{O}_{\mathcal{X}_s,x}$$

where $\mathcal{O}'_{\mathcal{X}_s,x}$ denotes the integral closure of $\mathcal{O}_{\mathcal{X}_s,x}$ in its field of fractions. The reduced projective curve $\mathcal{X}_s$ satisfies [23, Remark 3.3.33, Proposition 7.5.4]

$$g_{\text{arith}}(\mathcal{X}_s) = 1 - n + \sum_{x \in \mathcal{X}_s} \dim_k \mathcal{S}_x + \sum_{i=1}^{n} g(\Gamma_i').$$

Since $\delta_x = 0$ if x is regular and $\delta_x = 1$ if x is an ordinary double point, (a) holds. If $g(X) = \Delta$, then all $\delta_{x_i} = 1$. The only way how $\mathcal{X}$ could not be semistable was if some x_i had only a single preimage in the normalization $\mathcal{X}_s'$. This proves (b).■

Proposition 5.8 *Let X be an irreducible smooth projective curve over K, and let $\mathcal{X}$ be a normal model of X with reduced special fiber $\mathcal{X}_s$. Let $\Gamma \subseteq \mathcal{X}_s$ be an irreducible component, and let $v \in V(\mathcal{X})$ be the corresponding discrete valuation. Then $K(\Gamma)$ is isomorphic to the residue field of v.*

Proof Let $\xi \in \Gamma$ be generic. Since Γ is reduced, π is uniformizing in $\mathcal{O}_{\mathcal{X},\xi} = \mathcal{O}_v$ (Proposition 5.4). Therefore, $K(\Gamma) = \mathcal{O}_{\mathcal{X},\xi}/(\pi) = \mathcal{O}_v/(\pi)$ the residue field of v. ■

Example 5.9 In Example 5.5 we have considered the smooth projective curve Y over $K \coloneqq \mathbb{Q}_3(\pi)$, where π is a third root of 3, given by the equation

$$y^3 = 1 + 3x^3 + 3x^5.$$

We determined a normal model of Y which corresponded to the single valuation

$$v = [v_0, v_1(y + 2) = v(\pi), v_2(y^3 - 1 - 3x^3 - 3x^5) = \infty].$$

The residue field of v is $\mathbb{F}_2(x)(u)$ with $u^3 = x^5 + x^3$. As the special fiber is reduced, this is also the function field of $\mathcal{Y}_s$, a function field of genus 1. Since Y_s has only one singularity and the genus of Y is 4, Proposition 5.7 implies that $\mathcal{Y}$ is not semistable.

Remark 5.10 A valuation $v \in V(\mathcal{X})$ can be written as an inductive pseudo-valuation. If v is an infinite inductive valuation, then the residue field can be read off the inductive description of v. For a limit valuation the situation is slightly more complicated since we usually only have access to finitely many terms of $v = \lim v_n$. The residue field can then be taken from the field $\mathbb{F}_n$ associated to v_n as soon as the degrees of the key polynomials stagnate. The details of this are in the proof of Lemma 4.73.

Chapter 6

Eliminating Ramification

We have seen in Chapter 3 that a normal model $\mathcal{X}$ of an irreducible smooth projective curve X can be described by a set of valuations on $K(X)$, the function field of X. Although it was difficult to extract specific information about $\mathcal{X}$ from such sets of valuations, we had seen in Section 5.2 that the ramification indices encode whether the special fiber $\mathcal{X}_s$ is reduced. Before we discuss this in more detail, let us fix some notation with the following definitions.

Definition 6.1 Let L/K be an extension of fields. Let v_L be a discrete valuation on L which restricts to a discrete valuation v_K on K. Let l/k be the residue fields of v_L and v_K, respectively.

The index of the value group of v_K in the value group of v_L is called the *ramification index* of v_L over v_K and is denoted by $e = e(v_L \mid v_K)$. We say that v_L is *weakly unramified* over v_K if $e = 1$. If L/K is a finite extension, then we say that

(i) v_L is *unramified* over v_K if $e = 1$ and l/k is separable,

(ii) v_L is *tamely ramified* over v_K if l/k is separable and if either the residue field characteristic is zero or if it is $p > 0$ and does not divide e, and

(iii) v_L is *wildly ramified* over v_K if it is not tamely ramified.

Definition 6.2 Let K be a field with a discrete valuation v_K. Let L/K be an extension of fields, and let v_L be a discrete valuation on L which extends v_K. Let K'/K be a finite extension. Consider $K'L$ in a fixed algebraic closure of L. We say that K'/K *eliminates the ramification* of v_L over v_K if all extensions of v_L to $K'L$ are weakly unramified over their restriction to K'. We say that K'/K *eliminates the ramification for one extension* of v_L over v_K if one extension of v_L to $K'L$ is weakly unramified over its restriction to K'. If v_L and v_K are clear from the context, we will also say that K'/K *eliminates the ramification* of L/K.

Given a normal model $\mathcal{X}$ of an irreducible smooth projective curve X over K, we want to determine a finite extension of K'/K such that all discrete valuations w which extend some $v \in V(\mathcal{X})$ to $K'K(X)$ are weakly unramified over $w\big|_{K'}$. (In our application, K is often complete with respect to v_K, therefore $w\big|_{K'}$ is simply the unique extension of v_K to K'.)

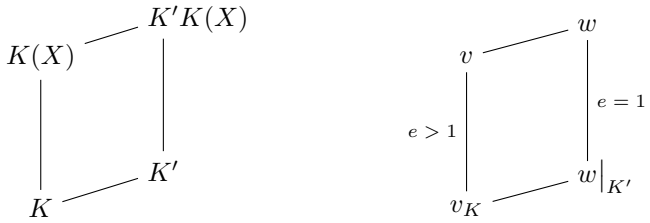


Figure 6.1: A finite extension K'/K eliminates the ramification of v over v_K.

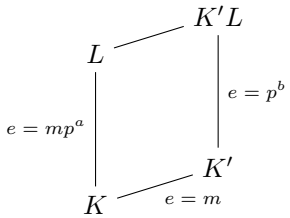
As $K(X)$ is the function field of a curve, i.e., a finite extension of a rational function field $K(x)$, we can divide the construction of an extension K'/K which eliminates ramification into two steps. First, we construct an extension to eliminate ramification in $K(x)/K$. Then, assuming that $v\big|_{K(x)}$ is weakly unramified over v_K, we construct an extension of K which eliminates the ramification of v over v_K.

We begin this chapter with a review of two approaches, namely Abhyankar's Lemma and a Theorem of Epp [11]. We find that Epp's approach is not sufficiently constructive for our needs. Using the language of inductive valuations we discuss ways to eliminate ramification in an extension $K(x)/K$. Finally, we present a new algorithm to eliminate ramification in $L/K(x)$ which, though not applicable in all cases, seems to be more practical.

6.1 Abhyankar's Lemma

Roughly speaking, Abhyankar's Lemma says that tame ramification of index m can be eliminated by adjoining any m-th root of a uniformizer. A precise statement is the following.

Proposition 6.3 *Let K be a field which is complete with respect to a discrete valuation v_K with residue field of characteristic $p > 0$. Let L/K be a finite Galois extension and write $mp^a = e(L \mid K)$ with m prime to p. Let K'/K be a totally ramified extension of degree m. Then $e(K'L \mid K')$ is a power of p.*



For the proof we need the following lemma.

Lemma 6.4 *Let K be a field which is complete with respect to a discrete valuation v_K with residue field of characteristic $p > 0$. Let K'/K be a totally and tamely ramified extension of degree m. Then K'/K is generated by an element π' such that π'^m is a uniformizer in K.*

Proof (of the Lemma) Let $\pi_1 \in K'$ be a uniformizer and consider its minimal polynomial over K

$$t^m - a_{m-1}t^{m-1} - \cdots - a_0.$$

Let $f(t) \coloneqq t^m - {}^{a_0}/_{\pi_1^m}$. Then 1 is a root of f modulo $v_{K'}$ but not a multiple root. By Hensel's Lemma, f has a root $\gamma \in K'$. Let $\pi' \coloneqq \gamma\pi_1$. Then $\pi'^m = a_0$ as required. ∎

Proof (of the Proposition) Lemma 6.4 shows that K' is generated by an m-th root of a uniformizer in K, i.e., $K' = K(\pi')$ with $\pi'^m = \pi$ for some uniformizer $\pi \in K$. Let us first suppose that K contains a primitive m-th root of unity. Let $I \subseteq G \coloneqq \mathrm{Gal}(L/K)$ denote the inertia group of L/K (cf. [28, II.§9].) Then L^I/K is unramified. Let $R \subseteq I$ denote the ramification group of L/K. Then I/R is cyclic of order m [28, II.§10.2]. As K contains a primitive m-th root of unity, the extension L^R/L^I is a Kummer extension, i.e., it is defined by an equation of the form $z^m = u\pi^n$ with a unit $u \in L^I$. Over K' the extension $K'L^R/K'L^I$ is therefore given by an equation of the form $(z\pi^{-n/m})^m = u$, an unramified extension. (Note that the extension is also unramified if $t^m - u$ is not irreducible over $K'L^I$.) The statement follows since the extension $K'L^I/K'$ remains unramified [28, II.§7.2].

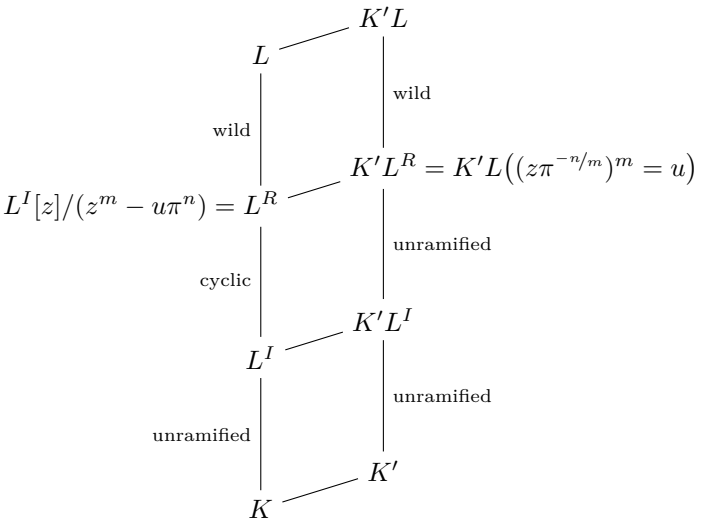


Figure 6.2: The fields involved in the first part of the proof of Abhyankar's Lemma.

We now drop the assumption that K contains a primitive m-th root of unity. Let $\zeta \in K^{\mathrm{ac}}$ be a primitive m-th root of unity. Then $K(\zeta)/K$ is an unramified Galois extension [28, II.§7.12]. Therefore $L(\zeta)/L$ is unramified [28, II.§7.2] and so $L(\zeta)/K(\zeta)$ has ramification index mp^a. As $L(\zeta)/K$ is Galois, $L(\zeta)/K(\zeta)$ is Galois. We have now reduced the setting to the case which we have treated already, i.e., any totally ramified extension of $K(\zeta)$ of degree m eliminates the tame ramification of $L(\zeta)$ over $K(\zeta)$. Let K'/K be a totally ramified extension of degree m. Then $K'(\zeta)/K(\zeta)$ is totally ramified of degree m and by the above,

$K'L(\zeta)/K'(\zeta)$ is ramified with a ramification index p^b. Since $K'L(\zeta)/K'L$ is unramified [28, II.§7.2], $e(K'L \mid K') = p^b$.

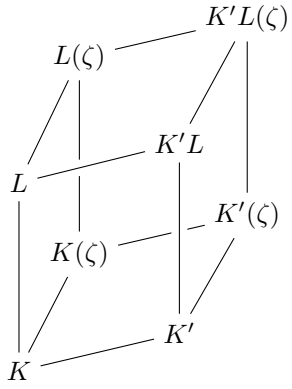
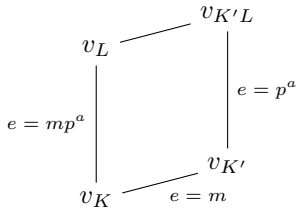


Figure 6.3: The fields involved in the second part of the proof of Abhyankar's Lemma. ∎

We can prove a similar statement using the theory of inductive valuations developed in Chapter 4.

Proposition 6.5 *Let K be a field of characteristic zero with a discrete valuation v_K whose residue field has characteristic $p > 0$. Let L/K be a finite extension of fields which is such that v_K has a unique extension v_L. Write $mp^a = e(v_L \mid v_K)$ with m prime to p. Let K'/K be a totally ramified extension of degree m which is such that $v_{K'}$ has a unique extension $v_{K'L}$ to $K'L$. Then $e(v_{K'L} \mid v_{K'}) = p^a$.*



Proof Let $G \in K[t]$ be the minimal polynomial over K of a uniformizing parameter in L which generates L/K. (As in the proof of the primitive element theorem [5, 3.6/12] such an element can be constructed by considering $\psi + p^n\alpha$ with a uniformizing parameter ψ, a generator α and n sufficiently large.) Since the image of t is uniformizing in $L = K[t]/(G)$, its valuation is $1/mp^a$. If we write v_L as an inductive pseudo-valuation, we therefore assign that valuation to t in the first step (Lemma 4.22.) We may write

$$v_L =: v_n = [v_0, v_1(t) = 1/mp^a, v_2(\phi_2) = \lambda_2, \ldots, v_n(G) = \infty]$$

with key polynomials of strictly increasing degrees. (The following argument can easily be adapted if v_L is not an infinite inductive valuation but a limit valuation.) Note that all λ_i are in the value group of v_1. To prove the proposition it suffices

to show that $v_{K'L}$ has the same presentation as an inductive pseudo-valuation over $v_{K'}$, i.e., that

$$v_{K'L} = w_n = [w_0, w_1(t) = 1/mp^a, w_2(\phi_2) = \lambda_2, \ldots, w_n(G) = \infty]$$

where we normalized such that a uniformizing element $\pi \in K'$ has valuation $v_{K'}(\pi) = 1/m$.

It is clear that w_1 is an approximant for $v_{K'L}$. If we were to apply the algorithm from Subsection 4.6.2 to determine an approximant over v_1, we would determine a monic polynomial $F(y)$ in the residue ring of v_1 and consider its factorization into irreducible factors. As the extension of v_K to L is unique, $F(y)$ factors as a power of an irreducible polynomial, i.e., $F(y) = (f(y))^l$. The key polynomial ϕ_2 is then a *lift* of $f(y)$ in the sense of Subsection 4.6.2. To see that ϕ_2 also leads to an approximant over $v_{K'}$, let us perform the same steps over w_1. For this we have to factor the monic polynomial $F(y^m) = (f(y^m))^l$ in the residue ring of w_1. Since $v_{K'}$ has a unique extension to $K'L$, $f(y^m)$ does not have coprime factors. It is easy to see that $f(y^m)$ does not factor as a power because m is prime to p. This shows that

$$w_2 \coloneqq [w_1, w_2(\phi_2) = \lambda_2]$$

is an approximant for $v_{K'L}$. Note that the residue fields of w_2 is a separable extension of the residue field of v_2, defined by the equation $z^m = y$.

The statement now follows inductively. Suppose that for some $i \geq 2$,

$$w_i = [w_0, w_1(t) = 1/mp^a, \ldots, w_i(\phi_i) = \lambda_i]$$

is an approximant for $v_{K'L}$ and that its residue field is a finite separable extension of the residue field of v_i. Again, write $F(y) = (f(y))^l$ for the polynomial in the residue ring of v_i which was used to determine the key polynomial ϕ_{i+1}. Since $v_{K'}$ has a unique extension to $K'L$, $f(y)$ has no coprime factors over the residue field of w_i and since the residue field of w_i is separable over the residue field of v_i, $f(y)$ remains irreducible. This shows that

$$w_{i+1} = [w_i, w_{i+1}(\phi_{i+1}) = \lambda_{i+1}]$$

is an approximant for $v_{K'L}$ as required. ∎

We rewrite Abhyankar's Lemma in the following corollary to make it applicable to our setting.

Corollary 6.6 *Let L/K be a finite separable extension of fields. Let w be a discrete valuation on L with residue field of characteristic $p > 0$ and let v be its restriction to K. Then there is a number m which is prime to p such that any totally ramified extension K'/K of degree m and any extension w' of w to $K'L$ satisfy: the ramification index of w' over its restriction to K' is a power of p.*

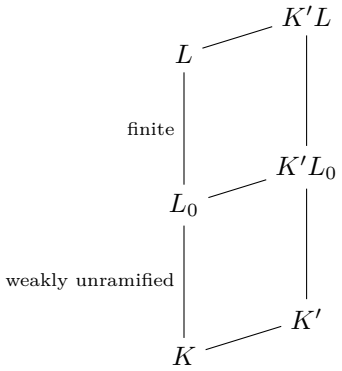
Proof Let us first assume that L and K are complete with respect to w and v, respectively. Let M be a Galois closure of L over K. Write $mp^a = e(M \mid K)$ with m prime to p. By Abhyankar's Lemma, any totally ramified extension K'/K of degree m satisfies $e(K'M \mid K') = p^b$. Therefore $e(K'L \mid K')$ is a power of p as required.

We now drop the requirement that L and K are complete. Let us denote by L_w/K_v the completions of L and K with respect to w and v, respectively. Let m be the degree of a totally ramified extension which eliminates the tame part of L_w/K_v as in the first part. Let K'/K be a totally ramified extension of degree m. We may assume that $K' = K[t]/(E)$ with an Eisenstein polynomial $E \in K[t]$. Let v' be the unique extension of v to K'. The polynomial E remains irreducible over K_v and therefore $K'_v \coloneqq K_v[t]/(E)$ is the completion of K' with respect to v'. From the first part of the proof, we know that the ramification index of $K'_v L_w/K'_v$ is a power of p. As $K'_v L_w$ is the completion of $K'L$ with respect to w', it follows that $e(w' \mid v')$ is a power of p as well. ∎

6.2 The Method of Epp

Let L/L_0 be a finite extension of fields with discrete valuations v_L and v_{L_0}, respectively. In view of Abhyankar's Lemma one could be lead to think that if v_L is ramified over v_{L_0} with ramification index $e > 1$, then adjoining an e-th root of any uniformizer of L_0 eliminates that ramification. The following example shows that this in not the case if v_L is wildly ramified over v_{L_0}.

Example 6.7 Consider the rational function field $L_0 = \mathbb{Q}_2(x)$ with the discrete valuation v_{L_0} induced by the Gauss valuation on $\mathbb{Q}_2[x]$ in turn induced by the 2-adic valuation on $K \coloneqq \mathbb{Q}_2$. Let $L \coloneqq L_0[t]/(G)$ where $G \coloneqq t^2 + 8x + 2$.



With the method described in Subsection 4.6.2 we determine that v_{L_0} has precisely one extension to L which is

$$w_L \coloneqq w_2 \coloneqq [w_0, w_1(t) = 1/2, w_2(G) = \infty].$$

Hence w_L is ramified over v_2 with ramification index $e = 2$. If Abhyankar's Lemma applied in this situation, $K' \coloneqq K(\sqrt{2})$ would eliminate that ramification. Of course, after such an extension, the valuation of t is in the value group of K'. But now G is not a key polynomial over $[w_0, w_1(t) = 1/2]$ anymore. Instead, w_L has a unique extension to $K'L$ which is

$$w_{K'L} \coloneqq w_2 \coloneqq [w_0, w_1(t + 2 + \sqrt{2}) = 5/4, w_2(G) = \infty].$$

This extension is again ramified with ramification index 2 over $v_{K'}$. More generally, if we set

$$K' \coloneqq K\left(2^{2^{-N}}\right)$$

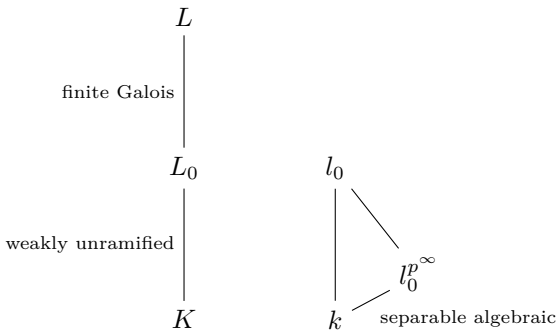
with $N \geq 1$, then there is a unique extension which is

$$w_{K'L} \coloneqq w_2 \coloneqq [w_0, w_1(t + \sum_{n=0}^{N} 2^{3/2-2^{-n}}) = \frac{3 \cdot 2^N - 1}{2^{N+1}}, w_2(G) = \infty].$$

We see that the ramification index does not change. It is 2 no matter how large an extension of this kind we take.

The article [11] shows that in the situation of the example one can always find a finite extension K'/K which eliminates the ramification of v_L over v_K. Let us fix some notation to describe the approach which we will in the following call the *Method of Epp*. Let $K \subseteq L_0 \subseteq L$ be an extension of fields with L/L_0 finite. Let v_K, v_{L_0}, v_L be the discrete valuations on these fields and let $k \subseteq l_0 \subseteq l$ be the respective residue fields. To simplify the exposition, we assume that all fields are complete, in mixed characteristic, that k is perfect, and that L/L_0 is Galois. The Method of Epp determines a finite extension K'/K which eliminates the ramification of v_L over v_K. For this the following assumption is needed.

Assumption 6.8 The field $l_0^{p^\infty}$, the largest perfect subfield of l_0, is contained in the separable algebraic closure of k.



We now outline the construction of K'/K to conclude that the Method of Epp is not sufficiently practical for our needs. With Abhyankar's Lemma, we may assume that the ramification index of v_L over v_{L_0} is a power of p. Since L is complete, we may further assume that the residue fields of L and L_0 are isomorphic (Lemma 6.11.) The Galois group of L/L_0 is therefore its ramification group, a p-group. As such, this group has a composition series of cyclic groups of order p. This series turns L/L_0 into a tower of Galois extensions with cyclic Galois groups of order p. These extensions can now be treated one by one to eliminate ramification. Let therefore L/L_0 be a cyclic extension of order p. This extension is generated by an element z which satisfies an equation $z^p = 1 + a\psi^j$ where ψ is a uniformizing parameter in L_0. A technical case by case discussion for different values of j and the reduction of a then shows explicitly how to construct an extension of K which eliminates the ramification.

6.2.1 Why the Method of Epp is not Practical

To eliminate wild ramification one would like to use the Method of Epp in practice, ideally implemented in a computer algebra system. There are a number

of reasons why this does not seem to be feasible. First, the Method of Epp assumes that L/L_0 is a Galois extension. This seems to be essential in the procedure since the process of breaking down the extension into cyclic parts of order p depends on it. However, if L/L_0 is an extension of order m, e.g., given by the minimal polynomial of a generator, then passing to the Galois closure often means increasing the degree of the extension to $m!$. Doing the necessary Galois theory in extensions of that degree should be entirely out of range even for relatively small values of m.

But even if L/L_0 was already Galois, there are problems which stem from passage to the completion. It seems to be fairly difficult but one could probably work out how to do arithmetic in the completion of L and even implement this on a computer. However, one reason why the Method of Epp needs to pass to the completion is that there is a complete intermediate field $K \subseteq L_0' \subseteq L$ which is weakly unramified over K and has the same residue field as L (Lemma 6.11.) The proof of this is not constructive and it seems to be very difficult to construct this intermediate field in practice.

This discussion shows that it is desirable to have alternative methods to eliminate ramification. In the following we present such algorithms for extensions of the form $L/K(x)/K$. While these are less generic than the Method of Epp, they can easily be implemented in a computer algebra system.

6.3 Ramification in Rational Function Fields

Throughout this section let $L \coloneqq K(x)$ be a rational function field over a field K, and let v_L be a discrete valuation on L which extends a discrete valuation v_K on K. We denote by $K_v \subseteq L_v$ the completions of K and L with respect to v_K and v_L respectively. We will frequently consider composite fields. These should always be taken as subfields of an appropriate algebraic closure.

In this section we want to discuss ways to construct an extension K'/K which eliminates the ramification of v_L over v_K. We begin with a brief discussion on how Abhyankar's Lemma and the Method of Epp can be applied to this situation. We will see that the Method of Epp is not practical for our purposes. However, using the theory developed in Chapter 4, we provide a new algorithm which eliminates ramification in a more specialized setting.

6.3.1 Abhyankar's Lemma

We discussed in Section 6.1 how Abhyankar's Lemma can be used to eliminate tame ramification in finite extensions of fields. In this section we want to extend this to infinite extensions L/K. The following lemma often allows us to assume that K is complete with respect to v_K.

Lemma 6.9 *Let the residue field of v_L have transcendence degree one over the residue field of v_K. Let K'/K be a finite extension which is such that v_K has a unique extension to K'. Let K_v'/K_v be the completions of K'/K. Then v_L has a unique extension v_{K_vL} to K_vL. Suppose that K_v'/K_v eliminates the ramification of v_{K_vL} over v_{K_v}. Then K'/K eliminates the ramification of v_L over v_K.*

Proof By Theorem 4.31 v_L is induced by an inductive valuation on $K[x]$ (possibly after a substitution $x \mapsto 1/x$)

$$v_L = [v_0, \ldots, v_n(\phi_n) = \lambda_n].$$

Since all key polynomials remain irreducible over K_v, it has a unique extension to $K_vL = K_v(x)$. Let w be an extension of v_L to $K'L$. By the same argument w has a unique extension to $K'_vL = K'_v(x)$. Since that extension is weakly unramified over K'_v, the same is true for w. ∎

Remark 6.10 In the Lemma we started with an extension K'/K and considered the corresponding extension K'_v/K_v. A discussion when an extension K'_v/K_v can be approximated by an extension K'/K can be found in the proof of [11, Theorem 2.0].

To apply Abhyankar's Lemma, we need to replace L/K with a finite extension. The following proposition allows us to do so when K is complete and in mixed characteristic.

Lemma 6.11 [38] *Let K be complete and in mixed characteristic. Let L_v be the completion of $L = K(x)$ with respect to v_L. Then there is a complete intermediate field $K \subseteq L_0 \subseteq L_v$ which is weakly unramified over K and which is such that L_v/L_0 is a totally ramified finite extension.*

Proof We give only a rough sketch of the proof to show that it can not directly be turned into an algorithm. To the field L_v, one can construct an extension M/L_v with perfect residue field. The complete field M has a subfield M' which has the same perfect residue field as M and is totally unramified, i.e., p is uniformizing. On the other hand, there is a field K' which is totally unramified and has a residue field isomorphic to that of L_v. With the same construction as before, one can construct an extension of K' which is complete and has a perfect residue field. One can show that this field has to be isomorphic to M'. Within M' one finds K' as a subfield of L_v. Setting $L_0 := K'K$ produces the desired field.

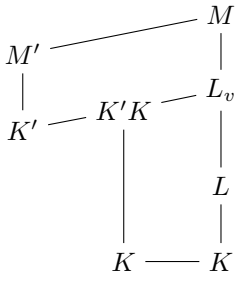


Figure 6.4: The fields involved in the proof. Fields connected by sloped lines have isomorphic residue fields. ∎

Proposition 6.12 *Let v_L have a residue field of characteristic $p > 0$ which is transcendental over the residue field of v_K. Then there is a number m such that for any totally ramified extension K'/K of degree m, any extension of v_L to $K'L$ has a ramification index which is a power of p over its restriction to K'.*

Proof Let us first assume that K and L are complete. Let L_0 be the field constructed in the previous lemma. Then L/L_0 is finite, and by Corollary 6.6 any totally ramified extension of some degree m eliminates the tame ramification. Let K'/K be a totally ramified extension of degree m. Then $K'L_0$ is totally ramified over L_0 of degree m and the ramification index of $K'L/K'L_0$ is a power of p. Since $K'L_0$ is weakly unramified over K', the ramification index of $K'L/K'$ is a power of p.

Let us now assume that only K is complete. Let L_v be the completion of L with respect to v_L. As we have seen, the ramification index of $K'L_v$ over K' is a power of p. Since $K'L$ embeds into $K'L_v$ corresponding to the extensions of v_L to $K'L$, these extensions also have ramification indices which are powers of p.

If K is not complete, then an immediate analog of Lemma 6.9 can be used to pass to the completion of K. ∎

6.3.2 Rigid Diskoids

Let K again be a field with a discrete valuation v_K and let $L \coloneqq K(x)$. Let v_L be an extension of v_K which is such that the residue field of v_L has transcendence degree one over k, the residue field of v_K. We may then assume that v_L is induced by an inductive valuation on $K[x]$, Theorem 4.31; we write

$$v_L = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

with key polynomials ϕ_i of strictly increasing degree. The ramification index $e(v_L \mid v_K)$ is one unless a λ_i is not in the value group of v_K (Corollary 4.30.) We want to construct a finite extension K'/K which eliminates the ramification of v_L over v_K. Let us first consider an easy special case.

Lemma 6.13 *Let v_L be a discrete valuation on $K(x)$ which is induced by an inductive valuation on $K[x]$ which is of the form*

$$v_1 \coloneqq [v_0, v_1(\phi) = \lambda].$$

Let K'/K be a totally ramified extension which contains an element of valuation λ. Then K' eliminates the ramification of v_L over v_K.

Proof As K'/K is totally ramified, ϕ is a key polynomial over v_0', the Gauss valuation over K'. The valuation induced by $v_1' \coloneqq [v_0', v_1'(\phi) = \lambda]$ extends v_L to $K'L$ and is weakly unramified over $v_{K'}$. ∎

We are now going to reduce the general case to this special case using the language of diskoids developed in Section 4.4.

Lemma 6.14 *Let v_L be a discrete valuation on $K(x)$ which is induced by an inductive valuation on $K[x]$ which is of the form*

$$v_n \coloneqq [v_0, \ldots, v_n(\phi_n) = \lambda_n].$$

Let K'/K be a finite extension which contains a splitting field of ϕ_n. Then the extensions of v_L to $K'L$ are induced by valuations of the form

$$v_1' \coloneqq [v_0', v_1'(t - \alpha) = \lambda]$$

where $\alpha \in K'$ is a root of ϕ_n and $\lambda \in \mathbb{Q}$.

Proof This is an immediate consequence of Lemma 4.48 and Theorem 4.56. ∎

Remark 6.15 The proof shows that to have at least one extension of v_L which is of the form

$$v_1' \coloneqq [v_0', v_1'(t-\alpha) = \lambda]$$

it suffices to adjoin a root of ϕ to K.

Proposition 6.16 *Let v_L be a discrete valuation on $K(x)$ whose residue field has transcendence degree one over the residue field of v_K. Then there is a finite extension K'/K which eliminates the ramification of v_L over v_K.*

Proof The valuation v_L is induced by an inductive valuation whose ramification can be eliminated by adjoining the roots of the last key polynomial and an additional totally ramified extension (Lemmata 6.13 and 6.14.) ∎

Example 6.17 Let $K \coloneqq \mathbb{Q}$ with the 3-adic valuation v_K. Consider on $L = K(x)$ the valuation induced by

$$v_L \coloneqq v_2 = [v_0, v_1(x) = 1/3, v_2(x^3 + 6x^2 + 15x + 3) = 2],$$

ramified over v_K with ramification index 3.

Let us first ignore Proposition 6.16 and adjoin to K an element π with $\pi^3 = 3$. Over $K' \coloneqq K(\pi)$, v_L has a unique extension

$$v_{K'L} \coloneqq w_2 = [w_0, w_1(x+\pi) = 4/9, w_2(x^3 + 6x^2 + 15x + 3) = 2]$$

which is still ramified over $v_{K'}$ with ramification index 3.

We now follow Proposition 6.16 and adjoin to K an element α with $\alpha^3 + 6\alpha^2 + 15\alpha + 3 = 0$. Over $K' \coloneqq K(\alpha)$, v_L has two extension

$$v_{K'L,1} \coloneqq w_1 = [w_0, w_1(x+2\alpha) = 1],$$
$$v_{K'L,2} \coloneqq w_2' = [w_0, w_1'(x+2\alpha) = 1/2, w_2'(x^2 + 4\alpha x - 2\alpha^2 - 15\alpha - 3) = 3/2].$$

Since 1 is in the value group of $v_{K'}$ we do not need Lemma 6.13 here, i.e., we do not have to adjoin any element to make the first valuation weakly unramified over $v_{K'}$. By Abhyankar's Lemma, the second extension can be made weakly unramified by adjoining a square root of α.

6.4 Ramification in Finite Extensions

We have seen earlier that the Method of Epp is not practical to eliminate ramification in finite extensions like the ones we are concerned with. In this section we develop a new method to eliminate ramification which appears to be more practical and in particular easy to implement. It does, however, not provide the full generality of the Method of Epp. We need a few mild conditions which are clearly satisfied in our application. However, the proof only works for extensions of certain types, in particular it works for extensions whose ramification index is not divisible by p^2.

Throughout this section let K be a field of characteristic zero with a discrete valuation v_K and perfect residue field k of characteristic $p > 0$. Let L_0 be an extension of K (typically transcendental,) and let v_{L_0} be a discrete valuation

which extends v_K to L_0 and is weakly unramified over v_K with residue field ℓ_0. Let L/L_0 be a finite extension, and let v_L be an extension of v_{L_0} to L with residue field ℓ. All valuations are normalized such that $v(p) = 1$.

Assumption 6.18 We make the following assumptions on the residue fields of these valuations:

(A) Let ℓ_1/ℓ_0 be a finite extension, and let $x \in \ell_1$ be a p^n-th power for all $n \geq 1$, then $k(x)/k$ is finite Galois.

(B) The extension ℓ/ℓ_0 is simple.

Example 6.19 Let $K \coloneqq \mathbb{Q}_p$, and let $L_0 \coloneqq K(x)$. Let v_K be the p-adic valuation, and let v_{L_0} be the extension induced by the Gauss valuation on $K[x]$. Let ℓ_1 be a finite extension of $\ell_0 = \mathbb{F}_p(x)$. Then ℓ_1 is a finite separable extension of $\mathbb{F}_p(y)$ for some transcendental $y \in \ell_1$. Any $s \in \ell_1$ which is a p^n-th power for all $n \geq 1$ generates a finite separable extension of $k = \mathbb{F}_p$ [11, Remark 0.4 (2)]. Since finite extensions of $\mathbb{F}_p$ are Galois, assumption (A) holds. Furthermore, finite extensions of $\mathbb{F}_p(x)$ are simple [3], i.e., (B) holds.

6.4.1 Stability under Base Change

Our algorithm uses two kinds of extensions K'/K, totally ramified extensions and unramified extensions. Our setting is stable under both kinds of extensions.

Lemma 6.20 *Let K'/K be a finite extension such that v_K has a unique extension $v_{K'}$ to K' which is totally ramified, and let $v_{K'L}$ be an extension of v_L to $K'L$. Then v_{L_0} has a unique extension $v_{K'L_0}$ to $K'L_0$ which is weakly unramified over $v_{K'}$. Additionally, the analogs of assumptions (A) and (B) are still satisfied by $v_{K'L}$, $v_{K'L_0}$, and $v_{K'}$.*

Proof Since v_{L_0} is weakly unramified over v_K, all extensions of v_{L_0} to $K'L_0$ must have the same ramification index as $v_{K'}$ over v_K. Therefore there can only be one such extensions. The rest of the statement follows since the residue field does not change when passing from v_{L_0} to $v_{K'L_0}$. ∎

Lemma 6.21 *Let K'/K be finite extension such that v_K has a unique extension $v_{K'}$ to K' which is unramified and induces a Galois extension on the residue fields, let $v_{K'L}$ be an extension of v_L to $K'L$, and let $v_{K'L_0}$ be its restriction to $K'L_0$. Then $v_{K'L_0}$ is weakly unramified over $v_{K'}$. Additionally, the analogs of assumptions (A) and (B) are still satisfied by $v_{K'L}$, $v_{K'L_0}$, and $v_{K'}$.*

Proof Let k'/k be the residue field extension of $v_{K'}$ over v_K. Since k'/k is finite Galois, there is either a unique extension of v_{L_0} to $K'L_0$ or there are $[k'\colon k]$ many. In either case, these extensions are unramified and therefore weakly unramified over $v_{K'}$. ∎

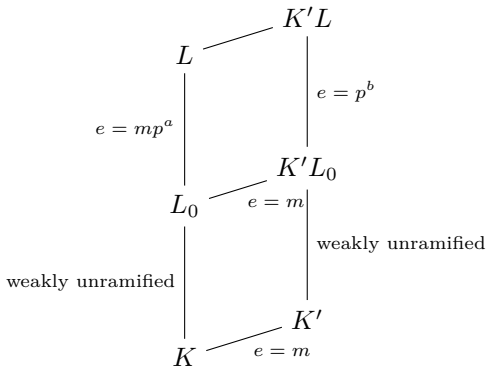
It is also stable under the finite extensions of L_0 which we are going to use.

Lemma 6.22 *Let L_1/L_0 be a finite extension which permits a unique extension v_{L_1} of v_{L_0} to L_1. Suppose that this extension is weakly unramified and let ℓ_1 be the residue field of v_{L_1}. Then assumption (A) still holds for ℓ_1 over k.* ∎

Since all extensions K'/K which we construct will be such that v_K has a unique extension to K', and since most of the time, K'/K will be totally ramified and therefore the extension of v_{L_0} to $K'L_0$ will be unique as well, we denote v_{L_0}, v_K, and finite extensions thereof by v when no confusion can arise.

6.4.2 Abhyankar's Lemma

Write $mp^a = e(v_L \mid v_K)$ with m prime to p. Since v_{L_0} is weakly unramified over v_K, the ramification index of v_L over v_{L_0} is mp^a as well. By Corollary 6.6, any totally ramified extension of some degree m' eliminates the tame ramification of v_L over v_{L_0}. If we let K'/K be a totally ramified extension of degree m', then $K'L_0/L_0$ is totally ramified of degree m' and therefore such K'/K eliminates the tame part of the ramification of v_L over v_K.



6.4.3 Approximating Inductive Limit Valuations

We discussed in Chapter 4 how to write $w \coloneqq v_L$ as an inductive pseudo-valuation over v_{L_0} given an irreducible monic integral polynomial $G \in L_0[t]$ with $L = L_0[t]/(G)$. Typically, w will not be an infinite inductive valuation but a limit valuation, i.e., a valuation of the form

$$w = \lim w_n$$

with inductive valuations w_n. To be precise, this is the case if and only if G factors over the completion of L_0 (Theorem 4.65.)

Example 6.23 Let $K \coloneqq \mathbb{Q}_2$. Let v_{L_0} be the valuation on the rational function field $L_0 \coloneqq K(x)$ which is induced by the Gauss valuation on $K[x]$. Consider the irreducible polynomial $G \coloneqq t^2 + t + x^2 + x \in K(x)[t]$. The algorithm of Subsection 4.6.2 determines the extensions of v_{L_0} to $L \coloneqq K(x)[t]/(G)$. There are two extensions w, w' and both are limit valuations

$$w = \lim w_n,$$
$$w' = \lim w'_n.$$

The first entries of these limits are readily determined from the factorization of $G \equiv (t + x)(t + x + 1)$ in reduction mod 2:

$$w_1 = [w_0, w_1(t + x) = 1]$$
$$w'_1 = [w_0, w'_1(t + x + 1) = 1]$$

Working with a limit valuation can be cumbersome. One would rather use an infinite inductive valuation which shares the essential properties. That it is possible to do so is the content of this subsection. As a first step, we replace the factors G_i with approximations $\tilde{G}_i$ which are defined over L_0. Then we show that an extension which eliminates ramification for the latter also does so for the former.

Lemma 6.24 *Let M be a field with a discrete valuation v and let M_v be its completion. Let N/M be a finite separable extension, let w be an extension of v to N, and let N_w/M_v be the completion of N with respect to w. Then there is a monic integral irreducible $\tilde{G} \in M[t]$ which remains irreducible over M_v such that $M_v[t]/(\tilde{G})$ and N_w are isomorphic as extensions of M_v.*

Proof Without loss of generality we may assume that $N = M[t]/(G)$ with a monic integral irreducible $G \in M[t]$. The valuation w corresponds to an irreducible factor G_i of G over M_v [28, II.§8.2]. Since w is a discrete pseudo-valuation it must be an infinite inductive valuation or a limit valuation (Theorem 4.65.) If w is an infinite inductive valuation, then we can take $\tilde{G} = G$. Let us assume that this is not the case and that

$$w =: \lim_n w_n = [w_0, \dots, w_n(\phi_n) = \lambda_n].$$

For a sufficiently large n, in particular such that $\deg \phi_n = \deg G_i$, let

$$\tilde{G} \coloneqq \phi_n \in M[t].$$

Consider embeddings of $M_v[t]/(G_i)$ and $M_v[t]/(\tilde{G})$ into an algebraic closure of M_v, and let $\alpha_1, \dots, \alpha_m$ and $\tilde{\alpha}_1, \dots, \tilde{\alpha}_m$ be the roots of G_i and $\tilde{G}$, respectively. To prove that $M_v[t]/(G_i) \simeq M_v[t]/(\tilde{G})$ it suffices to show that the latter contains a root of G_i. For all α_k

$$\sum_{j=1}^{m} v(\alpha_k - \tilde{\alpha}_j) = v(\tilde{G}(\alpha_k)) = w(\tilde{G}(t)) = w_n(\phi_n) = \lambda_n.$$

Since G and therefore G_i and $\tilde{G}$ have integral coefficients, we have for some k and j that

$$v(\alpha_k - \tilde{\alpha}_j) \geq \frac{\lambda_n}{m}.$$

As the λ_n tend to infinity, we can choose n sufficiently large so that for all $l \neq k$

$$v(\alpha_k - \tilde{\alpha}_j) > v(\alpha_k - \alpha_l).$$

By Krasner's Lemma [28, II.§6 Aufgabe 2], $\alpha_k \in M_v[t]/(\tilde{G})$, as required. ∎

Remark 6.25 The proof provides an algorithm to compute the polynomial $\tilde{G}$. We had seen in Subsection 4.6.2 how to construct arbitrarily many terms of the limit valuation

$$w =: \lim w_n = [w_0, \dots, w_n(\phi_n) = \lambda_n].$$

As the roots of (the unknown) G_i form a subset of the roots of G, we can bound their distance with the algorithm described in Section 4.8, i.e., we get a δ such that $v(\alpha_k - \alpha_l) \geq \delta$ for all pairwise distinct roots α_k, α_l. If we pick ϕ_n such that $\lambda_n / \deg G_i > \delta$, then G_i and ϕ_n describe isomorphic extensions of the completion of L_0.

Example 6.26 Let us see how this algorithm works out in the previous example. For the two roots α, α' of G, we determine that $v(\alpha - \alpha') = 1 =: \delta$. We already computed that the limit valuations w, w' corresponding to the α and α' start with

$$w_1 = [w_0, w_1(t + x) = 1]$$
$$w_1' = [w_0, w_1'(t + x + 1) = 1].$$

Since $\lambda_1, \lambda_1' = 1 \not> \delta$, the lemma does not apply. We compute the next approximants as

$$w_2 = [w_1, w_2(t + 2x^2 + x) = 2],$$
$$w_2' = [w_1, w_2'(t + 2x^2 + 3x + 1) = 2].$$

Now $\lambda_2, \lambda_2' = 2 > \delta$.

Proposition 6.27 *Let M be a field with a discrete valuation v, let N/M be a finite separable extension, and let w be an extension of v to N. Then there is a monic integral irreducible $\tilde{G} \in M[t]$, and an infinite inductive valuation $\tilde{w}$ which extends v to $\tilde{N} \coloneqq M[t]/(\tilde{G})$ such that a finite extension M'/M eliminates ramification of w over v if and only if it eliminates ramification of $\tilde{w}$ over v.*

Proof Let N_w/M_v be the completions of N/M with respect to w. An extension M'/M eliminates the ramification of N/M if and only if it eliminates the ramification of N_w/M_v. By the previous lemma, there is a $\tilde{G} \in M[t]$ such that N_w is isomorphic to $M_v[t]/(\tilde{G})$ as extensions of M_v. Since $M_v[t]/(\tilde{G})$ is the completion of $\tilde{N} \coloneqq M[t]/(\tilde{G})$ with respect to the unique extension of v, any extension M'/M eliminates the ramification of that extension if and only if it does so for $M_v[t]/(\tilde{G})$ over M_v. ∎

This proposition tells us that if v_{L_0} has more than one extension to $L = L_0[t]/(G)$, then we can find approximate factors $\tilde{G}_i$ of G which describe only one of these extensions. If we eliminate the ramification of the extensions of v_{L_0} to the $L_0[t]/(\tilde{G}_i)$, then this also eliminates the ramification of the original extensions.

6.4.4 Ramification in Infinite Inductive Valuations

We want to determine a finite extension K'/K which eliminates the ramification of v_L over v_{L_0}. In view of the previous subsection, we may assume that v_L is the unique extension of v_{L_0} to v_L and that it is given by an infinite inductive valuation

$$v_L = [v_0, v_1(\phi_1) = \lambda_1, \ldots, v_L(G) = \infty].$$

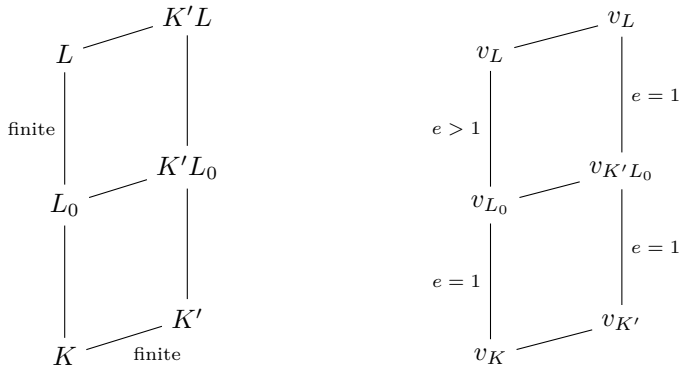


Figure 6.5: A finite extension K'/K eliminates the ramification of v_L over v_K.

Outline of the Algorithm

Suppose that v_L is totally ramified over v_{L_0}. If we let G be the minimal polynomial of a uniformizing parameter which generates L, then v_L is of the form

$$v_L = [v_0, v_1(t) = \lambda, v_L(G) = \infty].$$

In a first step we construct an extension K'/K, which *eliminates total ramification* of v_L over v_{L_0}, i.e., which is such that there is an extension of v_L to $K'L$ whose ramification index is strictly smaller than $e(v_L \mid v_{L_0})$. We can then assume that v_L is not totally ramified over v_{L_0} (or that L/L_0 can be replaced by an extension of smaller degree, Proposition 6.27, on which we repeat the process.) Assumption (B) allows us to find an element $\alpha \in L$ which generates L and which reduces to a generator of ℓ/ℓ_0. If H denotes the minimal polynomial of α, then v_L is of the form

$$v_L = [v_0, v_1(\phi) = \mu, \ldots, v_L(H) = \infty]$$

with a polynomial ϕ which reduces to the minimal polynomial of the reduction of α. Passing to $L_1 \coloneqq L_0[s]/(\phi)$ and considering an approximation $H' \in L_1[t]$ with $\deg H' < \deg H$, lets us recursively eliminate ramification in $L' \coloneqq L_1[t]/(H')$. The extension K'/K which eliminates ramification there can then be used to eliminate the ramification for one extension of v_L over v_K.

To summarize, our algorithm has two parts. The first part turns a totally ramified extension into one which is not totally ramified, and the second part replaces an extension which is not totally ramified with an extension of smaller degree. We begin with the first part of the algorithm (which is more difficult.) To illustrate the strategy for this part, we start with a special case.

Definition 6.28 For $x = a\pi^s \in L_0$ with $v_{L_0}(a) = 0$ we call the image of a in ℓ_0 the *normalized reduction* of x (with respect to π) and denote it by $[x]_\pi$. For $M \in \mathbb{N}$, we say that $y \in \ell_0$ is an M^∞-th power if it is an M^n-th power for all $n \geq 1$.

Remark 6.29 If $\pi' \in K$ is another uniformizer in K, then $[x]_\pi$ and $[x]_{\pi'}$ differ by an element of k which is a p^∞-th power since k is perfect.

Remark 6.30 Unramified extension K'/K might lead to multiple extension of v_{L_0} to $K'L_0$. Since we only want to eliminate ramification of one extension of v_L to $K'L$, we can essentially assume that any unramified extension of K has been taken if we need an element which only exists after such an extension (see also Lemma 6.21.)

Total Ramification with $G = t^p - f(x)$

We can use the algorithm from Subsection 4.6.2 to describe the extensions of v_{L_0} to L as inductive pseudo-valuations, i.e., as pseudo-valuations which augment the Gauss valuation on $L_0[t]$ which we want to denote by v_0. The following example recalls the idea of that algorithm and also indicates how to construct K'/K which eliminates total ramification.

Example 6.31 Let us reconsider Example 6.7, i.e., let $L \coloneqq L_0[t]/(G)$ with $G = t^2 + 8x + 2$ and $L_0 = \mathbb{Q}_2(x)$. We have seen that v_{L_0}, the valuation induced by the 2-adic valuation on $\mathbb{Q}_2$, has a single extension to L

$$w_L \coloneqq w_2 \coloneqq [w_0, w_1(t) = 1/2, w_2(G) = \infty].$$

To eliminate the ramification we certainly need an element π' of valuation $1/2$. Let $K' \coloneqq K(\pi')$. To understand why taking $\pi'^2 = 2$ does not eliminate ramification, let us review the computation of the extension of $v_{K'L_0}$ to $K'L$. We begin with $w_1 \coloneqq [w_0, w_1(t) = 1]$ and compute an equivalence decomposition of G over w_1, i.e., we multiply G by a power of π' such that its w_1-valuation is zero, reduce modulo w_1, factor the result over the residue field $\mathbb{F}_2(x)$, and lift the factors back to $K'(x)[t]$. Actually performing these steps produces

$$\pi'^{-2}G = (t/\pi')^2 + 8x/\pi'^2 + 2/\pi'^2$$

which reduces to $y^2 + 1$ and factors as $(y + 1)^2$. Lifting the factor back to $K'(x)[t]$ gives $t + \pi'$ as the next key polynomial. We replace w_1 with $w_1 \coloneqq [w_0, w_1(t + \pi') = \lambda]$ and repeat the process. What happens next depends on our choice of π'. If we choose $\pi'^2 = 2$, then $\lambda = 2$ and $\pi'^{-4}G$ reduces again to $y^2 + 1$ which factors as $(y+1)^2$. This yields another linear key polynomial $t+2+\pi'$ but this time its valuation is $5/4$ and $v_{K'L}$ is still ramified over $v_{K'(x)}$. The problem with this choice of π' seems to be that $\pi'^{-m}G$ reduces to something which is a power of a linear polynomial. We can avoid this by adjoining a different element, namely an element which satisfies $\pi'^2 = -2$. Then $\lambda = 3$ and $\pi'^{-6}G$ reduces to $y^2 + x$, an irreducible polynomial which lifts to G and we get the weakly unramified extension

$$w_{K'L} = [w_0, w_1(t + \pi'x) = 3/2, w_{K'L}(G) = \infty].$$

We limit our attention in this paragraph to a special case, namely, we let $L \coloneqq L_0[t]/(G)$ with an irreducible $G = t^p - f$ with $f \in L_0$ and $v(f) = 0$ which is such that the unique extension of v_L of v_{L_0} to L is totally ramified.[1] We repeat the steps of the example under these assumptions. We determine a first key polynomial $\phi_1 \in L_0[t]$. If we were lucky, then G would already be a key

[1] The previous example only has this form after an easy substitution. This substitution is explicitly performed in the example at the end of this paragraph.

polynomial and the extension weakly unramified, but we assumed that this was not the case.

Recall that ϕ_1 is determined by reducing G modulo v_0, factoring the result, and lifting the irreducible factors back to $L_0[t]$. Since G is not a key polynomial and since there is only one extension of v_{L_0} to L, the reduction of G factors as a power of a polynomial of degree one. The key polynomial ϕ_1 will therefore have degree one and will be assigned a value λ_1. If λ_1 is not in the value group of K, then this process will lead to an extension of v_{L_0} which is not weakly unramified. Let us therefore assume that we started with a larger field K whose value group contains λ_1. (There is a choice in how we extend our field K.) The algorithm now continues to determine the next key polynomial $\phi_2 \in L_0[t]$, a key polynomial over

$$v_1 = [v_0, v_1(\phi_1) = \lambda_1].$$

Again, if G is a key polynomial, then this leads to a weakly unramified extension

$$v_L = v_2 = [v_0, v_1(\phi_1) = \lambda_1, v_2(G) = \infty].$$

G is a key polynomial if and only if the reduction of the ϕ_1-adic expansion of G remains irreducible over the residue field of v_1. The statement of Proposition 6.36 below is that we can make sure that this is the case by choosing an appropriate extension of K and a first key polynomial ϕ_1. The idea of the proof is to make sure that the constant term of the reduction is not a p-th power. The finite extension of K and the key polynomial $\phi_1 =: t - h$ are constructed in the following lemmata.

Lemma 6.32 *Let $L := L_0[t]/(G)$ with $G = t^p - f$, $f \in L_0$, and $v(f) = 0$. Let v_L be an extension of v_{L_0} to L. Let $h \in L_0$ with $f \sim_v h^p$ be such that $g := f - h^p$ satisfies one of the following:*

(a) $v(g) \geq \frac{p}{p-1}$, or

(b) $[g]_\pi$ is not a p-th power.

Then there is a totally ramified extension K'/K which eliminates the ramification of v_L over v_{L_0}.

Proof Let $\phi := \phi_1 := t - h$, a key polynomial over v_0. We compute the ϕ-adic expansion of G as

$$\begin{aligned} G &= t^p - h^p + g \\ &= (\phi + h)^p - h^p + g \\ &= \phi^p + \left(\sum_{i=2}^{p-1} \tbinom{p}{i} h^{p-i} \phi^i \right) + p h^{p-1} \phi + g. \end{aligned}$$

To compute λ, which is essentially the valuation of ϕ mod G, we have to determine the slopes of the corresponding Newton polygon. Note that the constant term has valuation $v(g)$, the linear term has valuation $v(p) = 1$, and the degree p term has valuation 0.

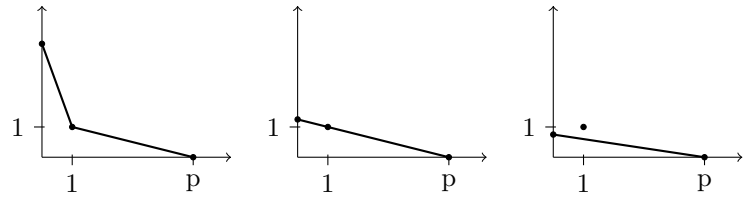


Figure 6.6: Possible Newton polygons for the ϕ-adic expansion of G if $v(g) > \frac{p}{p-1}$, $v(g) = \frac{p}{p-1}$, and $v(g) < \frac{p}{p-1}$, respectively.

If (a) holds with $v(g) > \frac{p}{p-1}$, then the Newton polygon consists of two segments, i.e., there are two extensions of v_{L_0} to L. Since these extensions can only have a ramification index which is prime to p, Abhyankar's Lemma can be used to eliminate their ramification over v_{L_0}.

For the other cases, let K'/K be any totally ramified extension of degree p, let λ be the valuation of ϕ mod G, and let $v_1 = [v_0, v_1(\phi) = \lambda]$. We can assume that λ is in the value group of K'. Recall that a key polynomial over v_1 can now be determined by reducing the coefficients of the ϕ-adic expansion of G (after multiplication with an appropriate power of a uniformizer.) If (a) holds with $v(g) = \frac{p}{p-1}$, then this reduction has a linear term, so it can not factor as a power of a linear polynomial. If (b) holds, then this reduction can also not factor as a power of a linear polynomial. In either case, if the reduction does not factor, then a next key polynomial has degree p, whence G itself is a key polynomial over v_1. If the reduction has coprime factors, then there would be more than one extension to L whose ramification can be eliminated by Abhyankar's Lemma. ■

The following three lemmata show that we can find an extension K'/K such that the conditions of the previous lemma are satisfied.

Lemma 6.33 *Let $f, h \in L_0$ with $v(f) = 0$ and $f \sim_v h^p$. Then there is $h' \in L_0$ with $f \sim_v h'^p$ such that $g' \coloneqq f - h'^p$ satisfies one of the following:*

(a) $v(g') \geq \frac{p}{p-1}$,

(b) $[g']_\pi$ is not a p-th power, or

(c) $v(g')/p$ is not in the value group of v_K.

Proof We construct h' inductively, starting from $h' \coloneqq h$. Suppose that $g' \coloneqq f - h'$ does not satisfy any of (a), (b), (c) yet. Let $\alpha \in L_0$ with $v(\alpha) = 0$ and $s \in \mathbb{N}$ be such that $g' \sim_v \alpha^p \pi^s$, and let $h'' \coloneqq h' + \alpha\pi^{s/p} \in L_0$. Then

$$f - h''^p = g - \alpha^p \pi^s - \left(\sum_{i=1}^{p-1} \tbinom{p}{i} h'^{p-i} \alpha^i \pi^{si/p} \right)$$

The sum is $O(\pi^{s+1})$ since all the summands are. If we set $h' \coloneqq h''$, we see that after finitely many iterations of this process one of the conditions above must be violated since the valuation of $f - h'^p$ increases in a discrete value group while (a) bounds it by $\frac{p}{p-1}$. ■

Lemma 6.34 *Let $f, h \in L_0$ with $v(f) = 0$ and $f \sim_v h^p$ be such that $g \coloneqq f - h^p$ satisfies*

(α) $[g]_\pi$ is a p^∞-th power, and

(β) $v(g)/p$ is not in the value group of v_K.

Then there is a finite extension K'/K (which consists of a totally ramified extension of degree p on top of an unramified extension) with uniformizer $\pi' \in K'$, and an element $h' \in K'L_0$ with $f \sim_{v_{K'L_0}} h'^p$ such that $g' \coloneqq f - h'^p$ satisfies

(a) $v_{K'L_0}(g') \geq \frac{p}{p-1}$,

(b) $[g']_{\pi'}$ (with respect to $v_{K'L_0}$) is not a p-th power, or

(c) $[g']_{\pi'}$ (with respect to $v_{K'L_0}$) is not a p^∞-th power and $v(g')/p$ is not in the value group of $v_{K'}$,

for a fixed extension $v_{K'L_0}$ of v_{L_0} to $K'L_0$.

Proof Following Remark 6.30 we suppose that a sufficiently large unramified extension of K has already been taken so that the elements which are needed later exist in K. We adjoin to K an element ψ which satisfies

$$\psi^p + \sum_{i=0}^{p-1} \delta_i \psi^i = 0$$

with $\delta_i \in K$, $v(\delta_0) = v(g)$, and $v(\delta_i) \geq \frac{p-i}{p} v(g)$; the exact values of the δ_i will be determined during the following process, but any element of this kind will have $v(\psi) = v(g)/p$, and therefore lead to a totally ramified extension K'/K. Independent of the specific choice of the δ_i, there are $j \in \{0, \ldots, p-1\}$ and $k \in \mathbb{Z}$ such that $\pi' \coloneqq \pi^k \psi^j$ is a uniformizer in this field. Additionally, let $\delta \in K'L_0$ be an element with $v(\delta) > v(\psi)$, also to be determined later.

Set $h' \coloneqq h + \psi + \delta$ and consider $g' \coloneqq f - h'^p$ which we can write as

$$g' = \sum_{i=0}^{p-1} b_i \psi^i$$

with $b_i \in L_0$. If $v(g') \geq \frac{p}{p-1}$, then (a) holds. Assuming that this is not the case, there is a unique i such that $v(b_i \psi^i)$ is minimal. Let us first consider the case that $i = 0$. Write

$$b_0 = \beta_0 \pi'^r + \beta_1 \pi'^{r+1} + \cdots$$

with all $\beta_j \in K'L_0$, $v(\beta_j) = 0$. If $[\beta_0 \pi'^r]_{\pi'}$ is not a p-th power, then (b) holds, so we may in fact write

$$b_0 = \beta_0^p \pi'^r + \beta_1 \pi'^{r+1} + \beta_2 \pi'^{r+2} + \cdots .$$

As p divides r, we can replace δ by $\delta' \coloneqq \delta + \beta_0 \pi'^{r/p}$. Since $v(g') < \frac{p}{p-1}$ this increases the valuation of g' and so this case can happen only finitely many times. Let us now consider the case that $i \neq 0$. Write

$$b_i = \beta_0 \pi^r + \beta_1 \pi^{r+1} + \cdots$$

with all $\beta_j \in L_0$, $v(\beta_j) = 0$. Since $[\beta_0\pi^r]_{\pi'}$ and $[\beta_0]_\pi$ only differ by an element of the perfect field k, the former is a p^∞-th power if and only if the latter is. We may therefore choose $\beta_0 \in K$ if $[g']_{\pi'}$ is a p^∞-th power. (Here we used Assumption (A).) If $[g']_{\pi'}$ is not a p^∞-th power, then (c) holds. Otherwise, we modify the defining polynomial of ψ to eliminate β_0. Namely, we replace δ_i with $\delta_i + \beta_0\pi^r$ which satisfies $v(\beta_0\pi^r) \geq \frac{p-i}{p}v(g)$. Again this leads to an increase in the valuation of g' which can only happen finitely many times. ∎

Lemma 6.35 *Let $f \in L_0$ be an element which reduces to an element in k. Let $h \in L_0$ with $f \sim_v h^p$ be such that the normalized reduction of $g \coloneqq f - h^p$ is not a p^∞-th power and $v(g)/p$ is not in the value group of v_K. Then there is a totally ramified extension K'/K with uniformizer $\pi' \in K'$ and an $h' \in K'L_0$ with $f \sim_v h'^p$ such that $g' \coloneqq f - h'^p$ satisfies one of the following:*

(a) $v(g') \geq \frac{p}{p-1}$, or

(b) $[g']_{\pi'}$ is not a p-th power.

Proof Throughout the proof we ignore the trivial possibility that $v(g') \geq \frac{p}{p-1}$ which would give (a). Write

$$g = \sum_{i=0}^{\infty} a_i \pi^{s+i}.$$

We can assume that all a_i which reduce to a p-th power are already a p-th power, i.e., $a_i =: \alpha_i^p$. We are going to modify h to get a first term $a_0\pi^s$ in the above expansion which does not reduce to a p-th power at all, which implies (b).

Let $n \in \mathbb{N}$ be maximal such that a_0 reduces to a p^n-th power. Let $m \in \mathbb{N}$ be minimal such that a_m does not reduce to a p-th power. If no such m exists, choose $m \in \mathbb{N}$ sufficiently large. Adjoin to K a p-th root of π, i.e., let $\pi'^p \coloneqq \pi$. Let

$$h' \coloneqq h + \sum_{i=0}^{m-1} \alpha_i \pi'^{s+i}.$$

Dropping terms whose valuation exceeds $v(\pi^{s+m})$ or $v(p\pi'^s)$, we have

$$\begin{aligned} g' \coloneqq f - h'^p &= f - h^p - \left(\sum_{i=0}^{m-1} \alpha_i^p \pi'^{p(s+i)}\right) - ph^{p-1}\alpha_0\pi'^s \\ &= f - h^p - \left(\sum_{i=0}^{m-1} a_i \pi^{s+i}\right) - ph^{p-1}\alpha_0\pi'^s \\ &= a_m\pi^{s+m} - ph^{p-1}\alpha_0\pi'^s. \end{aligned}$$

Since s is prime to p, the valuation of $a_m\pi^{s+m}$ and the valuation of $ph^{p-1}\alpha_0\pi'^s$ are different. If the valuation of $a_m\pi^{s+m}$ is smaller than the valuation of $ph^{p-1}\alpha_0\pi'^s$, then condition (b) holds. Otherwise,

$$[g']_{\pi'} = \left[ph^{p-1}\alpha_0\right]_{\pi'}$$

which differs from $[\alpha_0]_{\pi'}$ only by an element of the perfect field k which is a p^∞-th power. Therefore, $[g']_{\pi'}$ is not a p^n-th power anymore but only a p^{n-1}-th

power. Since the valuation of g' is $s \cdot v(\pi')$ which is not divisible by p in the value group of $v_{K'}$, we can repeat this proces. After finitely many repetitions, (b) holds. ∎

Proposition 6.36 *Let $L \coloneqq L_0[t]/(G)$ with $G = t^p - f$, $f \in L_0$, and $v(f) = 0$. Let v_L be an extension of v_{L_0} to L. Then there is a finite extension K'/K which eliminates the ramification of some extension of v_L over v_K.*

Proof Let us first assume that $[f]_\pi = 1$. We may assume that v_L is totally ramified over v_{L_0} and that there is $h \in L_0$ such that $f \sim_v h^p$. If $v(g) \geq \frac{p}{p-1}$, we find an extension which eliminates ramification with Lemma 6.32. If this is not the case, then Lemma 6.33 shows that we can assume that $v(g)/p$ is not in the value group of v_K. By Lemma 6.34 we may assume that $[g]_\pi$ is not a p^∞-th power. Finally, Lemma 6.35 shows that we can modify h such that Lemma 6.32 applies, which proves the proposition in this case.

For the general case we assume that $[f]_\pi$ is a p-th power. We can write $f = \delta^p f'$ with $\delta \in L_0$, $v(\delta) = 0$, and $[f']_\pi = 1$. For f' we can find an h' (over a finite extension K'/K with uniformizer π') such that $g' \coloneqq f' - h'^p$ satisfies $v(g') \geq \frac{p}{p-1}$ or that $[g']_{\pi'}$ is not a p-th power. Let $h \coloneqq \delta h'$, $g \coloneqq f - h^p$. If $v(g') \geq \frac{p}{p-1}$, then $v(g) \geq \frac{p}{p-1}$ and Lemma 6.32 applies. If $[g']_{\pi'}$ is not a p-th power, then $[g]_{\pi'}$ is not a p-th power (it differs by an element of the perfect field k and $[\delta^p]_{\pi'}$) and Lemma 6.32 applies again. ∎

Example 6.37 Let us consider Example 6.7, i.e., let $L \coloneqq \mathbb{Q}_2[t]/(G)$ with $G(t) = t^2 + 8x + 2$. Since the proposition assumes that the constant term of G has valuation zero, we adjoin π with $\pi^2 = 2$ to the ground field $\mathbb{Q}_2$ and substitute t with πt which shows that the image of t then satisfies the equation $t^2 + 4x + 1$, i.e., $f = -4x - 1$ which reduces to 1 modulo v.

With $h = 1$ we get $v(f - h^2) = v(-4x - 2) = 1$ which does not exceed $\frac{p}{p-1} = 2$ yet. The π-adic expansion of $g \coloneqq f - h^2$ is

$$g = -1\pi^2 + 0\pi^3 - x\pi^4,$$

and so $[g]_\pi$ is a p-th power and we have $v(g)/2$ in the value group of $\mathbb{Q}_2(\pi)$. Following Lemma 6.33, we replace h with $1 + \pi$ which gives the expansion

$$g \coloneqq f - (1 + \pi)^2 = -\pi^3 - (1 + x)\pi^4.$$

Now $v(g)/2 = 3/4$ is not in the value group of $\mathbb{Q}_2(\pi)$ but still $v(g) < \frac{p}{p-1}$.

As $[-1]_\pi = 1$ is a p^∞-th power, we take the totally ramified extension (see Lemma 6.34) defined by $\psi^2 + \delta_1\psi + \delta_0 = 0$ with $\delta_0 = \pi^3 + O(\pi^4)$ and $\delta_1 = O(\pi^2)$; initially we take $\delta_0 = \pi^3$ and $\delta_1 = 0$. For $\delta \coloneqq 0$, and $h \coloneqq (1 + \pi) + \psi + \delta$, we get that $f - h^2 = ((-x - 1)\pi^4 - \pi^5) + (-\pi^2 - \pi^3)\psi$. This shows that our choice of δ_1 was wrong, we should have chosen $\delta_1 = \pi^2 + O(\pi^3)$. With this choice we get $f - h^2 = ((-x - 1)\pi^4 - \pi^5) + (-\pi^3)\psi$ which has valuation $2 = \frac{p}{p-1}$. And indeed, over this totally ramified extension $K'/\mathbb{Q}_2$ of degree 4, there is a unique weakly unramified extension of the valuation on $K'(x)$ to $K'(x)[t]/(G)$. This extension is

$$v_2 = [v_0, v_1(t - 2\psi - \pi\psi + \pi + 2) = 1, v_2(t^2 + 8x + 2) = \infty].$$

Remark 6.38 The extension we found in the example is not optimal. We had seen in Example 6.31 that an extension of degree 2 suffices. This seems to be due to the first extension which we took to normalize the constant coefficient f to valuation zero.

Total ramification in degree p (and some other cases)

We want to generalize the discussion to totally ramified extensions $L = L_0[t]/(G)$ of degree M. Because of Abhyankar's Lemma, we may assume that M is a power of p. Our approach is again to replace the key polynomial t with a key polynomial $\phi := t - h$ for some $h \in L_0$ and to consider the ϕ-adic expansion

$$\begin{aligned} G &= t^M - \sum_{j=0}^{M-1} f_j t^j \\ &= \phi^M \\ &\quad + \sum_{j=1}^{M-1} \left(\tbinom{M}{j} h^{M-j} - \sum_{i=j}^{M-1} \tbinom{i}{j} f_i h^{i-j} \right) \phi^j \\ &\quad + h^M - f_0 - \sum_{i=1}^{M-1} f_i h^i \\ &=: \phi^M - \sum_{j=0}^{M-1} g_j \phi^j. \end{aligned} \tag{Υ}$$

As in the previous paragraph, we try to construct h such that the *constant term*

$$g_0 = f_0 + \sum_{i=1}^{M-1} f_i h^i - h^M$$

has large valuation or its normalized reduction is not an M-th power. We can then eliminate the total ramification as in Lemma 6.32.

Lemma 6.39 *Let*

$$G = t^M - \sum_{j=0}^{M-1} f_j t^j \in L_0[t]$$

be a monic integral irreducible polynomial. Let v_L be the unique extension of v_{L_0} to $L_0[t]/(G)$. Let $w = [v_0, v(\phi) = \lambda]$ be an approximant for v_L. Suppose that for the ϕ-adic expansion

$$G = \phi^M - \sum_{j=0}^{M-1} g_j \phi^j$$

one of the following holds:

1. *$[g_0]_\pi$ is not an M-th power, or*
2. *there is $1 \le j < M$ such that $v(g_0) \ge v(g_j) \cdot \frac{M}{M-j}$.*

Then there is a totally ramified extension K'/K which eliminates the total ramification of v_L over v_K. ∎

Let us suppose that G is such that $v(f_0) = 0$. The lemma shows that we may assume that f_0 reduces to an M-th power. Let

$$v_n = [v_0, \ldots, v_n(\phi_n) = \lambda_n]$$

be an approximant to the unique extension of v_{L_0} to $L = L_0[t]/(G)$ with key polynomials of strictly increasing degree. As this extension is totally ramified, ϕ_1 can be written as $\phi_1 = t - h$ where h is such that $f_0 \sim_v h^M$ and λ_1 is not in the value group of v_K. As before let

$$g_0 \coloneqq f_0 + \sum_{i=1}^{M-1} f_i h^i - h^M.$$

We want to generalize the construction of Lemma 6.35. For this to work, we need to make a few assumptions on G and h, namely

(♖) For all $j \in \{1, \ldots, M-1\}$ there is a unique minimum among

$$v\Big(\tbinom{j}{j} f_j\Big), \ldots, v\Big(\tbinom{M-1}{j} f_{M-1}\Big), v\Big(\tbinom{M}{j}\Big).$$

(♘) There is $i \in \{1, \ldots, M-1\}$ with $p \nmid i$ such that

$$v(f_i) = \min\{v(f_1), \ldots, v(f_{M-1})\}.$$

(♌) The value $v(g_0)/M$ is not in the value group of v_K.

Suppose that $[g_0]_\pi$ is an M-th power. We construct h' to approximate f_0 as follows. We write

$$g_0 = \left(\sum_{k=0}^{m-1} \alpha_k^M \pi^{s+k}\right) + \alpha_m \pi^{s+m}$$

with $m > 0$ and $\alpha_k \in L_0$ for $0 \le k \le m$. Let $K' \coloneqq K(\pi')$ with $\pi'^M = \pi$, and let

$$h' \coloneqq h + \sigma \coloneqq h + \sum_{k=0}^{m-1} \alpha_k \pi'^{s+k}.$$

For future reference, let us call h' the *approximation of f_0 which improves h by σ* or just the *improved approximation*. Let $\phi' \coloneqq t - h'$ and consider the ϕ'-adic expansion $G = \phi'^M - \sum g'_j \phi'^j$ which looks essentially like the one in equation (♈). Because of (♖) and since $v(h') = v(h) = 0$, we have $v(g'_i) = v(g_i)$ for $1 \le i < M$; the only term whose valuation has changed is the constant term. Writing this term in a few different ways, we get

$$\begin{aligned}
g'_0 &= f_0 + \sum_{i=1}^{M-1} f_i h'^i - h'^M \\
&= f_0 + \sum_{i=1}^{M-1} f_i h^i - h^M - \sigma^M \\
&\quad - \sum_{j=1}^{M-1} \sigma^j \left(\tbinom{M}{j} h^{M-j} - \sum_{i=j}^{M-1} \tbinom{i}{j} f_i h^{i-j}\right) \\
&= \left(f_0 + \sum_{i=1}^{M-1} f_i h^i - h^M - \sigma^M\right) + \left(\sum_{j=1}^{M-1} \sigma^j g_j\right). \qquad (♉)
\end{aligned}$$

Let us determine the valuations of the summands which make up this last expression. On the one hand we get

$$f_0 + \sum_{i=1}^{M-1} f_i h^i - h^M - \sigma^M = \alpha_m \pi^{s+m} + O(p\pi^s\pi').$$

On the other hand, among the terms $\sigma^j \binom{i}{j} f_i h^{i-j}$ with $1 \leq j \leq i \leq M$ the terms of minimal valuation satisfy $j = 1$. Indeed, if $\sigma^j \binom{i}{j} f_i h^{i-j}$ had minimal valuation with $j \neq 1$, then $p \mid i$ since otherwise $\sigma \binom{i}{1} f_i h^{i-1}$ had smaller valuation; but then there is some $p \nmid i'$ with $v(f_{i'}) = v(f_i)$ by (⋊) and so $\sigma \binom{i'}{1} f_{i'} h^{i'-1}$ had smaller valuation. With (⫿) the terms with $j = 1$ have a unique minimum (which occurs at $\sigma \binom{i}{1} f_i h^{i-1}$ with $i = M$ or $p \nmid i$) and so $\sum \sigma^j g_j$ is v-equivalent to that $\sigma \binom{i}{1} f_i h^{i-1}$. Finally, $v(\sigma \binom{i}{1} f_i h^{i-1})$ is different from $\alpha_m \pi^{s+m}$ by (⋋), and so g_0' is v-equivalent to exactly one of the two. If the former is minimal, then g_0' still satisfies condition (⋋) and we could repeat the process.

Previously, we used the assumption $f_1, \ldots, f_{M-1} = 0$. This is now not the case anymore. For (⫿), we need some control on the f_i. If G is the minimal polynomial of a uniformizer, then we can perform a substitution to achieve this.

Lemma 6.40 *Let*

$$G = t^M - \sum_{i=0}^{M-1} f_i t^i \in L_0[t]$$

be a monic integral irreducible polynomial which is such that $v(f_0) = v(\pi^s)$ for some $s > 0$ which is prime to M. Suppose that $v_{L_0}(f_0) < v(f_i) \cdot \frac{M}{M-i}$ for all $1 \leq i < M$. Let $K' \coloneqq K(\pi')$ with $\pi'^M = \pi$ and suppose that G remains irreducible over $K'L_0$. Then there is a monic integral irreducible polynomial

$$H = t^M - \sum_{i=0}^{M-1} f_i' t^i \in K'L_0[t]$$

with $v(f_i') = 0$ such that

$$K'L_0[t]/(G) \simeq K'L_0[t]/(H)$$

are isomorphic as extensions of $K'L_0$. Furthermore, if for the f_i' with $1 \leq i < M$ and $v(f_i') \neq \infty$ we write $f_i' =: a_i \pi'^{s_i}$ with a unit a_i, then none of the s_i is divisible by M and the s_i are pairwise distinct mod M.

Proof This is immediate with $H \coloneqq \pi^{-s} \cdot G(t\pi'^s)$. ∎

Proposition 6.41 *Let $L = L_0[t]/(G)$ be an extension of degree $M = p^N$ with $G = t^M - \sum f_i t^i$ and $v(f_0) = 0$. Suppose that v_{L_0} has a unique totally ramified extension v_L to L and let $h \in L_0$ be such that $f_0 \sim_v h^M$. With $\phi \coloneqq t - h$, we write*

$$G =: \phi^M - \sum_{j=0}^{M-1} g_j \phi^j.$$

Suppose that $v(g_0)/p$ is not in the value group of v_K (a stronger requirement than (⋋)) and that the f_i satisfy (⫿) and (⋊). Then there is a finite extension K'/K (which consists of a totally ramified extension on top of an unramified extension) which eliminates total ramification of v_L over v_{L_0}.

Corollary 6.42 *Let L/L_0 be an extension of degree p and let v_L be the unique extension of v_{L_0} to L. Then there is a finite extension K'/K (which consists of a totally ramified extension on top of an unramified extension) which eliminates total ramification of v_L over v_{L_0}.*

Proof (of the Corollary) If $M = p$ then we can bring ourselves in the position of the proposition if we start with G a minimal polynomial of a uniformizer and perform the substitution of Lemma 6.40. ∎

Proof (of Proposition 6.41) We may suppose that the following conditions hold (otherwise we are done by Lemma 6.39.)

(a) $[g_0]_\pi$ is an M-th power, and

(b) $v(g_0) < v(g_i) \cdot \frac{M}{M-i}$ for all $1 < i < M$.

Let γ be a lift of an M-th root of $[g_0]_\pi$. Let us perform the substitution $G \coloneqq G(t\gamma)/\gamma^M$ and replace h with h/γ. (This does not change the validity of any of the assumptions we made at the beginning.) Then $[g_0]_\pi = 1$.

We can construct an approximation of f_0 which improves h by $\sum_{k=0}^{m-1} \alpha_k \pi'^{s+k}$ where we set

$$g_0 = \left(\sum_{k=0}^{m-1} \alpha_k^M \pi^{s+k} \right) + \alpha_m \pi^{s+m}$$

and choose m such that α_m does not reduce to an M-th power or, if this is not possible, sufficiently large such that the minimum in $(\Cocktail)$ is not attained for $a_m \pi^{s+m}$. If after finitely many repetitions of constructing such improved approximations (a) or (b) fails, then Lemma 6.39 shows that we are done. We may therefore assume that this procedure can be applied indefinitely. In each iteration, the minimal valuation in $(\Cocktail)$ is attained by $\sigma\binom{i}{1} f_i h^{i-1}$ for some fixed $i \in \{1, \dots, M\}$.

We now go back and assume that we have not done any of these iterations yet.

Let us study again what happens if we construct improved approximations as above. In a first iteration $[\sigma]_\pi = 1$ by our normalization of g_0, and so $\left[\sigma\binom{i}{1} f_i h^{i-1}\right]_\pi = \left[i f_i h^{i-1}\right]_\pi =: \delta_0^M$. The next σ satisfies $[\sigma]_\pi = \delta_0$ and we get $\left[\delta_0 i f_i h^{i-1}\right]_\pi =: \delta_1^M$. The next σ has $[\sigma]_\pi = \delta_1$ and so $\left[\delta_1 i f_i h^{i-1}\right]_\pi \coloneqq \delta_2^M$, and so on.[2] Since this process does not terminate, we have for $k \geq 1$

$$\begin{aligned} \left(\frac{\delta_{k+1}}{\delta_k}\right)^{M^{k+1}} &= \left(\frac{\delta_k \delta_0^M}{\delta_{k-1}\delta_0^M}\right)^{M^k} \\ &= \left(\frac{\delta_k}{\delta_{k-1}}\right)^{M^k} \\ &= \cdots = \left(\frac{\delta_1}{\delta_0}\right)^M = \frac{\delta_0^{M+1}}{\delta_0^M} = \delta_0. \end{aligned}$$

[2] Notationally this is slightly incorrect. Instead of writing $[\sigma]_\pi$ in all places, we should write $[\sigma]_\pi$, $[\sigma]_{\pi'}$, $[\sigma]_{\pi''}$, and so on. However, since $\pi''^{M^2} = \pi'^M = \pi$, we can compute the normalized reduction with respect to any of these uniformizing parameters and get the same result.

Hence δ_0 is a p^∞-th power and so by assumption (A) (after an unramified extension) in k.

Once again we go back and assume that we have not performed any of the iterations yet. We claim that there is a finite totally ramified extension K'/K and h' such that

$$G =: \phi^M - \sum_{j=0}^{M-1} g'_j \phi'^j$$

with $\phi' \coloneqq t - h'$ satisfies one of the following:[3]

(a) there is $1 \leq j < M$ such that $v(g'_0) \geq v(g'_j) \cdot \frac{M}{M-j}$,

(b) $[g'_0]_{\pi'}$ is not an M-th power, or

(c) $[g'_0]_{\pi'}$ is not an M^∞-th power and $v(g'_0)/M$ is not in the value group of $v_{K'}$.

Write

$$g_0 = a_0 \pi^s + a_1 \pi^{s+1}$$

with $a_0 \in K$, $a_1 \in L_0$. We adjoin to K an element ψ which satisfies

$$\psi^M + \sum_{i=0}^{M-1} \delta_i \psi^i = 0$$

with $\delta_i \in K$, $v(\delta_0) = v(\pi^s)$, and $v(\delta_i) \geq v(\pi^s) \cdot \frac{M-i}{M}$; the exact values of the δ_i will be determined during the following process, but any element of this kind will have $v(\psi) = v(\pi^s)/M$, and therefore lead to a totally ramified extension K'/K. (Here we used the assumption that $v(g_0)/p$ is not in the value group of v_K.) Independent of the specific choice of the δ_i, there is a $1 < \ell < M$ and $k \in \mathbb{Z}$ such that $\pi' \coloneqq \pi^k \psi^\ell$ is a uniformizer in this field. Let $\delta \in K' L_0$ be an element with $v(\delta) > v(\psi)$, also to be determined later.

Set $h' \coloneqq h + \psi + \delta$ and consider $g'_0 \coloneqq f_0 + \sum_{i=1}^{M-1} f_i h'^i - h'^M$ as usual. We can write this as

$$g'_0 = \sum_{i=0}^{M-1} b_i \psi^i$$

with $b_i \in L_0$. There is a unique i such that $v(b_i \psi^i)$ is minimal. Let us first consider the case $i = 0$. Write

$$b_0 = \beta_0 \pi'^r + \beta_1 \pi'^{r+1} + \cdots$$

with all $\beta_j \in K' L_0$, $v(\beta_j) = 0$. If β_0 does not reduce to an M-th power, then (b) holds, so we may in fact write

$$b_0 = \beta_0^M \pi'^r + \beta_1 \pi'^{r+1} + \beta_2 \pi'^{r+2} + \cdots .$$

As M divides r, we can replace δ by $\delta + \beta_0 \pi'^{r/M}$. Since this increases the valuation of g'_0, this case can only happen finitely many times. Let us now consider the case that $i \neq 0$. Write

$$b_i = \beta_0 \pi^r + \beta_1 \pi^{r+1} + \cdots .$$

[3] The following construction is the analogue of Lemma 6.34.

Since $[\beta_0\pi^r]_{\pi'}$ and $[\beta_0]_\pi$ only differ by an element of the perfect field k, the former is a M^∞-th power if and only if the latter is. We may therefore choose $\beta_0 \in K$ if $[g']_{\pi'}$ is a M^∞-th power. (Here we used Assumption (A).) If $[g']_{\pi'}$ is not a M^∞-th power, then (c) holds. Otherwise, we modify the defining polynomial of ψ to eliminate β_0. Namely, we replace δ_i with $\delta_i + \beta_0\pi^r$ which satisfies $v(\beta_0\pi^r) \geq \frac{M-i}{M} v(g)$. Again this leads to an increase in the valuation of g' which can only happen finitely many times.

We can now assume that one of (a), (b), or (c) holds. If (a) or (b) holds, then Lemma 6.39 applies and we are done. Let us assume that (c) holds. We repeatedly improve h with the same construction as in the first paragraph of the proof. If during this process the minimum in ($\Cocktail$) is ever attained by $a_m\pi^{s+m}$, then another finite extension eliminates the ramification in degree one. Otherwise, in each iteration the constant coefficient g_0 is replaced with $\sigma i f_i h^{i-1}$. As $\left[i f_i h^{i-1}\right]_\pi \in k$, this essentially means that we replace $[g_0]_\pi$ with its M-th root. Since $[g_0]_\pi$ is only an M-th power for finitely many n, this process eventually terminates which proves the proposition. ∎

The General Case

We are now going to combine the findings of this section into a full algorithm which eliminates ramification in an extension L/L_0; at least if the conditions of the above proposition are satisfied whenever we invoke it. To make this formal, we work under the following assumption.

Assumption 6.43 For all totally ramified extensions there is a finite extension of the base field which eliminates total ramification.

Proposition 6.44 *Let L/L_0 be an extension of degree M and let v_L be an extension of v_{L_0} to L. Then there is a finite extension K'/K which eliminates ramification of one extension of v_L over v_{L_0}.*

Proof We may assume that v_{L_0} has a unique extension to L and that $M = p^N$ for some $N \in \mathbb{N}$. If the degree of L/L_0 is p, then Proposition 6.41 shows that there is a finite extension K'/K which eliminates ramification. The rest of the proof is an induction on N. Suppose that we can construct extensions of the base field to eliminate ramification for one extension for degrees strictly less than p^N.

We may assume that L/L_0 is not totally ramified. We can then use assumption (B), i.e., that ℓ/ℓ_0 is simple. Let $\bar{\alpha} \in \ell$ be such that $\ell = \ell_0(\bar{\alpha})$. Let $\alpha \in L$ be any lift of $\bar{\alpha}$. In the (unlikely) case that $L_0(\alpha) \subsetneq L$, we have found a subfield and reduced the problem of eliminating ramification to one of smaller degree, so let us assume that $L = L_0(\alpha)$. Let $G \in L_0[t]$ be the minimal polynomial of α. We can use G to write down v_L as

$$v_L = [v_0, v_1(\psi_1) = \lambda_1, v_2(\psi_2) = \lambda_2, \ldots, v_n(G) = \infty]$$

where we may assume that we chose α such that $\deg \psi_2 > \deg \psi_1$. Since α generates the residue field of L, $\psi \coloneqq \psi_1$ reduces to the minimal polynomial of $\bar{\alpha}$. All the following steps, $v_2, \ldots, v_n$ do not increase the residue field any further and only add ramification. Write G in its ψ-adic expansion

$$G = \psi(t)^N - \sum f_i(t)\psi(t)^i.$$

Let $L_1 \coloneqq L_0[s]/(\psi)$ and write

$$G' = t^N - \sum f_i(s)t^i \in L_1[t].$$

Then v_{L_0} has a unique and weakly unramified extension to L_1, namely

$$v_{L_1} = [v_0, v_{L_1}(\psi) = \infty].$$

The idea is now to recursively eliminate ramification in $L' \coloneqq L_1[t]/(G')$, an extension of strictly smaller degree than L/L_0, and use the same extension to eliminate ramification in the original extension L/L_0.

Let us denote an extension of v_{L_1} to L' by $v_{L'}$ (there is possibly more than one.) When we write this as an inductive pseudo-valuation, we get

$$v_{L'} = [v_0, v_1(t) = \lambda_1, \dots]$$

with $\lambda_1 = v_L(\psi)$ since $v_{L_1}(f_0(s)) = v_{L_0}(f_0(t))$. By the inductive hypothesis, we may replace the base field with a finite extension K'/K which eliminates the ramification of $v_{L'}$ over v_K. Let $\pi' \in K'$ be a uniformizing parameter. Let w be one of the extensions of $v_{L'}$ to $K'L'$. Written as an inductive pseudo-valuation it starts like

$$w = [w_0, w_1(t) = \lambda_1, w_2(t-h) = \mu_2, \dots].$$

Write

$$G' = (t-h)^N - \sum g'_i \cdot (t-h)^i$$

for the $(t-h)$-adic expansion of G'. Since w is weakly unramified over $w\big|_{K'}$, we can choose h such that one of the following hold:

(a) The constant coefficient $[g'_0]_{\pi'}$ does not reduce to an N-th power in the residue field, or

(b) the Newton polygon of G' over w_2 touches in more than just the endpoints, i.e., there is $1 \leq i < N$ such that $v(g'_i) \cdot \frac{N}{N-i} w(g'_i) \leq w(g'_0)$.

We can not conclude directly from these conditions that K'/K eliminates the ramification of v_L over v_K, however, we will show that after finitely many such extensions this will be the case.

We want to *lift* h from $K'L_1$ to $K'L_0[t]$. If ψ remains irreducible over $K'L_0$, then $h \in K'L_1 = K'L_0[s]/(\psi)$ lifts to a polynomial $h \in K'L_0[t]$ with $\deg h < \deg \psi$. If ψ factors over $K'L_0$, then this is not possible. In this case, the reduction of ψ factors as well over ℓ'_0, the residue field of $K'L_0$. We claim that ψ then has coprime factors over ℓ'_0, which shows that we get multiple extensions of $v_{K'L_0}$ to $v_{K'L}$ which means that we have reduced the problem to one of smaller degree. To prove the claim we may assume that K'/K is unramified or totally ramified. If it is unramified, then the residue field of ℓ'_0 is separable over ℓ_0 which implies that the reduction of ψ must have coprime factors. If it is totally ramified, then $K'L_0/L_0$ is totally ramified as well since L_0 is weakly unramified over K, and so $\ell'_0 = \ell_0$, which proves the claim.

We may therefore assume that we have lifts $h \in K'L_0[t]$ and equally lifts $g'_i \in K'L_0[t]$. Let $\phi \coloneqq \psi - h$ and write

$$G = \phi^M - \sum g_i \phi^i$$

for the ϕ-adic expansion. Contrast this to the familiar formula

$$\begin{aligned} G &= \phi^M \\ &\quad + \sum_{j=1}^{M-1} \left(\tbinom{M}{j} h^{M-j} - \sum_{i=j}^{M-1} \tbinom{i}{j} f_i h^{i-j} \right) \phi^j \\ &\quad + h^M - f_0 - \sum_{i=1}^{M-1} f_i h^i \\ &=: \phi^M - \sum_{j=0}^{M-1} g_j'' \phi^j. \end{aligned} \tag{$\curlyvee$}$$

The latter is not the ϕ-adic expansion of G since the degrees of the g_i'' are not bounded by $\deg \phi$. The following discussion is a comparison of g_i, g_i', and g_i''; the essence is that if g_i and g_i' do not share essential properties (which prove that some ramification has disappeared,) then the valuation of g_i has to be significantly larger than that of f_i. We begin with the easier case in which we only have to consider g_0, g_0', and g_0''.

Let us suppose that (a) holds. Since $g_0''(s) = g_0'(s)$, both differ only by a multiple of ψ,

$$\begin{aligned} g_0'' &= \delta\psi + g_0' \\ &= \delta\phi + \delta h + g_0'. \end{aligned}$$

At the same time, g_0 is the remainder of g_0'' in a division by ϕ. Therefore $g_0 = g_0' + \delta'$ where δ' is the remainder of δh in a division by ϕ. If the valuation of δ' exceeds that of g_0', then the reductions of $[g_0]_{\pi'}$ and $[g_0'(s)]_{\pi'}$ are the same; in particular, they are not an N-th power and so the extensions of v_L to $K'L$ can not have ramification index $e(v_L \mid v_{L_0})$ anymore (similar to Lemmata 6.32 and 6.39.) If the valuation of δ' does not exceed that of g_0', then we can not say much about the reduction of $[g_0]_{\pi'}$. In this case however, the valuation of δ' bounds that of g_0 from below. If we show that the valuation of δ' is significantly larger than that of f_0, then we can repeat this process, i.e., we repeat it for the same G but $f_i \coloneqq g_i$, $K \coloneqq K'$, and $\psi \coloneqq \phi$; if this never stopped, then the valuation of f_0 would become arbitrarily large. But then G would factor over the completion of $K'L_0$ for some finite extension K'/K at some point, so the process would in fact stop.

It remains to prove a bound for the valuation $v_0(\delta')$. Since $v_0(\delta') \geq v_0(\delta h)$ it suffices to bound the latter from below. If we write the quotient with remainder $f_i h^i = \delta_i \psi + \gamma_i$, then $\delta = \sum_{i=0}^{M} \delta_i = \sum_{i=1}^{M} \delta_i$, and

$$\begin{aligned} v_0(\delta_i) &= v_0(\delta_i \psi) \\ &\geq v_0(f_i h^i) && \text{by Lemma 4.12} \\ &= v_1(f_i) + i v_0(h) \\ &\geq v_1(f_i) + i v_1(\psi) \\ &\geq v_1(f_i \psi^i) \\ &\geq v_0(f_0), \end{aligned}$$

where the last inequality holds since otherwise the Newton polygon of G with respect to v_1 would touch at i. Hence $v_0(\delta') \geq v_0(f_0) + \lambda_1$.

Case (b) is similar: If the Newton polygon of G with respect to the ϕ-adic expansion does not touch in another point then this can have two reasons. It could be that $v_0(g_0) < v_0(g_0')$, but in this case the exact argument from above shows that $v_0(g_0)$ is significantly larger than $v_0(f_0)$. Or it could be that the point where the Newton polygon of G' with respect to ϕ'-adic expansion touched does not touch anymore, i.e., $v_0(g_i) > v_0(g_i')$. An analog of the above shows that $v_0(g_i')$ is then significantly larger than $v_0(f_0) \cdot \frac{N-i}{N}$ which implies that $v_0(g_0')$ is significantly larger than $v_0(f_0)$. The latter (as before) means that $v_0(g_0)$ is significantly larger than $v_0(f_0)$. ∎

Example 6.45 Let $K \coloneqq \mathbb{Q}_2$, $L_0 \coloneqq K(x)$, and $L \coloneqq L_0[t]/(G)$ with

$$G \coloneqq t^4 + (-6x - 2)t^2 + x^2 + 2x + 1 \in \mathbb{Q}_2(x)[t].$$

Let v_{L_0} be the extension on L_0 which is induced by the Gauss valuation on $K[x]$. Then v_{L_0} has a unique extension to L which is

$$v_L = v_2 = [v_0, v_1(t^2 + 2t + x + 1) = 3/2, v(G) = \infty].$$

Following the notation of the proof, let $\psi \coloneqq s^2 + 2s + x + 1$. The ψ-adic expansion of G is

$$G = \psi^2 + (-4t - 8x)\psi + 16xt + 8x^2 + 8x.$$

Consider $L_1 \coloneqq L_0[s]/(\psi)$ and let

$$G' \coloneqq t^2 + (-4s - 8x)t + 16xs + 8x^2 + 8x.$$

Write $v_{L_1} = [v_0, v(\psi) = \infty]$ for the unique extension of v_{L_0} to L_1. Then v_{L_1} has a unique extension to $L' \coloneqq L_1[t]/(G')$ which is

$$v_{L'} = [v_0, v_1(t) = 3/2, v_{L'}(G') = \infty].$$

This is a totally ramified extension and we find that an extension $K' \coloneqq K(\pi)$ with $\pi^4 = 2$ eliminates its ramification. Indeed, the unique extension of v_{L_1} to $K'L'$ is

$$w_{K'L'} = [w_0, w_1(t + 2\pi^2 s + 2\pi^2 x + 2\pi^2) = 7/4, w_2(G') = \infty].$$

Already this extension is sufficient to eliminate the ramification of v_L over v_K; the unique extension of v_L to $K'L$ is

$$v_{K'L} = [v_0, v_1(\psi + 2\pi^2 t + 2\pi^2 x + 2\pi^2) = 7/4, v_2(G) = \infty].$$

Chapter 7

Examples

We illustrate the techniques we developed in the earlier chapters with a few examples of computations of semistable models. All the necessary computations were performed with a modified version of Sage [35]. Internally to Sage, much of the heavy lifting is done by other software packages. Arithmetic with p-adic numbers is implemented through MPIR [19], FLINT [20], and NTL [34]; other computations also make use of Pari [31] and Singular [8].

Throughout, we give no reasoning for the centers of the disks for which we perform blowups. The process of finding the right centers will be discussed in more detail in [32] which generalizes [22]. How to obtain good centers and radii is also discussed in detail in [1].

7.1 A First Example in Sage

We consider again the example from Section 2.1, i.e., the smooth projective curve Y over $\mathbb{Q}_3$ given by the equation

$$y^3 = 1 + 3x^3 + 3x^5,$$

and show how the steps to compute a semistable model of Y can be performed in Sage.[1] We start by defining the base field and the curve.

```
sage: %attach ssred.sage
sage: K = Qp(3)
sage: v = pAdicValuation(K)
sage: K.<x> = FunctionField(K)
sage: R.<t> = K[]
sage: G = t^3 - 1 - 3*x^3 - 3*x^5
sage: L.<y> = K.extension(G)
```

We begin with the standard model of $\mathbb{P}^1$ and find that the special fiber of its normalization is not reduced.

```
sage: X = NormalModel(L, v)
sage: Y = X.blowup(0,0).normalization()
```

[1] As of this writing, the following does not work in Sage, i.e., in version 6.4. When the necessary functionality has been included into Sage, it is also very unlikely that the code will work as is and that the interface will not have changed. If the reader wants to reproduce the steps performed here, he could checkout commit `5969319` of the branch `experimental` at `https://github.com/saraedum/sage-renamed.git` which was used to produce these computations.

```
sage: Y.is_special_fiber_reduced()
False
```

After an extension of the base field it is reduced, and we see that the special fiber is not smooth.

```
sage: Y = Y.make_special_fiber_reduced()
sage: Y.is_special_fiber_reduced()
True
sage: Y.special_fiber()
Affine Space Curve over Finite Field of size 3 defined by z1 - 1, z0^5 + z0^3 - z2^3
sage: _.is_smooth()
False
```

We adjoin to our field a root of the *monodromy polynomial* [22]

$$m(T) = 145T^{12} + 342T^{10} + 189T^8 + 180T^7 + 198T^5 + 18T^3 + 30T^2 + 3,$$

and perform a blowup corresponding to a disk of radius $1/12$.

```
sage: K = X.base()
sage: R.<T> = K[]
sage: m = 145*T^12 + 342*T^10 + 189*T^8 + 180*T^7 + 198*T^5 + 18*T^3 +
    30*T^2 + 3
sage: L.<zeta> = K.extension(m.monic())
sage: X = X.change_ring(L)
sage: Y = X.blowup(zeta, 1/12).normalization()
sage: Y.is_special_fiber_reduced()
False
```

Again, we extend the base field to make the special fiber reduced and see that there are now four singularities on the special fiber.

```
sage: Y = Y.make_special_fiber_reduced()
sage: C = Y.special_fiber(); C
Affine Space Curve over Finite Field of size 3 defined by z1 - 1, z0 + z2 +
    1, z2^5 - z2^3 - z3^3 + z2
sage: D = C.ambient_space().subscheme(C.defining_ideal() + C.Jacobian()
    )
sage: k.<a> = GF(9)
sage: D.rational_points(k)
[(0, 1, 2, 2), (1, 1, 1, 1), (a, 1, 2a + 2, 0), (2a + 1, 1, a + 1, 0)]
```

We perform a blowup with center ζ and radius $1/8$ and make the special fiber reduced.

```
sage: M, to_M = L.totally_ramified_extension(2)
sage: zeta = to_M(zeta)
sage: X = X.change_ring(M)
sage: Y = X.blowup(zeta,1/8).normalization()
sage: Y = Y.make_special_fiber_reduced()
sage: Y.special_fiber()
Affine Space Curve over Finite Field of size 3 defined by z2 + 1, z1 - 1, z0 +
    z3, z4^3 + z3^2 - z4
sage: Y.genus()
[1]
```

This completes the construction. The whole process takes about five minutes. The computation also works if the precision of the p-adic numbers is reduced and all computations are performed modulo 9. This reduces the time needed slightly. In any case almost all the time is spent in the construction of minimal polynomials for the iterated p-adic field extensions.

7.2 The Curve $y^2 = x(x^2 - 1)$

We now want to consider the curves $y^{2^n} = x(x^2-1)$ for $n = 1, 2$. These are (after a change of variables) isomorphic to the three point covers $y^{2^{n+1}} = x(x-1)^2$. We begin with the easier case $n = 1$.

We consider the elliptic curve Y given by the affine equation

$$y^2 = x(x^2 - 1)$$

over $K = \mathbb{Q}_2$, and consider it as a degree 2 cover of the projective line $X \coloneqq \mathbb{P}^1$. Let $\mathcal{X}_1$ be the standard model of X, i.e., the model with one component on the special fiber which corresponds to the Gauss valuation v_0. Let $\mathcal{Y}_1$ be the normalization of $\mathcal{X}_1$ in Y. The reduced special fiber $\mathcal{Y}_{1,s}$ has one irreducible component, an affine patch is given by the equation $y^2 = x(x^2-1)$ over the residue field $\mathbb{F}_2$. Hence, $\mathcal{Y}_{1,s}$ has a singularity at $(1, 0)$ which is not an ordinary double point. To compute a semistable model of Y we need to find an appropriate modification $\mathcal{X}_2 \to \mathcal{X}_1$, i.e., in the language of Chapter 3, we need to add valuations to the set $V(\mathcal{X}_1) = \{v_0\}$.

Let $\mathcal{X}_2$ be the model corresponding to the set $V(\mathcal{X}_2) = \{v_0, v_1\}$ where, in the language of Chapter 4, v_1 is the inductive valuation $v_1 = [v_0, v_1(x - \zeta) = \lambda]$ with values ζ and λ which still need to be determined. In the language of [1, 2] ζ is the center and λ the radius of the disk which corresponds to the blowup of $\mathcal{X}_1$. A good center for a blowup is given by a root of

$$m(T) = 3T^4 - 6T^2 - 1,$$

which is essentially the monodromy polynomial from [22]. Let $K' \coloneqq K(\zeta)$ where $m(\zeta) = 0$, a totally ramified extension of degree 4. A uniformizing parameter in K' is given by

$$\pi \coloneqq \frac{\zeta^3 + 3\zeta^2 + 5\zeta + 3}{4}.$$

The Correct Radius λ.

In this simple example, we could just guess the value for $\lambda > 0$ or deduce it from the results of [1, 22]. We want to indicate a more algorithmic way of determining λ. The idea is to treat λ as a variable when computing the normalization of $\mathcal{X}_2$ in Y, i.e., the extensions of v_1 to $K(Y)$.[2] We perform the steps of the algorithm of Subsection 4.6.2.

We start with w_0 the Gauss valuation on $K'(x)[y]$ induced by the valuation v_1 on $K'(x)$. Let $\xi \coloneqq x - \zeta$. The y-adic expansion of $G \coloneqq y^2 - x(x^2 - 1)$ is $G = y^2 + a_0$ with

$$a_0 = \big(1 + \pi^4 + O(\pi^7)\big)\xi^3 + \big(1 + \pi^2 + O(\pi^7)\big)\xi^2 + \big(\pi^6 + O(\pi^7)\big)\xi + \big(\pi^4 + O(\pi^7)\big).$$

The terms which make up a_0 therefore have valuations $3\lambda, 2\lambda, 3/2 + \lambda, 1$. The next key polynomial depends on our choice of λ. If we choose $\lambda < \frac{1}{2}$, the term of smallest valuation is $(1+\pi^2+O(\pi^7))\xi^2$ and the next key polynomial will be $t+\xi$. If we choose $\lambda = \frac{1}{2}$, the term of smallest valuation is $(1+\pi^2+O(\pi^7))\xi^2+(\pi^4+O(\pi^7))$ and the next key polynomial will be determined by factoring $T^2 + 1 = (T + 1)^2$

[2] This has not been implemented and currently has to be done manually.

over the residue field and lifting the factors back, i.e., we will get $t+\xi+1$ as a key polynomial. If we choose λ any larger than this, the term of smallest valuation is $(\pi^4 + O(\pi^7))$ and the next key polynomial is $\phi := t + \pi^2$. This essentially gives us three "ranges" in which to search for good radii, $(0, 1/2)$, $\{1/2\}$, $(1/2, \infty)$.

We now perform our algorithm for the radius $1/2$, i.e., we compute the normalization $\mathcal{Y}'$ of $\mathcal{X}'$ in Y and compute the affine patch of $\mathcal{Y}_s$ which lies over the new component of $\mathcal{X}_s$ minus the point where it intersects the other components. We still get a singularity on this affine patch, so our radius has been too small. (Note that $1/2$ gives the smallest disk which contains ζ and the two branch points -1, 1.) This leaves the range $(1/2, \infty)$. (Had we obtained smooth genus zero curves, then we would know that $1/2$ was too large.)

Let us now assume that $\lambda > 1/2$. We repeat the process from above and determine the ϕ-adic expansion $G = \phi^2 + a_1\phi + a_0$. We get

$$\begin{aligned} a_0 &= \big(1 + \pi^4 + O(\pi^7)\big)\xi^3 + \big(1 + \pi^2 + O(\pi^7)\big)\xi^2 \\ &\quad + \big(\pi^6 + O(\pi^7)\big)\xi + \big(\pi^8 + O(\pi^9)\big), \\ a_1 &= \big(\pi^6 + O(\pi^7)\big). \end{aligned}$$

The valuations of terms of a_0 are $3\lambda, 2\lambda, 3/2 + \lambda, 2$. Since we agreed that $\lambda \geq \frac{1}{2}$, this shows that we have $w_1 = [w_0, w_1(\phi) = 1]$.

To find a next key polynomial, we try to split our search space $(1/2, \infty)$ again by determining for which values of λ we get distinct behavior, i.e., for which values the entries which attain the minimum of $3\lambda, 2\lambda, 3/2 + \lambda, 2$ changes. With the same discussion as above this splits our search space into ranges

$$(1/2, 2/3),\ \{2/3\},\ (2/3, 3/4),\ \{3/4\},\ (3/4, 1),\ \{1\},\ (1, 3/2),\ \{3/2\},\ (3/2, \infty).$$

We try the different radii in order to find that for $2/3$ and $3/4$ the special fiber still has a singularity which is not an ordinary double point, which excludes the entire range $(0, 3/4)$. Finally, for the radius 1, we find that the special fiber has a component which is an elliptic curve, which shows that this is the right radius (as we will discuss later.)

The above is of course not a full algorithm but it hopefully indicates a practical way of trying radii systematically.

Eliminating Ramification

Let $\mathcal{X}_2$ be the normal model of X with $V(\mathcal{X}_2) = \{v_0, v_1\}$ where

$$v_1 = [v_0, v_1(y - \zeta) = 1].$$

Let $\mathcal{Y}_2$ be the normalization of $\mathcal{X}_2$ in Y. To determine whether the special fiber of $\mathcal{Y}_2$ is reduced, we determine the extensions of w_0, the Gauss valuation on $K'(x)[y]$ induced by v_1, to $K'(x)[y]/(G)$. Performing the steps of the algorithm described in Subsection 4.6.2 we find that w_0 has a unique extension w which we can approximate as a limit valuation, $w = \lim w_n$. The first two terms of such an approximation are

$$w_1 = [w_0, w_1(y - (x - \zeta - \pi^2 + \pi^4 + O(\pi^5))) = 9/8].$$

This shows hat w is not weakly unramified over v_1, its ramification index is 2.

The naïve approaches, adjoining a root of 2 (which is not present in K' yet) or adjoining a root of π to the base field both fail, i.e., the special fiber is still not reduced after the base change. The algorithm described in Proposition 6.41 determines that an element ψ which satisfies $\psi^2 + \pi^6\psi + \pi^9 = 0$ eliminates the ramification. (Note that since p^2 does not divide $\deg G$ the assumption under which Proposition 6.41 has been proved are trivially satisfied.) We assume in the following that we have performed a base change to this field, a totally ramified extension of $\mathbb{Q}_2$ of degree eight.

Affine Equations for the Special Fiber

Let w be the unique and weakly unramified extension of v_1 to $K(Y)$, and let ℓ be the residue field of w. From the description of w as an infinite inductive valuation, one can readily determine the residue field ℓ which is by Proposition 5.8 isomorphic to the function field of the normalization of the component on the special fiber corresponding to w. As the genus of that function field is one, we can deduce from Proposition 5.7 that we have found a semistable model of Y.

We can also use the algorithm from Subsection 5.1.3 to compute affine equations for a patch of that new component. We find that the component satisfies an Artin-Schreier equation of the form $w^2 + w = z^3 + z^2 + z + 1$ and that this is indeed a smooth curve of genus one. Our program, which needed about twenty seconds to perform the computations described in this section, also produces elements which reduce to the generators.

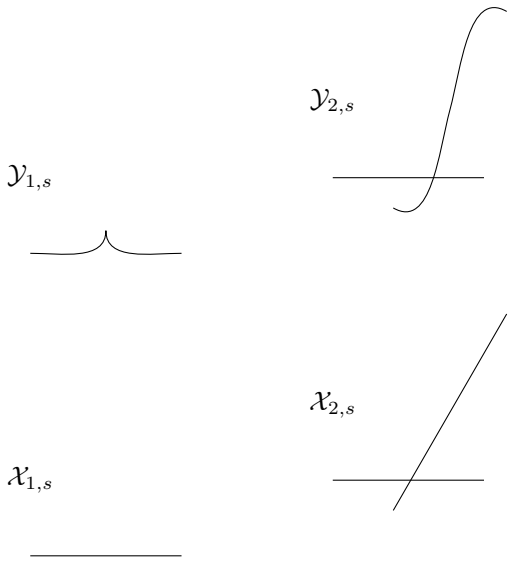


Figure 7.1: The reduced special fibers of the models of X and Y which occur during the computation.

7.3 The Curve $y^4 = x(x^2 - 1)$

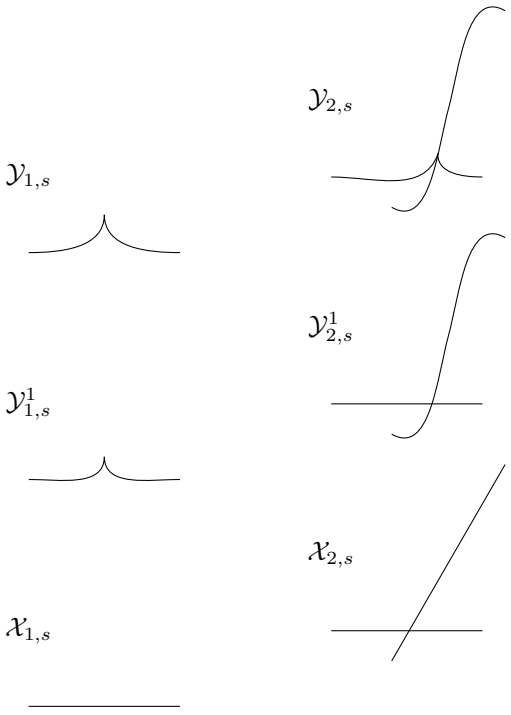
We consider the curve Y given by the affine equation

$$y^4 = x(x^2 - 1)$$

over $K = \mathbb{Q}_2$. To compute a semistable model of Y, we consider Y as a degree four cover of $X \coloneqq \mathbb{P}^1$. Let $\mathcal{X}_1$ be the standard model of X, i.e., the model with one component on the special fiber which corresponds to the Gauss valuation v_0. Let $\mathcal{Y}_1$ be the normalization of $\mathcal{X}_1$ in Y. The reduced special fiber $\mathcal{Y}_{1,s}$ has one irreducible component, one affine patch is given by the equation $y^4 = x(x^2 - 1)$ over the residue field $\mathbb{F}_2$. Hence, $\mathcal{Y}_{1,s}$ has a singularity at $(1, 0)$ which is not an ordinary double point. To compute a semistable model of Y we need to find an appropriate modification of $\mathcal{X}_1$.

7.3.1 As a Cover of $y^2 = x(x^2 - 1)$

Let Y^1 be the curve from the previous section. The curve Y is a degree two cover of Y^1, so we can try to use the semistable model of X which worked for Y^1 to compute a semistable model of Y. Let us denote this semistable model by $\mathcal{X}_2$ and let us again write v_0 and v_1 for the valuations corresponding to the irreducible components Z_0 and Z_1 of $\mathcal{X}_{2,s}$ Let $\mathcal{Y}_2^1$ and $\mathcal{Y}_2$ be the normalization of $\mathcal{X}_2$ in Y^1 and Y, respectively. Using our algorithms we can compute the components of the special fiber of $\mathcal{Y}_2$ which lie above Z_1. We find that there is one reduced component and we can compute the affine patch which lies over $Z_1 \setminus \{*\}$ where $*$ is the point where Z_0 and Z_1 intersect. The affine patch describes a smooth curve whose function field has genus one. Since the genus of Y is three, there must be a singularity which is not an ordinary double point above $*$, i.e., we have the following picture.



7.3.2 As a Cover of the Projective Line

We now consider Y again as a degree four cover of $X = \mathbb{P}^1$. Let $K \coloneqq \mathbb{Q}_2(\sqrt{i})$ where $\sqrt{i}$ is a root of the polynomial $T^4 + 1$ and fix $\pi \coloneqq \sqrt{i} + 1$ as a uniformizer in K.

To determine a model of X whose normalization in Y is semistable, we use the centers and radii which are described in [29, Proposition 7.8]. With our choice of variables we get the two centers

$$\pm\xi \coloneqq \sqrt{\frac{1}{3} + \frac{4}{9}\sqrt{i}} \in K,$$

and the radius $3/2$.

The two centers have distance 1, so $D(\xi, 3/2)$ and $D(-\xi, 3/2)$ define disjoint disks; in the language of inductive valuations, the two valuations

$$v_1 = [v_0, v_1(x - \xi) = 3/2] \quad \text{and} \quad v_1' = [v_0, v_1(x + \xi) = 3/2]$$

are incomparable. As the distance of $\pm\xi$ to ζ is $3/4$, they are also disjoint to the disk $D(\zeta, 1)$ which we considered earlier.

Let $\mathcal{X}_2$ be the model of X with $V(\mathcal{X}_2) = \{v_0, v_1\}$. (The following discussion does not change if we replace v_1 with v_1'.) As there is an element of valuation $3/2$ in K, this defines a semistable model of X. Let $\mathcal{Y}_2$ be the normalization of $\mathcal{X}_2$ in Y.

To understand $\mathcal{Y}_{2,s}$ we determine the extensions of v_1 to $K(Y)$. Using the algorithm from Subsection 4.6.2 we determine that there is a unique extension w. Writing $w = \lim w_n$ as a limit valuation, we find that a first approximant is

given by $w_1 = [w_0, w_1(y+\pi) = 11/16]$. This shows that w is totally ramified over v_1 with ramification index 4.

Eliminating Ramification

The algorithm described in Proposition 6.41 determines that an element ψ_1 which satisfies $\psi_1^4 + \pi^6\psi_1 + \pi^{11} = 0$ eliminates the total ramification. (Note that in this case, the conditions (♊) and (♌) of the proposition fail to hold, the algorithm works nevertheless.) Let $K_1 \coloneqq K(\psi_1)$ and write $\pi_1 \coloneqq \frac{\psi_1^3}{\pi^8} \in K_1$ for a uniformizer. After a base change to such an extension, we find that v_1 still has unique extension w to $K(Y)$ which is given by a limit valuation $w = \lim w_n$ whose first terms are

$$\begin{aligned} w_2 = [w_0, w_1(y + \pi_1^4 + \pi_1^6 + \pi_1^{11} + O(\pi_1^{280})) = 3/4,\\ w_2(y^2 + (\pi_1^{12} + \pi_1^{14} + \pi_1^{20} + \pi_1^{22} + \pi_1^{24} + \pi_1^{27} + O(\pi_1^{28}))y\\ + x + 1 + \pi_1^{23} + \pi_1^{24} + \pi_1^{25} + O(\pi_1^{28})) = 55/32]. \end{aligned}$$

From this we deduce that the residue field of w is a rational function field; as an extension of the residue field of v_1 it is given by an equation of the form $t^2 + t + s = 0$. We also see that w is still ramified over v_1, but this time only with ramification index 2

To eliminate ramification, we have to rely on the method described in Theorem 6.44. Since w_1 does not have the required shape for that method, we need to determine a different generator for $K(Y)/K(X)$. Instead of y we use a generator which generates the residue field of w and which is such that $w = \lim w_n$ has an approximant

$$w_1 = [w_0, w_1(\Phi) = \lambda]$$

with λ not in the value group of K_1. (By this choice of the generator, Φ reduces to an equation for the residue field extension.) Let $L_1 \coloneqq K(x)[s]/(\Phi)$ with valuation $v_{L_1} = [w_0, w_1(\Phi(s)) = \infty]$. We write $K(Y) = K(x)[t]/(G)$ and consider the Φ-adic expansion $G = \sum a_i(t)\Phi^i$ with $a_i(t) \in K_1(x)[t]$ polynomials of degree at most one. We set $H \coloneqq \sum a_i(s)t^i \in L_1[t]$ and let w_{L_1} be the unique extension of v_{L_1} to $L_1[t]/(H)$, a totally ramified extension with ramification index 2.

The algorithm from Proposition 6.41 finds an extension of K_1 which eliminates the ramification of w_{L_1} over v_{L_1} (because the degree is not divisible by p^2 there is no problem with the assumptions the proposition makes.) It determines the extension $K_2 = K_1(\psi_2)$ with an element ψ_2 which satisfies

$$\psi_2^2 + (\pi_1^8 + \pi_1^9 + \pi_1^{10} + \pi_1^{11} + \pi_1^{12})\psi_2 + \pi_1^7 = 0.$$

Let $\pi_2 \coloneqq \frac{\psi_2}{\pi_1^3}$ be a uniformizer in K''.

This extension is however not sufficient to eliminate the ramification of w. The unique extension of v_1 to $K(Y)$ now starts with

$$w_2 = [w_0, w_1(y + \pi_1^4 + \pi_1^6 + \pi_1^{11} + O(\pi_1^{280})) = 3/4, w_2(\cdots) = 127/64].$$

We have to repeat the process and get another element ψ_3 which satisfies

$$\psi_3^2 + \pi_2^{16}\psi_3 + \pi_2^{31}.$$

Let $K_3 \coloneqq K_2(\psi_3)$ with uniformizer $\pi_3 \coloneqq \frac{\psi_3}{\pi_2^{15}}$.

Over this extension, v_1 finally has a unique and weakly unramified extension w which is given by the infinite inductive valuation

$$w = [w_0, w_1(y+\pi_1^4+\pi_1^6+\pi_1^{11}+O(\pi_1^{280}))=3/4, w(y^2+\cdots)=2, w(y^4-x^3+x)=\infty].$$

The residue field of w is therefore an extension of degree 4 which adds to the step given by $t^2+t+s=0$ an extension which is given by an equation of the form $w^2+w+st+s^2+1=0$. Since we can rewrite the latter as $(w+s)^2+(w+s)=t^3+t+1$ we see that the genus of this function field is one. Hence, the genus of the normalization of the component of $\mathcal{Y}_{2,s}$ corresponding to w is an elliptic curve.

A Semistable Model of Y

To obtain a semistable model of Y we would like to take a modification of $\mathcal{X}_2$ which adds v_1' and v_1'' where $v_1'' = [v_0, v_1''(x-\zeta)=1]$ is the valuation which we considered for the curve $y^2 = x(x^2-1)$. However, ζ is not an element of our base field yet.

Using the algorithm from Subsection 4.6.2 we determine the best approximation to ζ in our field. For this let $R \coloneqq K_3[t]$ and let us construct the extensions of the valuation on K_3 to $K_3[t]/(m(t))$ where $m(T)$ is the minimal polynomial of ζ. We find that there is a unique extension of the form

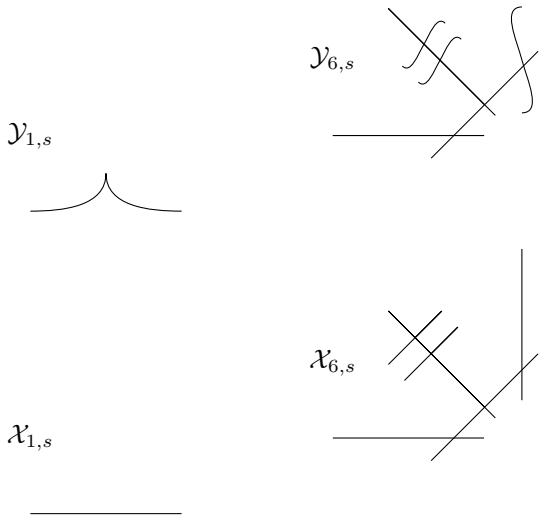
$$w_2 = [w_0, w_1(t+1+\pi_3^{32}+\pi_3^{48})=1, w_2(m(t))=\infty].$$

Hence $\zeta' \coloneqq 1+\pi_3^{32}+\pi_3^{48}$ is a best approximation to ζ with $v(\zeta-\zeta')=1$, so using it as a center instead of ζ does indeed define the same disk. Note also that this shows that $K_3(\zeta)/K_3$ would be an unramified extension of degree four.

Let $\mathcal{X}_4 \to \mathcal{X}_2$ be the modification with $V(\mathcal{X}_4) = \{v_0, v_1, v_1', v_1''\}$ where $v_1'' = [v_0, v_1''(x-\zeta')=1]$. We note that this does not define a semistable model of $\mathbb{P}^1$ since all components of the special fiber intersect in one point. To separate the components we add $v_{\zeta,\xi} = [v_0, v(t-\zeta')=3/4]$ which separates the components corresponding to v_1, v_1' from the component corresponding to v_1''. To separate the components which correspond to v_1 and v_1' from each other, we add the valuation $v_\xi = [v_0, v(t-\xi)=1]$. Let $\mathcal{X}_6 \to \mathcal{X}_2$ be the modification with $V(\mathcal{X}_6) = \{v_0, v_1, v_1', v_1'', v_{\zeta,\xi}, v_\xi\}$. Let $\mathcal{Y}_6$ be the normalization of $\mathcal{X}_6$ in Y. We find that the special fiber of $\mathcal{Y}_6$ is not reduced as the unique extension of v_1'' to $K(Y)$ is ramified with ramification index 2. We could just run our algorithm to eliminate ramification again here but since we are now already working over a totally ramified extension of degree 64, it is worthwhile to use the following alternative approach. Namely, we go back in our tower of field extensions and try to find an alternative element for ζ' which lives in a smaller field. We find that already K_1 contains such an element, namely $1+\pi_1^8$. Over this field our algorithm quickly determines that adjoining an element ψ_4 which satisfies $\psi_4^2+\pi_1^{24}\psi_4+\pi_1^{45}$ makes the component reduced.

In conclusion, we obtained a normal model of Y with reduced special fiber over a totally ramified extension of degree 128 over $\mathbb{Q}_2$. Our model has three components on the special fiber whose normalization is an elliptic curve and three components whose normalization is a projective line. Since the genus of Y is three, this shows that we have found a semistable model of Y; any

further singularities would add to the arithmetic genus of the special fiber. The configuration of the irreducible components follows from the relation of the disks which we used to describe the model of X. We could of course blow-down two of the projective lines and obtain a semistable model which corresponds to the normalization of the model $\mathcal{X}$ with $V(\mathcal{X}) = \{v_\xi, v_1, v_1', v_1''\}$.



The whole computation necessary for this example took about 20 minutes. Most of the time was spent during the construction of minimal polynomials of the uniformizers of the degree 64 extensions with which our algorithm tried to eliminate ramification.

Bibliography

[1] Kai Arzdorf, *Semistable Reduction of Prime-Cyclic Galois Covers*, dissertation thesis, Leibniz University Hanover, 2012.

[2] Kai Arzdorf and Stefan Wewers, *Another proof of the Semistable Reduction Theorem*, arXiv preprint arXiv:1211.4624 (2012).

[3] M. F. Becker and Saunders MacLane, *The Minimum Number of Generators for Inseparable Algebraic Extensions*, Bulletin of the American Mathematical Society **46** (1940), no. 2, 182–186.

[4] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Springer, 1990.

[5] Siegfried Bosch, *Algebra*, Springer, 2006.

[6] Paul M. Cohn, *Basic Algebra: Groups, Rings, and Fields*, Springer, 2003.

[7] Gary Cornell, *On the Construction of Relative Genus Fields*, Transactions of the American Mathematical Society **271** (1982), no. 2, 501–511.

[8] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR *3-1-6 — A computer algebra system for polynomial computations*, 2012. `http://www.singular.uni-kl.de`.

[9] Theo De Jong, *An Algorithm for Computing the Integral Closure*, Journal of Symbolic Computation **26** (1998), no. 3, 273–277.

[10] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **36** (1969), no. 1, 75-109.

[11] Helmut P. Epp, *Eliminating Wild Ramification*, Inventiones mathematicae **19** (1973), no. 3, 235–249.

[12] Julio Fernández, Jordi Guàrdia, Jesús Montes, and Enric Nart, *Residual ideals of MacLane valuations*, arXiv preprint arXiv:1305.0775 (2013).

[13] Jean Fresnel and Marius van der Put, *Rigid Analytic Geometry and Its Applications*, Progress in Mathematics, vol. 218, 2004.

[14] William Fulton, *Algebraic Curves*: *An Introduction to Algebraic Geometry*, 2008. `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`.

[15] P. Gianni and B. Trager, *Square-Free Algorithms in Positive Characteristic*, Applicable Algebra in Engineering, Communication and Computing **7** (1996), no. 1, 1–14.

[16] Alexander Grothendieck and Jean Dieudonné, *Éléments de géométrie algébrique*. III, Publications Mathématiques de l'IHÉS **11** (1961).

[17] Barry Green, *On curves over valuation rings and morphisms to* $\mathbb{P}^1$, Journal of Number Theory **59** (1996), no. 2, 262–290.

[18] Jordi Guárdia, Enric Nart, and Sebastian Pauli, *Single-Factor Lifting and Factorization of Polynomials over Local Fields*, Journal of Symbolic Computation **47** (2012), no. 11, 1318–1346.

[19] W. Hart et al., *MPIR: Multiple Precision Integers and Rationals*, 2012. `http://mpir.org`.

[20] W. Hart, F. Johansson, and S. Pancratz, *FLINT: Fast Library for Number Theory*, 2013. `http://flintlib.org`.

[21] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer, 1977.

[22] Claus Lehr and Michel Matignon, *Wild monodromy and automorphisms of curves*, Duke Mathematical Journal **135** (2006), no. 3, 569–586.

[23] Qing Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics, Oxford University Press, 2002.

[24] Saunders MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society **40** (1936), no. 3, 363–395.

[25] ———, *A construction for prime ideals as absolute values of an algebraic field*, Duke Math. J **2** (1936), no. 3, 492–510.

[26] Hideyuki Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1989.

[27] Jesús Montes Peral, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, dissertation thesis, Universitat de Barcelona, 1999.

[28] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer, 2006.

[29] Andrew Obus, *On Colmez's product formula for periods of CM-abelian varieties*, Mathematische Annalen **356** (2013), no. 2, 401–418.

[30] Alexander Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper*, Mathematische Zeitschrift **39** (1935), no. 1, 321–404.

[31] The PARI Group, *PARI/GP (Version 2.7.1)*, Bordeaux, 2014. `http://pari.math.u-bordeaux.fr/`.

[32] Julian Rüth and Stefan Wewers, *Semistable reduction of superelliptic curves with exponent p* (2015). in preparation.

[33] Jean-Pierre Serre, *Corps locaux*, Hermann, 1980.

[34] Victor Shoup et al., *NTL: A Library for doing Number Theory*. `http://www.shoup.net/ntl`.

[35] W. A. Stein et al., *Sage Mathematics Software (Version 6.4)*, The Sage Development Team, 2014. `http://www.sagemath.org`.

[36] Henning Stichtenoth, *Algebraic Function Fields and Codes*, Graduate Texts in Mathematics, vol. 254, Springer, 2009.

[37] C. Huneke and I. Swanson, *Integral Closure of Ideals, Rings, and Modules*, London Mathematical Society Lecture Note Series, vol. 336, Cambridge University Press, 2006.

[38] Oswald Teichmüller, *Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper*, Journal für die reine und angewandte Mathematik **176** (1937), 141–152.

[39] Michel Vaquié, *Extension d'une valuation*, Transactions of the American Mathematical Society **359** (2007), no. 7, 3439–3481.