Multivariate Hensel Lemma for ultrametric fields

María Emilia Alonso García[†,1], Henri Lombardi[‡], and Stefan Neuwirth[‡]

[†]Departamento de Álgebra, Geometría y Topología, Facultad de Ciencias Matemáticas, Universidad Complutense Madrid, Spain, mariemi@mat.ucm.es.
[‡]Université Marie et Louis Pasteur, CNRS, LmB (UMR 6623), 25000 Besançon, France, henri.lombardi@univ-fcomte.fr, stefan.neuwirth@univ-fcomte.fr.

January 31, 2025

Abstract

The Multivariate Hensel Lemma for local rings is usually proved as a consequence of the Grothendieck version of Zariski's Main Theorem, which is designed for a more general situation that is a priori much more difficult. In this paper, we give a direct proof of the Multivariate Hensel Lemma for ultrametric fields, in the framework of constructive mathematics and without using ZMT. In the framework of classical mathematics, our result entails the Lemma for rank-one valued fields.

Keywords: Multivariate Hensel Lemma, valued field, ultrametric field, henselisation of a local ring, henselisation of a valued field, constructive mathematics.

MSC2020: 13B40, 13J15, 03F65.

Contents

[1]Partially supported by the research project PID2020-114750GB-C32 (Agencia Estatal de Investigación, Spain) and by the Instituto de Matemática Interdisciplinar (IMI, Universidad Complutense Madrid, Spain).

Introduction

This paper is written in Bishop's style of constructive mathematics (Bishop 1967, Bishop and Bridges 1985, Bridges and Richman 1987, Mines, Richman, and Ruitenburg 1988, Lombardi and Quitté 2015, Yengui 2015, Lombardi and Quitté 2021).

It is a natural sequel to the articles Coste, Lombardi, and Roy 2001, Kuhlmann and Lombardi 2000, Kuhlmann, Lombardi, and Perdry 2003, Alonso García, Lombardi, and Perdry 2008 and, to a lesser extent, Alonso García, Lombardi, and Neuwirth 2021, Coquand and Lombardi 2016a,b, Lombardi and Mahboubi 2023.

Hensel's lemma was introduced in mathematics in the context of Hensel's work on p-adic fields $\mathbb{Q}_p$. In his work, valued fields are in fact ultrametric fields, i.e. fields $\mathbf{K}$ given with a nonarchimedean absolute value $x \mapsto |x|$, $\mathbf{K} \to \mathbb{R}$ (see Section 2).

In 1930, Krull (1930) and Deuring (1931) introduced the notion of general valued fields, where ultrametric fields correspond to rank-one valued fields. The general notion of valued field was necessary to obtain Krull's fundamental theorem stating that the integral closure of a domain is the intersection of its overrings which are valuation domains.

The abstract notion of a henselian ultrametric field (an ultrametric field satisfying Hensel's Lemma) along with the henselisation of an ultrametric field were introduced by Ostrowski (1934) in a seminal paper. He introduced the henselisation of $(\mathbf{K}, |.|)$ as the separable closure $\widetilde{\mathbf{K}}$ of $\mathbf{K}$ in its completion $\hat{\mathbf{K}}$. See Roquette 2002 for more details on this topic. From a modern viewpoint, Ostrowski was dealing with valued fields in the case of rank-one valuations.

At a first glance one could consider the Multivariate Hensel Lemma to be obvious for ultrametric fields, insofar as a zero of a Newton polynomial system can be calculated by Newton's method in a completion of the ultrametric field. However the fact that this zero of the Newton polynomial system belongs to the valuation ring of the henselisation turns out to be difficult to prove, even for the most simple discrete valuation rings. In fact, reference books in classical mathematics for the theory of valuation domains, as Nagata 1962, Bourbaki 1972, and Engler and Prestel 2005, do not pay any attention to the Multivariate Hensel Lemma, even in the exercises.

In the fifties, the more general notion of henselian local ring was introduced by Azumaya (1951) and Nagata (1953), becoming afterwards a very important tool in Algebraic Geometry. In this framework, the Multivariate Hensel Lemma states that on a local ring, a Newton polynomial system always has a zero with coordinates in the henselisation of the ring. The Multivariate Hensel Lemma for local rings is usually proved as a consequence of the Grothendieck version of Zariski's Main Theorem (ZMT). This version of ZMT is designed for a more general situation that is a priori much more difficult (for a constructive treatment, see Alonso García, Coquand, and Lombardi 2014).

The aim of this paper is to give a direct constructive proof of the Multivariate Hensel Lemma for ultrametric discrete fields, without using ZMT. In classical mathematics, this provides an ad hoc proof of the Lemma for henselian rank-one valuations.

The plan is the following.

In the first section we introduce the general framework of the Multivariate Hensel Lemma for local rings. We recall the notions of Newton polynomial system, étale polynomial system and étale algebra. Then we present the constructive version of a structure theorem for strictly finite étale algebras over discrete fields and the structure theorem for unramified finitely presented algebras over discrete fields, as given in Lombardi and Quitté 2015, Theorems VI-1.7, VI-1.9 and Corollary VI-6.15.

In Section 2, we deal with ultrametric fields. Let $(\mathbf{K}, |\cdot|)$ be an ultrametric field with a nontrivial absolute value. We denote by $\widetilde{\mathbf{K}}$ the separable closure of $\mathbf{K}$ in its completion $\widehat{\mathbf{K}}$, by $\widetilde{\mathbf{V}} = \{\, x \in \widetilde{\mathbf{K}} \,;\, |x| \leqslant 1 \,\}$ its "valuation ring", and let $\widetilde{\mathfrak{m}} = \{\, x \in \widetilde{\mathbf{K}} \,;\, |x| < 1 \,\}$. Our crucial result is the following theorem, where we compare the henselisation $(\mathbf{K}^{\mathrm{H}}, \mathbf{V}^{\mathrm{H}})$ constructed in Kuhlmann and Lombardi 2000 to $(\widetilde{\mathbf{K}}, \widetilde{\mathbf{V}})$.

Theorem 2.2.5 (two equivalent versions of the henselisation of an ultrametric discrete field)**.** *Let* $(\mathbf{K}, |\cdot|)$ *be an ultrametric discrete field. The henselisation* $(\mathbf{K}^{\mathrm{H}}, \mathbf{V}^{\mathrm{H}})$ *is isomorphic to* $(\widetilde{\mathbf{K}}, \widetilde{\mathbf{V}})$*. More precisely, there exists a unique* $\mathbf{K}$*-homomorphism* $\mathbf{K}^{\mathrm{H}} \to \widetilde{\mathbf{K}}$ *sending* $\mathbf{V}^{\mathrm{H}}$ *into* $\widetilde{\mathbf{V}}$*, and this homomorphism is an isomorphism.*

We have got that an arbitrary element of $\widetilde{\mathbf{K}}$ is precisely the image of an element γ in a field $\mathbf{K}[\xi] \subseteq \mathbf{K}^{\mathrm{H}}$, where ξ is the special zero of a special polynomial.

Finally we prove our Multivariate Hensel Lemma.

Theorems 2.3.4 and 2.4.3 (Multivariate Hensel Lemma for an ultrametric discrete field)**.** *Let* $(\mathbf{K}, |\cdot|)$ *be an ultrametric discrete field and* $(f_1, \ldots, f_n)$ *a Newton polynomial system at* $(\underline{0})$ *over* $(\mathbf{V}, \mathfrak{m})$*. This system admits a unique zero with coordinates in* $\widetilde{\mathfrak{m}}$*. It admits also a unique zero with coordinates in* $\mathfrak{m}\mathbf{V}^{\mathrm{H}}$*.*

1 Newton polynomial systems, étale algebras

Constructive terminology

In constructive mathematics, a *local ring* is defined as a ring where for all x, x or $1-x$ is invertible (with an explicit "or").

The *Jacobson radical of a ring* $\mathbf{A}$ is the ideal $\mathrm{Rad}(\mathbf{A}) = \{\, x \in \mathbf{A} \,;\, 1 + x\mathbf{A} \subseteq \mathbf{A}^{\times} \,\}$.

For a local ring, the Jacobson radical is its unique maximal ideal, generally denoted by $\mathfrak{m}_{\mathbf{A}}$ or $\mathfrak{m}$. We shall simply say: *the local ring* $(\mathbf{A}, \mathfrak{m})$.

A *Heyting field* is a nontrivial local ring whose Jacobson radical is 0. The *residual field* of a nontrivial local ring $(\mathbf{A}, \mathfrak{m})$ is the Heyting field $\mathbf{A}/\mathfrak{m}$ also denoted by $\overline{\mathbf{A}}$.

A *discrete field* is a nontrivial ring in which any element is zero or invertible. It is the same thing as a Heyting field with a zero test.

The local ring is said to be *residually discrete* if its residual field is discrete. This amounts to saying that we have explicitly the disjunction $x \in \mathbf{A}^{\times}$ or $x \in \mathfrak{m}_{\mathbf{A}}$ for all x in $\mathbf{A}$.

For local rings $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$ and $(\mathbf{B}, \mathfrak{m}_{\mathbf{B}})$, a ring morphism $\varphi\colon \mathbf{A} \to \mathbf{B}$ is said to be *local* when $\varphi^{-1}(\mathbf{B}^{\times}) \subseteq \mathbf{A}^{\times}$. In this case we say that $(\mathbf{B}, \mathfrak{m}_{\mathbf{B}})$ is an $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$-algebra.

Hensel codes over local rings

A *Hensel code* over a local ring $(\mathbf{A}, \mathfrak{m})$ is a pair $(f, a) \in \mathbf{A}[X] \times \mathbf{A}$, where f is a monic polynomial, $f(a) \in \mathfrak{m}$ and $f'(a) \in \mathbf{A}^{\times}$ (in other words $\overline{a}$ is a simple zero of $\overline{f}$). In this case we say that f is a *Hensel polynomial* or a *Nagata polynomial*.

A *special polynomial* is a polynomial $h(X) = X^n - X^{n-1} + \sum_{k=0}^{n-2} a_k X^k$ with the a_k's $\in \mathfrak{m}$. In this case $(h, 1)$ is a Hensel code.

A *Hensel zero for the Hensel code* (f, a) in an $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$-algebra $(\mathbf{B}, \mathfrak{m}_{\mathbf{B}})$ is an element $\xi \in \mathbf{B}$ such that $\varphi_\star(f)(\xi) = 0$ and $\xi - \varphi(a) \in \mathfrak{m}_{\mathbf{B}}$.

A local ring $(\mathbf{A}, \mathfrak{m})$ is said to be *henselian* if any Hensel code has a *Hensel zero* α in $(\mathbf{A}, \mathfrak{m})$. In this case we say that *the zero* α *of* f *is the lifting in* $\mathbf{A}$ *of the simple zero* $\overline{a}$ of $\overline{f}$ in $\overline{\mathbf{A}}$. The Hensel zero for the Hensel code $(h, 1)$ of a special polynomial h is called the *special zero* of the polynomial.

A Hensel zero for a Hensel code (f, a) is necessarily unique, regardless of the hypothesis that f be monic: one writes

$$0 = f(\alpha') - f(\alpha) = f'(\alpha)\mu + b\mu^2 = \mu \cdot (f'(\alpha) + b\mu) \quad \text{with } b \in \mathbf{A}, \qquad (+)$$

where $\mu = \alpha' - \alpha \in \mathfrak{m}$, and as $f'(\alpha) + b\mu \in \mathbf{A}^{\times}$ we get $\mu = 0$.

The *completion* of $\mathbf{A}$ for the $\mathfrak{m}$-adic topology, i.e. the projective limit of $(\mathbf{A}/\mathfrak{m}^k)_{k\in\mathbb{N}}$, is denoted by $\widehat{\mathbf{A}}$. We have a natural morphism $\varphi\colon \mathbf{A} \to \widehat{\mathbf{A}}$ and we let $\widehat{\mathfrak{m}} := \varphi(\mathfrak{m})\widehat{\mathbf{A}}$. The morphism φ is injective if and only if $\bigcap_{k\in\mathbb{N}} \mathfrak{m}^k = 0$. If $(\mathbf{A}, \mathfrak{m})$ is a residually discrete local ring, $(\widehat{\mathbf{A}}, \widehat{\mathfrak{m}})$ is a local ring and it is henselian. In fact, Newton's method (as in Theorem 1.2.1) allows us to compute a Hensel zero for any Hensel code.

The henselisation of a local ring

The notion of henselisation of a local ring corresponds to the solution of the universal problem for the full subcategory of henselian local rings in the category of local rings and local homomorphisms.

For a residually discrete local ring the paper Alonso García, Lombardi, and Perdry 2008 constructs this henselisation by iteratively adding formal Hensel zeroes for Hensel polynomials. We denote by $\mathbf{A}^{\mathrm{h}}$ the *henselisation* of $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$.

Our first result explains how to lift a simple residual zero of a not necessarily monic (viz. not Hensel) polynomial on $\mathbf{A}$ to a henselian extension. It is stated for residually discrete local rings in Alonso García, Lombardi, and Perdry 2008, Lemma 5.3 and Proposition 5.4. Here we state it in the context of a local ring $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$, a polynomial $f \in \mathbf{A}[X]$ and a local morphism from $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$ to a henselian local ring $(\mathbf{B}, \mathfrak{m}_{\mathbf{B}})$.

Lemma 1.0.1 (Hervé's trick)**.** *Let $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$ be a local ring, $\varphi\colon \mathbf{A} \to \mathbf{B}$ a local morphism with $(\mathbf{B}, \mathfrak{m}_{\mathbf{B}})$ henselian, and $f(X) = \sum_{k=0}^{n} a_k X^k \in \mathbf{A}[X]$ with $a_0 \in \mathfrak{m}_{\mathbf{A}}$ and $a_1 \in \mathbf{A}^{\times}$. The polynomial f has a zero γ in $a_0\mathbf{B} \subseteq \mathfrak{m}_{\mathbf{B}}$, with $f'(\gamma)$ invertible in $\mathbf{B}$. It is the unique zero of f in $\mathfrak{m}_{\mathbf{B}}$. In particular, if $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$ is henselian, f admits a zero in $a_0 \cdot \mathbf{A} \subseteq \mathfrak{m}_{\mathbf{A}}$, and it is the unique zero of f in $\mathfrak{m}_{\mathbf{A}}$.*

Proof. We define the special polynomial

$$\begin{aligned} g(X) &= X^n - X^{n-1} + a_0 \cdot \big(\textstyle\sum_{j=2}^{n} (-1)^j a_j a_0^{j-2} a_1^{-j} X^{n-j}\big) \\ &= X^n - X^{n-1} + a_0 \ell(X) \quad \text{with } \ell(X) \in \mathbf{A}[X]. \end{aligned}$$

The following equality is correct in $\mathbf{A}[X, 1/X]$

$$a_0 g(X) = X^n f\Big(\frac{-a_0 a_1^{-1}}{X}\Big). \tag{$*$}$$

Let $\delta = 1 + \alpha$ (where $\alpha \in \mathfrak{m}_{\mathbf{B}}$) be the special zero of the special polynomial g. Then $\delta \in \mathbf{B}^{\times}$. Let $\gamma = \frac{-a_0 a_1^{-1}}{\delta} = -a_0(a_1\delta)^{-1} \in \mathfrak{m}_{\mathbf{B}}$. Applying $(*)$ we see that $a_0 g(\delta) = \delta^n f(\gamma)$, so $f(\gamma) = 0$. Moreover $f'(\gamma) \in \mathbf{B}^{\times}$ because $f'(0) \in \mathbf{A}^{\times}$ and $\gamma \in \mathfrak{m}_{\mathbf{B}}$.
Uniqueness is already proved, see $(+)$. □

Remark 1.0.2. In the case of a residually discrete local ring $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$ with henselisation $\mathbf{A}^{\mathrm{h}}$, the element δ in the previous proof appears in the construction of the henselisation $\mathbf{A}^{\mathrm{h}}$ as an element of

$$\mathbf{A}_g := S^{-1}\mathbf{A}[x], \text{ where } \mathbf{A}[x] = \mathbf{A}[X]/\langle g \rangle \text{ and } S = \{\, s(x) \in \mathbf{A}[x] \;;\; s(1) \in \mathbf{A}^{\times} \,\}\,.$$

The ring $\mathbf{A}_g$ is a residually discrete local ring, faithfully flat over $\mathbf{A}$, and $\mathrm{Rad}(\mathbf{A}_g) = \mathfrak{m}\mathbf{A}_g$. So δ is the image of $x \in \mathbf{A}[x]$ in $\mathbf{A}_g$ via the localisation morphism. As the canonical morphism $\mathbf{A} \to \mathbf{A}_g$ is injective, we can identify $\mathbf{A}$ with a subring of $\mathbf{A}_g$. These rings $\mathbf{A}_g$ are the elementary building blocks in the construction of the henselisation of the residually discrete local ring $(\mathbf{A}, \mathfrak{m}_{\mathbf{A}})$ given in Alonso García, Lombardi, and Perdry 2008. ■

1.1 Newton polynomial system in a local ring

Given $(\mathbf{A}, \mathfrak{m})$ a local ring, a *Newton polynomial system* (or *Hensel polynomial system*) *at the point* $(\underline{a}) = (a_1, \dots, a_n) \in \mathbf{A}^n$ is given by a polynomial system $(\underline{f}) = (f_1, \dots, f_n)$ in $\mathbf{A}[X_1, \dots, X_n]^n$ when $(\underline{a})$ is an *approximate simple zero* in the following sense:

- the $f_j(\underline{a})$ are in $\mathfrak{m}$;
- the Jacobian matrix of the system is invertible at $(\underline{a})$ modulo $\mathfrak{m}$.

The second condition amounts to saying that the Jacobian determinant $\mathrm{Jac}(\underline{a})$ is invertible in $\mathbf{A}$ modulo $\mathfrak{m}$.[1]

The *Multivariate Hensel Lemma* says that a Newton polynomial system at $(\underline{a})$ on a local ring $(\mathbf{A}, \mathfrak{m})$ has a zero $(\underline{\xi})$ with coordinates in the henselisation $\mathbf{A}^{\mathrm{h}}$ with $\xi_j - a_j \in \mathfrak{m}\mathbf{A}^{\mathrm{h}}$ for each j.

By definition, a Hensel code is a one-variable Newton polynomial system.

We remark here that Lafon (1963) and the Stacks Project, Section 15.11, give the Multivariate Hensel Lemma in a slightly hidden form for henselian pairs (see e.g. implication (5) ⇒ (2) in Lemma 15.11.6 in the Stacks Project), but they use ZMT for their proof.

Uniqueness of the Hensel zero

Lemma 1.1.1. *Let $(\mathbf{A}, \mathfrak{m})$ be a local ring and $(\underline{f}) = (f_1, \dots, f_n)$ a Newton polynomial system at $(\underline{a}) \in \mathbf{A}^n$. If $(\underline{\alpha})$ and $(\underline{\gamma})$ are Hensel zeroes at $(\underline{a})$ for this system, then $(\underline{\alpha}) = (\underline{\gamma})$.*

Proof. Let $J(\underline{X})$ be the Jacobian matrix of the system. Write $(\underline{\gamma}) = (\underline{\alpha}) + (\underline{\delta})$ with the δ_i's in $\mathfrak{m}$. We see $(\underline{f}(\underline{\alpha})) = (f_i(\underline{\alpha}))_{i \in [\![1..n]\!]}$, $(\underline{f}(\underline{\gamma}))$, and $(\underline{\delta})$ as column vectors. Taylor's formula in several variables for polynomials yields an equality

$$(\underline{f}(\underline{\gamma})) = (\underline{f}(\underline{\alpha})) + J(\underline{\alpha})(\underline{\delta}) + M(\underline{\delta}),$$

where M is a square matrix with coefficients in the ideal $\langle \underline{\delta} \rangle$ and $(\underline{f}(\underline{\gamma})) = (\underline{f}(\underline{\alpha})) = (\underline{0})$. So $(\mathrm{I}_n + J(\underline{\alpha})^{-1} M)(\underline{\delta}) = (\underline{0})$, and $(\underline{\delta}) = (\underline{0})$. □

The image of a Newton polynomial system by a local morphism is a Newton polynomial system. The uniqueness of a zero (if it exists) in an $(\mathbf{A}, \mathfrak{m})$-algebra is proved in the same way.

1.2 Newton's method

The following theorem describes the so-called quadratic Newton method in a purely algebraic context.

This result holds true also for a general ideal $\mathfrak{a}$ of any ring $\mathbf{A}$ (instead of $\mathfrak{m}_{\mathbf{A}}$ for a local ring), as explained in Lombardi and Quitté (2015, Theorem III-10.3). In many cases it is relevant to consider the ideal $\mathfrak{a}$ generated by the $f_i(\underline{a})$'s.

Theorem 1.2.1 (quadratic Newton method)**.**
Let $(\mathbf{A}, \mathfrak{m})$ be a local ring and $(\underline{f}) = (f_1, \dots, f_n)$ a Newton polynomial system in $\mathbf{A}[X_1, \dots, X_n]$ at $(\underline{a}) = (a_1, \dots, a_n) \in \mathbf{A}^n$. We denote by $J(\underline{\xi})$ the Jacobian matrix of $(\underline{f})$ at $(\underline{\xi})$. Let U be an inverse of $J(\underline{a})$ modulo $\mathfrak{m}$. We define sequences $(\underline{a}^{(m)})_{m \geqslant 0}$ in $\mathbf{A}^n$ and $(U^{(m)})_{m \geqslant 0}$ in $\mathbb{M}_n(\mathbf{A})$ by the following iteration:

$$\begin{aligned} \underline{a}^{(0)} &= \underline{a}, & \underline{a}^{(m+1)} &= \underline{a}^{(m)} - U^{(m)} \cdot \underline{f}(\underline{a}^{(m)}), \\ U^{(0)} &= U, & U^{(m+1)} &= U^{(m)} \left(2\mathrm{I}_n - J(\underline{a}^{(m+1)}) U^{(m)} \right). \end{aligned}$$

Then for each integer m we get the following congruences:

$$\begin{aligned} \underline{a}^{(m+1)} &\equiv \underline{a}^{(m)} \quad \text{and} \quad U^{(m+1)} \equiv U^{(m)} \quad \bmod \mathfrak{m}^{2^m}, \\ \underline{f}(\underline{a}^{(m)}) &\equiv 0 \quad \text{and} \quad U^{(m)} J(\underline{a}^{(m)}) \equiv \mathrm{I}_n \quad \bmod \mathfrak{m}^{2^m}. \end{aligned}$$

This theorem says that if we have a Newton polynomial system $(\underline{f}) = (f_1, \dots, f_n)$ in $\mathbf{A}[X_1, \dots, X_n]$ with $(\underline{a})$ an approximate simple zero in the local ring $(\mathbf{A}, \mathfrak{m})$, we can find a much better approximate simple zero $(\underline{a}^{(m)})$ of $(\underline{f})$, with $\underline{a}^{(m)} \equiv \underline{a} \bmod \mathfrak{m}$ $(m > 1)$.

We shall use the following terminology in constructive mathematics: a local ring $(\mathbf{A}, \mathfrak{m})$ is said to be *quasi-noetherian* if $\mathbf{A}$ is a coherent strongly discrete ring, $\mathfrak{m}$ is a finitely generated

[1] Note that because $(\mathbf{A}, \mathfrak{m})$ is a local ring, invertibility and invertibility modulo $\mathfrak{m}$ coincide.

ideal, and $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = 0$.[2] In this context, each $\mathfrak{m}^n$ is a coherent strongly discrete $\mathbf{A}$-module and the natural morphism $\mathbf{A} \to \widehat{\mathbf{A}}$ is injective. This happens in the following case: $\mathbf{A} = \mathbf{B}_{1+\mathfrak{m}_\mathbf{B}}$, where $\mathbf{B}$ is a finitely presented algebra over $\mathbb{Z}$ or over a discrete field, $\mathfrak{m}_\mathbf{B}$ is a finitely generated ideal, and $\mathfrak{m}_\mathbf{A} = \mathfrak{m}_\mathbf{B}\mathbf{A}$.[3]

Applying Newton's method in two contexts, namely, to a quasi-noetherian local ring and to the valuation ring of an ultrametric discrete field, we can get what we call "two weak forms of the Multivariate Hensel Lemma", where the coordinates of the zeroes of the polynomial system are not asserted to be in the henselisation of the ring:

Corollary 1.2.2 (Multivariate Hensel Lemma, first weak form).
Let $(\mathbf{K}, |\cdot|)$ be an ultrametric discrete field [4] *and $(f_1, \dots, f_n)$ a polynomial system as in Theorem 1.2.1, with $\mathbf{A} = \mathbf{V} = \{\, x \in \mathbf{K} \,;\, |x| \leqslant 1 \,\}$ and $\mathfrak{m} = \{\, x \in \mathbf{K} \,;\, |x| < 1 \,\}$. Then the system has a unique zero $(\underline{\xi}) = (\xi_1, \dots, \xi_n)$ with coordinates in $\widehat{\mathbf{K}}$ satisfying $\xi_i - a_i \in \widehat{\mathfrak{m}}$ for $i = 1, \dots, n$.*

Corollary 1.2.3 (Multivariate Hensel Lemma, second weak form).
Let $(\mathbf{A}, \mathfrak{m})$ be a quasi-noetherian local ring and $(f_1, \dots, f_n)$ a polynomial system as in Theorem 1.2.1. Then the system has a unique zero $(\underline{\xi}) = (\xi_1, \dots, \xi_n)$ with coordinates in $\widehat{\mathbf{A}}$ satisfying $\xi_i - a_i \in \mathfrak{m}\widehat{\mathbf{A}}$ for $i = 1, \dots, n$.

1.3 Étale algebras

The context of Newton's method can be generalised and formalised under the name of basic étale algebra.

Definition 1.3.1 (étale polynomial system, étale $\mathbf{A}$-algebra).
Let $\mathbf{A}$ be a commutative ring.

1. Let $(\underline{f}) = (f_1, \dots, f_n)$ be a system of n polynomials in $\mathbf{A}[X_1, \dots, X_n]$ and $\mathbf{B} = \mathbf{A}[\underline{X}]/\langle \underline{f} \rangle$. The $\mathbf{A}$-algebra $\mathbf{B} = \mathbf{A}[x_1, \dots, x_n]$ is said to be *basic étale* for the presentation $(\underline{f})$ if the Jacobian matrix $J(\underline{x})$ of the system $(\underline{f})$ is invertible in $\mathbf{B}$. In this case we say that the polynomial system $(f_1, \dots, f_n)$ is an *étale polynomial system*.

2. A finitely presented $\mathbf{A}$-algebra $\mathbf{C} = \mathbf{A}[X_1, \dots, X_m]/\langle g_1, \dots, g_s \rangle$ is said to be *étale* if we know comaximal elements $(u_i)_{i\in I}$ in $\mathbf{C}$ such that each $\mathbf{A}$-algebra $\mathbf{C}[1/u_i]$ is basic étale for a convenient presentation $(\underline{f_i}) = (f_{i,1}, \dots, f_{i,n_i})$.

The notion of étale algebra, introduced by Grothendieck, is a fundamental concept of commutative algebra. One result of that theory asserts that any étale algebra is basic étale for a convenient presentation.

Let us remark that a finite product of étale algebras is étale and a localisation $\mathbf{C}[1/s]$ of an étale algebra $\mathbf{C}$ is étale. In particular the trivial algebra is étale.

Lemma 1.3.2. *It is always possible to replace a Newton polynomial system $((f_1, \dots, f_n), (\underline{0}))$ over a local ring $(\mathbf{A}, \mathfrak{m})$ with a basic étale Newton polynomial system $((f_1, \dots, f_{n+1}), (\underline{0}, 0))$, i.e. with a Newton polynomial system over $(\mathbf{A}, \mathfrak{m})$ which is a basic étale polynomial system over $\mathbf{A}$. Moreover, the new polynomial system leaves the notion of Hensel zero unchanged.*

Proof. We denote by $\mathrm{Jac}(\underline{X})$ the Jacobian determinant, we add an indeterminate X_{n+1} and the polynomial $f_{n+1} := (1 + X_{n+1})\mathrm{Jac}(\underline{0})^{-1}\mathrm{Jac}(\underline{X}) - 1$. We have $f_{n+1}(\underline{0}, 0) = 0$. The new polynomial system has its Jacobian determinant $\mathrm{Jac}_1(\underline{x}, x_{n+1})$ invertible in the new quotient $\mathbf{A}$-algebra, and a Hensel zero $(\underline{\xi})$ of the first system with coordinates in an $\mathbf{A}$-algebra gives the Hensel zero $(\underline{\xi}, \eta)$ for the new Newton polynomial system with $(1 + \eta)\mathrm{Jac}(\underline{0})^{-1}\mathrm{Jac}(\underline{\xi}) = 1$, i.e. $\eta = \mathrm{Jac}(\underline{0})\mathrm{Jac}(\underline{\xi})^{-1} - 1$. □

[2] In some constructive proofs, it will be important that, for any $x \neq 0$, the integer k such that $x \in \mathfrak{m}^k \setminus \mathfrak{m}^{k+1}$ be known.

[3] A quasi-noetherian local pair is said to be noetherian if the ring $\mathbf{A}$ is noetherian. We shall not use this notion.

[4] See Section 2.

This elementary manipulation gives some properties (of the coordinates) of the zero. For example, as a consequence of Theorem 1.3.5, if $(\mathbf{A}, \mathfrak{m})$ is an integral local ring with $\mathbf{K} = \operatorname{Frac} \mathbf{A}$, the coordinates of the Hensel zero of a Newton polynomial system over $(\mathbf{A}, \mathfrak{m})$ in a $\mathbf{K}$-algebra are always separable over $\mathbf{K}$.

Structure of étale algebras over a discrete field

Let $\mathbf{K}$ be a discrete field and $\mathbf{K}'$ a field extension which is a finitely generated $\mathbf{K}$-vector space. We say in this case that $\mathbf{K}'$ is a *finite algebraic extension* of $\mathbf{K}$.

More generally a $\mathbf{K}$-algebra $\mathbf{C}$ which is a finitely generated $\mathbf{K}$-vector space is said to be *finite over* $\mathbf{K}$. The elements of $\mathbf{C}$ are algebraic over $\mathbf{K}$, but perhaps we don't know the dimension of $\mathbf{C}$ as $\mathbf{K}$-vector space. If $\mathbf{C}$ is generated by n elements as $\mathbf{K}$-vector space, we write $[\mathbf{C} : \mathbf{K}] \leqslant n$. If $\mathbf{C}$ contains m $\mathbf{K}$-linearly independent elements, we write $[\mathbf{C} : \mathbf{K}] \geqslant m$. Finally $\mathbf{C}$ is said to be *strictly finite* over $\mathbf{K}$ when the dimension of $\mathbf{C}$ as $\mathbf{K}$-vector space is known, and we write $[\mathbf{C} : \mathbf{K}] = n$. In this case,

- we know how to compute the minimal polynomial over $\mathbf{K}$ of each element of $\mathbf{C}$;
- any intermediate finite $\mathbf{K}$-algebra $\mathbf{D}$ is strictly finite over $\mathbf{K}$;
- if moreover $\mathbf{D}$ is a field, $\mathbf{C}$ is strictly finite over $\mathbf{D}$ and we get the usual formula $[\mathbf{C} : \mathbf{K}] = [\mathbf{C} : \mathbf{D}][\mathbf{D} : \mathbf{K}]$.

Definition 1.3.3 (strictly étale algebras over a discrete field)**.**
Let $\mathbf{K}$ be a discrete field. A strictly finite $\mathbf{K}$-algebra $\mathbf{B}$ is *strictly étale* if the trace form $\phi(x, y) = \operatorname{Tr}_{\mathbf{B}/\mathbf{K}}(xy) \colon \mathbf{B} \times \mathbf{B} \to \mathbf{K}$ is *nondegenerate*, i.e. letting $\varphi(x) := \phi(x, \bullet)$, the $\mathbf{K}$-linear map φ defines an isomorphism from the $\mathbf{K}$-vector space $\mathbf{B}$ onto its dual.[5]

We state a first structure theorem for strictly étale $\mathbf{K}$-algebras. A constructive proof is given in Lombardi and Quitté 2015, Theorems VI-1.7 and VI-1.9. It shows in particular that strictly étale algebras over a discrete field are strictly finite étale algebras. Moreover Theorem 1.3.5 will show that étale algebras over a discrete field are strictly étale algebras.

Note that this constructive Theorem 1.3.4 is more precise than its classical counterpart, and the constructive proof is rather subtle. In fact, the hypotheses are given in a form that allows to obtain an algorithm for the conclusions.

Theorem 1.3.4 (primitive element theorem)**.** *Let* $\mathbf{K}$ *be a discrete field and* $\mathbf{B}$ *a strictly finite* $\mathbf{K}$*-algebra.*

1. *The following are equivalent.*
   - *(a)* $\mathbf{B}$ *is strictly étale.*
   - *(b)* $\mathbf{B}$ *is generated by elements which are separable over* $\mathbf{K}$*.*
   - *(c) All elements of* $\mathbf{B}$ *are separable over* $\mathbf{K}$*.*
   - *(d)* $\mathbf{B}$ *is isomorphic to a finite product of* $\mathbf{K}$*-algebras* $\mathbf{K}[X]/\langle h_i \rangle$ *with separable monic polynomials* h_i*.*

   In particular, strictly étale $\mathbf{K}$*-algebras are étale.*
2. *When* $\mathbf{B}$ *is a discrete field or* $\mathbf{K}$ *is infinite, the properties of Item 1 are equivalent to:*
   - *(e)* $\mathbf{B}$ *is isomorphic to a* $\mathbf{K}$*-algebra* $\mathbf{K}[\zeta] = \mathbf{K}[Z]/\langle g \rangle$*, where* g *is a separable monic polynomial in* $\mathbf{K}[Z]$*.*

[5]These definitions may be generalised to algebras over an arbitrary commutative ring (Lombardi and Quitté 2015, Theorem VI-5.5).

In the last case, if g is factorised as $g = g_1 \cdots g_r$, we have a canonical isomorphism $\mathbf{B} \simeq \prod_{j=1}^{r} \mathbf{K}[Z]/\langle g_j \rangle$.

An $\mathbf{A}$-algebra $\mathbf{B}$ is said to be *unramified* (or *neat*) if it is finitely presented and its *module of (Kähler) differentials* reduces to zero. The $\mathbf{B}$-module of differentials is isomorphic to the cokernel of the transpose of the Jacobian matrix (seen in $\mathbf{B}$). In other words, the module of differentials reduces to zero if and only if the transpose of the Jacobian matrix is surjective. It is clear that an étale algebra over an arbitrary commutative ring is unramified.

The following important theorem provides a strengthening of Theorem 1.3.4. Concerning the notion of simple isolated zero in this theorem, see the constructive approach in Lombardi and Quitté 2015, Section IX-4.

Theorem 1.3.5 (unramified algebra over a discrete field)**.**
Over a discrete field $\mathbf{K}$ *any unramified* $\mathbf{K}$*-algebra is strictly finite, étale, strictly étale. In particular, for an étale polynomial system, all zeroes of the corresponding variety in an algebraically closed overfield are isolated, simple, and with coordinates separable over* $\mathbf{K}$.

A constructive proof is in Lombardi and Quitté 2015, Corollary VI-6.15. In the second French edition Lombardi and Quitté 2021, a more elementary constructive proof is given at the end of Section VI-6.

We now give a more precise description of the situation.

Description 1.3.6 (étale polynomial system over a discrete field, precisions)**.**
Let $(\underline{f}) = (f_1, \ldots, f_n)$ be an étale polynomial system in $\mathbf{K}[X_1, \ldots, X_n]$ over an infinite discrete field $\mathbf{K}$[6] and let

$$\mathbf{D} = \mathbf{K}[\underline{X}] \big/ \langle \underline{f} \rangle = \mathbf{K}[x_1, \ldots, x_n]$$

be the quotient $\mathbf{K}$-algebra.

- We can construct a primitive element ζ of $\mathbf{D}$. Its minimal polynomial g over $\mathbf{K}$ is separable, so $\mathbf{D} = \mathbf{K}[z] \simeq \mathbf{K}[Z]/\langle g(Z) \rangle$. So we have polynomials $q_i \in \mathbf{K}[Z]$ such that $x_i = q_i(z)$ in $\mathbf{D}$.
- A zero $(\underline{\alpha}) = (\alpha_1, \ldots, \alpha_n)$ of the polynomial system in a $\mathbf{K}$-algebra $\mathbf{C}$ gives a $\mathbf{K}$-morphism $\varphi \colon \mathbf{D} \to \mathbf{K}[\underline{\alpha}] \subseteq \mathbf{C}$ satisfying $\varphi(\underline{x}) = (\underline{\alpha})$. The algebra $\mathbf{K}[\underline{\alpha}]$ is then isomorphic to a quotient of $\mathbf{D}$. If $\mathbf{K}[\underline{\alpha}]$ is connected and nontrivial, it is a discrete field, for it is zero-dimensional reduced (Lombardi and Quitté 2015, Fact IV-8.8).
- In the following we assume $\mathbf{K}[\underline{\alpha}]$ to be connected and nontrivial.
  - If we know a factorisation of g as a product of r irreducible polynomials g_j over $\mathbf{K}$, then $\mathbf{D} \simeq \mathbf{L}_1 \times \cdots \times \mathbf{L}_r$ with $\mathbf{L}_j \simeq \mathbf{D}/\langle g_j(z) \rangle$, and we get a corresponding fundamental system of orthogonal idempotents $(e_1(z), \ldots, e_r(z))$ in $\mathbf{D}$.[7] And $\mathbf{K}[\underline{\alpha}]$ is isomorphic to one of the discrete fields $\mathbf{L}_j$ via φ, with $\varphi(e_j(z)) = 1$.
  - Otherwise if $\mathbf{L}$ is a separable extension of $\mathbf{K}$ and g is completely factorised over $\mathbf{L}$, the quotient algebra seen over $\mathbf{L}$, i.e. $\mathbf{L} \otimes_{\mathbf{K}} \mathbf{D} \simeq \mathbf{L}[Z]/\langle g(Z) \rangle$, is isomorphic to $\mathbf{L}^d$, where $d = \deg(g)$. So the polynomial system has exactly d zeroes with coordinates in $\mathbf{L}$. If we embed $\mathbf{L} \subseteq \mathbf{K}^{\mathrm{sep}} \subseteq \mathbf{K}^{\mathrm{ac}}$ we get in this way all the zeroes with coordinates in $\mathbf{K}^{\mathrm{ac}}$.[8] ∎

What is going on in the more general situation where we don't know a factorisation of g over $\mathbf{K}$? This case is not very different from the preceding one. Indeed, if at a certain step we

[6] When $\mathbf{K}$ is finite, or more generally when we don't know whether it is infinite, slight modifications are to be introduced in this description, using Item *1.(d)* of Theorem 1.3.4. A valued field with a nontrivial valuation is always infinite.

[7] The ideal $\langle g_j(z) \rangle$ is generated by the idempotent $1 - e_j(z)$. The case $r = 0$ remains possible. An étale polynomial system may be impossible.

[8] Here $\mathbf{K}^{\mathrm{sep}}$ and $\mathbf{K}^{\mathrm{ac}}$ are respectively a separable and an algebraic closure of $\mathbf{K}$.

have found an idempotent $e \neq 0, 1$ in $\mathbf{D}$,[9] it is equal to 1 or 0 in $\mathbf{K}[\underline{\alpha}]$ and we can replace $\mathbf{D}$ with $\mathbf{D}[\frac{1}{e}]$ or $\mathbf{D}[\frac{1}{1-e}]$ (this amounts to replacing g with a strict divisor). The new algebra remains strictly étale. All previous computations remain valid, and the new version of g is better. The possible improvements of this type are bounded in number by $\deg(g)$. In consequence most of the concrete results obtained when we assume that we know a factorisation of g remain valid without this hypothesis. We are here at the heart of the dynamical method in algebra.

2 The case of ultrametric discrete fields

2.1 The henselisation of a valued discrete field

Valued discrete fields

First we recall the constructive definition of a *valued discrete field* $(\mathbf{K}, \mathbf{V})$ as in Kuhlmann and Lombardi 2000 or Coste, Lombardi, and Roy 2001:

- $\mathbf{K}$ is a discrete field;
- $\mathbf{V}$ is a subring of $\mathbf{K}$;
- for all $x \in \mathbf{K}^\times$ we have x or $1/x \in \mathbf{V}$;
- divisibility in $\mathbf{V}$ is explicit.[10]

In this case $\mathbf{V}$ is an integrally closed residually discrete local ring.

This definition is equivalent in classical mathematics to the usual one. We have added decidability hypotheses in order to facilitate computations.

Definition 2.1.1 (henselisation of a valued discrete field)**.**
Let $(\mathbf{K}, \mathbf{V})$ be a valued discrete field.

- An *extension* of $(\mathbf{K}, \mathbf{V})$ is a valued discrete field $(\mathbf{L}, \mathbf{W})$ together with a homomorphism $\phi\colon \mathbf{K} \to \mathbf{L}$ such that $\mathbf{V} = \mathbf{K} \cap \phi^{-1}(\mathbf{W})$.
- A *henselisation of* $(\mathbf{K}, \mathbf{V})$ is an extension which is a henselian valued discrete field $(\mathbf{K}^{\mathrm{H}}, \mathbf{V}^{\mathrm{H}})$ and such that the corresponding homomorphism $\phi^H : \mathbf{K} \to \mathbf{K}^{\mathrm{H}}$ factorises in a unique way through every extension of $(\mathbf{K}, \mathbf{V})$ which is a henselian valued discrete field.

Being the solution of a universal problem, a henselisation of a valued discrete field is unique up to unique isomorphism.

Kuhlmann and Lombardi (2000) construct the henselisation of a valued discrete field $(\mathbf{K}, \mathbf{V})$, denoted by $(\mathbf{K}^{\mathrm{H}}, \mathbf{V}^{\mathrm{H}})$. It is obtained by adding successively Hensel zeroes of Hensel polynomials.

In fact, given a Nagata polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ in $\mathbf{V}[X]$, the authors describe explicitly an extension $(\mathbf{K}[\alpha], \mathbf{V}_\alpha)$ of $(\mathbf{K}, \mathbf{V})$ for which the image of f in $\mathbf{K}[\alpha][X]$ has a henselian zero α, and such that the extension map $\mathbf{K} \to \mathbf{K}[\alpha]$ factorises in a unique way every extension of $(\mathbf{K}, \mathbf{V})$ to $(\mathbf{L}, \mathbf{W})$ for which the image of f in $\mathbf{L}[X]$ has a henselian zero. Furthermore, the residue field and the value group of $(\mathbf{K}[\alpha], \mathbf{V}_\alpha)$ are canonically isomorphic to the residue field and the value group of $(\mathbf{K}, \mathbf{V})$, respectively. This explicit construction is based on the study of the *Newton polygon* of f. Note that we do not assume to know whether the base field contains a special zero of f. So, the finite extension $\mathbf{K}[\alpha]$ which is constructed is a discrete field but it is not necessarily a strictly finite extension of $\mathbf{K}$. The construction of the henselisation of a valued discrete field is very similar in its rigid but hesitating character to the

[9] This happens each time an element $\neq 0$ of $\mathbf{D}$ is not invertible, i.e. when its minimal polynomial has degree > 1 and its constant coefficient is zero.

[10] This means that for $x, y \in \mathbf{V}$ we have a test for the existence of a $z \in \mathbf{V}$ such that $yz = x$. This amounts to saying that $\mathbf{V}$ is a detachable subring of $\mathbf{K}$. This is always true in classical mathematics by the Law of Excluded Middle.

construction of the real closure of discrete ordered field, which works even when we are not able to decide whether an arbitrary polynomial has a zero in the base field (compare Lombardi and Roy 1991, Section 3.2, proof of Proposition 1).

Remark 2.1.2. We point out that, even though the construction of the henselisation of a valued field given in Kuhlmann and Lombardi (2000) is similar to the construction of the henselisation of a local ring, the tools used in the two cases are different. In fact, the first one takes entirely place in the framework of valued discrete fields and is a priori less general than the construction in the framework of residually discrete local rings given in Alonso García, Lombardi, and Perdry 2008. So, a priori we should use two distinct notations for these two henselisations, namely $\mathbf{V}^{\mathrm{h}}$ (henselisation as local ring) and $\mathbf{V}^{\mathrm{H}}$ (valuation ring of the henselisation of the valued field). Although the nonobvious fact that they coincide seems to be accepted, we have not found a proof in the literature (but see Alonso García, Lombardi, and Neuwirth 2024). ■

2.2 Ultrametric fields

In the book Mines, Richman, and Ruitenburg 1988, the theory of absolute values is treated constructively using the following definition which is the usual one in classical mathematics for fields with an absolute value.[11]

Definition 2.2.1 (field with an absolute value, ultrametric field)**.**

1. An *absolute value* over a ring $\mathbf{K}$ is a function $\mathbf{K} \to \mathbb{R}^{\geqslant 0}$, $x \mapsto |x|$ satisfying the following properties.

   - $|x| = 0$ if and only if $x = 0$;
   - $|x| > 0$ if and only if x is invertible;
   - $|xy| = |x||y|$;
   - $|x + y| \leqslant |x| + |y|$.

   One says that $(\mathbf{K}, |\cdot|)$ is a *field with an absolute value.*[12]

2. The absolute value is said to be *ultrametric* if $|x + y| \leqslant \sup(|x|, |y|)$ for all x, y.[13] In this case we speak of an *ultrametric field.* Note that if $|x| < |y|$ then $|x + y| = |y|$.

3. An ultrametric absolute value defines a "valuation domain" $\mathbf{V}$:

$$\begin{cases} \mathbf{V} & := \{\, x \in \mathbf{K} \,;\, |x| \leqslant 1 \,\}, \text{ with} \\ \mathbf{V}^{\times} & := \{\, x \in \mathbf{K} \,;\, |x| = 1 \,\} \text{ and} \\ \mathfrak{m} & := \mathrm{Rad}(\mathbf{V}) = \{\, x \in \mathbf{K} \,;\, |x| < 1 \,\}. \end{cases}$$

4. Two nontrivial ultrametric absolute values on $\mathbf{K}$ defining the same valuation domain are said to be *equivalent*, and each is a positive power of the other (see Mines, Richman, and Ruitenburg 1988, Theorem XII-1.2).

5. The distance $d(x, y) = |x - y|$ makes $\mathbf{K}$ a metric space, whose completion is denoted by $\widehat{\mathbf{K}}$. The absolute value extends uniquely to $\widehat{\mathbf{K}}$, and $(\widehat{\mathbf{K}}, |\cdot|)$ is also an ultrametric field[14]. The completions of $\mathbf{V}$ and $\mathfrak{m}$ are denoted by $\widehat{\mathbf{V}}$ and $\widehat{\mathfrak{m}}$. The image of $\mathbf{K}^{\times}$ in $(\mathbb{R}^{>0}, \times)$ is the *value group* of $(\mathbf{K}, |\cdot|)$.

[11] In fact, they start with a Heyting field $\mathbf{K}$, but the two definitions are clearly equivalent. In classical mathematics one starts also usually with $\mathbf{K}$ a discrete field.

[12] The book Mines, Richman, and Ruitenburg 1988 uses "valued field", as very often in the English literature, but this is in conflict with our terminology for general valued discrete fields, which follows Krull and Bourbaki.

[13] Note that from a constructive viewpoint, $z = \sup(x, y)$ is well defined for real numbers, but it cannot be proved that $z = x$ or $z = y$ with an explicit "or".

[14] In the archimedean case, $(\widehat{\mathbf{K}}, |\cdot|)$ is also a field with an absolute value.

A field with an absolute value $\mathbf{K}$ is a nontrivial local ring whose Jacobson radical is reduced to 0, i.e. a *Heyting field*.[15]

The definition does not require $\mathbf{K}$ to be a discrete field. In general the completion $\widehat{\mathbf{K}}$ is not discrete even when $\mathbf{K}$ is discrete.

Remark 2.2.2. In Item 4 we have put "valuation domain" in quotation marks because $\mathbf{V}$ needs not, from the constructive viewpoint, be a local ring, nor discrete, nor residually discrete.

Let us consider an ultrametric field $(\mathbf{K}, |\cdot|)$.

The Heyting field $\mathbf{K}$ is discrete if and only if for all $x \in \mathbf{K}$ we have the disjunction "$|x| = 0$ or $|x| > 0$". This amounts to saying that $\mathbf{V}$ is an integral domain.

The pair $(\mathbf{K}, \mathbf{V})$ is a valued discrete field in the constructive meaning if moreover the disjunction "$|x| = 1$ or $|x| < 1$ or $|x| > 1$" is valid for all $x \in \mathbf{K}$.

This amounts to saying that $\mathbf{V}$ is an integral residually discrete local ring. In this case we say that $(\mathbf{K}, |\cdot|)$ is an *ultrametric discrete field*.

Translation in terms of valuations

Let us consider the map $\ell\colon (\mathbb{R}^{\geqslant 0}, \times) \to (\mathbb{R} \cup \{+\infty\}, +)$ defined by $\ell(r) = -\log(r)$ for $r \neq 0$ and by $\ell(0) = +\infty$; endow $\mathbb{R} \cup \{+\infty\}$ with the topology that makes ℓ a homeomorphism. For an ultrametric field we define the valuation $v\colon \mathbf{K} \to (\mathbb{R} \cup \{+\infty\}, +)$ by $v(x) = \ell(|x|)$. We simply translate the properties of $(x \mapsto |x|, \mathbf{K} \to \mathbb{R}^{\geqslant 0})$ into properties of v, reversing the order relation, replacing multiplication with addition and sup with inf. This gives the following properties:

- $v(x) = \infty$ if and only if $x = 0$;
- $v(x) \neq \infty$ if and only if x is invertible;
- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geqslant \inf(v(x), v(y))$, with equality if $v(x) \neq v(y)$;
- $v(x) \geqslant 0$ if and only if $x \in \mathbf{V}$;
- $v(x) > 0$ if and only if $x \in \mathfrak{m}$.

When replacing the absolute value with an equivalent absolute value, the valuation v is simply multiplied by a constant $r > 0$.

For an ultrametric discrete field, $\mathbf{K}$ and the residual ring $\mathbf{V}/\mathfrak{m}$ are discrete fields, the subgroup $\{\, |x| \,;\, x \in \mathbf{K}^\times \,\}$ is a discrete multiplicative subgroup Δ of $\mathbb{R}^{\geqslant 0}$, $\Gamma = \{\, v(x) \,;\, x \in \mathbf{K}^\times \,\}$ is a discrete additive subgroup of $(\mathbb{R}, +)$, and the union $\Gamma \cup \{+\infty\}$ is a disjoint union: the topology is discrete.

In this case, we have the following useful result, also valid for general valued discrete fields:

- if $\sum_{i=1}^{n} x_i = 0$, with the x_i's not all zero, the infimum of the $v(x_i)$'s is attained at least for two distinct i.

Three basic examples

In constructive mathematics we define a *discrete valuation ring* (a DVR in short) as an integral domain $\mathbf{V}$ (with field of fractions $\mathbf{K}$) in which we give an element $\pi \neq 0$ (called a *regular parameter*) such that each element of $\mathbf{V}^*$ is written as $a = u\pi^k$ with $u \in \mathbf{V}^\times$ and $k \in \mathbb{N}$. This makes $(\mathbf{K}, \mathbf{V})$ a valued discrete field with valuation $v(a) = k$. Letting $|u\pi^k| = e^{-k}$ for a fixed real number $e > 0$, $(\mathbf{K}, |\cdot|)$ is an ultrametric discrete field.

Three basic examples are now given. In Examples 2 and 3, the absolute value is not in $\mathbb{R}^{\geqslant 0}$ but in a submonoid of $(\mathbf{K}, \times)$ isomorphic to the closure of $\{\, 1/2^n \,;\, n \in \mathbb{N} \,\}$ in $\mathbb{R}^{\geqslant 0}$.

[15] The ring $\mathbf{K}$ is not necessarily a discrete field. So we have given the definition for a ring $\mathbf{K}$. This avoids to recall first the definition of a Heyting field.

1. Here $\mathbf{K} = \mathbb{Q}$, the standard p-adic absolute value is $|r|_p = p^{-k}$ if $r = \frac{m}{n} p^k$ with m and $n \in \mathbb{Z}$ coprime with p. The corresponding discrete valuation ring is $\mathbf{V} = \mathbb{Z}_{1+p\mathbb{Z}}$ (the ring $\mathbb{Z}$ localised at the prime $\langle p \rangle$) with $\operatorname{Rad} \mathbf{V} = p\mathbf{V}$, the regular parameter is p, and the residual field is $\mathbb{F}_p$.

2. Here $\mathbf{K} = \mathbb{Q}(t)$, the standard t-adic absolute value is $|r|_t = t^{-k}$ if $r = \frac{m}{n} t^k$ with $m, n \in \mathbb{Q}[t]$, $m(0)$ and $n(0) \neq 0$ in $\mathbb{Q}$. The corresponding discrete valuation ring is $\mathbf{V} = (\mathbb{Q}[t])_{1+t\mathbb{Q}[t]}$ (the ring $\mathbb{Q}[t]$ localised at the prime $\langle t \rangle$) with $\operatorname{Rad} \mathbf{V} = t\mathbf{V}$, the regular parameter is t, and the residual field is $\mathbb{Q}$.

3. Here $\mathbf{K} = \mathbb{F}_p(t)$, the standard t-adic absolute value is $|r|_t = t^{-k}$ if $r = \frac{m}{n} t^k$ with $m, n \in \mathbb{F}_p[t]$, $m(0)$ and $n(0) \neq 0$ in $\mathbb{F}_p$. The corresponding discrete valuation ring is $\mathbf{V} = (\mathbb{F}_p[t])_{1+t\mathbb{F}_p[t]}$ (the ring $\mathbb{F}_p[t]$ localised at the prime $\langle t \rangle$) with $\operatorname{Rad} \mathbf{V} = t\mathbf{V}$, the regular parameter is t, and the residual field is $\mathbb{F}_p$.

In the second example, the field $\mathbb{Q}$ may be replaced with an arbitrary discrete field (as in the third example).

2.3 The Multivariate Hensel Lemma for ultrametric discrete fields

A crucial result in Mines, Richman, and Ruitenburg 1988 and a simpler proof

Notation 2.3.1. Let $(\mathbf{K}, |\cdot|)$ be an ultrametric field with a nontrivial absolute value.[16] We let

- $\widetilde{\mathbf{K}}$ be the separable closure of $\mathbf{K}$ in its completion $\widehat{\mathbf{K}}$,
- $\widetilde{\mathbf{V}} = \{\, x \in \widetilde{\mathbf{K}} \,;\, |x| \leqslant 1 \,\}$ be its "valuation ring", and
- $\widetilde{\mathfrak{m}} = \{\, x \in \widetilde{\mathbf{K}} \,;\, |x| < 1 \,\}$.

Mines, Richman, and Ruitenburg (1988) prove that for an ultrametric discrete field $(\mathbf{K}, |\cdot|)$, $(\widetilde{\mathbf{K}}, \widetilde{\mathbf{V}})$ is a henselian valued discrete field with the usual meaning (any Hensel polynomial has a Hensel zero).

The proof of this result is rather complicated because Mines, Richman, and Ruitenburg (1988) prove general results concerning the nondiscrete case. Therefore we consider appropriate to include here a simpler proof of the result, which is provided by the following two lemmas.

Lemma 2.3.2. *Let $(\mathbf{K}, |\cdot|)$ be an ultrametric discrete field.*

1. *Then $(\widehat{\mathbf{K}}, |\cdot|)$ is an ultrametric field, $\widehat{\mathbf{V}}$ is a local ring with Jacobson radical $\widehat{\mathfrak{m}}$, and the residual ring $\widehat{\mathbf{V}}/\widehat{\mathfrak{m}}$ is isomorphic to $\mathbf{V}/\mathfrak{m}$ (it is a discrete field).*

2. *The local ring $(\widehat{\mathbf{V}}, \widehat{\mathfrak{m}})$ is henselian. More generally any Newton polynomial system $(f_1, \dots, f_n) \in \widehat{\mathbf{V}}[\underline{X}]^n$ at $(a_1, \dots, a_n) \in \widehat{\mathbf{V}}^n$ has a zero $(\xi_1, \dots, \xi_n)$ with $\xi_k \in a_k + \widehat{\mathfrak{m}}$ $(k \in [\![1..n]\!])$.*

Proof. The first item is easy. So $\widehat{\mathbf{K}}$ is a Heyting field, a fortiori a local ring. The second item is Corollary 1.2.2, a consequence of Newton's method explained in Theorem 1.2.1. □

Lemma 2.3.3. *The elements of $\widetilde{\mathbf{K}}$ form a discrete subring of $\widehat{\mathbf{K}}$ and $(\widetilde{\mathbf{K}}, |\cdot|)$ is a henselian ultrametric discrete field.*

Proof. The fact that $\widetilde{\mathbf{K}}$ is a subring is classical. Let us now consider an element $\xi \in \widehat{\mathbf{K}}$ annihilating a separable polynomial $f \in \mathbf{K}[X]$. We let $\mathbf{K}[x] = \mathbf{K}[X]/\langle f \rangle$. We have a $\mathbf{K}$-algebra morphism $\varphi\colon \mathbf{K}[x] \to \mathbf{K}[\xi]$ satisfying $\varphi(x) = \xi$. As $\mathbf{K}[\xi]$ is connected (it is a subring of the local ring $\widehat{\mathbf{K}}$), it is a discrete field as quotient of a strictly étale $\mathbf{K}$-algebra: a connected zero-dimensional reduced ring is a discrete field (Lombardi and Quitté 2015, Fact IV-8.8). So $\widetilde{\mathbf{K}}$ is a discrete field. □

[16] I.e. there exists an x such that $|x| \neq 0, 1$.

Multivariate Hensel Lemma (Ostrowski version)

Theorem 2.3.4 (Multivariate Hensel Lemma for an ultrametric discrete field, Ostrowski version)**.** *Let* $(\mathbf{K}, |\cdot|)$ *be an ultrametric discrete field and* $(f_1, \ldots, f_n)$ *a Newton polynomial system at* $(\underline{0})$ *over* $(\mathbf{K}, \mathbf{V})$*. This system admits a unique zero with coordinates in* $\widetilde{\mathfrak{m}}$*.*

Proof. We assume that the Newton polynomial system is étale (Lemma 1.3.2). Newton's method constructs a zero $(\underline{\alpha})$ with coordinates in $\widehat{\mathfrak{m}} \subseteq \widehat{\mathbf{K}}$ (Corollary 1.2.2). We let $\mathbf{D} = \mathbf{K}[x_1, \ldots, x_n] = \mathbf{K}[X_1, \ldots, X_n]/\langle f_1, \ldots, f_n \rangle$ be the quotient $\mathbf{K}$-algebra of the polynomial system. It is strictly finite, strictly étale (see Theorem 1.3.5). We have the natural morphism of $\mathbf{K}$-algebras $\varphi \colon \mathbf{D} \to \mathbf{K}[\underline{\alpha}] \subseteq \widehat{\mathbf{K}}$, where $(\underline{\alpha})$ is the Hensel zero of the polynomial system ($\varphi(x_i) = \alpha_i$ for each i). So the α_i's are separable over $\mathbf{K}$. By Theorem 1.3.4, for each i, $\alpha_i \in \widetilde{\mathbf{K}}$ and $v(\alpha_i) > 0$: the coordinates of $(\underline{\alpha})$ are in $\widetilde{\mathfrak{m}}$. □

2.4 The isomorphism between two variations on henselisation

First we recall a variant in the Hensel-Newton style of Hensel's Lemma for univariate polynomials (Lang 2002, Proposition XII-7.6). It works for all henselian valued discrete fields.

Lemma 2.4.1 (Hensel-Newton Lemma for valued discrete fields)**.**
Let $(\mathbf{K}, \mathbf{V})$ *be a valued discrete field. We let* $v \colon \mathbf{K} \to \Gamma \cup \{+\infty\}$ *be the associated valuation. Let* $F(x) = \sum_{k=0}^{n} a_k x^k \in \mathbf{V}[x]$ *with* $a_1 \neq 0$ *and* $v(a_0) > 2v(a_1)$*.*

1. *The polynomial* F *has a zero in* $\frac{a_0}{a_1} \cdot \mathbf{V}^{\mathrm{H}} \subseteq a_1 \cdot \mathfrak{m}\mathbf{V}^{\mathrm{H}}$*, and it is the unique zero of* F *in* $a_1 \cdot \mathfrak{m}\mathbf{V}^{\mathrm{H}}$*.*

2. *In particular if* $(\mathbf{K}, \mathbf{V})$ *is henselian,* F *has a zero* $\xi \in \frac{a_0}{a_1} \cdot \mathbf{V} \subseteq a_1 \cdot \mathfrak{m}$*, and it is the unique zero of* F *in* $a_1 \cdot \mathfrak{m}$*.*

Proof. Let us consider the polynomial

$$f(x) = \frac{1}{a_1^2} F(a_1 x) = \frac{a_0}{a_1^2} + X + \sum\nolimits_{k=2}^{n} a_k a_1^{k-2} X^k.$$

The hypotheses of Hervé's trick (Lemma 1.0.1) are satisfied, so the polynomial f has a zero $\zeta \in \frac{a_0}{a_1^2} \cdot \mathbf{V}^{\mathrm{H}} \subseteq \mathfrak{m}\mathbf{V}^{\mathrm{H}}$, and it is the unique zero of f in $\mathfrak{m}\mathbf{V}^{\mathrm{H}}$. This yields the zero $\xi = a_1\zeta$ of F in the ideal $\frac{a_0}{a_1} \cdot \mathbf{V}^{\mathrm{H}} \subseteq a_1 \cdot \mathfrak{m}\mathbf{V}^{\mathrm{H}}$, and it is the unique zero of F in $a_1 \cdot \mathfrak{m}\mathbf{V}^{\mathrm{H}}$. □

Rereading the proof of Lemma 1.0.1, we see that the computation shows that ζ is in the image of an initial stage of the construction of the henselisation $\mathbf{V}^{\mathrm{h}}$, obtained by adding the special zero of a special polynomial, but ζ itself is not necessarily a Hensel zero of a Hensel code. Moreover $v(\zeta) > 0$.

Theorem 2.4.2 (two equivalent versions of the henselisation of an ultrametric discrete field)**.**
Let $(\mathbf{K}, |\cdot|)$ *be an ultrametric discrete field.*

1. *The henselisation* $(\mathbf{K}^{\mathrm{H}}, \mathbf{V}^{\mathrm{H}})$ *of* $(\mathbf{K}, \mathbf{V})$ *constructed as in Kuhlmann and Lombardi 2000 is isomorphic to* $(\widetilde{\mathbf{K}}, \widetilde{\mathbf{V}})$*.*

More precisely,

1. *there exists a unique* $\mathbf{K}$*-homomorphism* $\mathbf{K}^{\mathrm{H}} \to \widetilde{\mathbf{K}}$ *sending* $\mathbf{V}^{\mathrm{H}}$ *into* $\widetilde{\mathbf{V}}$*, and this homomorphism is an isomorphism;*

2. *the natural morphism* $\mathbf{V}^{\mathrm{h}} \to \widetilde{\mathbf{V}}$ *is onto (so that the morphism* $\mathbf{V}^{\mathrm{H}} \to \widetilde{\mathbf{V}}$ *is an isomorphism).*

Proof. Since $(\widetilde{\mathbf{K}}, \widetilde{\mathbf{V}})$ is a henselian valued discrete field extension of $(\mathbf{K}, \mathbf{V})$, we have a unique $(\mathbf{K}, \mathbf{V})$-morphism $\varphi\colon (\mathbf{K}^{\mathrm{H}}, \mathbf{V}^{\mathrm{H}}) \to (\widetilde{\mathbf{K}}, \widetilde{\mathbf{V}})$. It is injective because $\mathbf{K}^{\mathrm{H}}$ is a discrete field and $\widetilde{\mathbf{K}}$ is not trivial. We have to show that φ is surjective.

It is sufficient to prove that $\varphi(\mathbf{V}^{\mathrm{h}}) = \widetilde{\mathbf{V}}$, i.e. Item *2.*[17]

We call v the valuation of $\widehat{\mathbf{K}}$. Let us consider an element $\xi \in \widetilde{\mathbf{V}}$: $\xi \in \widehat{\mathbf{K}}$, $v(\xi) \geqslant 0$, and $f(\xi) = 0$ for a polynomial $f \in \mathbf{V}[X]$ which is separable in $\mathbf{K}[X]$. In particular $f'(\xi) \neq 0$, i.e. $v(f'(\xi)) < +\infty$.

Since $\xi \in \widehat{\mathbf{K}}$ we know arbitrarily precise approximations of ξ in $\mathbf{K}$, i.e. written as $a = \xi + \zeta \in \mathbf{K}$ with $v(\zeta) \geqslant 0$ arbitrarily large. Since $v(\xi) \geqslant 0$, we have $v(a) \geqslant 0$.

For such an a we consider the polynomial $F_a(X) = f(-X + a) \in \mathbf{V}[X]$. The coefficient $c_0 = F_a(0) = f(a)$ is an arbitrarily precise approximation of $f(\xi) = 0$, i.e. $v(c_0)$ is arbitrarily large. The coefficient $c_1 = F_a'(0) = f'(a)$ is an arbitrarily precise approximation of $f'(\xi)$, so for $v(\zeta)$ sufficiently large $v(c_1) = v(f'(a)) = v(f'(\xi)) < +\infty$. For $v(\zeta)$ sufficiently large we get $v(c_0) > 2v(c_1)$. Lemma 2.4.1 says that F_a has a zero $\alpha \in \frac{c_0}{c_1} \cdot \mathbf{V}^{\mathrm{H}} \subseteq c_1 \cdot \mathfrak{m}\mathbf{V}^{\mathrm{H}}$.

The image of α in $\widetilde{\mathbf{K}}$ is equal to ζ, for these are two Hensel zeroes in $\widetilde{\mathbf{K}}$ for the same Hensel code $(F_a, 0)$. So the image of $a - \alpha \in \mathbf{V}^{\mathrm{h}}$ is $a - \zeta = \xi$. Moreover, as explained just after Lemma 2.4.1, ξ is also in the range of the natural morphism $\mathbf{V}^{\mathrm{h}} \to \widetilde{\mathbf{V}}$. □

So we have got that any element of $\widetilde{\mathbf{K}}$ is precisely the image of an element γ belonging to a field $\mathbf{K}[\xi] \subseteq \mathbf{K}^{\mathrm{H}}$, where ξ is the special zero of a special polynomial. Since $\mathbf{K}^{\mathrm{H}} \simeq \widetilde{\mathbf{K}}$, this implies that any element of $\mathbf{K}^{\mathrm{H}}$ can be obtained as an element at the first stage of some construction of $\mathbf{K}^{\mathrm{H}}$. This result was not clear a priori in Kuhlmann and Lombardi 2000 (but there the valued discrete field is arbitrary).

Multivariate Hensel Lemma

Now we get the desired result.

Theorem 2.4.3 (Multivariate Hensel Lemma for an ultrametric discrete field)**.**
Let $(\mathbf{K}, |\cdot|)$ be an ultrametric discrete field and $(f_1, \dots, f_n)$ a Newton polynomial system at $(\underline{0})$ over $(\mathbf{K}, \mathbf{V})$. This system admits a unique zero with coordinates in $\mathfrak{m}\mathbf{V}^{\mathrm{H}}$.

Proof. This follows from Theorem 2.3.4 because we have proved (Theorem 2.4.2) that $\widetilde{\mathbf{V}}$ is canonically isomorphic to $\mathbf{V}^{\mathrm{H}}$. The elements in $\mathbf{V}^{\mathrm{H}}$ that correspond to the α_i's give the Hensel zero of the polynomial system with coordinates in $\mathfrak{m}\mathbf{V}^{\mathrm{H}}$. □

Note that according to Description 1.3.6, since the $\mathbf{K}$-algebra $\mathbf{K}[\underline{\alpha}]$ is connected nontrivial, $\mathbf{K}[\underline{\alpha}]$ is a discrete field isomorphic to a quotient of $\mathbf{D}$, but it seems that there is no general algorithm for determining the dimension of $\mathbf{K}[\underline{\alpha}]$ as $\mathbf{K}$-vector space.

Final remark. Note that many classical texts using variants of Multivariate Hensel Lemma as e.g. Fisher (1997) and Smart (1998) give the solution under the form of zeroes with coordinates in some completion of the local ring, and not in the henselisation of the local ring.
The papers Kuhlmann (2011) and Priess-Crampe and Ribenboim (2000) give a nonalgorithmic solution by using the notion of spherically complete field. Their proofs are very difficult to interpret constructively.

References

María Emilia Alonso García, Henri Lombardi, and Hervé Perdry. Elementary constructive theory of Henselian local rings. *Math. Log. Q.*, 54:253–271, 2008. doi:10.1002/malq.200710057. 2, 4, 10

[17] Note that we ignore whether the morphism $\mathbf{V}^{\mathrm{h}} \to \widetilde{\mathbf{V}}$ is injective; in particular, we ignore whether $\mathbf{V}^{\mathrm{h}}$ is an integral domain (but see Alonso García, Lombardi, and Neuwirth 2024).

María Emilia Alonso García, Thierry Coquand, and Henri Lombardi. Revisiting Zariski main theorem from a constructive viewpoint. *J. Algebra*, 406:46–68, 2014. doi:10.1016/j.jalgebra.2014.02.003. 2

María Emilia Alonso García, Henri Lombardi, and Stefan Neuwirth. On a theorem by de Felipe and Teissier about the comparison of two henselisations in the non-Noetherian case. *J. Algebra*, 570:587–594, 2021. doi:10.1016/j.jalgebra.2020.11.020. 2

María Emilia Alonso García, Henri Lombardi, and Stefan Neuwirth. Note on the coincidence of two henselisations. 2024. URL `http://arxiv.org/abs/2411.18186`. 10, 14

Gorô Azumaya. On maximally central algebras. *Nagoya Math. J.*, 2:119–150, 1951. doi:10.1017/S0027763000010114. 2

Errett Bishop. *Foundations of constructive analysis*. McGraw-Hill, New York, 1967. 2

Errett Bishop and Douglas Bridges. *Constructive analysis*. Grundlehren der mathematischen Wissenschaften, 279. Springer-Verlag, Berlin, 1985. doi:10.1007/978-3-642-61667-9. 2

Nicolas Bourbaki. *Commutative algebra*. Elements of mathematics. Hermann, Paris, 1972. Translated from the French. 2

Douglas Bridges and Fred Richman. *Varieties of constructive mathematics*. London Mathematical Society Lecture Note Series, 97. Cambridge University Press, Cambridge, 1987. doi:10.1017/CBO9780511565663. 2

Thierry Coquand and Henri Lombardi. Anneaux à diviseurs et anneaux de Krull (une approche constructive). *Comm. Algebra*, 44:515–567, 2016a. doi:10.1080/00927872.2014.975346. 2

Thierry Coquand and Henri Lombardi. Some remarks about normal rings. In *Concepts of proof in mathematics, philosophy, and computer science*. Ontos Mathematical Logic, 6, pages 141–149. De Gruyter, Berlin, 2016b. 2

Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra: effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111:203–256, 2001. doi:10.1016/S0168-0072(01)00026-4. 2, 9

Max Deuring. Verzweigungstheorie bewerteter Körper. *Math. Ann.*, 105:277–307, 1931. doi:10.1007/BF01455820. 2

Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer, Berlin, 2005. doi:10.1007/3-540-30035-X. 2

Benji Fisher. A note on Hensel's lemma in several variables. *Proc. Am. Math. Soc.*, 125:3185–3189, 1997. doi:10.1090/S0002-9939-97-04112-9. 14

Wolfgang Krull. Galoissche Theorie bewerteter Körper. *Sitzungsberichte der mathematisch-naturwissenschaftlichen Abteilung der Bayerischen Akademie der Wissenschaften zu München*, 1930:225–238, 1930. 2

Franz-Viktor Kuhlmann. Maps on ultrametric spaces, Hensel's lemma, and differential equations over valued fields. *Commun. Algebra*, 39:1730–1776, 2011. doi:10.1080/00927871003789157. 14

Franz-Viktor Kuhlmann and Henri Lombardi. Construction du hensélisé d'un corps valué. *J. Algebra*, 228(2):624–632, 2000. 2, 9, 10, 13, 14

Franz-Viktor Kuhlmann, Henri Lombardi, and Hervé Perdry. Dynamic computations inside the algebraic closure of a valued field. In Franz-Viktor Kuhlmann, Salma Kuhlmann, and Murray Marshall, editors, *Valuation theory and its applications. Volume II. Proceedings of the international conference and workshop, University of Saskatchewan, Saskatoon, Canada, July 28–August 11, 1999*. Fields Institute Communications, 33, pages 133–156. American Mathematical Society, Providence, 2003. 2

Jean-Pierre Lafon. Anneaux henséliens. *Bull. Soc. Math. Fr.*, 91:77–107, 1963. doi:10.24033/bsmf.1590. 5

Serge Lang. *Algebra*. Graduate Texts in Mathematics, 211. Springer, New York, 3rd revised edition, 2002. 13

Henri Lombardi and Assia Mahboubi. Valuative lattices and spectra. In Jean-Luc Chabert, Marco Fontana, Sophie Frisch, Sarah Glaz, and Keith Johnson, editors, *Algebraic, number theoretic, and topological aspects of ring theory*, pages 275–341. Springer, Cham, 2023. doi:10.1007/978-3-031-28847-0_17. URL http://arxiv.org/abs/2210.16558. 2

Henri Lombardi and Claude Quitté. *Commutative algebra: constructive methods. Finite projective modules.* Algebra and applications, 20. Springer, Dordrecht, 2015. doi:10.1007/978-94-017-9944-7. Translated from the French (Calvage & Mounet, Paris, 2011, revised and extended by the authors) by Tania K. Roblot. URL https://arxiv.org/abs/1605.04832. 2, 5, 7, 8, 12

Henri Lombardi and Claude Quitté. *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini. Cours et exercices.* Paris: Calvage & Mounet, 2021. Revised and extended edition of a book originally published in 2011. 2, 8

Henri Lombardi and Marie-Françoise Roy. Elementary constructive theory of ordered fields. In Teo Mora and Carlo Traverso, editors, *Effective methods in algebraic geometry: papers from the symposium (MEGA-90) held in Castiglioncello, April 17–21, 1990*, pages 249–262. Birkhäuser, Boston, 1991. 10

Ray Mines, Fred Richman, and Wim Ruitenburg. *A course in constructive algebra.* Universitext. Springer-Verlag, New York, 1988. doi:10.1007/978-1-4419-8640-5. 1, 2, 10, 12

Masayoshi Nagata. On the theory of Henselian rings. *Nagoya Math. J.*, 5:45–57, 1953. 2

Masayoshi Nagata. *Local rings.* Interscience Tracts in Pure and Applied Mathematics, 13. Interscience Publishers, New York, 1962. 2

Alexander Ostrowski. Untersuchungen zur arithmetischen Theorie der Körper. (Die Theorie der Teilbarkeit in allgemeinen Körpern. I-III.). *Math. Z.*, 39:269–404, 1934. URL http://eudml.org/doc/168554, http://eudml.org/doc/168555.2

Sibylla Priess-Crampe and Paulo Ribenboim. A general Hensel's lemma. *J. Algebra*, 232:269–281, 2000. doi:10.1006/jabr.2000.8401. 14

Peter Roquette. History of valuation theory. I. In Franz-Viktor Kuhlmann, Salma Kuhlmann, and Murray Marshall, editors, *Valuation theory and its applications. Volume I. Proceedings of the international conference and workshop, University of Saskatchewan, Saskatoon, Canada, July 28–August 11, 1999.* Fields Institute Communications, 32, pages 291–355. American Mathematical Society, Providence, 2002. 2

Nigel P. Smart. *The algorithmic resolution of Diophantine equations.* London Mathematical Society Student Texts, 41. Cambridge: Cambridge University Press, 1998. 14

Stacks Project Authors. *Stacks Project.* https://stacks.math.columbia.edu, 2022. 5

Ihsen Yengui. *Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases.* Lecture Notes in Mathematics, 2138. Springer, Cham, 2015. doi:10.1007/978-3-319-19494-3. 2