UNIVERSITY OF CALIFORNIA

Los Angeles

Uniform Properties of Ideals in Rings of Restricted Power Series

A dissertation submitted in partial satisfaction
of the requirements for the degree
Doctor of Philosophy in Mathematics

by

Madeline Grace Barnicle

2019

ABSTRACT OF THE DISSERTATION

Uniform Properties of Ideals in
Rings of Restricted Power Series

by

Madeline Grace Barnicle
Doctor of Philosophy in Mathematics
University of California, Los Angeles, 2019
Professor Matthias J. Aschenbrenner, Chair

When is an ideal of a ring radical or prime? By examining its generators, one may in many cases definably and uniformly test the ideal's properties. We seek to establish such definable formulas in rings of p-adic power series, such as $\mathbb{Q}_p\langle X\rangle$, $\mathbb{Z}_p\langle X\rangle$, and related rings of power series over more general valuation rings and their fraction fields. We obtain a definable, uniform test for radicality, and, in the one-dimensional case, for primality. This builds upon the techniques stemming from the proof of the quantifier elimination results for the analytic theory of the p-adic integers by Denef and van den Dries, and the linear algebra methods of Hermann and Seidenberg.

The dissertation of Madeline Grace Barnicle is approved.

Igor Pak

Richard S. Elman

Artem Chernikov

Matthias J. Aschenbrenner, Committee Chair

University of California, Los Angeles

2019

To my parents

TABLE OF CONTENTS

1 Introduction **1**

2 Preliminaries **14**

2.1 Rings of Restricted Power Series 14

2.2 Parametric Weierstrass Preparation 18

2.3 Weierstrass Division for Nonstandard Restricted Power Series 29

I Uniform Basic Ideal Theory 37

3 Hermann's Method and Generalizations **38**

3.1 Hermann's Method 38

3.2 Hermann's Method for Restricted Power Series 44

3.3 Uniform Linear Algebra 49

4 Uniform Noether Normalization and Uniform Noetherianity **59**

4.1 Weierstrass Sequences 59

4.2 Uniform Noether Normalization 68

4.3 Uniform Noetherianity 73

II Detecting Radical Ideals 78

5 Radicals in Rings of Restricted Power Series **79**

5.1 Radicals in Polynomial Rings over Perfect Fields 79

5.2 Radicals in $\mathbb{Q}_p\langle X\rangle$ 83

5.3 Radical ideals in $\mathbb{Z}_p\langle X\rangle$ 87

III Defining Primality **90**

6 Newton, Hensel, and Dedekind **91**

6.1 The Newton-Hensel Lemma 91

6.2 Valuation-Theoretic Preliminaries 103

7 Prime Ideals **110**

7.1 Prime Ideals in Polynomial Rings over Perfect Fields 111

7.2 Solving Polynomial Equations in $\mathbb{Q}_p\langle X\rangle$ 116

7.3 Prime Ideals in Rings of Restricted Power Series 124

References **130**

ACKNOWLEDGMENTS

Thanks are due to many people, among them:

My thesis advisor, Matthias Aschenbrenner, for his collaboration and support throughout this endeavor. We intend to publish this material as a joint collaboration.

The other members of my thesis committee: Artem Chernikov, Richard Elman, and Igor Pak, for their time and effort.

The late Paul Sally of the University of Chicago, for fostering my interest in the p-adic numbers.

The professors at UCLA for whom I have TAed, especially the non-mathematicians for taking a chance on my multifaceted interests. I was also supported by the Eugene Cota-Robles fellowship in my first and fourth years at UCLA.

Many sources of friendship and camaraderie over the years, especially the UCLA Women in Mathematics Group; the Lutheran Church of the Master community; Dustan Levenstein, Brent Woodhouse, Konstantin Samoilov, Riley Thornton, Tandré Oey, and all my other gaming friends and rivals.

My siblings and parents, for their constant love and support.

VITA

2009-2011	Barcoder, Regenstein Library
2011-2013	Office Assistant, University of Chicago Department of Mathematics
2013	A.B., major in Mathematics, minor in English and Creative Writing, University of Chicago
2015	M.S., Mathematics, UCLA
2013-19	Research Assistant, Department of Mathematics; Teaching Assistant, Departments of Mathematics, Life Sciences, and Linguistics, UCLA
2019	Presenter, Graduate Student Conference in Logic, University of Illinois at Chicago

CHAPTER 1

Introduction

Given generators of an ideal in a ring, such as a polynomial ring of one or several variables, can one effectively compute the properties of such an ideal (primeness, radicality, and so on)? For many rings the answers are known to be positive. For instance, in polynomial rings over fields the Euclidean Algorithm allows one to compute a single polynomial generating the ideal in question, and testing whether an ideal is prime (radical) reduces to testing whether this polynomial is irreducible (squarefree). A generalization of the Euclidean Algorithm to multivariable polynomial rings over fields is provided by the theory of Gröbner bases, extensively developed since the 1960s, which make the effective computation with ideals of such rings possible [2, 12].

Defining properties of ideals

Much earlier Grete Hermann (1901–1984), a student of Emmy Noether, had studied questions of this kind. Her work [42] was later corrected and augmented by Seidenberg [69] and others [59, 60, 61]. (A translation of [42] into English is available [43].) A sample result shown in her 1926 dissertation [42, Satz 2] is the following (see also Theorem 3.2.3 below):

> *Consider polynomials* $f_0, \ldots, f_n \in K[X] = K[X_1, \ldots, X_N]$ *of (total) degree at most* d *over a field* K*. If* $f_0 \in (f_1, \ldots, f_n)$*, then*
>
> $$f_0 = g_1 f_1 + \cdots + g_n f_n$$
>
> *for certain* $g_1, \ldots, g_n \in K[X]$ *whose degrees are bounded by a number* $I(N, d)$ *depending only on* N *and* d *(not on the field* K *or the particular polynomials* $f_0, \ldots, f_n$*).* [In fact, one may take $I(N, d) = N(2d)^{2^{N-1}}$.]

Let now $f_0(C,X),\dots,f_n(C,X)$ be polynomials with "indeterminate coefficients", that is, each f_i has integer coefficients, and the $C=(C_1,\dots,C_M)$ are new "parametric" variables. Given a field K, substitution of a tuple $c\in K^M$ (of "parameters") for C yields a polynomial $f_i(c,X)\in K[X]$; we denote the ideal of $K[X]$ generated by $f_1(c,X),\dots,f_n(c,X)$ by $I(c,X)$. The starting point of this thesis is the observation that the existence of the uniform bound $I(N,d)$ is equivalent to the following statement: for each field K, the subset

$$\big\{c\in K^M : f_0(c,X)\in I(c,X)\big\} \tag{1.1}$$

of K^M is *constructible*, i.e., a finite boolean combination of algebraic subsets of K^M. Results on dependence on parameters such as this can best expressed using the terminology of mathematical logic: for example, Hermann's Theorem in the form stated above simply asserts that the set (1.1) above is definable by a quantifier-free formula in the (first-order) language $\mathcal{L}_{\text{ring}}=\{0,1,+,-,\cdot\}$ of rings, uniformly for all fields K. (For a generalization of sorts to Bézout domains see [8].) As a special case, we see that the property of the ideal $I(c,X)$ to be *proper* (not to equal $K[X]$) is uniformly definable in this way. One may ask whether other properties of $I(c,X)$, such as being maximal, prime, radical, etc., are similarly definable.

For primality, a positive answer was given by Lambert [47, 48], based on Hermann's work, who showed the existence of an $\mathcal{L}_{\text{ring}}$-formula $\pi(C)$ such that for every field K and $c\in K^M$,

$$K\models\pi(c) \quad\Longleftrightarrow\quad I(c,X) \text{ is prime.}$$

A crucial difference to Hermann's theorem here is that π, in general, may involve quantifiers (corresponding to taking *projections* of constructible sets); we can take π to be quantifier-free if we are only interested in algebraically closed fields K. A similar result for defining primary ideals was much earlier shown by A. Robinson [62], and for maximality this is due to van den Dries [21, (1.6)]. Definability of the dimension of $I(c,X)$ was shown by Eklof [29] and Stützer [72]. Following the lead of A. Robinson [64], van den Dries and Schmidt [20, 25] later unified and vastly extended these results via an elegant non-standard approach. Besides being of interest in themselves, they play an important role in applications of logic to field theory and algebraic geometry. Many extensions to other notions of "polynomial" (e.g., differential polynomials [39]) have been considered.

In the present thesis, we seek to find such tests for rings of power series. Here, the question of "bounds" does not make sense anymore (power series don't have a "degree"), but the formulation in terms of definability does. More specifically, we work with the ring $\mathbb{Q}_p\langle X\rangle$ of restricted p-adic power series. This ring, also known as the Tate algebra over $\mathbb{Q}_p$, consists of all power series

$$f = \sum_{\nu} f_\nu X^\nu \quad \text{where } f_\nu \in \mathbb{Q}_p \text{ and } |f_\nu|_p \to 0 \text{ as } |\nu| \to \infty.$$

Here, as before, $X = (X_1, \ldots, X_N)$; moreover, for $\nu = (\nu_1, \ldots, \nu_N) \in \mathbb{N}^N$ we write $X^\nu = X_1^{\nu_1} \cdots X_N^{\nu_N}$ and $|\nu| := \nu_1 + \cdots + \nu_N$, and $|a|_p = p^{-\operatorname{ord}_p(a)}$ denotes the p-adic norm of $a \in \mathbb{Q}_p$. The p-adic norm on $\mathbb{Q}_p$ extends to the Gauss norm on $\mathbb{Q}_p\langle X\rangle$, denoted by the same notation:

$$|f|_p := \max_{\nu} |f_\nu|_p.$$

(See also Section 2.1 below.) Let $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leqslant 1\}$ be the ring of p-adic integers. Then for $f \in \mathbb{Q}_p\langle X\rangle$ and $x \in \mathbb{Z}_p^N$ the series $f(x) = \sum_\nu f_\nu x^\nu$ converges in $\mathbb{Q}_p$, so f gives rise to an analytic function $x \mapsto f(x)\colon \mathbb{Z}_p^N \to \mathbb{Q}_p$. More generally, a polydisk $B(a, r)$ with center $a = (a_1, \ldots, a_N) \in \mathbb{Z}_p^N$ and radius $r = (r_1, \ldots, r_N)$ (where $r_i = p^{-e_i}$, $e_i \in \mathbb{N}$, for $i = 1, \ldots, N$) is the set

$$B(a, r) := \big\{x \in \mathbb{Z}_p^N : |x - a| \leqslant r\big\},$$

and a function $f\colon B(a, r) \to \mathbb{Q}_p$ is said to be *analytic* if the function $f \circ \gamma\colon \mathbb{Z}_p^N \to \mathbb{Q}_p$ is given by a restricted power series, where $\gamma\colon \mathbb{Z}_p^N \to B(a, r)$ is the natural bijection given by

$$\gamma(y) = (r_1 y_1 + a_1, \ldots, r_N y_N + a_N) \quad \text{for } y = (y_1, \ldots, y_N) \in \mathbb{Z}_N^p.$$

In [19], Denef and van den Dries investigated the sets definable in $\mathbb{Z}_p$ using such analytic functions. We briefly recall the basic definitions and the main result of [19, §1].

Definition. One says that a subset S of $\mathbb{Z}_p^N$ is

(1) *semianalytic at* $a \in \mathbb{Z}_p^N$ if there is a polydisk $B = B(a, r)$ such that $S \cap B(a, r)$ is a boolean combination of sets of the form

$$\big\{x \in B : f(x) = y^n \text{ for some } y \in \mathbb{Q}_p^\times\big\},$$

where f is an analytic function on B and $n \geqslant 1$ is an integer;

(2) *semianalytic* if it is semianalytic at each $a \in \mathbb{Z}_p^N$;

(3) *subanalytic* if there is a semianalytic set $S' \subseteq \mathbb{Z}_p^{N+N'}$, for some $N' \in \mathbb{N}$, such that $S = \pi(S')$, where $\pi\colon \mathbb{Z}_p^{N+N'} \to \mathbb{Z}_p^N$ is the natural projection onto the first N coordinates.

These concepts are modeled on the perhaps better-known notions of semi- and subanalytic subsets of $\mathbb{R}^N$ [51]. It is not hard to see that the semi-analytic subsets of $\mathbb{Z}_p^N$ form a boolean algebra of subsets of $\mathbb{Z}_p^N$. In [19], the authors show that the subanalytic subsets of $\mathbb{Z}_p^N$ also form a boolean algebra of subsets of $\mathbb{Z}_p^N$ (with closure under complement being the decisive fact to be established). In fact, let $\mathcal{L}_{\mathbb{Z}_p}$ be the language $\mathcal{L}_{\text{ring}}$ of rings augmented by a binary predicate $|$ and function symbols for each power series $f \in \mathbb{Z}_p\langle X\rangle$, for varying $X = (X_1, \ldots, X_N)$, $N \in \mathbb{N}$, and view $\mathbb{Z}_p$ as an $\mathcal{L}_{\mathbb{Z}_p}$-structure in the natural way, interpreting $|$ by divisibility in $\mathbb{Z}_p$ and each $f \in \mathbb{Z}_p\langle X\rangle$ by the corresponding analytic function $x \mapsto f(x)\colon \mathbb{Z}_p^N \to \mathbb{Z}_p$. Then *the subanalytic subsets of* $\mathbb{Z}_p^N$ *are exactly the subsets of* $\mathbb{Z}_p^N$ *definable in the* $\mathcal{L}_{\mathbb{Z}_p}$*-structure* $\mathbb{Z}_p$ [19, (1.6)]. (Later applications of this important result include, for example, the study of the subgroup growth of p-adic analytic groups by du Sautoy [67].)

In general, the class of subanalytic subsets of $\mathbb{Z}_p^N$ is much bigger than that of the semi-analytic subsets of $\mathbb{Z}_p^N$; however, for $N \leqslant 2$, they agree [19, (2.5), (2.6)]. Subanalytic sets are piecewise given by manifolds; more precisely, each subanalytic $S \subseteq \mathbb{Z}_p^N$ is a finite disjoint union of p-adic submanifolds of $\mathbb{Z}_p^N$ which are also subanalytic [19, (3.14)]. As a consequence there is a reasonable notion of dimension for subanalytic sets, cf. [19, §3].

Main results

Let $C = (C_1, \ldots, C_M)$ be a tuple of parametric variables and $f_1, \ldots, f_n \in \mathbb{Z}_p\langle C, X\rangle$. We may consider varying $c \in \mathbb{Z}_p^M$ and examining how the corresponding ideals $I(c, X)$ of $\mathbb{Q}_p\langle X\rangle$ generated by $f_1(c, X), \ldots, f_n(c, X)$ vary. As in the case of polynomial ideals, a first simple case is to check whether $I(c, X)$ is proper. Hermann's method for solving system of linear equations over polynomial rings is based on repeated use of Euclidean Division of

polynomials and suitable changes of variables to make its application possible. In Chapter 3 we reproduce an adaptation of Hermann's method to $\mathbb{Q}_p\langle X\rangle$ from [6, 7, 9] which replaces Euclidean Division by Weierstrass Division in $\mathbb{Q}_p\langle X\rangle$. (In fact, we need a variant of the Weierstrass Division Theorem which is uniform in parameters, established in the course of the proof of the "theorem of the complement" for subanalytic sets in [19] explained above.) Among other things, we show there that *the set of $c \in \mathbb{Z}_p^M$ with $1 \in I(c, X)$ can be defined by a quantifier-free $\mathcal{L}_{\mathbb{Z}_p}^{\mathrm{d}}$-formula.* Here $\mathcal{L}_{\mathbb{Z}_p}^{\mathrm{d}}$ is the expansion of $\mathcal{L}_{\mathbb{Z}_p}$ by a binary function symbol d for "restricted division", interpreted in $\mathbb{Z}_p$ as

$$\mathrm{d}(x, y) = \begin{cases} x/y & \text{if } |x|_p \leqslant |y|_p \text{ and } y \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

(See also Section 2.2 below.) In particular, this set is subanalytic. Moreover, the defining formula in question can be chosen to be independent of the prime p, in a suitable framework, namely van den Dries' theory of *valuation rings with analytic structure* from [23] (see also Definition 2.2.1 below). Although uniformity of this kind in this result and others below is important for applications (for example, it makes the use of model-theoretic compactness arguments possible), we will not further elaborate on it in this introduction, for ease of exposition, and rather refer the reader to the precise statements in later chapters.

Our first main result concerns radical ideals:

Theorem A. *There is a quantifier-free $\mathcal{L}_{\mathbb{Z}_p}^{\mathrm{d}}$-formula which defines the set of all $c \in \mathbb{Z}_p^M$ such that the ideal $I(c, X)$ of $\mathbb{Q}_p\langle X\rangle$ is radical.*

We prove this theorem in Chapter 5, where we also establish several variants. First, there is the uniformity in p hinted at above. Moreover, we are able to parametrize generators for the (nil)radical

$$\sqrt{I(c, X)} = \left\{ f \in \mathbb{Q}_p\langle X\rangle : f^E \in I(c, X) \text{ for some integer } E \geqslant 1 \right\}$$

of $I(c, X)$ by certain $\mathcal{L}_{\mathbb{Z}_p}^{\mathrm{d}}$-terms (Theorem 5.2.2). As a consequence, one can uniformly bound the exponent E such that $f^E \in I(c, X)$ for $f \in \sqrt{I(c, X)}$, mimicking a result of A. Robinson [64, 63] for polynomial ideals, see Corollary 5.2.4. And finally, in Proposition 5.3.1 we

show an analogue of Theorem A with $\mathbb{Q}_p\langle X\rangle$ replaced by its subring

$$\mathbb{Z}_p\langle X\rangle = \mathbb{Z}_p[[X]] \cap \mathbb{Q}_p\langle X\rangle.$$

As a sample application of the latter, let us mention the following test for an ideal of $\mathbb{Z}_p\langle X\rangle$ to be radical. (Corollary 5.3.5.) A map $\mathbb{Z}_p^M \to \mathbb{Z}_p^L$ is said to be subanalytic if its graph, viewed as a subset of $\mathbb{Z}_p^{M+L}$, is subanalytic.

Corollary. *There exist a finite family $\{f_\lambda\}$ of elements of $\mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new indeterminates ($L \in \mathbb{N}$), an integer $E \geqslant 1$, and a subanalytic map $c \mapsto a(c)\colon \mathbb{Z}_p^M \to \mathbb{Z}_p^L$, such that for all $c \in \mathbb{Z}_p^M$, the ideal I of $\mathbb{Z}_p\langle X\rangle$ generated by the power series $f_1(c, X), \ldots, f_n(c, X)$ is radical iff for each λ the following implication holds:*

$$f_\lambda\big(a(c), X\big)^E \in I \quad \Longrightarrow \quad f_\lambda\big(a(c), X\big) \in I.$$

In Section 4.2 we show that maximal ideals of $\mathbb{Q}_p\langle X\rangle$ and $\mathbb{Z}_p\langle X\rangle$ are uniformly definable, as is the dimension of ideals of $\mathbb{Q}_p\langle X\rangle$. However, our second main result deals with prime ideals of $\mathbb{Q}_p\langle X\rangle$; here, unfortunately we have to place a restriction on the dimension:

Theorem B. *The set of all $c \in \mathbb{Z}_p^M$ such that $I(c, X)$ is prime and $\dim I(c, X) \leqslant 1$ is subanalytic.*

As a consequence, we obtain a uniform parametrization of primary decompositions of one-dimensional ideals:

Corollary. *There are a finite family $\big\{(\vec{f}_{1,\lambda}, \ldots, \vec{f}_{n,\lambda})\big\}$ where each $\vec{f}_{i,\lambda}$ is an m-tuple of power series in $\mathbb{Z}_p\langle V, X\rangle$, for some m, n and tuple $V = (V_1, \ldots, V_L)$ of new indeterminates ($L \in \mathbb{N}$), as well as a subanalytic map $c \mapsto a(c)\colon \mathbb{Z}_p^M \to \mathbb{Z}_p^L$, such that for all $c \in \mathbb{Z}_p^M$ satisfying $\dim I(c, X) \leqslant 1$, for some λ the ideals of $\mathbb{Q}_p\langle X\rangle$ generated by the components of the tuple $\vec{f}_{i,\lambda}\big(a(c), X\big) \in \mathbb{Z}_p\langle X\rangle^m$ ($i = 1, \ldots, n$) are an irredundant primary decomposition of $I(c, X)$.*

We also have an analogue of Theorem B for prime ideals of $\mathbb{Z}_p\langle X\rangle$; see Corollary 7.3.7. A similar result for defining prime ideals of $\mathbb{Z}_p[X]$ was shown in [8, Corollary 5.12], without restriction on the dimension but with less uniformity than in the full version of Theorem B proved in Section 7.3 (see Remark 7.3.9).

Strategy of the proof of Theorem B

Why do we need the restriction on the dimension in Theorem B? To explain this, it may be useful to briefly discuss the strategy behind our proof of this theorem. Using standard techniques (induction on dimension) and a uniform version of the Noether Normalization Theorem (4.2.1), checking whether $I(c, X)$ is prime reduces to testing the primality of ideals in *polynomial* rings of the form $K[Y]$, where $K = \mathrm{Frac}(\mathbb{Q}_p\langle X\rangle)$ is the fraction field of the integral domain $\mathbb{Q}_p\langle X\rangle$ and Y is a finite tuple of new indeterminates. It is well-known (for example, see [8, Section 5] or Section 7.1 below) that this can be further reduced to answering the following question:

> *Let $P(Y) \in \mathbb{Q}_p\langle X\rangle[Y]$ be separable over K, with Y a* single *indeterminate. Is there some $y \in \mathbb{Q}_p\langle X\rangle$ with $P(y) = 0$?*

To be able to decide this, two natural approaches to find y by an approximation argument suggest themselves; however, as we shall see, neither one seems to work straight away. Let $\Delta \in \mathbb{Q}_p\langle X\rangle$ be the discriminant of P; thus $\Delta \neq 0$ by separability of P.

Use that $\mathbb{Z}_p\langle X\rangle$ is henselian: This fact (a consequence of the completeness of $\mathbb{Z}_p\langle X\rangle$ with respect to the Gauss norm) implies the following useful lifting principle for "approximate zeros" of P: *given $a \in \mathbb{Z}_p\langle X\rangle$ such that $P(a) \equiv 0 \bmod p\Delta^2$, there is a unique $y \in \mathbb{Z}_p\langle X\rangle$ such that $P(y) = 0$ and $y \equiv a \bmod p\Delta$.* (See, e.g., Section 6.1 below.) Reducing (as we may) to the case where P has coefficients in $\mathbb{Z}_p\langle X\rangle$, one could thus hope to reduce the task at hand to finding zeros of one-variable polynomials over the seemingly "simpler" quotient rings $\mathbb{Z}_p\langle X\rangle/p\Delta^2\mathbb{Z}_p\langle X\rangle$ (which are, indeed, finite if X is a single variable). However, it is not clear how to treat these rings in a uniform manner: recall that the coefficients of P are thought of as depending on parameters $c \in \mathbb{Z}_p^M$, and we cannot even bound $|\Delta|_p$ uniformly as these parameters vary.

Use Hensel's Lemma in $\mathbb{Q}_p[[X]]$: Now $\mathbb{Z}_p\langle X\rangle$ is a subring of the ring $\mathbb{Q}_p[[X]]$ of formal power series over $\mathbb{Q}_p$, and since the latter is complete with respect to the X-adic norm,

we may try to use the Newton-Hensel Lemma in this setting instead: *given* $a \in \mathbb{Z}_p[X]$ *with* $P(a) \equiv 0 \bmod X\Delta^2$, *there is a unique* $y \in \mathbb{Q}_p[[X]]$ *such that* $P(y) = 0$ *and* $y \equiv a \bmod X\Delta$. It is well-known that such a zero $y \in \mathbb{Q}_p[[X]]$ of P converges on some polydisk B with center 0; but how to tell whether one can choose $B \supseteq \mathbb{Z}_p^N$ (i.e., whether y lies in $\mathbb{Q}_p\langle X\rangle$)? This seems difficult to do in a uniform manner, and is related to the problem of computing the optimal value of Eisenstein's constant [27, 53].

Nevertheless, in our proof of Theorem B we were able to combine aspects of both of these seemingly failing approaches. The key is the following uniform bound on the discriminant of certain polynomials established in Section 6.2. For this let $\mathcal{O}$ be a valuation ring with fraction field $K = \mathrm{Frac}(\mathcal{O})$ of characteristic zero. Let $P \in \mathcal{O}[Y]$ be monic irreducible, with discriminant Δ. Call P *integrally closed* if the integral closure of $\mathcal{O}$ in the field extension $K[y] := K[Y]/PK[Y]$ of K equals $\mathcal{O}[y]$; here $y := Y + PK[Y]$. A $\mathbb{Z}$*-group* is an ordered abelian group Γ which has a smallest positive element and satisfies $|\Gamma/n\Gamma| = n$ for each $n \geqslant 1$. One says that $\mathcal{O}$ is *unramified* if either the residue field $\boldsymbol{k}$ of $\mathcal{O}$ has characteristic zero, or if $\mathrm{char}\,\boldsymbol{k} = p > 0$ and $v(p)$ is the smallest element of the value group $v(K^\times)$ of $\mathcal{O}$.

Proposition. *Suppose* $\mathcal{O}$ *is unramified and its value group is a* $\mathbb{Z}$*-group. If* P *is integrally closed then*

$$v(\Delta) \leqslant d - 1 + C(d,p)v(p) \quad \textit{where } d = \deg P,\ p = \textit{characteristic of the residue field of } \mathcal{O}.$$

Here the bound $C(d,p) \in \mathbb{N}$ *only depends on* d, p, *not on* $\mathcal{O}$ *and the coefficients of* P.

If $\mathcal{O}$ is a DVR (that is, its value group is $\mathbb{Z}$), this is a classical fact due to Hensel [41]; we deduce the general case using the Ax-Kochen-Eršov Principle and a first-order characterization of integrally closed polynomials due to Eršov [34] and Khanduja-Kumar [44], generalizing a theorem of Dedekind [17]. (A version of this proposition also holds for finitely ramified $\mathcal{O}$, but in the applications later only the unramified case is used.) Below we say that a monic polynomial $P \in \mathcal{O}[Y]$ (possibly reducible) has *large discriminant* if its discriminant obeys the bound in the proposition.

Let now T be the theory of unramified valued fields of characteristic $(0, p)$ whose value group is a $\mathbb{Z}$-group and whose residue field is infinite and perfect. We formulate this theory in a suitably chosen language $\mathcal{L}$ so that T is universally axiomatized. In $\mathcal{L}$ we also include Skolem functions for the zeros of polynomials with large discriminant, and T incorporates the necessary defining axioms. (We refer to Section 7.1 for the details, where we denote $\mathcal{L}$, T by $\mathcal{L}_1^*$, $T_1^*(1, p)$, respectively.) A compactness argument based on the proposition above then shows that zeros of polynomials in models of T can be uniformly parametrized by $\mathcal{L}$-terms:

Proposition. *There is a finite family $\{\tau_i^d\}_{i\in I}$ of $\mathcal{L}$-terms $\tau_i^d = \tau_i^n(x_1, \dots, x_d)$ such that for all $K \models T$ and $a_1, \dots, a_d \in K$, if*

$$P(Y) = Y^d + a_1 Y^{d-1} + \cdots + a_d \in K[Y]$$

has a zero in K, then $P\big(\tau_i^d(a_1, \dots, a_d)\big) = 0$ for some $i \in I$.

Here the condition that the residue field is infinite perfect guarantees that the relevant integral closures are monogenic, see (6.2.10).

We now hope to apply this fact to the fraction field of $\mathbb{Q}_p\langle X\rangle$ equipped with the natural extension of the Gauss norm to a (multiplicatively written) valuation on $\mathrm{Frac}(\mathbb{Q}_p\langle X\rangle)$; but although this valued field has value group $\mathbb{Z}$ and infinite residue field $\mathbb{F}_p(X)$, this residue field is not perfect. To remedy this we pass from the Tate algebra $\mathbb{Q}_p\langle X\rangle$ to the ring

$$\mathbb{Q}_p\langle X^{1/p^\infty}\rangle = \bigcup_n \mathbb{Q}_p\langle X^{1/p^n}\rangle$$

obtained by introducing p^nth roots of the indeterminates X_i for each n. One can then turn the fraction field K of $\mathbb{Q}_p\langle X^{1/p^\infty}\rangle$ into a model of T in a natural way (Section 7.2). Thus the last proposition essentially reduces the task which we set ourselves at the beginning of this subsection to the problem of uniformly parametrizing the zeros of monic polynomials with large discriminant over $\mathcal{O}$ = valuation ring of K. However, to be able to continue, we need to make an extra assumption (reflecting the restriction on $\dim I(c, X)$ in Theorem B):

Suppose from now on that X is a single indeterminate.

The benefit of this assumption is that now the Newton diagram method for polynomials over the field

$$\mathrm{P}(\mathbb{Q}_p) = \bigcup_{m \geqslant 1} \mathbb{Q}_p(\!(X^{1/m})\!)$$

of Puiseux series over $\mathbb{Q}_p$ (which contains K as a subfield) with respect to the X-adic valuation on $\mathrm{P}(\mathbb{Q}_p)$ applies, and this allows us to reduce the task of computing zeros of polynomials over K to the analogous task over $\mathbb{Q}_p\langle X\rangle$ (7.2.2). Thus by the considerations above, we arrive at the following simpler problem: *given a polynomial $P \in \mathbb{Q}_p\langle X\rangle[Y]$ with large discriminant, compute the zeros of P in $\mathbb{Q}_p\langle X\rangle$.* This can further be reduced to the consideration of monic polynomials with large discriminant having coefficients in $\mathbb{Z}_p\langle X\rangle$ (and then by Gauss' Lemma, all zeros of these polynomials in $\mathbb{Q}_p\langle X\rangle$ actually lie in $\mathbb{Z}_p\langle X\rangle$). In this case the Newton diagram method with respect to the p-adic norm and the henselian property of $\mathbb{Z}_p\langle X\rangle$ can be used to compute the zeros, the punchline being that *the uniform bound on $|\Delta|_p$ gives an upper bound on the number of steps which are needed to reach a situation where Hensel's Lemma in $\mathbb{Z}_p\langle X\rangle$ applies.* (See Proposition 6.1.15 below, the proof of which also involves another use of the hypothesis $N = 1$.)

Organization of the thesis

To begin with, we introduce rings of restricted power series (Section 2.1). We also introduce Weierstrass Division, which will be an important tool for partially emulating Euclidean Division of polynomials for power series. We then extend these methods to restricted power series with parameters (Section 2.2), and to more general power series over valuation rings which are not necessarily complete DVRs like $\mathbb{Z}_p$ (Section 2.3).

In Chapter 3 we then develop techniques of linear algebra for solving systems of linear equations over rings of restricted power series. Hermann's Method can be used to inductively reduce the complexity of matrix equations; this often requires a process of desingularization (Section 3.1). As an application we establish the uniform definability of various basic ideal-theoretic operations, including simple cases of elimination of variables (Section 3.3).

Next, with the process of Weierstrass Division as motivation, we introduce Weierstrass

sequences of polynomials and power series (Section 4.1), which are useful for making the Noether Normalization Theorem uniform in parameters (Section 4.2). This allows us to compute radicals of ideals in Chapter 5, first in polynomial rings and then extending to rings of restricted power series.

Results of Hermann and Robinson (reproved using non-standard analysis by van den Dries and Schmidt) provide parametrizations for generators of radicals of polynomial ideals over fields. (Section 5.1.) In the case of restricted power series, we combine these with a strategy indicated in [35] for computing radicals in polynomial rings over fields: we seek a "universal denominator" $a \neq 0$ such that the ideal I may be written $(I : a) \cap (I, a)$; it then suffices to compute the radicals of each of these ideals separately, giving rise to an induction by dimension. This results in a proof of Theorem A.

For the case of primality, we first show a uniform version of the Newton-Hensel Lemma for $\mathbb{Z}_p\langle X\rangle$ and explain the basics of the Newton diagram method, leading to a parametrization of the zeros of polynomials over $\mathbb{Z}_p\langle X\rangle$ with bounded discriminant when $N = 1$ (Section 6.1). We then establish the bounds on the valuation of the discriminant of integrally closed polynomials (Section 6.2) and develop a language in which we may define conditions for a polynomial ideal over a valued field to be primary, as discussed above (Section 7.1). In Section 7.2 we introduce the ring $\mathbb{Q}_p\langle X^{1/p^\infty}\rangle$ and in Section 7.3 we finally give a definable condition for one-dimensional prime ideals and complete the proof of Theorem B.

Some open questions

Besides the obvious question whether one can remove the condition on the dimension of the ideal $I(c, X)$ in Theorem B and its corollary, several other issues deserve to be pursued in the future; we finish this introduction by listing a few.

First, in order to make Theorems A and B useful for applications, one needs to strengthen their connection with the geometric situation of subanalytic sets. Here a first step would be to answer the following question: *can we find, uniformly in* $c \in \mathbb{Z}_p^M$*, generators for the*

vanishing ideal

$$\big\{g \in \mathbb{Q}_p\langle X\rangle : g(x) = 0 \text{ for all } x \in \mathbb{Z}_p^N \text{ with } f_1(c,x) = \cdots = f_n(c,x) = 0\big\}$$

of $f_1(c,X),\ldots,f_n(c,X)$*?* For the case where the ideal $I(c,X)$ of $\mathbb{Q}_p\langle X\rangle$ has dimension 0, this follows from work of Sander [66].

We mentioned earlier in this introduction that the question of bounds does not make sense for power series; however, there is a subring of $\mathbb{Q}_p\langle X\rangle$ for which these questions *do* make sense, namely the ring $\mathbb{Q}_p\langle X\rangle_{\text{alg}}$ of restricted power series which are algebraic over the polynomial ring $\mathbb{Q}_p[X]$. These rings satisfy many properties of $\mathbb{Q}_p\langle X\rangle$; for example, they are closed under Weierstrass Division. A suitable notion of complexity for power series in $\mathbb{Q}_p\langle X\rangle_{\text{alg}}$ was developed in [9], and bounds in Hermann's method were established. It may be worthwhile to compute similar bounds in Theorems A and B, although this may be difficult in the latter, due to the uses of model-compactness in its proof. Similar questions for *formal* algebraic power series were pursued in [3, 4, 5]; in [4], the authors give an algorithm for computing radicals in this situation, and they write that *by lack of a factorization algorithm for polynomials over an algebraic power series ring, we can only reduce* [...] *primary decomposition, primality and primariety tests to univariate polynomial factorization.* This difficulty is what we were able to circumvent (although non-constructively) in the setting of restricted p-adic power series in our proof of Theorem B. Related to this question, it seems plausible that if the f_i are algebraic, then the sets of parameters c in Theorems A and B are p-adic semialgebraic (i.e., definable in the sublanguage $\mathcal{L}_{\text{ring}}$ of $\mathcal{L}_{\mathbb{Z}_p}$). For Theorems 3.3.1 and 3.3.3 below, this was shown already in [6].

It would also be interesting to pursue analogues of the questions considered in this thesis in the setting of rigid analytic geometry [14]. Here, the model-theoretic analogues of the theorems of Denef-van den Dries were established by Lipshitz and Z. Robinson [50]. First steps in this direction were undertaken by Çelikler [15], who showed a uniform version of Noether Normalization in this context.

Notations and conventions

Throughout this thesis m, n range over the set $\mathbb{N} = \{0, 1, 2, \dots\}$ of natural numbers. By $C = (C_1, \dots, C_M)$ and $X = (X_1, \dots, X_N)$ we always denote tuples of distinct indeterminates, where $M, N \in \mathbb{N}$. Given an additively written abelian group A we set $A^{\neq} := A \setminus \{0\}$. All rings in this paper are commutative with 1. The group of units of a ring R is denoted by $R^{\times}$.

CHAPTER 2

Preliminaries

In this chapter we introduce rings of restricted power series, which are the main objects of interest in this thesis, as well as the tools of Weierstrass Division and Preparation for simplifying such power series. These methods generalize the notion of Euclidean Division for single-variable polynomials. In Section 2.1 we first introduce Weierstrass Division and Preparation for rings of restricted power series over an integral domain D with a distinguished prime element t such that D is t-adically complete (2.1.3, 2.1.4). The "standard" example is $D = \mathbb{Z}_p$. In Section 2.2 we then discuss uniformity in parameters in the Weierstrass Division and Preparation Theorems, described using suitable first-order languages $\mathcal{L}_D$ and $\mathcal{L}_D^{\mathrm{d}}$ (2.2.11, 2.2.12). Both of these languages contain function symbols for power series, as well as binary divisibility predicates, while the latter expands the former by adding a symbol for "restricted division". This uniformity allows us to formulate and prove a version of Weierstrass Division and Preparation for restricted power series over "nonstandard" valuation rings (Section 2.3). These results also hold for power series rings over the fraction fields of our rings (such as $\mathbb{Q}_p$) and their nonstandard equivalents.

2.1 Rings of Restricted Power Series

Let D be an noetherian integral domain. We assume that we are given a prime element t of D (that is, $t \neq 0$ and the ideal tD of D generated by t is prime). We also assume that D is t-adically complete (that is, complete with respect to the linear topology on D with fundamental system of neighborhoods of 0 given by the ideals $t^n D$). We set $\overline{D} := D/tD$, with residue morphism $a \mapsto \overline{a} := a + tD \colon D \to \overline{D}$. Some examples to keep in mind are:

(1) $D = \mathbb{Z}[[t]]$, the ring of formal power series over $\mathbb{Z}$ in the single variable t, in which case $\overline{D} = \mathbb{Z}$;

(2) D is a complete discrete valuation ring (DVR) with maximal ideal tD; e.g., $D = \mathbb{Z}_p$, with $t = p$, where we have $\overline{D} = \mathbb{F}_p$.

The completion of the polynomial ring $D[X] = D[X_1, \ldots, X_N]$ with respect to the t-adic topology is called the ring of **restricted power series** with coefficients in D and will be denoted by $D\langle X\rangle = D\langle X_1, \ldots, X_N\rangle$. It may be regarded as a subring of the ring $D[[X]]$ of formal power series over D in a natural way: its elements are the power series

$$f = \sum_{\nu} f_\nu X^\nu \in D[[X]] \qquad (f_\nu \in D)$$

such that $f_\nu \to 0$ (in the t-adic topology on D) as $|\nu| \to \infty$. Here and below $\nu = (\nu_1, \ldots, \nu_N)$ ranges over all multiindices in $\mathbb{N}^N$, $X^\nu := X_1^{\nu_1} \cdots X_N^{\nu_N}$, and $|\nu| := \nu_1 + \cdots + \nu_N$. Given $g = (g_1, \ldots, g_N) \in D\langle C\rangle^N$ we set $g^\nu := g_1^{\nu_1} \cdots g_N^{\nu_N} \in D\langle C\rangle$ for each ν; then $f_\nu g^\nu \to 0$ as $|\nu| \to \infty$, hence we may define

$$f(g) = f(g_1, \ldots, g_N) := \sum_{\nu} f_\nu g^\nu \in D\langle C\rangle. \tag{2.1}$$

The map $f \mapsto f(g)$ is the unique D-algebra morphism $D\langle X\rangle \to D\langle C\rangle$ with $X_i \mapsto g_i$ for $i = 1, \ldots, N$. Given $a \in D^{\neq}$ there is some n such that $a \in t^n D \setminus t^{n+1}D$, and we let $v_t(a) := n$, the t-adic valuation of a. The map $v_t\colon D^{\neq} \to \mathbb{N}$ indeed is a valuation on the integral domain D, that is,

$$v_t(ab) = v_t(a) + v_t(b) \qquad \text{for } a, b \in D^{\neq},$$

and

$$v_t(a+b) \geqslant \min\big\{v_t(a), v_t(b)\big\} \qquad \text{for } a, b \in D^{\neq} \text{ with } a + b \in D^{\neq}.$$

The t-adic valuation on D extends to $D\langle X\rangle$ by setting

$$v_t(f) = \min_{\nu} v_t(f_\nu) \qquad \text{for } f = \sum_{\nu} f_\nu X^\nu \in D\langle X\rangle^{\neq}.$$

See [14, p. 44, Corollary 2] for a proof that $v_t\colon D\langle X\rangle^{\neq} \to \mathbb{N}$ is a valuation on the integral domain $D\langle X\rangle$. We denote the image of $f \in D\langle X\rangle$ under the canonical surjection

$$D\langle X\rangle \to D\langle X\rangle/tD\langle X\rangle \cong \overline{D}[X]$$

by $\overline{f}$. The group of units of $D\langle X\rangle$ is

$$D\langle X\rangle^{\times} = D^{\times}\big(1 + tD\langle X\rangle\big) = \big\{f \in D\langle X\rangle : \overline{f} \in \overline{D}^{\times}\big\}. \tag{2.2}$$

(To see this note that if $f \in tD\langle X\rangle$ then $f^n \to 0$ as $n \to \infty$, hence $\sum_n f^n$ exists in $D\langle X\rangle$ by completeness of $D\langle X\rangle$, and this is an inverse of $1 - f$.)

Suppose from now on that $N \geqslant 1$, and let $X' := (X_1, \ldots, X_{N-1})$. Then $D\langle X'\rangle$ is a subring of $D\langle X\rangle$, and every $f \in D\langle X\rangle$ can be written uniquely in the form

$$f = \sum_{i=0}^{\infty} f_i X_N^i \quad \text{with } f_i(X') \in D\langle X'\rangle \text{ for all } i \in \mathbb{N}, \tag{2.3}$$

where the infinite sum converges with respect to the t-adic topology on $D\langle X\rangle$. An element f of $D\langle X\rangle$, expressed as in (2.3), is called **regular in X_N of degree $s \in \mathbb{N}$** if its reduction $\overline{f} \in \overline{D}[X]$ is unit-monic of degree s in X_N, that is,

(1) $\overline{f_s}$ is a unit in $\overline{D}$, and

(2) $\overline{f_i} = 0$ for all $i > s$.

An element f of $D\langle X'\rangle[X_N]$ which is monic of degree s in X_N (so that in particular f is regular in X_N of degree s, as an element of $D\langle X\rangle$) is called a **Weierstrass polynomial in X_N of degree s.** For a proof of the following standard facts see, e.g., [14]:

Lemma 2.1.1 (Noether Normalization)**.** *Let A be an integral domain and $f \in A[X]$, $f \neq 0$, be of total degree $< d$, where $d > 1$. Then the A-algebra automorphism T_d of $A[X]$ given by*

$$X_i \mapsto X_i + X_N^{d^{N-i}} \qquad (\textit{for } 1 \leqslant i < N)$$
$$X_N \mapsto X_N$$

has the property that for some $s < d^N$ and $u \in A^{\neq}$,

$$T_d(f) = uX_N^s + \textit{terms of lower degree in } X_N.$$

Applying this to $A = \overline{D}$, we get:

Lemma 2.1.2. *Let $d > 1$ and $f \in D\langle X\rangle$ be such that $\overline{f} \in \overline{D}[X]$ is non-zero of degree $< d$. Let T_d be the D-algebra automorphism of $D\langle X\rangle$ defined by*

$$X_i \mapsto X_i + X_N^{d^{N-i}} \qquad (\textit{for } 1 \leqslant i < N)$$
$$X_N \mapsto X_N.$$

Then for some $e < d^N$ and some $u \in D$ with $v_t(u) = 0$,

$$T_d(f) = uX_N^e + \textit{terms of lower degree in } X_N \mod t.$$

(In particular, if $\overline{D}$ is a field, then $T_d(f)$ is regular in X_N of degree $< d^N$.)

The ring $D\langle X\rangle$ has the following fundamental property:

Theorem 2.1.3 (Weierstrass Division Theorem for $D\langle X\rangle$)**.** *Let $g \in D\langle X\rangle$ be regular in X_N of degree s. Then for each $f \in D\langle X\rangle$ there are uniquely determined elements $q \in D\langle X\rangle$ and $r \in D\langle X'\rangle[X_N]$ with $\deg_{X_N} r < s$ such that $f = qg + r$.*

So in particular, we get

$$D\langle X\rangle/gD\langle X\rangle \cong D\langle X'\rangle \oplus D\langle X'\rangle\overline{X_N} \oplus \cdots \oplus D\langle X'\rangle\overline{X_N}^{s-1} \tag{2.4}$$

as $D\langle X'\rangle$-algebras, where $\overline{X_N} = X_N \bmod g$. Applying Weierstrass Division with $f = X_N^s$, we obtain an important corollary:

Corollary 2.1.4 (Weierstrass Preparation Theorem for $D\langle X\rangle$)**.** *Let $g \in D\langle X\rangle$ be regular in X_N of degree s. There are a unique Weierstrass polynomial $w \in D\langle X'\rangle[X_N]$ of degree s and a unique unit $u \in D\langle X\rangle$ such that $g = u \cdot w$.*

One useful consequence of Weierstrass Division is that the ring $D\langle X\rangle$ is noetherian; here is another one:

Corollary 2.1.5. *Let $w \in D\langle X'\rangle[X_N]$ be a Weierstrass polynomial. Then the natural inclusion $D\langle X'\rangle[X_N] \subseteq D\langle X\rangle$ induces an isomorphism*

$$D\langle X'\rangle[X_N]/wD\langle X'\rangle[X_N] \xrightarrow{\cong} D\langle X\rangle/wD\langle X\rangle.$$

Proof. The surjectivity of the map follows from the existence part of Weierstrass Division. For injectivity, we have to show: if $fw = g \in D\langle X'\rangle[X_N]$ for some $f \in D\langle X\rangle$, then $f \in D\langle X'\rangle[X_N]$. This follows by Euclidean Division of g by the monic polynomial w in $D\langle X'\rangle[X_N]$, and by the uniqueness statement in the Weierstrass Division Theorem. □

2.2 Parametric Weierstrass Preparation

We let D and t be as in the previous section. Consider a restricted power series $f \in D\langle C, X\rangle$, so

$$f(C, X) = \sum_{\nu} f_\nu(C)X^\nu \qquad \text{where } f_\nu \in D\langle C\rangle \text{ for each } \nu. \tag{2.5}$$

We let $\mu = (\mu_1, \dots, \mu_M)$ range over $\mathbb{N}^M$, and given an M-tuple $c = (c_1, \dots, c_M)$ of elements of a ring we set $c^\mu := c_1^{\mu_1} \cdots c_M^{\mu_M}$. Suppose R is a complete DVR with maximal ideal $\mathfrak{m}$ and $\phi\colon D \to R$ is a ring morphism with $\phi(t)R = \mathfrak{m}$ (so ϕ is continuous with respect to the t-adic topology on D and the $\mathfrak{m}$-adic topology on R). Then for each $c \in R^M$ and $g = \sum_\mu g_\mu C^\mu \in D\langle C\rangle$ ($g_\mu \in D$), the infinite sum $\sum_\mu \phi(g_\mu)c^\mu$ converges to an element $g(c) \in R$. In this way, for each $c \in R^M$ we get a restricted power series $f(c, X) := \sum_\nu f_\nu(c)X^\nu \in R\langle X\rangle$. We want to discuss how certain operations on restricted power series, like Weierstrass Preparation and Division (with respect to one of the X-variables) depend on the parameters $c \in R^M$, uniformly for all R. Here is the appropriate context for this:

Definition 2.2.1 (van den Dries [23])**.** Let R be a valuation ring with maximal ideal $\mathfrak{m} = \mathfrak{m}_R$. An **analytic D-structure** (for short: a D-structure) on R is a family $\phi = (\phi_M)_{M \geqslant 0}$ of ring morphisms

$$\phi_M\colon D\langle C\rangle = D\langle C_1, \dots, C_M\rangle \to \big\{\text{ring of functions } R^M \to R\big\}$$

such that:

(A1) $\phi_0(t)R = \mathfrak{m}$,

(A2) $\phi_M(C_i) = i$-th coordinate function on R^M, for each $i = 1, \dots, M$,

(A3) the map ϕ_{M+1} extends ϕ_M, if we identify in the obvious way functions on R^M with functions on R^{M+1} that do not depend on the last coordinate,

(A4) for each $f \in D\langle C\rangle$, $g_1, \ldots, g_M \in \mathbb{Z}[C]$ and $c \in R^M$, we have

$$\phi_M\big(f(g_1, \ldots, g_M)\big)(c) = \phi_M(f)\big(g_1(c), \ldots, g_M(c)\big).$$

A valuation ring with D-structure is a pair (R, ϕ) where R is a valuation ring and ϕ is a D-structure on R.

Note that by (A1), the maximal ideal $\mathfrak{m}$ of R is a principal ideal, generated by $t_R := \phi_0(t)$, but R is not required to be a DVR. Nevertheless, DVRs give rise to interesting examples of valuation rings with D-structures:

Example 2.2.2. If R is a complete DVR and $\phi\colon D \to R$ a ring morphism with $\phi(t)R = \mathfrak{m}_R$, then R carries a unique D-structure $(\phi_M)_{M\geqslant 0}$ with $\phi_0 = \phi$. In particular, for $D = \mathbb{Z}[[t]]$ and a prime p:

(1) The complete DVR $R = \mathbb{Z}_p$ carries a unique D-structure (ϕ_M) where $\phi_0\colon \mathbb{Z}[[t]] \to \mathbb{Z}_p$ is the ring morphism with kernel $(t-p)\mathbb{Z}[[t]]$, given by

$$a(t) = \sum_n a_n t^n \mapsto a(p) := \sum_n a_n p^n.$$

Slightly more generally: given a generator π of $p\mathbb{Z}_p$, $\mathbb{Z}_p$ carries a unique D-structure (ϕ_M) with $\phi_0(t) = \pi$.

(2) The complete DVR $R = \mathbb{F}_p[[t]]$ carries a unique D-structure (ϕ_M) such that $\phi_0(t) = t \in \mathbb{F}_p[[t]]$.

In the rest of this subsection we let (R, ϕ) be a valuation ring with D-structure. As a special case of (A4), for each permutation σ of $\{1, \ldots, M\}$ and $c \in R^M$ we have

$$\phi_M\big(f(C_{\sigma(1)}, \ldots, C_{\sigma(M)})\big)(c) = \phi_M(f)\big(c_{\sigma(1)}, \ldots, c_{\sigma(M)}\big).$$

Hence we can generalize (A3) as follows:

(A3′) For $f \in D\langle C\rangle$, $c \in R^{M+1}$, and $i \in \{1, \dots, M+1\}$, setting

$$\widehat{C} := (C_1, \dots, C_{i-1}, C_{i+1}, \dots, C_{M+1}),$$
$$\widehat{c} := (c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_{M+1}) \in R^M,$$

we have $\phi_{M+1}\big(f(\widehat{C})\big)(c) = \phi_M(f)(\widehat{c})$.

Definition 2.2.1 was formulated using a distinguished sequence $C_1, C_2, \dots$ of indeterminates. We extend ϕ to arbitrary restricted power series with coefficients in D in the natural way: given $f \in D\langle X\rangle$, where $X = (X_1, \dots, X_N)$ is any N-tuple of indeterminates, we let $\phi_N(f) := \phi_N\big(f(C_1, \dots, C_N)\big)$. In (A4) we also get more than we bargained for. (See (2.1) for composition of restricted power series.)

Lemma 2.2.3. *For each $f \in D\langle X\rangle$ and $g_1, \dots, g_N \in D\langle C\rangle$ we have*

$$\phi_M\big(f(g_1, \dots, g_N)\big)(c) = \phi_N(f)\big(\phi_M(g_1)(c), \dots, \phi_M(g_N)(c)\big) \quad \textit{for all } c \in R^M.$$

Proof. By induction on N we prove something which (thanks to (A3′)) is a bit more general: for each $f \in D\langle C, X\rangle$ and $g_1, \dots, g_N \in D\langle C\rangle$ we have

$$\phi_M\big(f(C, g_1, \dots, g_N)\big)(c) = \phi_{M+N}(f)\big(c, \phi_M(g_1)(c), \dots, \phi_M(g_N)(c)\big) \quad \text{for } c \in R^M.$$

The case $N = 0$ being trivial, suppose $N \geqslant 1$. Let $f \in D\langle C, X\rangle$ and $g_1, \dots, g_N \in D\langle C\rangle$. By Theorem 2.1.3 we take $q \in D\langle C, X\rangle$, $r \in D\langle C, X'\rangle$ such that

$$f(C, X) = q(C, X) \cdot \big(X_N - g_N(C)\big) + r(C, X'). \tag{2.6}$$

Let $g = (g_1, \dots, g_N)$, $g' = (g_1, \dots, g_{N-1})$. Then $f(C, g) = r(C, g')$, thus for $c \in R^M$,

$$\begin{aligned}
\phi_M\big(f(C, g)\big)(c) &= \phi_M\big(r(C, g')\big)(c) \\
&= \phi_{M+N-1}(r)\big(c, \phi_M(g')(c)\big) \\
&= \phi_{M+N}(r)\big(c, \phi_M(g)(c)\big) \\
&= \phi_{M+N}(f)\big(c, \phi_M(g)(c)\big),
\end{aligned}$$

where the second equation holds by inductive hypothesis with r in place of f, the third equation by (A3), and the last one follows from (2.6) by applying ϕ_{M+N} on both sides and evaluating at $\big(c, \phi_M(g)(c)\big)$ using (A2). □

We often drop ϕ from the notation, and from now on, for $c \in R^M$ and $g \in D\langle C\rangle$ we write $g(c)$ instead of $\phi_M(g)(c)$. So the displayed equation in the statement of the lemma above may be written in a more succinct form as

$$f(g_1, \ldots, g_N)(c) = f\big(g_1(c), \ldots, g_N(c)\big).$$

Similarly, given $f = f(C, X)$ as in (2.5) we write $f(c, X)$ for the series $\sum_\nu f_\nu(c)X^\nu \in R[[X]]$. We may view $f(c, X)$ as a restricted power series whose coefficients depend on a parameter $c \in R^M$. Clearly for fixed c the map $f \mapsto f(c, X)$ is a D-algebra morphism $D\langle C, X\rangle \to R[[X]]$, where we regard $R[[X]]$ as a D-algebra via the composition of $\phi_0 \colon D \to R$ with the natural inclusion $R \to R[[X]]$. Following [24], we define

$$R\langle X\rangle := \big\{f(c, X) : f \in D\langle C, X\rangle,\, C = (C_1, \ldots, C_M),\, M \in \mathbb{N},\, c \in R^M\big\} \subseteq R[[X]].$$

(For a complete DVR R, this indeed coincides with the set of restricted power series over R denoted by the same symbol introduced in the previous section.)

Lemma 2.2.4. *For $g_1(X), \ldots, g_n(X) \in R\langle X\rangle$ there exists a single $M \in \mathbb{N}$, some $c \in R^M$, and $f_1, \ldots, f_n \in D\langle C, X\rangle$ such that $g_i = f_i(c, X)$ for $i = 1, \ldots, n$.*

(By introducing extra parametric indeterminates and relabeling if necessary.)

Corollary 2.2.5. *$R\langle X\rangle$ is an R-subalgebra of $R[[X]]$ which contains $R[X]$.*

Proof. By the previous lemma, given $g_1(X), g_2(X) \in R\langle X\rangle$ there are $M \in \mathbb{N}$, $c \in R^M$ and $f_1(C, X), f_2(C, X) \in D\langle C, X\rangle$ such that $g_i = f_i(c, X)$ for $i = 1, 2$. So

$$g_1(X) + g_2(X) = (f_1 + f_2)(c, X),$$
$$g_1(X) \cdot g_2(X) = (f_1 \cdot f_2)(c, X),$$

hence $R\langle X\rangle$ is closed under addition and multiplication. □

Let $T_1, \ldots, T_N \in \mathbb{Z}[X]$ with $T_i(0) = 0$ for $i = 1, \ldots, N$, and set $T := (T_1, \ldots, T_N)$. Then given a ring A and $f = \sum_\nu f_\nu X^\nu \in A[[X]]$, the sum $\sum_\nu f_\nu T^\nu$ converges to an element $f(T)$ of $A[[X]]$, with respect to the (X)-adic topology on $A[[X]]$. Here T^ν denotes the image

of $T_1^{\nu_1} \cdots T_N^{\nu_N}$ under the natural ring morphism $\mathbb{Z}[X] \to A[X] \subseteq A[[X]]$. The coefficients of $f(T)$ are given by polynomials with integer coefficients, independent of A and f, in the coefficients f_ν of f. This implies that if $g \in R\langle X\rangle$, say $g(X) = f(c, X)$ with $f \in D\langle C, X\rangle$, $c \in R^M$, then $g(T) = h(c, X) \in R\langle X\rangle$ for $h(C, X) = f(C, T) \in D\langle C, X\rangle$. Therefore:

Lemma 2.2.6. *The R-algebra morphism $g \mapsto g(T)\colon R[[X]] \to R[[X]]$ restricts to an R-algebra morphism $R\langle X\rangle \to R\langle X\rangle$.*

Below, given $f \in D\langle C, X\rangle$, $c \in R^M$, we write $f(c, T)$ for $h(c, X)$ where $h(C, X) := f(C, T) \in D\langle C, X\rangle$. If $g \mapsto g(T)$ is an automorphism of $\mathbb{Z}[X]$, then the R-algebra endomorphism $g \mapsto g(T)$ of $R\langle X\rangle$ is an automorphism of $R\langle X\rangle$. We call the R-algebra automorphisms of $R\langle X\rangle$ which arise in this way **polynomial automorphisms** of $R\langle X\rangle$. The polynomial automorphisms of $R\langle X\rangle$ form a group under composition. Given an automorphism σ of $\mathbb{Z}[X]$ with $T_i := \sigma(X_i)$ satisfying $T_i(0) = 0$ for each $i = 1, \dots, N$, we also denote the corresponding R-algebra automorphism $g \mapsto g(T)$ of $R\langle X\rangle$ by σ. One particularly important example is $g \mapsto g\big(T_d(X)\big)$ where for $d \in \mathbb{N}$ we denote by $T_d(X)$ the tuple

$$\big(T_d(X_1), \dots, T_d(X_N)\big) = \Big(X_1 + X_N^{d^{N-1}}, \dots, X_{N-1} + X_N^d, X_N\Big).$$

(See Lemma 2.1.2.)

The languages $\mathcal{L}_D$ and $\mathcal{L}_D^{\mathrm{d}}$

Let $f(C, X) \in D\langle C, X\rangle$ be as in (2.5). We want to formulate a key fact from [23]: the parameter space R^M, where R is a valuation ring with D-structure, can be partitioned into finitely many "basic" subsets on each of which Weierstrass Preparation for $f(c, X)$ is *uniform in both c and R*. To describe these subsets, we introduce a first-order language $\mathcal{L}_D$, which is the language $\mathcal{L}_{\mathrm{div}} = \{0, 1, +, -, \cdot, |\,\}$ of rings with a divisibility predicate $|$, augmented by an M-ary function symbol for each power series in $D\langle C\rangle = D\langle C_1, \dots, C_M\rangle$. We consider a valuation ring with D-structure (R, ϕ) as an $\mathcal{L}_D$-structure by interpreting $|$ as divisibility in R, and associating to each $g \in D\langle C\rangle = D\langle C_1, \dots, C_M\rangle$ the corresponding function $\phi_M(g)\colon R^M \to R$, for $M \in \mathbb{N}$. The valuation rings with D-structure, when viewed as $\mathcal{L}_D$-structures in this way, form an elementary class. Let T_D be the theory of valuation rings

with D-structure in the language $\mathcal{L}_D$. Note that T_D depends not only on D but also on the choice of distinguished prime element t of D, but t is usually understood from context. In the rest of this thesis $T_{\mathbb{Z}_p}$ denotes the $\mathcal{L}_{\mathbb{Z}_p}$-theory of valuation rings with D-structure where $D = \mathbb{Z}_p$ with distinguished prime element $t = p$ (see Example 2.2.2).

We will also have to consider a variant of $\mathcal{L}_D$: the expansion $\mathcal{L}_D^{\mathrm{d}}$ of $\mathcal{L}_D$ by a single binary function symbol d for "restricted division." We expand each valuation ring R with D-structure, viewed as an $\mathcal{L}_D$-structure as explained above, to an $\mathcal{L}_D^{\mathrm{d}}$-structure by interpreting d as

$$\mathrm{d}(a,b) = \begin{cases} a/b & \text{if } b \neq 0,\ a/b \in R, \\ 0 & \text{else,} \end{cases}$$

for all $a, b \in R$. The $\mathcal{L}_D^{\mathrm{d}}$-theory of valuation rings with D-structure is universally axiomatizable, by the axioms of integral domains, the universal closures of the formulas $x|y \longleftrightarrow \big(x = 0 \vee x \cdot \mathrm{d}(y,x) = y\big)$ and $x|y \vee y|x$, as well as axioms (A1)–(A4) in Definition 2.2.1 above formulated (as universal closures of equations) in $\mathcal{L}_D^{\mathrm{d}}$.

Lemma 2.2.7. *Each $\mathcal{L}_D^{\mathrm{d}}$-term $\tau(C,X)$ in which the function symbol* d *is only applied to subterms not involving the X-variables is equivalent in T_D to some $\mathcal{L}_D^{\mathrm{d}}$-term $f\big(\tau'(C),X\big)$, where $f \in D\langle V,X\rangle$, $V = (V_1,\ldots,V_L)$ is a tuple of new distinct indeterminates, $L \in \mathbb{N}$, and $\tau'(C)$ is an L-tuple of $\mathcal{L}_D^{\mathrm{d}}$-terms.*

Proof. It suffices to deal with $\mathcal{L}_D^{\mathrm{d}}$-terms $\tau(C,X)$ that do not involve the function symbols $+, -, \cdot$ of $\mathcal{L}_D^{\mathrm{d}}$ (since those can be expressed by composition with certain restricted power series). For constants and single variables there is nothing to show, and if $\tau = \mathrm{d}\big(\alpha(C),\beta(C)\big)$, where $\alpha(C)$, $\beta(C)$ are $\mathcal{L}_D^{\mathrm{d}}$-terms, then we can take $f(V) = V$ and $\tau' = \tau$ (where V is a single variable). It remains to treat composition, so say we have

$$\tau(C,X) = g\big(\tau_1(C,X),\ldots,\tau_K(C,X)\big)$$

where $U = (U_1,\ldots,U_K)$ is a K-tuple of distinct indeterminates, $K \in \mathbb{N}$, $g \in D\langle U\rangle$, and $\tau_1(C,X),\ldots,\tau_K(C,X)$ are $\mathcal{L}_D^{\mathrm{d}}$-terms in which the function symbol d is only applied to subterms not involving the X-variables. By induction, for $i = 1,\ldots,K$ take $h_i \in D\langle V_i,X\rangle$,

where $V_i = (V_{i1}, \dots, V_{iL_i})$ is a tuple of new distinct indeterminates, $L_i \in \mathbb{N}$, and an L_i-tuple $\tau_i'(C)$ of $\mathcal{L}_D^{\mathrm{d}}$-terms such that $\tau_i(C, X)$ is equivalent in T_D to $h_i\big(\tau_i'(C), X\big)$. We can assume here that the V_{ij} $(i = 1, \dots, K,\ j = 1, \dots, L_i)$ are distinct, and then we can take $V = (V_1, \dots, V_K)$, $f = g(h_1, \dots, h_K) \in D\langle V, X\rangle$, and $\tau' = (\tau_1', \dots, \tau_K')$. □

Parametric Weierstrass Preparation

Let $f = \sum_\nu f_\nu(C)X^\nu \in D\langle C, X\rangle$ be as in (2.5), and let λ, μ range over $\mathbb{N}^N$. We also let R range over models of T_D and c over R^M. Given any family $\mathcal{F}$ of elements of $D\langle C\rangle$, there is a quantifier-free $\mathcal{L}_D$-formula $\mathrm{Z}_{\mathcal{F}}(C)$ such that for all R and c we have

$$R \models \mathrm{Z}_{\mathcal{F}}(c) \quad \iff \quad f(c) = 0 \text{ for all } f \in \mathcal{F}.$$

This is a simple consequence of the noetherianity of the ring $D\langle C\rangle$: the ideal of $D\langle C\rangle$ generated by $\mathcal{F}$ is generated by finitely many $f_1, \dots, f_m \in \mathcal{F}$, so

$$\mathrm{Z}_{\mathcal{F}}(C) := \bigwedge_i f_i(C) = 0$$

does the job. In particular, there is a quantifier-free $\mathcal{L}_D$-formula $\mathrm{Z}(C) = \mathrm{Z}_f(C)$ such that for all R and c,

$$R \models \mathrm{Z}(c) \quad \iff \quad f_\nu(c) = 0 \text{ for all } \nu \quad \iff \quad f(c, X) = 0.$$

The following is a somewhat more delicate consequence of the noetherianity of $D\langle C\rangle$ (see [23, Lemma 1.5]):

Lemma 2.2.8. *There is some $d \in \mathbb{N}$ such that for all ν with $|\nu| \geqslant d$:*

$$f_\nu = \sum_{|\mu|<d} g_{\nu\mu} f_\mu \qquad \text{where } g_{\nu\mu} \in tD\langle C\rangle.$$

Moreover, the $g_{\nu\mu}$ can be chosen such that $g_{\nu\mu} \to 0$ as $|\nu| \to \infty$, for each fixed μ with $|\mu| < d$.

Take d and $g_{\nu\mu}$ as in Lemma 2.2.8. We then have, for all R, c and ν with $|\nu| \geqslant d$:

$$v\big(f_\nu(c)\big) > \min_\mu v\big(f_\mu(c)\big) = \min_{|\mu|<d} v\big(f_\mu(c)\big). \tag{2.7}$$

Here and below, v denotes the valuation on the fraction field of R associated to the valuation ring R. We denote the lexicographic order on $\mathbb{N}^N$ by $\leqslant$. For each μ with $|\mu| < d$, we define the finite sets

$$A(\mu) := \big\{\nu : |\nu| < d,\ \nu < \mu\big\}, \qquad B(\mu) := \big\{\nu : |\nu| < d,\ \nu > \mu\big\},$$

and we set

$$g_\mu := X^\mu + \sum_{|\lambda| \geqslant d} g_{\lambda\mu} X^\lambda,$$

an element of $D\langle C, X\rangle$. Then by Lemma 2.2.8,

$$f = \sum_{\nu \in A(\mu)} f_\nu g_\nu + f_\mu g_\mu + \sum_{\nu \in B(\mu)} f_\nu g_\nu \qquad \text{(a finite sum)}. \tag{2.8}$$

We also introduce the quantifier-free $\mathcal{L}_D$-formulas $\mathrm{L}_{\mu,f}(C) = \mathrm{L}_\mu(C)$ $(|\mu| < d)$ given by

$$f_\mu(C) \neq 0 \wedge \bigwedge_{\nu \in A(\mu)} v\big(f_\mu(C)\big) \leqslant v\big(f_\nu(C)\big) \wedge \bigwedge_{\nu \in B(\mu)} v\big(f_\mu(C)\big) < v\big(f_\nu(C)\big).$$

Here and below, given $\mathcal{L}_D^{\mathrm{d}}$-terms s, t, we write $v(s) \leqslant v(t)$ instead of the atomic formula $s|t$, and similarly we abbreviate $s|t \wedge \neg t|s$ by $v(s) < v(t)$. By Lemma 2.2.8, given R and c, we have:

(1) $R \models \mathrm{Z}(c)$ if and only if $f_\mu(c) = 0$ for all μ with $|\mu| < d$,

(2) $R \models \mathrm{L}_\mu(c)$ if and only if $f_\mu(c) \neq 0$ and μ is the (lexicographically) largest multiindex μ for which $v\big(f_\mu(c)\big)$ assumes its minimal value;

in particular,

$$R \models \mathrm{Z}(C) \vee \bigvee_{|\mu| < d} \mathrm{L}_\mu(C). \tag{2.9}$$

Put $C(\mu) := A(\mu) \cup B(\mu)$, and for $\nu \in C(\mu)$ define the $\mathcal{L}_D^{\mathrm{d}}$-term $v_{\nu\mu}(C)$ by

$$v_{\nu\mu} := \begin{cases} \mathrm{d}\big(f_\nu, f_\mu\big) & \text{for } \nu \in A(\mu) \\ \mathrm{d}\big(f_\nu, t f_\mu\big) & \text{for } \nu \in B(\mu). \end{cases}$$

Set $v_\mu := \big(v_{\nu\mu}\big)_{\nu \in C(\mu)}$ and introduce the extra indeterminates $V_\mu = \big(V_{\nu\mu}\big)_{\nu \in C(\mu)}$. With these notations, we have (see [23, Theorem 1.12]):

Theorem 2.2.9. *For μ with $|\mu| < d$ there is a restricted power series $h_\mu(C, V_\mu, X) \in D\langle C, V_\mu, X\rangle$ such that:*

(1) *for all R and c such that $R \models \mathrm{L}_\mu(c)$, in $R\langle X\rangle$ we have*

$$f\big(c, T_d(X)\big) = f_\mu(c) h_\mu\big(c, v_\mu(c), X\big);$$

(2) *the reduction $\overline{h_\mu}(C, V_\mu, X) \in \overline{D}[C, V_\mu, X]$ is monic in X_N of degree*

$$s = \mu_1 d^{N-1} + \cdots + \mu_N.$$

Proof. By formally dividing all f_ν's by f_μ in (2.8) and replacing the quotients f_ν/f_μ by $V_{\nu\mu}$ or by $tV_{\nu\mu}$, depending on whether $\nu \in A(\mu) \cup \{\mu\}$ or $\nu \in B(\mu)$, we obtain the series

$$\widetilde{h}_\mu := \sum_{\nu \in A(\mu)} V_{\nu\mu} g_\nu + g_\mu + \sum_{\nu \in B(\mu)} tV_{\nu\mu} g_\nu$$

in $D\langle C, V_\mu, X\rangle$. By construction of $\widetilde{h}_\mu$ we have

$$f(c, X) = f_\mu(c) \widetilde{h}_\mu\big(c, v_\mu(c), X\big)$$

and

$$\widetilde{h}_\mu \bmod t = X^\mu + \sum_{\nu \in A(\mu)} V_{\nu\mu} X^\nu.$$

Now put $h_\mu := \widetilde{h}_\mu\big(C, V_\mu, T_d(X)\big) \in D\langle C, V_\mu, X\rangle$. □

Corollary 2.2.10. *Let $r \in R$. Then*

$$v\big(f(c, X)\big) \geqslant v(r) \quad \Longleftrightarrow \quad f(c, X) \in rR\langle X\rangle.$$

Proof. The case $f(c, X) = 0$ and the direction from right to left being trivial, assume that $v\big(f(c, X)\big) \geqslant v(r)$ and $f(c, X) \neq 0$. Take μ with $|\mu| < d$ and $R \models \mathrm{L}_\mu(c)$. Write

$$f(c, X) = f_\mu(c) \cdot \widetilde{h}_\mu\big(c, v_\mu(c), X\big)$$

as in the proof of Theorem 2.2.9. Then $v\big(f(c, X)\big) = v\big(f_\mu(c)\big) \geqslant v(r)$, hence $\widetilde{r} := f_\mu(c)/r \in R$ and

$$f(c, X)/r = \widetilde{r} \cdot \widetilde{h}_\mu\big(c, v_\mu(c), X\big) \in R\langle X\rangle,$$

showing that $f(c, X) \in rR\langle X\rangle$. □

Using Weierstrass Preparation and Division for $D\langle C, V_\mu, X\rangle$, from Theorem 2.2.9 we also obtain:

Corollary 2.2.11 (Parametric Weierstrass Preparation)**.** *For each μ with $|\mu| < d$, there are a unit $u_\mu \in D\langle C, V_\mu, X\rangle$ as well as a Weierstrass polynomial $w_\mu \in D\langle C, V_\mu, X'\rangle[X_N]$ of X_N-degree $\mu_1 d^{N-1} + \cdots + \mu_N$, such that if $R \models \mathrm{L}_\mu(c)$, then*

$$f\big(c, T_d(X)\big) = f_\mu(c) u_\mu\big(c, v_\mu(c), X\big) w_\mu\big(c, v_\mu(c), X\big).$$

Corollary 2.2.12 (Parametric Weierstrass Division)**.** *Let $g(C, X) \in D\langle C, X\rangle$. For every μ with $|\mu| < d$, there exist $q_\mu \in D\langle C, V_\mu, X\rangle$ and $r_\mu \in D\langle C, V_\mu, X'\rangle[X_N]$ of degree $< \mu_1 d^{N-1} + \cdots + \mu_N$, such that if $R \models \mathrm{L}_\mu(c)$, then with h_μ as in Theorem 2.2.9 we have*

$$g\big(c, T_d(X)\big) = q_\mu\big(c, v_\mu(c), X\big) h_\mu\big(c, v_\mu(c), X\big) + r_\mu\big(c, v_\mu(c), X\big).$$

The proof of Lemma 2.2.8 given in [23] shows that we can take for d *any* sufficiently large natural number. Hence, given any finite set of f's in $D\langle C, X\rangle$, we can take d so large that it serves for each of these f's. The discussion preceding Theorem 2.2.9 applies to all f's simultaneously, and this way we obtain a version of Theorem 2.2.9 for several (finitely many) power series:

Corollary 2.2.13. *Let $f_1, \ldots, f_n \in D\langle C, X\rangle$, where*

$$f_j = \sum_\nu f_{\nu j}(C) X^\nu \quad \text{with } f_{\nu j}(C) \in D\langle C\rangle.$$

There exists $d \in \mathbb{N}$ and a finite family $\big\{(\varphi_i, v_i)\big\}_{i \in I}$ consisting of quantifier-free $\mathcal{L}_D$-formulas $\varphi_i(C)$ and tuples $v_i(C) = \big(v_{i1}(C), \ldots, v_{iL}(C)\big)$ of $\mathcal{L}_D^{\mathrm{d}}$-terms, and for all $i \in I$ and $j \in \{1, \ldots, n\}$ there is $h_{ij} \in D\langle C, V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new variables, such that $T_D \models \bigvee_i \varphi_i$ and given i, j,

(1) *there is $\nu = \nu(i, j)$ such that if $R \models \varphi_i(c)$, then*

$$f_j\big(c, T_d(X)\big) = f_{\nu j}(c) h_{ij}\big(c, v_i(c), X\big);$$

(2) *either $h_{ij} = 0$ or $\overline{h_{ij}} \in \overline{D}[C, V, X]$ is monic in X_N.*

Corollaries 2.2.11 and 2.2.12 may be similarly generalized; we leave the formulation of the exact statements to the reader. Next a version of Lemma 2.5 in [24]:

Corollary 2.2.14. *If $f(c, X) = 0$ (that is, $f_\nu(c) = 0$ for all ν), then $f(c, x) = 0$ for all $x \in R^N$. Conversely, if R is infinite and $f(c, x) = 0$ for all $x \in R^N$, then $f(c, X) = 0$.*

Proof. The equation $f = \sum_{|\nu|<d} f_\nu g_\nu$ from (2.8) yields the first statement. Suppose R is infinite, and we have some μ with $|\mu| < d$ and $R \models \mathrm{L}_\mu(c)$. Then by Corollary 2.2.11,

$$f\big(c, T_d(X)\big) = f_\mu(c) u_\mu\big(c, v_\mu(c), X\big) w_\mu\big(c, v_\mu(c), X\big)$$

where $u_\mu \in D\langle C, V_\mu, X\rangle$ is a unit and $w_\mu \in D\langle C, V_\mu, X'\rangle[X_N]$ is a Weierstrass polynomial in X_N. We have $f_\mu(c) \neq 0$ and $u_\mu\big(c, v_\mu(c), x\big) \neq 0$ for each $x \in R^N$. Taking $x \in R^N$ such that $w_\mu\big(c, v_\mu(c), x\big) \neq 0$ (possible since R is infinite), we obtain $f\big(c, T_d(x)\big) \neq 0$. Hence if $f(c, x) = 0$ for all $x \in R^N$, then $R \not\models \mathrm{L}_\mu(c)$ for $|\mu| < d$, so $R \models \mathrm{Z}(c)$ by (2.9). □

If $f, f' \in D\langle C, X\rangle$ satisfy $f(c, X) = f'(c, X)$, then Corollary 2.2.14 applied to $f - f'$ in place of f yields $f(c, x) = f'(c, x)$ for all $x \in R^N$. Hence given $g \in R\langle X\rangle$ and $x \in R^N$, we can define an element $g(x)$ of R as follows: pick $f \in D\langle C, X\rangle$ and $c \in R^M$ such that $g = f(c, X)$, and set $g(x) := f(c, x)$. The argument above and Lemma 2.2.4 show that this definition does not depend on the choice of f, c. Corollary 2.2.14 also shows that if R is infinite, then the R-algebra morphism which assigns to $g \in R\langle X\rangle$ the function $x \mapsto g(x)\colon R^N \to R$ is injective. Therefore from Lemma 2.2.7 we obtain:

Corollary 2.2.15. *Let $\tau(C, X)$ be an $\mathcal{L}_D^{\mathrm{d}}$-term in which the function symbol* d *is only applied to subterms not involving the X-variables, and let $R \models T_D$ and $c \in R^M$. Then there is a unique $g \in R\langle X\rangle$ such that $\tau(c, x) = g(x)$ for all $x \in R^N$ (which we denote by $\tau(c, X)$ below).*

We can now also define the composition of power series from $R\langle X\rangle$. For this we may assume that the valuation of R is nontrivial, since otherwise $R\langle X\rangle = R[X]$; in particular, R is infinite. Let $f \in R\langle X\rangle$ and $g_1, \ldots, g_N \in R\langle Y\rangle$ where $Y = (Y_1, \ldots, Y_L)$ is a tuple of indeterminates, $L \in \mathbb{N}$. By Lemma 2.2.4 take $f^* \in D\langle C, X\rangle$, $g_1^*, \ldots, g_N^* \in D\langle C, Y\rangle$ and

$c \in R^M$ such that $f(X) = f^*(c, X)$ and $g_i(Y) = g_i^*(c, Y)$ and put

$$h(C, Y) := f^*\big(C, g_1^*(C, Y), \ldots, g_N^*(C, Y)\big) \in D\langle C, Y\rangle.$$

Then by Lemma 2.2.3 we have

$$h(c, y) = f\big(g_1(y), \ldots, g_N(y)\big) \quad \text{for all } y \in R^L.$$

Hence the power series $h(c, Y) \in R\langle Y\rangle$ only depends on $f, g_1, \ldots, g_N$. (Corollary 2.2.14.) This allows us to set

$$f(g_1, \ldots, g_N) := h(c, Y) \in R\langle Y\rangle.$$

One verifies easily that the map

$$f \mapsto f(g_1, \ldots, g_N)\colon R\langle X\rangle \to R\langle Y\rangle$$

is an R-algebra morphism.

2.3 Weierstrass Division for Nonstandard Restricted Power Series

The Gauss valuation

In this section we again let D and t be as in Section 2.1, and we let $R \models T_D$. The parametric Weierstrass Division and Preparation Theorems from the preceding section give rise to corresponding theorems for the ring $R\langle X\rangle$ of "nonstandard" restricted power series with coefficients in R. We formulate these theorems below and note some of their consequences.

Let $v\colon F^\times \to \Gamma := v(F^\times)$ be the valuation on $F = \mathrm{Frac}(R)$ associated to the valuation ring R. Given $g \in R\langle X\rangle^{\neq}$ we take $f = \sum_\nu f_\nu(C)X^\nu \in D\langle C, X\rangle$ and $c \in R^M$ (for some M) such that $g(X) = f(c, X)$; note that then by (2.7) there is some μ such that $v\big(f_\mu(c)\big) = \min_\nu v\big(f_\nu(c)\big)$, and we set $v(g) := v\big(f_\mu(c)\big)$. It is easy to check that $v\colon R\langle X\rangle^{\neq} \to \Gamma$ is a valuation on the integral domain $R\langle X\rangle$, which we call the **Gauss valuation** on $R\langle X\rangle$. This valuation extends uniquely to a valuation $v\colon K^\times \to \Gamma$ on the fraction field K of $R\langle X\rangle$, which we also call the Gauss valuation on K. Note that v extends the valuation on F denoted by the same symbol. We set $\overline{R} := R/t_R R$. Recall that $\mathfrak{m} = t_R R$ is the maximal ideal of R.

Reduction mod $\mathfrak{m}^n$

Let $f = \sum_\nu f_\nu X^\nu \in D\langle C, X\rangle$ where $f_\nu \in D\langle C\rangle$ for each ν. Note that in $D\langle C\rangle$ we have $f_\nu \to 0$ as $|\nu| \to \infty$. Hence given n there is some $d \in \mathbb{N}$ such that $f_\nu \in t^{n+1}D\langle C\rangle$ for $|\nu| > d$, and so for each $R \models T_D$ and $c \in R^M$ we have $f(c, X) \equiv \sum_{|\nu|\leqslant d} f_\nu(c)X^\nu \bmod \mathfrak{m}^n R\langle X\rangle$. The residue morphism

$$r \mapsto r \bmod \mathfrak{m}^n := r + \mathfrak{m}^n \colon R \to R/\mathfrak{m}^n$$

extends to the ring morphism

$$g = \sum_\nu g_\nu X^\nu \mapsto g \bmod \mathfrak{m}^n := \sum_\nu (g_\nu \bmod \mathfrak{m}^n)X^\nu \colon R[[X]] \to (R/\mathfrak{m}^n)[[X]].$$

By the remarks at the beginning of this section, if $g \in R\langle X\rangle$, then $g \bmod \mathfrak{m}^n$ lies in the subring $(R/\mathfrak{m}^n)[X]$ of $(R/\mathfrak{m}^n)[[X]]$. The resulting ring morphism

$$g \mapsto g \bmod \mathfrak{m}^n \colon R\langle X\rangle \to (R/\mathfrak{m}^n)[X]$$

is onto, and by Corollary 2.2.10 its kernel is $\mathfrak{m}^n R\langle X\rangle$, so we obtain an isomorphism

$$R\langle X\rangle/\mathfrak{m}^n R\langle X\rangle \xrightarrow{\cong} (R/\mathfrak{m}^n)[X]$$

via which we identify $R\langle X\rangle/\mathfrak{m}^n R\langle X\rangle$ with the polynomial ring $(R/\mathfrak{m}^n)[X]$ in the following. For $n = 1$ we obtain $R\langle X\rangle/\mathfrak{m}R\langle X\rangle = \overline{R}[X]$, and we set $\overline{g} := g \bmod \mathfrak{m}$ for $g \in R\langle X\rangle$.

The Jacobson radical of $R\langle X\rangle$

Given a ring A, we let

$$\operatorname{rad}(A) := \{a \in A : 1 + ba \in A^\times \text{ for all } b \in A\}$$

denote the Jacobson radical of A; this equals the intersection of all maximal ideals of A.

Lemma 2.3.1. $R\langle X\rangle^\times = R^\times\big(1 + t_R R\langle X\rangle\big) = \big\{g \in R\langle X\rangle : \overline{g} \in \overline{R}^\times\big\}$.

Proof. Clearly $R^\times \subseteq R\langle X\rangle^\times$. Let $g \in R\langle X\rangle$, and take $f \in D\langle C, X\rangle$ and $c \in R^M$ (for some M) with $g(X) = f(c, X)$; then $1 + tf \in D\langle C, X\rangle^\times$ by (2.2), so $g \in R\langle X\rangle^\times$. This yields $R^\times\big(1 + t_R R\langle X\rangle\big) \subseteq R\langle X\rangle^\times$. The other inclusions are easy. □

By the previous lemma we have $\operatorname{rad}(R\langle X\rangle) = t_R R\langle X\rangle$; hence:

Corollary 2.3.2. *Each maximal ideal of $R\langle X\rangle$ contains the maximal ideal $\mathfrak{m}_R$ of R.*

Weierstrass Division and Preparation for $R\langle X\rangle$

We call $g \in R\langle X\rangle$ **regular in X_N of degree** $s \in \mathbb{N}$ if $\overline{g}$ is a unit-monic polynomial of degree s in X_N. By Theorem 2.2.9, we have:

Corollary 2.3.3. *For each $g \in R\langle X\rangle^{\neq}$ there are $d \in \mathbb{N}$, $a \in R$, and $h \in R\langle X\rangle$ such that $g\big(T_d(X)\big) = a \cdot h(X)$ where $\overline{h}$ is monic in X_N (and hence h is regular in X_N).*

A monic polynomial in $R\langle X'\rangle[X_N]$ of degree s is called a **Weierstrass polynomial (in X_N) of degree s.** The parametric Weierstrass Division and Preparation Theorems give us versions of Weierstrass Division and Preparation for $R\langle X\rangle$:

Corollary 2.3.4 (Weierstrass Division for $R\langle X\rangle$)**.** *Let $f, g \in R\langle X\rangle$ be such that f is regular of degree s in X_N. Then there exist uniquely determined $q \in R\langle X\rangle$ and $r \in R\langle X'\rangle[X_N]$ such that $g = qf + r$ and $\deg_{X_N} r < s$.*

Proof. The existence part follows easily from parametric Weierstrass Division. For uniqueness, it suffices to show: if $f, g \in R\langle X\rangle$ and $r \in R\langle X'\rangle[X_N]$ are such that $\overline{f} \in \overline{R}[X]$ is monic in X_N, $\deg_{X_N} r < \deg_{X_N} \overline{f} = s$, and $0 = qf + r$, then $q = r = 0$. Suppose otherwise, that is, $q, r \neq 0$. Let $a \in R$ be such that $v(a) = \min\{v(q), v(r)\}$. After dividing q and r by a (using Corollary 2.2.10), we may assume $a = 1$. But then $\overline{r} = \overline{q}\,\overline{f}$ with $\overline{f} \in \overline{R}[X]$ monic in X_N of degree s and $\deg_{X_N} \overline{r} < s$. Hence $\overline{q} = \overline{r} = 0$, that is, $v(q), v(r) > 0$, a contradiction. □

In particular, we get, with R and f as in the corollary:

$$R\langle X\rangle / fR\langle X\rangle \cong R\langle X'\rangle \oplus R\langle X'\rangle\overline{X_N} \oplus \cdots \oplus R\langle X'\rangle\overline{X_N}^{s-1} \tag{2.10}$$

as $R\langle X'\rangle$-algebras, where $\overline{X_N} = X_N \bmod f$. Applying the previous corollary with $f = X_N^s$ also yields:

Corollary 2.3.5 (Weierstrass Preparation Theorem for $R\langle X\rangle$)**.** *Let $g \in R\langle X\rangle$ be regular in X_N of degree s. Then there are a unique Weierstrass polynomial $w \in R\langle X'\rangle[X_N]$ of degree s and a unique unit $u \in R\langle X\rangle$ such that $g = u \cdot w$.*

In the same way as Theorem 2.1.3 gave us Corollary 2.1.5, from Corollary 2.3.4 we obtain:

Corollary 2.3.6. *Let $w \in R\langle X'\rangle[X_N]$ be a Weierstrass polynomial. Then the natural inclusion $R\langle X'\rangle[X_N] \subseteq R\langle X\rangle$ induces an isomorphism*

$$R\langle X'\rangle[X_N]/wR\langle X'\rangle[X_N] \xrightarrow{\cong} R\langle X\rangle/wR\langle X\rangle.$$

Let now I be a finitely generated ideal of $R\langle X\rangle$ which contains a Weierstrass polynomial w of degree d in X_N. Then there are polynomials $f_1, \dots, f_n \in R\langle X'\rangle[X_N]$ of degree $< d$ which, together with w, generate the ideal I: indeed, if $f_1, \dots, f_n \in I$ are any power series which, together with w, generate I, then we may replace $f_1, \dots, f_n$ by their respective remainders upon Weierstrass Division by w. For such generators we have:

Corollary 2.3.7. *Let $f_1, \dots, f_n \in R\langle X'\rangle[X_N]$ be such that $f_1, \dots, f_n, w$ generate I. Then the ideal $I \cap R\langle X'\rangle[X_N]$ of $R\langle X'\rangle[X_N]$ is also generated by $f_1, \dots, f_n, w$.*

Proof. Let $g \in I \cap R\langle X'\rangle[X_N]$, say $g = f_1y_1 + \cdots + f_ny_n + wz$ where $y_1, \dots, y_n, z \in R\langle X\rangle$. Take $q_1, \dots, q_n \in R\langle X\rangle$, $r_1, \dots, r_n \in R\langle X'\rangle[X_N]$ (of degree $< d$) such that $y_i = q_iw + r_i$ for $i = 1, \dots, n$. Then $g = f_1r_1 + \cdots + f_nr_n + wz'$ where $z' := z + \sum_i q_i$, hence $wz' = g - \sum_i f_ir_i \in R\langle X'\rangle[X_N]$, and so $z' \in R\langle X'\rangle[X_N]$ by Corollary 2.3.6. □

Weierstrass Division for $F\langle X\rangle$

We let again $R \models T_D$ and $F = \mathrm{Frac}(R)$. We now define $F\langle X\rangle$ to be the subring of $F[[X]]$ generated by F and $R\langle X\rangle$, so

$$F\langle X\rangle = \left\{a^{-1}g : a \in R^{\neq},\ g \in R\langle X\rangle\right\}.$$

(In other words, $F\langle X\rangle$ is the localization of $R\langle X\rangle$ at its multiplicative subset $R^{\neq}$.) From Corollary 2.2.10 one obtains

$$F\langle X\rangle \cap R[[X]] = R\langle X\rangle,$$

and from Lemma 2.3.1 we get

$$F\langle X\rangle^\times = F^\times\big(1 + t_R R\langle X\rangle\big). \tag{2.11}$$

Every polynomial automorphism of $R\langle X\rangle$ extends uniquely to an automorphism of the F-algebra $F\langle X\rangle$; we call the F-algebra automorphisms of $F\langle X\rangle$ arising this way **polynomial automorphisms** of $F\langle X\rangle$. In particular, for each $d \in \mathbb{N}$, the F-algebra automorphism $g(X) \mapsto g\big(T_d(X)\big)$ of $F[[X]]$ maps the subring $F\langle X\rangle$ of $F[[X]]$ into itself. An element $f \in F\langle X\rangle$ is called **regular in X_N of degree** $s \in \mathbb{N}$ if there is some $a \in R$ such that $af \in R\langle X\rangle$ and af is regular in X_N of degree s (as an element of $R\langle X\rangle$). Corollary 2.3.3 implies that for each $f \in F\langle X\rangle^{\neq}$ there is some $d \in \mathbb{N}$ such that $f\big(T_d(X)\big) \in F\langle X\rangle$ is regular in X_N (of some degree). In $F\langle X\rangle$ we can divide by regular elements:

Corollary 2.3.8 (Weierstrass Division Theorem for $F\langle X\rangle$)**.** *Let $g \in F\langle X\rangle$ be regular in X_N of degree s. Then every $f \in F\langle X\rangle$ can be uniquely written as $f = qg + r$ with $q \in F\langle X\rangle$ and $r \in F\langle X'\rangle[X_N]$, $\deg_{X_N} r < s$.*

This is easily reduced to the Weierstrass Division Theorem for $R\langle X\rangle$. As before, it follows:

Corollary 2.3.9 (Weierstrass Preparation Theorem for $F\langle X\rangle$)**.** *Let $g \in F\langle X\rangle$ be regular in X_N of degree s. Then there are a unique Weierstrass polynomial $w \in R\langle X'\rangle[X_N]$ of degree s and a unique unit $u \in F\langle X\rangle$ such that $g = u \cdot w$.* □

From [14, (5.2.5)] we borrow the following convenient terminology: Let A' be a ring, Y be a single indeterminate over A', and A be a ring containing $A'[Y]$ as a subring; then A is *Rückert* over A' if there is a set $\mathcal{W}$ of monic polynomials in $A'[Y]$ such that the following three conditions are satisfied:

(R1) if $w, w^* \in A'[Y]$ are monic and $w \cdot w^* \in \mathcal{W}$, then $w, w^* \in \mathcal{W}$;

(R2) for all $w \in \mathcal{W}$ the natural inclusion $A'[Y] \to A$ induces an isomorphism

$$A'[Y]/wA'[Y] \to A/wA;$$

(R3) for each $g \in A^{\neq}$ there is an automorphism σ of A and a unit $u \in A^{\times}$ such that $u \cdot \sigma(g) \in \mathcal{W}$.

For an ideal I of a ring A we let

$$\sqrt[\mathrm{J}]{I} := \{a \in A : 1 + ab \text{ is a unit mod } I, \text{ for all } b \in A\}$$

be the Jacobson radical of I; this also equals the intersection of all maximal ideals of A containing I, so $\sqrt{I} \subseteq \sqrt[\mathrm{J}]{I}$. Also note that $\sqrt[\mathrm{J}]{\{0\}} = \mathrm{rad}(A)$. One says that A is a *Jacobson ring* if $\sqrt{I} = \sqrt[\mathrm{J}]{I}$ for each ideal I of A. The following is shown in [14, loc. cit.]:

Proposition 2.3.10. *Suppose A is Rückert over A'. Then*

(1) *if A' is noetherian, then so is A;*

(2) *if A is an integral domain and A' is a unique factorization domain, then so is A;*

(3) *if A' is a Jacobson ring and $I \neq \{0\}$ is an ideal of A, then $\sqrt{I} = \sqrt[\mathrm{J}]{I}$.*

As a consequence, we obtain:

Corollary 2.3.11. *The ring $F\langle X\rangle$ is noetherian, a unique factorization domain, and a Jacobson ring.*

Proof. We proceed by induction on N. The claims hold trivially for $N = 0$, so suppose $N \geqslant 1$, and we have shown our claims for $F\langle X'\rangle$ in place of $F\langle X\rangle$. Then $F\langle X\rangle$ is Rückert over $F\langle X'\rangle$, as witnessed by $Y = X_N$ and $\mathcal{W} =$ the set of Weierstrass polynomials $w \in R\langle X'\rangle[X_N]$. (See Corollaries 2.3.6 and 2.3.9.) Using Lemma 2.3.1 it is easy to see that $\mathrm{rad}(F\langle X\rangle) = \{0\}$. Hence our claims for $F\langle X\rangle$ follow from Proposition 2.3.10 and inductive hypothesis. □

Note that in contrast to the previous corollary, the ring $R\langle X\rangle$ is rarely noetherian. Later we will see that $R\langle X\rangle$ is always *coherent,* that is, for all $f_1, \ldots, f_m \in R\langle X\rangle$ the submodule of the $R\langle X\rangle$-module $R\langle X\rangle^m$ consisting of the solutions to the homogeneous linear equation

$$f_1 y_1 + \cdots + f_m y_m = 0$$

is finitely generated; see Theorem 3.3.5. Being a UFD, $F\langle X\rangle$ is integrally closed (in its fraction field). The following consequence of this will be useful later:

Corollary 2.3.12. *$R\langle X\rangle$ is integrally closed.*

Proof. Let $P \in R\langle X\rangle[Y]$ be a monic polynomial in the single indeterminate Y and $y \in F\langle X\rangle$ with $P(y) = 0$; by the remark preceding the corollary it is enough to show that $y \in R\langle X\rangle$. For this we can assume $y \neq 0$, hence write $y = z/a$ where $z \in R\langle X\rangle$ with $v(z) = 0$ and $a \in F^\times$. Let $P_0, \ldots, P_{n-1} \in R\langle X\rangle$ $(n \geqslant 1)$ with $P = Y^n + P_{n-1}Y^{n-1} + \cdots + P_0$. Then $P_{n-1}az^{n-1} + \cdots + P_0a^n = -z^n$ and hence $v(a) \leqslant 0$, so $y \in R\langle X\rangle$ as claimed. □

Let A be a ring. We let $\dim A$ denote the Krull dimension of A; it is well-known (Cohen-Seidenberg) that if B is an integral ring extension of A, then $\dim B = \dim A$ [11, Chapter 5]. For an ideal I of A we set $\dim I := \dim A/I$. The following corollary is a non-standard version of the fact that $\dim \mathbb{Q}_p\langle X\rangle = N$:

Corollary 2.3.13. $\dim F\langle X\rangle = N$.

Proof. By induction on N. The case $N = 0$ is trivial, so suppose $N \geqslant 1$. The sequence of prime ideals

$$\{0\} \subseteq (X_1) \subseteq (X_1, X_2) \subseteq \cdots \subseteq (X_1, \ldots, X_N)$$

of $F\langle X\rangle$ shows that $\dim F\langle X\rangle \geqslant N$. Let $P \neq \{0\}$ be a prime ideal of $F\langle X\rangle$. Take $g \in P\backslash\{0\}$; then $\dim gF\langle X\rangle \geqslant \dim P$. After replacing P, g by $T_d(P)$, $T_d(g)$ for suitable $d \in \mathbb{N}$, we can assume that g is regular in X_N, and then, by Corollary 2.3.9, that g is a Weierstrass polynomial (necessarily of positive degree) in X_N. By Corollary 2.3.8, the natural morphism $F\langle X'\rangle \to F\langle X\rangle/gF\langle X\rangle$ is injective, and identifying $F\langle X'\rangle$ with its image, $F\langle X\rangle/gF\langle X\rangle$ is an integral extension of $F\langle X'\rangle$. Hence $\dim F\langle X\rangle/gF\langle X\rangle = \dim F\langle X'\rangle = N-1$ by inductive hypothesis. This implies $\dim F\langle X\rangle \leqslant N$ as required. □

The case $N = 1$

In this subsection we restrict to the case $N = 1$, and we write X for our indeterminate X_1. Let $R \models T_D$ and $F = \mathrm{Frac}(R)$. Note that then each nonzero element f of $F\langle X\rangle$ is automatically

regular in X, and so by Corollary 2.3.9 and (2.11) there is a unique triple (a, u, g) where $a \in F^\times$, $u \in 1 + t_R R\langle X\rangle$ and $g \in R[X]$ is monic such that $f = a\,u\,g$. (In particular, $F\langle X\rangle$ is a PID.) More generally we have:

Lemma 2.3.14. *Let $f \in \mathrm{Frac}(F\langle X\rangle)^\times$. Then there is a unique tuple (a, u, g, h) where $a \in F^\times$, $u \in 1 + t_R R\langle X\rangle$, and $g, h \in R[X]$ are monic and coprime in $F[X]$, such that $f = a\,u\,\dfrac{g}{h}$.*

By model-theoretic compactness we obtain a parametric version, for simplicity formulated here only for $f \in D\langle C, X\rangle$:

Corollary 2.3.15. *There are a tuple $V = (V_1, \dots, V_L)$ of new indeterminates, where $L \in \mathbb{N}$, and finitely many tuples (a_i, u_i, v_i, g_i) $(i \in I)$ where $a_i \in D\langle C\rangle$, $u_i \in 1 + tD\langle V, X\rangle$, $v_i(C)$ are L-tuples of $\mathcal{L}_D^{\mathrm{d}}$-terms, and $g_i \in D\langle V\rangle[X]$ are monic, such that for all $R \models T_D$ there is some $i \in I$ such that*

$$f(c, X) = a_i(c) \cdot u_i\big(v_i(c), X\big) \cdot g_i\big(v_i(c), X\big).$$

Part I

Uniform Basic Ideal Theory

CHAPTER 3

Hermann's Method and Generalizations

In Section 3.1 we describe Grete Hermann's classical method [42] for constructing solutions of linear equations over polynomial rings over fields on a fairly general level, for systems of linear equations over any integral domain D. In the next section, following [7] we specialize it to the case where $D = \mathbb{Z}_p\langle X\rangle$ is a ring of restricted power series, and in Section 3.3 we discuss uniformity in parameters. We begin by establishing an inductive procedure to reduce the complexity of our systems, and incorporating a method of *p-desingularization* (from [9]) for ensuring that our power series are regular and amenable to Weierstrass Division. To prove the general definability results, we use the method of ultraproducts.

Solving a system of homogeneous equations is equivalent to computing the generators of ideal intersections and quotients. (3.1.4, 3.1.5.) Therefore, many of our investigations of radical and prime ideals in later chapters will rely on the methods in the present chapter. Section 3.3 already contains a few applications of Hermann's method to definability of basic ideal-theoretic operations in $\mathbb{Z}_p\langle X\rangle$.

3.1 Hermann's Method

Throughout this section we let D be an integral domain with fraction field K.

A high-level view of Hermann's method

Suppose we are given an $m \times n$ matrix $A = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$ as well as a column vector $b = [b_1, \ldots, b_m]^{\mathrm{tr}}$ with entries in D. We are interested in accomplishing the following two tasks:

(H) effectively finding a set of generators for the module $\mathrm{Sol}(A) = \mathrm{Sol}_D(A)$ of solutions of the homogeneous system of linear equations

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \tag{I}$$

(or $Ay = 0$) with coefficient matrix A;

(H_b) determining whether the system

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \tag{I_b}$$

(or $Ay = b$) is solvable for some $y = [y_1, \ldots, y_n]^{\mathrm{tr}} \in D^n$, and if it is, effectively finding such a solution.

Note that (H) and (H_b) combined then allow us to effectively obtain a complete description of *all* solutions to (I_b) in D^n. (Here we use "effectively" in an informal manner, essentially meaning "elementary recursively in the ring operations and division in D.") Of course, for this we may assume $A \neq 0$, so the rank $r = \mathrm{rank}_K(A)$ of A (considered as a matrix over K) is $\geqslant 1$. Let Δ be an $r \times r$ submatrix of A with $\delta = \det \Delta \neq 0$. After rearranging the order of the equations and permuting the unknowns $y_1, \ldots, y_n$ in the systems (I) and (I_b), we may assume that $\Delta = (a_{ij})_{1 \leqslant i,j \leqslant r}$. We now indicate how (H) and (H_b) can be reduced to similar problems over the homomorphic image $\overline{D} := D/\delta D$ of D. In general, the ring $\overline{D}$ is not an integral domain anymore, but it is often "simpler" than D; in the next section we shall see how this can be exploited for $D = \mathbb{Z}_p\langle X \rangle$.

Homogeneous equations

We first consider the problem of finding a set of generators for $\mathrm{Sol}(A)$. Each row $a_i = (a_{i1}, \ldots, a_{in})$ with $r < i \leqslant m$ is a K-linear combination of the first r rows $a_1, \ldots, a_r$ of A,

so (I) has the same solutions in D^n as the system

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rn} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Changing notation, we can assume $r = m$. Multiplying both sides of $Ay = 0$ on the left by the adjoint Δ^{ad} of Δ, (I) then turns into the system

$$\begin{bmatrix} \delta & & & c_{1,r+1} & \cdots & c_{1,n} \\ & \delta & & c_{2,r+1} & \cdots & c_{2,n} \\ & & \ddots & \vdots & \ddots & \vdots \\ & & \delta & c_{r,r+1} & \cdots & c_{rn} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{II}$$

with $c_{ij} \in D$ for $1 \leqslant i \leqslant r < j \leqslant n$, which has the same solutions in D^n as (I). We note the following $n - r$ linearly independent solutions of (II):

$$v^{(1)} = \begin{bmatrix} -c_{1,r+1} \\ \vdots \\ -c_{r,r+1} \\ \delta \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \; v^{(2)} = \begin{bmatrix} -c_{1,r+2} \\ \vdots \\ -c_{r,r+2} \\ 0 \\ \delta \\ \vdots \\ 0 \end{bmatrix}, \; \ldots, \; v^{(n-r)} = \begin{bmatrix} -c_{1,n} \\ \vdots \\ -c_{r,n} \\ 0 \\ \vdots \\ 0 \\ \delta \end{bmatrix}. \tag{3.1}$$

If δ is a unit, these vectors in fact form a basis for $\mathrm{Sol}(A)$. Suppose δ is not a unit, so $\overline{D} \neq 0$, and consider the system

$$\begin{bmatrix} \overline{c_{1,r+1}} & \cdots & \overline{c_{1n}} \\ \vdots & \ddots & \vdots \\ \overline{c_{r,r+1}} & \cdots & \overline{c_{rn}} \end{bmatrix} \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \tag{$\overline{\text{II}}$}$$

over $\overline{D}$. Here and below $\overline{a} := a + \delta D \in \overline{D}$ for $a \in D$. The following is now obvious:

Lemma 3.1.1. *Each collection $y^{(1)}, \ldots, y^{(M)} \in D^{n-r}$ of column vectors whose reductions $\overline{y^{(1)}}, \ldots, \overline{y^{(M)}} \in \overline{D}^{n-r}$ generate the $\overline{D}$-module of solutions to* ($\overline{\text{II}}$) *may be extended uniquely to M vectors in D^n which, together with the solutions of* (I) *in* (3.1)*, generate* $\mathrm{Sol}(A)$.

Inhomogeneous equations

Similarly to the case of homogeneous equations, finding solutions to an inhomogeneous system (I_b) of linear equations over D can be reduced to an analogous problem over the quotient $\overline{D} = D/\delta D$ of D. A *necessary condition* for (I_b) to have a solution $y \in D^n$ is clearly that

$$r = \mathrm{rank}_K(A) = \mathrm{rank}_K(A, b). \tag{NC}$$

Assume (NC) holds. Then (I_b) has the same solutions in D^n as the system

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rn} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_r \end{bmatrix}.$$

As above, after changing notation we may assume that $r = m$. Multiplying both sides of $Ay = b$ on the left by Δ^{ad}, (I) turns into the system

$$\begin{bmatrix} \delta & & & c_{1,r+1} & \cdots & c_{1,n} \\ & \delta & & c_{2,r+1} & \cdots & c_{2,n} \\ & & \ddots & \vdots & \ddots & \vdots \\ & & \delta & c_{r,r+1} & \cdots & c_{rn} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{bmatrix} \tag{II_b}$$

with $c_{ij}, d_i \in D$ for $1 \leqslant i \leqslant r < j \leqslant n$, which has the same solutions in D as (I_b). Clearly, a sufficient condition for (II_b) to have a solution $y = [y_1, \ldots, y_n]^{\mathrm{tr}} \in D^n$ is that $d_1, \ldots, d_r$ are each divisible by δ. This will be the case if δ is a unit; then a solution to (II_b) (and hence to (I_b)) in D is given by

$$y_j = \begin{cases} d_j/\delta & \text{for } 1 \leqslant j \leqslant r, \\ 0 & \text{for } r < j \leqslant n. \end{cases} \tag{3.2}$$

Suppose δ is not a unit, so $\overline{D} \neq 0$. Then, reducing the coefficients in (II_b) modulo δ, the system (II_b) turns into the system

$$\begin{bmatrix} \overline{c_{1,r+1}} & \cdots & \overline{c_{1n}} \\ \vdots & \ddots & \vdots \\ \overline{c_{r,r+1}} & \cdots & \overline{c_{rn}} \end{bmatrix} \begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} \overline{d_1} \\ \vdots \\ \overline{d_r} \end{bmatrix} \tag{$\overline{\mathrm{II}_b}$}$$

over $\overline{D}$. We now have an analogue of Lemma 3.1.1:

Lemma 3.1.2. *For all $y_{r+1}, \ldots, y_n \in D$ with the property that $[\overline{y_{r+1}}, \ldots, \overline{y_n}]^{\mathrm{tr}}$ is a solution of the reduced system $(\overline{\mathrm{II}_b})$ there are uniquely determined $y_1, \ldots, y_r \in D$ such that*

$$[y_1, \ldots, y_r, y_{r+1}, \ldots, y_n]^{\mathrm{tr}} \in D^n$$

is a solution of (II_b), and hence of (I_b).

In particular, (I_b) is solvable in D if and only if $(\overline{\mathrm{II}_b})$ is solvable in $\overline{D}$.

Remark 3.1.3. For use in Section 4.1 we note in passing that (3.2) also shows that we always find a solution $y \in K^n$ to (I_b) whose components lie in $\frac{1}{\delta}D$, where *the denominator δ only depends on the matrix A and not on the right-hand side b* in (I_b).

Desingularization

In our adaptation of Hermann's method in the case $D = \mathbb{Z}_p\langle X\rangle$ below, it will be crucial that we are able to arrange $\delta \bmod p \neq 0$ in the above (since otherwise Weierstrass Division by the restricted power series δ is *inapplicable*). In order to do so, we shall first transform the systems (I) and (I_b) into equivalent systems for which $\delta \bmod p \neq 0$ for a suitable $r \times r$ minor δ of the new coefficient matrix, which is also of rank r. This process of *p-desingularization* (cf. [9]) can also be formulated in the present general context. For this we suppose in addition that we are given a prime element p of D such that $\bigcap_{e\in\mathbb{N}} p^e D = \{0\}$. We let $v = v_p$ be the p-adic valuation on D, given by $v(a) = e \in \mathbb{N}$ if $a \in p^e D \setminus p^{e+1}D$ and $v(0) := \infty > \mathbb{N}$. As before $K = \mathrm{Frac}(D)$ denotes the fraction field of D; we also let $K(p) := \mathrm{Frac}\big(D/pD\big)$. As in the previous subsection we let $A = (a_{ij})$ be an $m \times n$ matrix over D, of rank $r = \mathrm{rank}_K(A) \geqslant 1$, and let $b = [b_1, \ldots, b_m]^{\mathrm{tr}} \in D^m$. We shall show how to construct an $r \times n$ matrix B over D, depending only on A (and not on b), and a vector $c = [c_1, \ldots, c_r]^{\mathrm{tr}} \in D^r$ with the following properties:

(1) $r = \mathrm{rank}_K(B) = \mathrm{rank}_{K(p)}(B \bmod p)$, and

(2) the systems $Ay = b$ and $By = c$ have the same solutions in every integral domain extending D.

It may happen that one of the steps of the algorithm to construct (B, c) cannot be carried out, but then we will know that $Ay = b$ has no solution $y \in D^n$.

As before, we may assume that the necessary condition (NC) above holds, and then, after removing superfluous rows from (A, b), we may further assume that the rows of A are K-linearly independent, i.e., $m = r$. Let Δ be an $r \times r$ submatrix of A chosen so that the value $v(\det \Delta)$ is *minimal* among all $r \times r$ submatrices of A. After rearranging the columns of A we can assume that $\Delta = (a_{ij})_{1 \leqslant i,j \leqslant r}$. As above, consider now the system

$$\begin{bmatrix} \delta & & & c_{1,r+1} & \cdots & c_{1,n} \\ & \delta & & c_{2,r+1} & \cdots & c_{2,n} \\ & & \ddots & \vdots & \ddots & \vdots \\ & & \delta & c_{r,r+1} & \cdots & c_{rn} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{bmatrix} \tag{II$_b$}$$

which is obtained by multiplying both sides of $Ay = b$ from the left with Δ^{ad}. It has the same solutions in every integral domain extending D as $Ay = b$. Here, $\delta = \det \Delta$, the c_{ij} are certain signed $r \times r$ minors of A, and the d_i are certain signed $r \times r$ minors of the extended matrix (A, b). In particular, $v(c_{ij}) \geqslant v(\delta)$ for all i, j, by choice of Δ. Therefore, if $v(d_i) < v(\delta)$ for some $i \in \{1, \ldots, m\}$, then (II$_b$) and hence the original system $Ay = b$ are not solvable in D. Suppose $v(d_i) \geqslant v(\delta) = e$ for all $i = 1, \ldots, m$. Dividing all coefficients δ, c_{ij} and d_i in (II$_b$) by p^e, we then obtain a system $By = c$ as required.

Ideal-theoretic operations

Let now $f_1, \ldots, f_m, g_1, \ldots, g_n \in D$, and consider the ideals

$$I := (f_1, \ldots, f_m), \quad J := (g_1, \ldots, g_n)$$

of D generated by the f_i, respectively, g_j. The following lemmas relate the task of effectively solving problem (H) above with the computation of generators for the ideals $I \cap J$ and $I : J = \{h \in D : hJ \subseteq I\}$ of D. These lemmas are well-known and included here for reference in Section 3.3 below.

Lemma 3.1.4. *Given generators*

$$\big(y_1^{(k)},\dots,y_m^{(k)},z_1^{(k)},\dots,z_n^{(k)}\big)\in D^{m+n}\qquad(k=1,\dots,K)$$

for the module of solutions in D to the single homogeneous equation

$$f_1y_1+\cdots+f_my_m=g_1z_1+\cdots+g_nz_n,$$

the elements

$$f_1y_1^{(k)}+\cdots+f_my_m^{(k)}\qquad(k=1,\dots,K)$$

of D generate the ideal $I\cap J$ of D.

Lemma 3.1.5. *We have $I:J=(I:g_1)\cap\cdots\cap(I:g_n)$. Moreover, given $g\in D$, if*

$$\big(y_1^{(l)},\dots,y_m^{(l)},z^{(l)}\big)\in D^{m+1}\qquad(l=1,\dots,L)$$

generate the module of solutions to the homogeneous equation

$$f_1y_1+\cdots+f_my_m=gz,$$

then $z^{(1)},\dots,z^{(L)}$ generate the ideal $I:g=\{h\in D:gh\in I\}$ of D.

3.2 Hermann's Method for Restricted Power Series

In this section we give an adaptation of Hermann's method to the case of linear equations over rings of restricted power series, following [7, Sections 3, 4] (for homogeneous equations) and [9, Section 5] (for the inhomogeneous case). For this we specialize the material in the preceding section to the case $D=\mathbb{Z}_p\langle X\rangle$. We let again $A=(a_{ij})$ be an $m\times n$ matrix with entries $a_{ij}\in D$ and $b=[b_1,\dots,b_m]^{\mathrm{tr}}\in D^m$. We assume that $N\geqslant 1$ and let $D'=\mathbb{Z}_p\langle X'\rangle$ where $X'=(X_1,\dots,X_{N-1})$; we are going to show how problems (H) and (H_b) formulated at the beginning of the preceding section can be reduced to similar problems over D'. After performing p-desingularization on the pair (A,b) as explained in the previous section, we can assume that

$$r:=\mathrm{rank}_K(A)=\mathrm{rank}_{K(p)}(A \bmod p)\geqslant 1,$$

where as before $K = \mathrm{Frac}(D)$ and $K(p) = \mathrm{Frac}(D/pD) = \mathbb{F}_p(X)$. Thus in the description of Hermann's method in the general setting above, we can choose our $r \times r$ minor $\delta = \det \Delta$ of A to satisfy $\delta \bmod p \neq 0$. After applying the $\mathbb{Z}_p$-automorphism T_d of D given by Lemma 2.1.2, where $d > \deg(\delta \bmod p)$, to all coefficients of (II) respectively of (II_b), we may even assume that δ is regular in X_N of some degree s. By Weierstrass Division we then have

$$\overline{D} := D/\delta D \cong D' \oplus D'\overline{X_N} \oplus \cdots \oplus D'\overline{X_N}^{s-1}$$

as D'-algebras. (See (2.4).) So each element $\overline{a} \in \overline{D}$ can be uniquely written as

$$\overline{a} = a_0 + a_1\overline{X_N} + a_2\overline{X_N}^2 + \cdots + a_{s-1}\overline{X_N}^{s-1}$$

with $a_0, \ldots, a_{s-1} \in D'$. In particular, each of the coefficients $\overline{c_{ij}}$ and $\overline{d_i}$ can be written in this way. Let us also write each unknown y_j, for $r < j \leqslant n$, as

$$y_j = y_{j0} + y_{j1}\overline{X_N} + \cdots + y_{j,s-1}\overline{X_N}^{s-1}$$

with new unknowns y_{jk} $(r < j \leqslant n,\ 0 \leqslant k < s)$ ranging over D'. Each product $\overline{c_{ij}}y_j$ in $(\overline{\mathrm{II}})$ can then be written as

$$\beta_0(y_{j0}, \ldots, y_{j,s-1}) + \beta_1(y_{j0}, \ldots, y_{j,s-1})\overline{X_N} + \cdots + \beta_{s-1}(y_{j0}, \ldots, y_{j,s-1})\overline{X_N}^{s-1},$$

where each β_k is a linear form in $y_{j0}, \ldots, y_{j,s-1}$ with coefficients in D'. From this, it is routine to construct a homogeneous system $A'y' = 0$ of rs linear equations over D' in the $s(n-r)$ unknowns y_{jk} whose solutions in D' are in one-to-one correspondence with the solutions of $(\overline{\mathrm{II}})$ in $\overline{D}$. Since we need to be careful about issues of uniformity in the next section, we shall describe explicitly how such a matrix A' can be obtained. First note that the coefficient matrix of the system $(\overline{\mathrm{II}})$ above may be written as

$$C(0) + C(1)\overline{X_N} + \cdots + C(s-1)\overline{X_N}^{s-1},$$

where

$$C(k) = (c_{ijk})_{\substack{1 \leqslant i \leqslant r \\ r < j \leqslant n}} \in (D')^{r \times (n-r)} \qquad \text{for } k = 0, \ldots, s-1.$$

We also set

$$\begin{bmatrix} y_{r+1} \\ \vdots \\ y_n \end{bmatrix} = y(0) + y(1)\overline{X_N} + \cdots + y(s-1)\overline{X_N}^{s-1}, \qquad y(k) = \begin{bmatrix} y_{r+1,k} \\ \vdots \\ y_{nk} \end{bmatrix}.$$

So our system (II) may be rewritten as

$$\sum_{k=0}^{2(s-1)} \left(\sum_{l=0}^{k} C(k-l)y(l) \right) \overline{X_N}^k = 0. \tag{3.3}$$

For $t \geqslant s$ take $\xi_{tk} \in D'$ such that

$$\overline{X_N}^t = \xi_{t0} + \xi_{t1}\overline{X_N} + \cdots + \xi_{t,s-1}\overline{X_N}^{s-1}. \tag{3.4}$$

Using the identities (3.4), the left-hand side of (3.3) then reduces to

$$\sum_{k=0}^{s-1} \left[\sum_{l=0}^{k} \left(C(k-l) + \sum_{t=s}^{2(s-1)} C(t-l)\xi_{tk} \right) y(l) + \sum_{l=k+1}^{s-1} \left(\sum_{t=s}^{2(s-1)} C(t-l)\xi_{tk} \right) y(l) \right] \overline{X_N}^k.$$

Comparing the coefficients of equal powers of $\overline{X_N}$ in (3.3) we thus obtain s systems of linear equations over D', one for each $k = 0, \ldots, s-1$:

$$\sum_{l=0}^{s-1} \left(C(k-l) + \sum_{t=s}^{2(s-1)} C(t-l)\xi_{tk} \right) y(l) = 0,$$

where we put $C(t) := 0$ for $t < 0$. Combining these systems into a single one yields a system

$$A'y' = 0, \tag{I'}$$

where

$$A' \in (D')^{m' \times n'}, \quad m' = rs, \quad n' = s(n-r),$$

whose solutions in D' are in one-to-one correspondence with the solutions in $\overline{D}$ of ($\overline{\text{II}}$) via $y \mapsto y'$, where given

$$y = y(0) + y(1)\overline{X_N} + \cdots + y(s-1)\overline{X_N}^{s-1} \text{ with column vectors } y(k) \in (D')^{n-r}$$

we set $y' = \begin{bmatrix} y(0) \\ \vdots \\ y(s-1) \end{bmatrix} \in (D')^{n'}$. In fact:

Lemma 3.2.1. *Let $y^{(1)}, \dots, y^{(M)} \in \overline{D}^n$ be such that $(y^{(1)})', \dots, (y^{(M)})' \in (D')^{n'}$ generate the D'-module of solutions to* (I′). *Then $y^{(1)}, \dots, y^{(M)}$ generate the $\overline{D}$-module of solutions to* ($\overline{\text{II}}$).

Similarly, writing

$$\begin{bmatrix} \overline{d_1} \\ \vdots \\ \overline{d_r} \end{bmatrix} = d(0) + d(1)\overline{X_N} + \cdots + d(s-1)\overline{X_N}^{s-1}, \qquad d(k) = \begin{bmatrix} d_{1k} \\ \vdots \\ d_{rk} \end{bmatrix},$$

and comparing the coefficients of equal powers of $\overline{X_N}$ we obtain from ($\overline{\text{II}_b}$) the following systems of linear equations over D':

$$\sum_{l=0}^{s-1} \left(C(k-l) + \sum_{t=s}^{2(s-1)} C(t-l)\xi_{tk} \right) y(l) = d(k) \qquad (k = 0, \dots, s-1).$$

Combining these systems into a single one yields a system

$$A'y' = b', \tag{I$'_b$}$$

where A' is as before and $b' \in (D')^{m'}$, whose solutions in D' are in one-to-one correspondence with the solutions in $\overline{D}$ of ($\overline{\text{II}_b}$) via $y \mapsto y'$. In particular, our original system (I) is solvable in D if and only if the system (I$'_b$) is solvable in D'.

We finish this section with some remarks about how to adapt Hermann's method to the integral domains $\mathbb{Q}_p\langle X\rangle$ and $K[X]$ (where K is a field).

Hermann's method for $\mathbb{Q}_p\langle X\rangle$

First note that since the ring extension $\mathbb{Z}_p\langle X\rangle \subseteq \mathbb{Q}_p\langle X\rangle$ is flat, problem (H) formulated at the beginning of the last section (the computation of syzygy modules) over the integral domain $\mathbb{Q}_p\langle X\rangle$ reduces to the analogous problem over $\mathbb{Z}_p\langle X\rangle$: if A is an $m \times n$ matrix over $\mathbb{Z}_p\langle X\rangle$, then each collection of generators for the $\mathbb{Z}_p\langle X\rangle$-module $\text{Sol}_{\mathbb{Z}_p\langle X\rangle}(A)$ also generates the $\mathbb{Q}_p\langle X\rangle$-module $\text{Sol}_{\mathbb{Q}_p\langle X\rangle}(A)$. The inductive procedure described above for using Weierstrass Division to reduce problem (H$_b$) over a ring of restricted power series in $N \geqslant 1$

indeterminates $X = (X_1, \ldots, X_N)$ to a similar ring of power series in $N-1$ indeterminates $X' = (X_1, \ldots, X_{N-1})$ also works for $\mathbb{Q}_p\langle X\rangle$, $\mathbb{Q}_p\langle X'\rangle$ instead of the rings $\mathbb{Z}_p\langle X\rangle$, $\mathbb{Z}_p\langle X'\rangle$, respectively (invoking Corollary 2.3.8 instead of Theorem 2.1.3). In fact, things are easier here since the preliminary step of desingularization is not required. We leave the details to the reader.

Hermann's method for polynomial rings over fields

The classical case of Hermann's method concerns the case where our ring D is of the form $K[X] = K[X_1, \ldots, X_N]$ for a field K. Here we may use Euclidean Division by δ to describe elements in the quotient ring $\overline{D} = D/D\delta$ in terms of polynomials from $K[X'] = K[X_1, \ldots, X_{N-1}]$. This leads to a concrete doubly exponential bound for the degree of solutions to the system $Ay = 0$ of homogeneous linear equations, in terms of the number N of indeterminates, maximum degree d of the entries in A, and number of rows m, as computed by Seidenberg [70] (see also [7] for an exposition); more precisely:

Theorem 3.2.2. *For every polynomial ring $D = K[X_1, \ldots, X_N]$ over a field K and $A \in D^{m\times n}$ of degree at most d, the solution module $\mathrm{Sol}_D(A)$ of the homogeneous system $Ay = 0$ is generated by solutions of degree at most $\beta(N, d, m) = (2md)^{2^N}$.*

Similarly one obtains a degree bound in the inhomogeneous case:

Theorem 3.2.3. *For every K, D, A as in the previous theorem and $b \in D^m$ of degree at most d, if the system of linear equations $Ay = b$ has a solution in D^n, then it has such a solution of degree at most $\beta(N, d, m)$.*

Note that the bound β above neither depends on the field K nor on (the coefficients of) the entries of A or b, but only on the parameters (N, d, m); the *existence* of such a uniform bound also has elegant non-standard proofs, cf. [21, 25].

3.3 Uniform Linear Algebra

We now return to the context of Section 2.1, that is, we fix a noetherian domain D which is t-adically complete with respect to a distinguished prime element t. We also let

$$A(C,X) = \big(a_{ij}(C,X)\big)_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$$

be an $m \times n$ matrix with entries $a_{ij}(C,X) \in D\langle C,X\rangle$, and

$$b(C,X) = \begin{bmatrix} b_1(C,X) \\ \vdots \\ b_m(C,X) \end{bmatrix}$$

with $b_i(C,X) \in D\langle C,X\rangle$. For every valuation ring with D-structure R and every tuple $c \in R^M$ of parameters, we obtain a system of linear equations

$$A(c,X)y = b(c,X) \tag{$\mathrm{I}_b(c)$}$$

over $R\langle X\rangle$. The first goal of this section is to show that solvability of this system in $R\langle X\rangle$ may be expressed quantifier-free in c, uniformly for all R, and to show that a set of generators for the $R\langle X\rangle$-module of solutions $\mathrm{Sol}_{R\langle X\rangle}\big(A(c,X)\big)$ to the homogeneous system

$$A(c,X)y = 0 \tag{$\mathrm{I}(c)$}$$

are (piecewise) given by terms. Theorems 3.3.1 and 3.3.3 below contain the precise statements, which are proved by combining the parametric versions of Weierstrass Division and Preparation from Section 2.2 with Hermann's method for rings of restricted power series as described in the previous section. In the rest of this section, "formula" will always mean "$\mathcal{L}_D^{\mathrm{d}}$-formula," and "term" will stand for "$\mathcal{L}_D^{\mathrm{d}}$-term," unless otherwise noted.

Theorem 3.3.1. *There exists a finite family $\big\{y^{(\lambda)}(C,X)\big\}$ of column vectors whose entries are terms in which the function symbol* d *is only applied to subterms not involving the X-variables, such that for all $R \models T_D$ and $c \in R^M$, if the system* $(\mathrm{I}_b(c))$ *has a solution in $R\langle X\rangle$, then for some λ, the column vector $y^{(\lambda)}(c,X) \in R\langle X\rangle^n$ is a solution to* $(\mathrm{I}_b(c))$.

We note an immediate consequence of Theorem 3.3.1:

Corollary 3.3.2. *There is a quantifier-free formula* $\mathrm{sol}(C)$ *such that for all* $R \models T_D$ *and* $c \in R^M$*, the system* $(\mathrm{I}_b(c))$ *has a solution in* $R\langle X\rangle$ *iff* $R \models \mathrm{sol}(c)$*.*

Proof. Take $y^{(\lambda)}(C, X)$ as in Theorem 3.3.1, and by the results of Section 2.2 take a quantifier-free formula $\mathrm{sol}^{(\lambda)}(C)$ such that for all $R \models T_D$ and $c \in R^M$ we have $R \models \mathrm{sol}^{(\lambda)}(c)$ iff $A(c, X)y^{(\lambda)}(c, X) = b(c, X)$. Set $\mathrm{sol} := \bigvee_\lambda \mathrm{sol}^{(\lambda)}$. □

The following is an analogue of Theorem 3.3.1 for homogeneous systems of linear equations.

Theorem 3.3.3. *There exist a finite set* Λ *and for each* $\lambda \in \Lambda$ *column vectors*

$$y_1^{(\lambda)}(C, X), \dots, y_k^{(\lambda)}(C, X) \qquad (k \in \mathbb{N})$$

whose entries are terms in which the function symbol d *is applied only to subterms not involving the* X*-variables, having the following property: if* $R \models T_D$*,* $c \in R^M$*, then for some* $\lambda \in \Lambda$*, the column vectors*

$$y_1^{(\lambda)}(c, X), \dots, y_k^{(\lambda)}(c, X) \in R\langle X\rangle^n$$

generate $\mathrm{Sol}_{R\langle X\rangle}\big(A(c, X)\big)$*.*

Again we note an immediate consequence:

Corollary 3.3.4. *Let* $z_1(C, X), \dots, z_l(C, X)$ $(l \in \mathbb{N})$ *be column vectors whose entries are terms in which the function symbol* d *is applied only to subterms not involving the* X*-variables. Then there is a quantifier-free formula* $\mathrm{gen}(C)$ *such that for* $R \models T_D$*,* $c \in R^M$ *we have*

$$R \models \mathrm{gen}(c) \iff z_1(c, X), \dots, z_l(c, X) \text{ generate } \mathrm{Sol}_{R\langle X\rangle}\big(A(c, X)\big).$$

Proof. Let $y_i^{(\lambda)}$ be as in Theorem 3.3.3. By the results of Section 2.2 and Corollary 3.3.2 we can take quantifier-free formulas $\mathrm{gen}_i^{(\lambda)}(C)$ and $\mathrm{gen}_j(C)$ such that for all $R \models T_D$ and $c \in R^M$ we have

$$R \models \mathrm{gen}_i^{(\lambda)}(c) \iff A(c, X)y_i^{(\lambda)}(c, X) = 0 \to y_i^{(\lambda)}(c, X) \in \sum_j R\langle X\rangle z_j(c, X),$$

$$R \models \mathrm{gen}_j(c) \iff A(c, X)z_j(c, X) = 0.$$

Then $\mathrm{gen} := \bigwedge_{i,\lambda} \mathrm{gen}_i^{(\lambda)} \wedge \bigwedge_j \mathrm{gen}_j$ has the required property. $\square$

As a consequence of Theorems 3.3.1 and 3.3.3, if R, R^* are valuation rings with D-structure such that $R \subseteq R^*$ as $\mathcal{L}_D$-structures, then $R^*\langle X\rangle$ is a faithfully flat ring extension of $R\langle X\rangle$.

Remark. Theorems 3.3.1 and 3.3.3 appear in [6, Chapter 5]. The thesis [36] also contains a variant of Theorem 3.3.3 which treats the parametrization of generators for the $\mathbb{Z}_p\langle X\rangle$-module $\mathrm{Sol}_{\mathbb{Z}_p\langle X\rangle}(A)$ of solutions (in $\mathbb{Z}_p\langle X\rangle$) to a linear system of homogeneous equations $Ay = 0$ over $\mathbb{Z}_p\langle X\rangle$, for a fixed $R = \mathbb{Z}_p$.

Proof of Theorems 3.3.1 and 3.3.3

For the proofs of these theorems we assume that the reader is familiar with the definition and basic properties of ultraproducts. (An overview may be found in [26].) We fix an infinite index set I and a non-principal ultrafilter $\mathcal{U}$ on I. Let $\{\boldsymbol{A}_i\}_{i\in I}$ be a family of $\mathcal{L}$-structures, for some first-order language $\mathcal{L}$. Then $\prod_{i\in I} \boldsymbol{A}_i/\mathcal{U}$ denotes the ultraproduct of $\{\boldsymbol{A}_i\}$ with respect to $\mathcal{U}$. The underlying set of this $\mathcal{L}$-structure consists of the equivalence classes $[a_i]$ of sequences $\{a_i\} \in \prod_{i\in I} A_i$ with respect to the equivalence relation $\sim$ on the cartesian product $\prod_{i\in I} A_i$ given by

$$\{a_i\} \sim \{b_i\} \quad \Longleftrightarrow \quad \{i \in I : a_i = b_i\} \in \mathcal{U}.$$

Let now $\{R_i\}_{i\in I}$ be a family of valuation rings with D-structure. Then

$$R^* := \prod_{i\in I} R_i \Big/ \mathcal{U}$$

is also a valuation ring with D-structure. We also consider the integral domain

$$R\langle X\rangle^* := \prod_{i\in I} R_i\langle X\rangle \Big/ \mathcal{U}.$$

Given $f \in D\langle C, X\rangle$ and $c^* = (c_1^*, \ldots, c_M^*) \in (R^*)^M$, take $c_{ij} \in R_i$ such that $[c_{ij}] = c_j^*$ for $j = 1, \ldots, M$ and set $c_i := (c_{i1}, \ldots, c_{iM}) \in R_i^M$. The equivalence class of the sequence $\big\{f(c_i, X)\big\}$ in $\prod_i R_i\langle X\rangle$ only depends on the element $f(c^*, X)$ of $R^*\langle X\rangle$; hence we can define

$$\iota\big(f(c^*, X)\big) := \big[f(c_i, X)\big] \in R\langle X\rangle^*,$$

and this way obtain a ring embedding

$$\iota\colon R^*\langle X\rangle \to R\langle X\rangle^*.$$

These claims are easily verified using the results of Section 2.2; as a demonstration, let us check that ι is injective: Suppose $\big[f(c_i, X)\big] = [0]$ in $R\langle X\rangle^*$; then the set of indices $i \in I$ such that $f(c_i, X) = 0$ (in $R_i\langle X\rangle$) is a member of our ultrafilter $\mathcal{U}$. By Section 2.2 we can take a (quantifier-free) formula $\mathrm{Z}(C)$ such that for all $R \models T_D$ and $c \in R^M$ we have $R \models \mathrm{Z}(c)$ iff $f(c, X) = 0$. In particular

$$R_i \models \mathrm{Z}(c_i) \iff f(c_i, X) = 0, \qquad R^* \models \mathrm{Z}(c^*) \iff f(c^*, X) = 0.$$

The claim now follows by Łos' Theorem.

In the following we identify the ring $R^*\langle X\rangle$ with its image under ι. We also fix a substructure R of R^*. Theorems 3.3.1 and 3.3.3 now follow from their nonstandard formulation, Theorem 3.3.5 below, which expresses that the ring $R\langle X\rangle$ is coherent and that the ring extension $R\langle X\rangle \subseteq R\langle X\rangle^*$ is faithfully flat.

Theorem 3.3.5. *Let $A = (a_{ij})$ be an $m \times n$ matrix with entries $a_{ij} \in R\langle X\rangle$ and $b = [b_1, \ldots, b_m]^{\mathrm{tr}} \in R\langle X\rangle^m$.*

(1) *If there is some $y^* \in (R\langle X\rangle^*)^n$ such that $Ay^* = b$, then there is some $y \in R\langle X\rangle^n$ with $Ay = b$; and*

(2) *the submodule $\mathrm{Sol}_{R\langle X\rangle^*}(A)$ of the $R\langle X\rangle^*$-module $(R\langle X\rangle^*)^n$ consisting of the solutions to the homogeneous system $Ay = 0$ is generated by finitely many solutions in $R\langle X\rangle^n$.*

Let us first show how Theorem 3.3.5 implies Theorems 3.3.1 and 3.3.3. Suppose Theorem 3.3.1 fails. Then by a standard argument we obtain an infinite family $\{R_i\}$ of models of T_D and a non-principal ultrafilter $\mathcal{U}$ on I as well as some $c^* \in (R^*)^M$, where $R^* = \prod_i R_i/\mathcal{U}$, such that the system of linear equations $(\mathrm{I}_b(c^*))$ over $R^*\langle X\rangle$ has a solution in $R\langle X\rangle^*$ but not in $R\langle X\rangle$, where R is the $\mathcal{L}_D^{\mathrm{d}}$-substructure of R^* generated by c^*; this contradicts part (1) of Theorem 3.3.5. Theorem 3.3.3 follows similarly from Theorem 3.3.5, (2).

The proof of Theorem 3.3.5 involves the following fact, which in the case $D = \mathbb{Z}[[t]]$, $R = \mathbb{Z}_p$ (see Example 2.2.2), amounts to a description of the p-desingularization of the pair $\big(A(c,X), b(c,X)\big)$ in $\mathbb{Z}_p\langle X\rangle$ which is uniform in the parameters $c \in \mathbb{Z}_p^M$ and in the prime p. In the statement, we let A, b be as in Theorem 3.3.5, and given a valuation ring R with D-structure we let $K = \mathrm{Frac}\big(R\langle X\rangle\big)$ and $\overline{K} = \overline{R}(X)$. We denote by $\overline{A} = (\overline{a_{ij}})$ the $m \times n$ matrix over $\overline{R}[X] \subseteq \overline{K}$ obtained by applying the residue morphism $R\langle X\rangle \to R\langle X\rangle/t_R R\langle X\rangle \cong \overline{R}[X]$ to each entry a_{ij} of A.

Proposition 3.3.6 (Uniform Desingularization)**.** *Suppose $A \neq 0$ and $Ay = b$ has a solution in $R\langle X\rangle^*$. Then there exist some $r \in \{1, \ldots, m\}$, an $r \times n$ matrix B over $R\langle X\rangle$, and a column vector $d \in R\langle X\rangle^n$, such that*

(1) $\mathrm{rank}_K(B) = \mathrm{rank}_{\overline{K}}(\overline{B})$*, and*

(2) *the systems $Ay = b$ and $By = d$ have the same solutions in every integral domain extending $R\langle X\rangle$.*

To see this, let $v_i \colon F_i^\times \to \Gamma_i = v_i(F_i^\times)$ be the valuation on $F_i = \mathrm{Frac}(R_i)$ associated to the valuation ring R_i of F_i. Set $\Gamma^* := \prod_{i\in I} \Gamma_i/\mathcal{U}$. Then the valuation on $F^* := \mathrm{Frac}(R^*)$ associated to the valuation ring R^* is given by

$$v \colon (F^*)^\times \to \Gamma^*, \qquad v(a) = \big[v_i(a_i)\big] \text{ for } 0 \neq a = [a_i] \in F^*.$$

Let $v \colon R^*\langle X\rangle^{\neq} \to \Gamma^*$ be the Gauss valuation on $R^*\langle X\rangle$. Denoting the Gauss valuation on $R_i\langle X\rangle$ by $v_i \colon R_i\langle X\rangle^{\neq} \to \Gamma_i$, the integral domain $R\langle X\rangle^*$ also carries a valuation

$$v^* \colon \big(R\langle X\rangle^*\big)^{\neq} \to \Gamma^* \quad \text{with } v^*(f) = \big[v_i(f_i)\big] \text{ for } 0 \neq f = [f_i] \in R\langle X\rangle^*,$$

and one verifies easily that v^* extends v. The proof of Proposition 3.3.6 now follows as in the description of p-desingularization in Section 3.1, with the role of D and the p-adic valuation on D taken over by $R\langle X\rangle$ and its Gauss valuation v.

To prove Theorem 3.3.5, we use induction on N for both parts, following the outline of Hermann's method in Sections 3.1 and 3.2. To show (1), suppose we have some $y^* \in$

$(R\langle X\rangle^*)^n$ such that $Ay^* = b$. This implies that the necessary condition (NC) from Section 3.1 holds: $r = \operatorname{rank}_K(A) = \operatorname{rank}_K(A, b)$. After replacing (A, b) by a suitable matrix (B, d) using Proposition 3.3.6, we reduce to the case that $r = \operatorname{rank}_{\overline{K}}(\overline{A}) \geqslant 1$. We can further assume that our system $Ay = b$ has the form (II_b) where $\delta \in R\langle X\rangle$ satisfies $\overline{\delta} \neq 0$. If $N = 0$, then this means that δ is a unit in R, hence we have a solution $y \in R^n$, given by (3.2), as required. Suppose $N \geqslant 1$. After applying a polynomial automorphism we can assume that δ is regular in X_N of some degree $s \in \mathbb{N}$. As described in Section 3.2 for the case $R = \mathbb{Z}_p$, from our system $Ay = b$ we now construct a system $A'y' = b'$ over $R\langle X'\rangle$, where $X' = (X_1, \ldots, X_{N-1})$, whose solutions in $R\langle X'\rangle$ are in one-to-one correspondence with the solutions of $Ay = b$ in $R\langle X\rangle$. By parametric Weierstrass Division the crucial isomorphism

$$R\langle X\rangle/\delta R\langle X\rangle \cong R\langle X'\rangle \oplus R\langle X'\rangle\overline{X_N} \oplus \cdots \oplus R\langle X'\rangle\overline{X_N}^{s-1} \quad (\overline{X_N} = X_N + \delta R\langle X\rangle)$$

of $R\langle X'\rangle$-algebras also holds for $R\langle X\rangle^*$ and $R\langle X'\rangle^* = \prod_i R_i\langle X'\rangle/\mathcal{U}$ in place of $R\langle X\rangle$ and $R\langle X'\rangle$, respectively, that is:

$$R\langle X\rangle^*/\delta R\langle X\rangle^* \cong R\langle X'\rangle^* \oplus R\langle X'\rangle^*\overline{X_N} \oplus \cdots \oplus R\langle X'\rangle^*\overline{X_N}^{s-1} \ (\overline{X_N} = X_N + \delta R\langle X\rangle^*).$$

Hence the solutions of $A'y' = b'$ in $R\langle X'\rangle^*$ are also in one-to-one correspondence with the solutions of $Ay = b$ in $R\langle X\rangle^*$. This allows us to appeal to the inductive hypothesis to finish the proof of (1).

To show (2) we proceed in a similar way. As indicated at the beginning of Section 3.1 we first reduce to the case that our system $Ay = 0$ has the form (II), where thanks to Proposition 3.3.6 we can assume that $\overline{\delta} \neq 0$. If $N = 0$, then the special solutions in R^n listed in (3.1) generate $\mathrm{Sol}_{R^*}(A)$, and we are done. If $N \geqslant 1$, we apply the inductive hypothesis as in the proof of (1), following the procedure in Sections 3.1 and 3.2. □

Let A and b be as at the beginning of this section. We note a version of Theorem 3.3.1 for solving inhomogeneous systems of linear equations over $\mathbb{Q}_p\langle X\rangle$. This is shown in a similar way as Theorem 3.3.1; cf. the remarks at the end of Section 3.2.

Theorem 3.3.7. *There exist finitely many column vectors $y^{(\lambda)}(C, X)$ whose entries are terms in which the function symbol* d *is only applied to subterms not involving the X-variables,*

as well as terms $d^{(\lambda)}(C)$*, such that for all* $R \models T_D$*,* $c \in R^M$*, and* $F = \operatorname{Frac}(R)$*, if the system* $(\mathrm{I}_b(c))$ *has a solution in* $F\langle X\rangle$*, then for some* λ *we have* $d^{(\lambda)}(c) \neq 0$ *and the column vector*

$$y^{(\lambda)}(c, X)/d^{(\lambda)}(c) \in F\langle X\rangle^n$$

is a solution to $(\mathrm{I}_b(c))$*.*

Theorems 3.3.3 and 3.3.7 are enough to show the uniform definability of many basic tasks of linear algebra in $F\langle X\rangle$-modules; we give an illustrative example needed later. (In the next subsection we will focus on ideal-theoretic applications of the theorems above.) Let $a \in D\langle C, X\rangle$. For $R \models T_D$, $c \in R^M$, and $F = \operatorname{Frac}(R)$ let $M(c, X)$ denote the submodule of the $F\langle X\rangle$-module $F\langle X\rangle^m$ generated by the columns of the matrix $A(c, X)$, and set

$$\big(M(c, X) : a(c, X)\big) := \big\{z \in F\langle X\rangle^m : a(c, X)z \in M(c, X)\big\},$$

an $F\langle X\rangle$-submodule of $F\langle X\rangle^m$. We say that a finite family $\big\{\varphi^{(\lambda)}(C)\big\}$ of formulas is **covering** if $T_D \models \bigvee_\lambda \varphi^{(\lambda)}$.

Corollary 3.3.8. *There are a covering family* $\big\{\mathrm{quot}^{(\lambda)}(C)\big\}$ *of quantifier-free formulas and column vectors*

$$y_1^{(\lambda)}(C, X), \ldots, y_k^{(\lambda)}(C, X) \qquad (k \in \mathbb{N})$$

whose entries are terms in which the function symbol d *is not applied to subterms involving the* X*-variables, such that if* $R \models T_D$*,* $c \in R^M$*, and* $R \models \mathrm{quot}^{(\lambda)}(c)$*, then*

$$\big(M(c, X) : a(c, X)\big) = F\langle X\rangle\, y_1^{(\lambda)}(c, X) + \cdots + F\langle X\rangle\, y_k^{(\lambda)}(c, X).$$

Proof. Apply Theorem 3.3.3 and its Corollary 3.3.4 to the homogeneous system of linear equations $A(c, X)y = a(c, X)z$. (See also Lemma 3.1.5 for this kind of argument.) □

Ideal-theoretic operations

In this subsection we let $f_1, \ldots, f_m \in D\langle C, X\rangle$, and we let R range over models of T_D and c over R^M, and we set $F = \operatorname{Frac}(R)$. As an immediate consequence of the material above, we

see that given $g \in D\langle C, X\rangle$, membership of $g(c, X)$ in the ideal

$$I(c, X) := \big(f_1(c, X), \dots, f_m(c, X)\big)$$

of $R\langle X\rangle$ generated by the power series $f_i(c, X)$ can be expressed by a quantifier-free condition on c, uniformly in R:

Corollary 3.3.9. *There exist finitely many column vectors $y^{(\lambda)}$ whose entries are terms $y_j^{(\lambda)}(C, X)$ in which the function symbol* d *is only applied to subterms not involving the X-variables, such that for all R, c satisfying $g(c, X) \in I(c, X)$, there is some λ with*

$$g(c, X) = y_1^{(\lambda)}(c, X) f_1(c, X) + \cdots + y_m^{(\lambda)}(c, X) f_m(c, X).$$

This is the special case of Theorem 3.3.1 for a single linear equation. In particular, we obtain a quantifier-free formula $\epsilon(C) = \epsilon_g(C)$ such that for all R, c,

$$R \models \epsilon(c) \quad \iff \quad g(c, X) \in I(c, X).$$

As an application, we see the intersection $I \cap R$ of a finitely generated ideal I of $R\langle X\rangle$ with the subring R of $R\langle X\rangle$ is definable in R. For this we let C' be a new parametric variable; applying the above in the case $g = C'$ then yields:

Corollary 3.3.10. *There is a quantifier-free formula $\epsilon(C, C')$ such that for all R, c, and $c' \in R$ we have $I(c, X) \cap R = \big\{c' \in R : R \models \epsilon(c, c')\big\}$.*

Similarly to Corollary 3.3.9, using Theorem 3.3.7 in place of Theorem 3.3.1, we obtain:

Corollary 3.3.11. *There is a finite family $\big\{\big(y^{(\lambda)}, d^{(\lambda)}\big)\big\}$, where each $y^{(\lambda)}(C, X)$ is a column vector whose entries $y_j^{(\lambda)}(C, X)$ are terms in which the function symbol* d *is only applied to subterms not involving the X-variables, and each $d^{(\lambda)}(C)$ is a term, with the following property: for all R, c with $g(c, X) \in I(c, X)F\langle X\rangle$ there is some λ such that*

$$d^{(\lambda)}(c)\, g(c, X) = y_1^{(\lambda)}(c, X) f_1(c, X) + \cdots + y_m^{(\lambda)}(c, X) f_m(c, X) \quad \text{and} \quad d^{(\lambda)}(c) \neq 0.$$

Let now in addition $g_1, \dots, g_n \in D\langle C, X\rangle$; we may then also consider the ideal

$$J(c, X) := \big(g_1(c, X), \dots, g_n(c, X)\big)$$

of $R\langle X\rangle$ generated by the $g_j(c, X)$. From Corollary 3.3.9 we get:

Corollary 3.3.12. *There is a quantifier-free formula $\iota(C)$ such that for all R and c we have $R \models \iota(c)$ iff $J(c, X) \subseteq I(c, X)$.*

Combining Lemmas 3.1.4 and 3.1.5 with Theorem 3.3.3 immediately yields:

Corollary 3.3.13. *There exist a covering family $\{\varphi^{(\lambda)}(C)\}$ of quantifier-free formulas, and for each λ tuples*

$$\big(r_1^{(\lambda)}, \ldots, r_k^{(\lambda)}\big), \quad \big(s_1^{(\lambda)}, \ldots, s_k^{(\lambda)}\big) \qquad (k \in \mathbb{N})$$

of terms in (C, X) where the function symbol d is not applied to subterms involving the X-variables such that for all R and c with $R \models \varphi^{(\lambda)}(c)$, we have

$$I(c, X) \cap J(c, X) = \big(r_1^{(\lambda)}(c, X), \ldots, r_k^{(\lambda)}(c, X)\big),$$
$$I(c, X) : J(c, X) = \big(s_1^{(\lambda)}(c, X), \ldots, s_k^{(\lambda)}(c, X)\big).$$

From Corollaries 3.3.12 and 3.3.13 we now obtain:

Corollary 3.3.14. *There is a formula $\psi(C, C')$ such that for each R, c, and $c' \in R$ we have*

$$R \models \psi(c, c') \quad \Longleftrightarrow \quad \big(I(c, X) : c'\big) \supseteq \big(I(c, X) : b\big) \text{ for all } b \in R^{\neq}.$$

As a consequence, we have:

Corollary 3.3.15. *Let I be a finitely generated ideal of $R\langle X\rangle$. Then the ideal*

$$\begin{aligned} J &:= \text{annihilator of the } R\text{-module } \big(IF\langle X\rangle \cap R\langle X\rangle\big)/I \\ &= \big\{r \in R : (I : r) \supseteq (I : b) \text{ for all } b \in R^{\neq}\big\} \end{aligned}$$

of R is definable. If I is radical, then so is J.

Proof. The definability follows from Corollary 3.3.14. Suppose I is radical, and let $r \in R$ with $r^2 \in J$. Then for all $b \in R^{\neq}$ and $f \in (I : b)$ we have $r^2 f \in I$, hence $(rf)^2 \in I$ and so $rf \in I$. Hence $r \in J$, and this shows that J is radical. □

Next we turn to the problem of eliminating variables. The following is similar to a lemma in [69]:

Lemma 3.3.16. *Let I be a finitely generated ideal of $R\langle X\rangle$ which contains a Weierstrass polynomial w in X_N. Then the ideal $I \cap R\langle X'\rangle$ of $R\langle X'\rangle$ is also finitely generated.*

Proof. Corollary 2.3.7 and the remarks preceding it yield $f_1, \dots, f_m \in R\langle X'\rangle[X_N]$ of degree $< d := \deg_{X_N} w$ which jointly with w generate the ideal $J := I \cap R\langle X'\rangle[X_N]$. Let $g \in I \cap R\langle X'\rangle = J \cap R\langle X'\rangle$; then $g = \sum_i f_i y_i + wz$ where $y_i, z \in R\langle X'\rangle[X_N]$. The proof of Corollary 2.3.7 shows that we can choose the y_i, z such that $\deg_{X_N} y_i < d$ for $i = 1, \dots, m$; hence also $\deg z < d$, since $wz = g - \sum_i f_i y_i$ has degree $< 2d$. Write $y_i = \sum_{j=0}^{d-1} y_{ij} X_N^j$ and $z = \sum_{j=0}^{d-1} z_j X_N^j$ where $y_{ij}, z_j \in R\langle X'\rangle$. The condition "$\deg_{X_N} g = 0$" can be expressed as a homogeneous system of linear equations over $R\langle X'\rangle$ in the y_{ij}, z_j. By coherence of $R\langle X\rangle$, the $R\langle X'\rangle$-module of solutions of this system is finitely generated; the y_i, z arising from a finite generating set of this $R\langle X'\rangle$-module give rise to a generating set for $I \cap R\langle X'\rangle$. □

We now let again $f_1, \dots, f_m \in D\langle C, X\rangle$. Analyzing the proof of the preceding lemma and using Theorem 3.3.7 and the results on uniform Weierstrass Division from Section 2.2, we obtain a version which is uniform in parameters:

Corollary 3.3.17. *Assume that one of the f_i is a Weierstrass polynomial in X_N. Then there exist a covering family $\{\varphi^{(\lambda)}(C)\}$ of quantifier-free formulas and tuples $\left(g_1^{(\lambda)}, \dots, g_n^{(\lambda)}\right)$ (for some n) of terms in (C, X') where the function symbol* d *is not applied to subterms involving the X'-variables, with the following property: if R and c are such that $R \models \varphi^{(\lambda)}(c)$, then $g_1^{(\lambda)}(c, X'), \dots, g_n^{(\lambda)}(c, X')$ generate the ideal $I(c, X) \cap R\langle X'\rangle$ of $R\langle X'\rangle$.*

CHAPTER 4

Uniform Noether Normalization and Uniform Noetherianity

In this chapter, we first explore generalizations and consequences of Noether Normalization. As we have already seen, a Noether Normalization trick often provides a way to change variables to create a regular power series (2.1.1). In Section 4.1 we begin by defining what it means for a collection of multivariable polynomials to be a *Weierstrass sequence*: this is essentially a Gröbner basis with respect to the lexicographic term ordering. The existence of a Weierstrass sequence in an ideal provides a sufficient condition for the existence of "universal denominators" which may be needed to compute ideal quotients (4.1.4). In Section 4.2 we then establish a uniform version of the usual Noether Normalization Theorem for restricted power series (4.1.14) and give some applications: defining the dimension of an ideal (4.2.2), and defining maximal ideals (4.2.3, 4.2.5). In the later chapters our main interest lies in rings of restricted power series over nonstandard models of the theory of $\mathbb{Z}_p$; in the last section of this chapter we prepare the ground by establishing a few basic facts about such rings, obtained by model-theoretic transfer from the noetherianity of $\mathbb{Z}_p\langle X\rangle$ using the definability results obtained in Section 3.3 of the previous chapter.

4.1 Weierstrass Sequences

In this section we introduce the formalism of *Weierstrass sequences* and summarize their basic properties. Such sequences appear naturally when the Weierstrass Preparation Theorem is applied repeatedly, and they play an important role in our formulation of uniform Noether Normalization in Section 4.2 below.

Weierstrass sequences in polynomial rings

We first introduce Weierstrass sequences in a fairly general setting. For this, let A be any ring. We say that $w_1, \ldots, w_N \in A[X]$ form a **Weierstrass sequence** over A if $w_1 \in A[X_1]$ is monic of positive degree (in X_1), $w_2 \in A[X_1, X_2]$ is monic of positive degree in X_2, etc., that is: $w_i \in A[X_1, \ldots, X_i]$ is monic of positive degree in X_i, for $i = 1, \ldots, N$. Note that a Weierstrass sequence over A remains a Weierstrass sequence over every ring extension of A. The presence of a Weierstrass sequence is useful for dimension computations:

Lemma 4.1.1. *Let I be an ideal of $A[X]$ containing a Weierstrass sequence over A. Then $\dim A[X]/I \leqslant \dim A$, with equality if $A \cap I = \{0\}$.*

Proof. Suppose first that $A \cap I = \{0\}$. Then the composition of the natural inclusion $A \subseteq A[X]$ with the residue morphism $A[X] \to A[X]/I$ yields a ring embedding $A \to A[X]/I$, and identifying A with its image, $A[X]/I$ is an integral ring extension of A, so $\dim A[X]/I = \dim A$. In general, put $\overline{A} := A/(A \cap I)$ and let $\overline{I}$ be the image of I under the surjective ring morphism $A[X] \to \overline{A}[X]$ which extends the residue morphism $A \to \overline{A}$ and satisfies $X_i \mapsto X_i$ $(i = 1, \ldots, N)$; this morphism then induces an isomorphism $A[X]/I \to \overline{A}[X]/\overline{I}$, we have $\overline{A} \cap \overline{I} = \{0\}$, and so by what we already showed: $\dim A[X]/I = \dim \overline{A}[X]/\overline{I} = \dim \overline{A} \leqslant \dim A$. □

Let now $w_1, \ldots, w_N \in A[X]$ be a Weierstrass sequence, set $d_i := \deg_{X_i} w_i$ for $i = 1, \ldots, N$, and let W be the ideal of $A[X]$ generated by $w_1, \ldots, w_N$. We say that a polynomial $g \in A[X]$ is in **normal form** with respect to $w_1, \ldots, w_N$ if $\deg_{X_i} g < d_i$ for $i = 1, \ldots, N$. The polynomials in $A[X]$ which are in normal form with respect to $w_1, \ldots, w_N$ form a finitely generated free A-submodule of $A[X]$ with basis given by the monomials X^ν with $\nu_i < d_i$ for $i = 1, \ldots, N$. With this terminology we have:

Lemma 4.1.2. *For each $f \in A[X]$ there is some $g \in A[X]$ such that*

$$f \equiv g \bmod W \quad \textit{and} \quad g \textit{ is in normal form with respect to } w_1, \ldots, w_N.$$

Proof. We proceed by induction on N. The case $N = 0$ being trivial, suppose that $N \geqslant 1$, and let $f \in A[X]$. By Euclidean Division in $A[X]$ take $q, r \in A[X]$ such that $f = q\, w_N + r$ and $\deg_{X_N} r < d_N$; thus $f \equiv r \bmod w_N A[X]$. Let $r_0, \ldots, r_{d_N - 1} \in A[X']$ such that $r = \sum_j r_j X_N^j$. Note that $w_1, \ldots, w_{N-1}$ is a Weierstrass sequence over A in $A[X']$, and let W' be the ideal of $A[X']$ generated by $w_1, \ldots, w_{N-1}$. By inductive hypothesis we obtain $g_0, \ldots, g_{d_N - 1} \in A[X']$ such that $r_j \equiv g_j \bmod W'$ and g_j is in normal form with respect to $w_1, \ldots, w_{N-1}$, for $j = 0, \ldots, d_N - 1$. Hence $r \equiv g \bmod W'A[X]$ where $g := \sum_j g_j X_N^j$ is in normal form with respect to $w_1, \ldots, w_N$ and $f \equiv g \bmod W$ as desired. □

Remark. We can always pass from the Weierstrass sequence $w_1, \ldots, w_N$ to a Weierstrass sequence $w_1^*, \ldots, w_N^*$ generating the same ideal W such that w_j^*, viewed as polynomial in X_j, has degree d_j and coefficients which are in normal form with respect to $w_1^*, \ldots, w_{j-1}^*$, for each $j = 1, \ldots, N$.

Next we show that the element g in the previous lemma is uniquely determined by f and our Weierstrass sequence $w_1, \ldots, w_N$. (This allows us to define *the* normal form of f with respect to $w_1, \ldots, w_N$ to be the unique g satisfying the conditions in Lemma 4.1.2.)

Lemma 4.1.3. *If $g \in W$ is in normal form with respect to $w_1, \ldots, w_N$, then $g = 0$.*

Proof. We proceed by induction on N. With the case $N = 0$ again being trivial, we suppose that $N \geqslant 1$, and let $g \in W$ be in normal form with respect to $w_1, \ldots, w_N$. Let $g = \sum_i w_i z_i$ where $z_i \in A[X]$. By Euclidean Division take $q_i, r_i \in A[X]$ such that $z_i = q_i w_N + r_i$ and $\deg_{X_N} r_i < d_N$, for $i < N$. Then $g = \sum_{i<N} w_i r_i + w_N \left(\sum_{i<N} q_i + z_N\right)$. Hence we can reduce to the case $\deg_{X_N} z_i < d_N$ for $i < N$. Setting $h := \sum_{i<N} w_i z_i$ we then have $g = w_N z_N + h$ and $\deg_{X_N} h < d_N$; by the uniqueness part of Euclidean Division in $A[X]$ we thus have $z_N = 0$, $g = h$. With W' denoting again the ideal of $A[X']$ generated by $w_1, \ldots, w_{N-1}$, we have $g \in W'A[X]$. In fact, write $g = \sum_j g_j X_N^j$ where $g_j \in A[X']$; then for each j we have $g_j \in W'$ and g_j is in normal form with respect to $w_1, \ldots, w_{N-1}$, thus $g_j = 0$ by inductive hypothesis and so $g = 0$ as claimed. □

Hence the A-module $A[X]/W$ is finitely generated and free, with basis given by the images

of the monomials X^ν with $\nu_i < d_i$ for $i = 1, \ldots, N$ under the natural surjection $A[X] \to A[X]/W$. In the next proposition (on "universal denominators") we assume that A is an integral domain, and we let $K = \mathrm{Frac}(A)$.

Proposition 4.1.4. *Let I be a finitely generated ideal of $A[X]$ containing $w_1, \ldots, w_N$. Then there is some $a \in A$ such that $IK[X] \cap A[X] = (I : a)$.*

Proof. Take $g_1, \ldots, g_n \in I$ which, together with $w_1, \ldots, w_N$, generate the ideal I. By Lemma 4.1.2 we may assume that the g_i are in normal form with respect to $w_1, \ldots, w_N$. Then

$$\begin{aligned} f \in IK[X] \quad &\iff \quad \text{there are } y_1, \ldots, y_n \in K[X] \text{ with } f \equiv \sum_i g_i y_i \bmod WK[X] \\ &\iff \quad \begin{cases} \text{there are } y_1, \ldots, y_n \in K[X] \text{ in normal form with respect} \\ \text{to } w_1, \ldots, w_N \text{ such that } f \equiv \sum_i g_i y_i \bmod WK[X]. \end{cases} \end{aligned}$$

We now convert the last congruence into a system of linear equations over A. Let ν range over the multiindices in $\mathbb{N}^N$ such that X^ν is in normal form with respect to $w_1, \ldots, w_N$ (i.e., $\nu_i < d_i$ for $i = 1, \ldots, N$), and similarly with ν', ν''; then take $g_{i\nu} \in A$ with $g_i = \sum_\nu g_{i\nu} X^\nu$ and $a^\nu_{\nu'\nu''} \in A$ with

$$X^{\nu'} X^{\nu''} \equiv \sum_\nu a^\nu_{\nu'\nu''} X^\nu \bmod W \qquad \text{for all } \nu', \nu''.$$

If $y_i = \sum_\nu y_{i\nu} X^\nu$ ($y_{i\nu} \in K$), then

$$y_i g_i \equiv \sum_{\nu', \nu''} y_{i\nu'} g_{i\nu''} X^{\nu'} X^{\nu''} \equiv \sum_\nu \left(\sum_{\nu', \nu''} y_{i\nu'} g_{i\nu''} a^\nu_{\nu'\nu''} \right) X^\nu \bmod W,$$

so the normal form of $y_i g_i$ with respect to $w_1, \ldots, w_N$ is given by the polynomial on the right. Therefore, setting $b^\nu_{i\nu'} := \sum_{\nu''} g_{i\nu''} a^\nu_{\nu'\nu''} \in A$, if $f = \sum_\nu f_\nu X^\nu$ ($f_\nu \in A$) is in normal form with respect to $w_1, \ldots, w_N$, then

$$f = \sum_i g_i y_i \qquad \iff \qquad f_\nu = \sum_{i, \nu'} b^\nu_{i\nu'} y_{i\nu'} \quad \text{for each } \nu,$$

therefore the existence of polynomials $y_1, \ldots, y_n \in K[X]$ which are in normal form with respect to $w_1, \ldots, w_N$ and satisfy $f \equiv \sum_i g_i y_i \bmod WK[X]$ is equivalent to the existence

of a solution $y_{i\nu'} \in K$ of the system of linear equations $f_\nu = \sum_{i,\nu'} b^\nu_{i\nu'} y_{i\nu'}$. Now apply Remark 3.1.3 to this system of linear equations over A to obtain an element a of A as desired. □

Remark. In [7, Corollary 3.5] it is claimed that an a with the property stated in the proposition above can be found even without assuming that the ideal I contains a Weierstrass sequence over A. In this generality, this now seems doubtful, see [10].

The next fact is useful in arguments by induction on dimension:

Corollary 4.1.5. *Suppose A is noetherian. Let I be an ideal of $A[X]$ containing $w_1, \ldots, w_N$, and let f be a non-zero-divisor of A. Then*

$$\dim A[X]/(I, f) < \dim A.$$

Proof. Since I contains W we have $\dim A[X]/(I, f) \leqslant \dim A[X]/(W, f)$, hence we may replace I by W and assume that $I = W$ is generated by $w_1, \ldots, w_N$. By Krull's Principal Ideal Theorem [11, Corollary 11.17] and Lemma 4.1.1 it is enough to show that f is not a zero-divisor in $A[X]/I$. Let $g \in A[X]$ with $fg \in I$; we claim that $g \in I$. By Lemma 4.1.2 we can assume that g is in normal form with respect to $w_1, \ldots, w_N$. Then fg is also in normal form with respect to $w_1, \ldots, w_N$, hence $fg = 0$ by Lemma 4.1.3. Since f is a non-zero-divisor of A, this yields $g = 0$. □

Weierstrass sequences in $D\langle C, X\rangle$

Next we consider the case $A := D\langle C\rangle$ where the integral domain D is as in Chapter 2.1; we also set $A\langle X\rangle := D\langle C, X\rangle$. The next lemma can be seen as a version of Weierstrass Division for Weierstrass sequences.

Lemma 4.1.6. *Let $w_1, \ldots, w_N \in A[X]$ be a Weierstrass sequence over A, and let W be the ideal of $A[X]$ generated by $w_1, \ldots, w_N$. Then for each $f \in A\langle X\rangle$ there is some $g \in A[X]$ such that*

$$f \equiv g \mod W A\langle X\rangle \quad \textit{and} \quad g \textit{ is in normal form with respect to } w_1, \ldots, w_N.$$

Proof. Similar to the proof of Lemma 4.1.2, using Weierstrass Division in $A\langle X\rangle = D\langle C, X\rangle$ instead of Euclidean Division. □

In the setting of the previous lemma, the natural inclusion $A[X] \to A\langle X\rangle$ induces an $A[X]$-algebra morphism $A[X]/W \to A\langle X\rangle/WA\langle X\rangle$. By Lemma 4.1.6 this morphism is surjective, hence the A-module $A\langle X\rangle/WA\langle X\rangle$ is also finitely generated. In fact, the A-algebra morphism in question is an isomorphism. (This generalizes Corollary 2.1.5.) We won't show this here, but we'll prove an analogous fact for rings of nonstandard restricted power series in the next section.

Weierstrass sequences in $R\langle X\rangle$

In the rest of this section we now let R range over models of T_D and c over R^M, and $F = \mathrm{Frac}(R)$. Moreover, in this subsection $A = R\langle V\rangle$ where $V = (V_1, \ldots, V_L)$ is a tuple of new distinct indeterminates, and $A\langle X\rangle := R\langle V, X\rangle$. We note that if $w_1, \ldots, w_N \in D\langle C, V\rangle[X]$ is a Weierstrass sequence over $D\langle C, V\rangle$, then $w_1(c, V, X), \ldots, w_N(c, V, X) \in A[X]$ is a Weierstrass sequence over A, and every Weierstrass sequence over A arises this way (for some choice of C, c, and $w_1, \ldots, w_N$). Moreover, if $g \in D\langle C, V\rangle[X]$ is in normal form with respect to a Weierstrass sequence $w_1, \ldots, w_N \in D\langle C, V\rangle[X]$ over $D\langle C, V\rangle$, then the polynomial $g(c, V, X) \in A[X]$ is in normal form with respect to the Weierstrass sequence $w_1(c, V, X), \ldots, w_N(c, V, X)$ over A. We have the following uniform version of Lemma 4.1.6.

Lemma 4.1.7. *For each $f \in D\langle C, V, X\rangle$ and each Weierstrass sequence $w_1, \ldots, w_N \in D\langle C, V\rangle[X]$ over $D\langle C, V\rangle$ there are $q_1, \ldots, q_N \in D\langle C, V, X\rangle$ as well as a polynomial $g \in D\langle C, V\rangle[X]$ in normal form with respect to $w_1, \ldots, w_N$ such that for all R and c,*

$$f(c, V, X) = \sum_{i=1}^{N} q_i(c, V, X) w_i(c, V, X) + g(c, V, X).$$

Let now $w_1, \ldots, w_N \in A[X]$ be a Weierstrass sequence over $A = R\langle V\rangle$ and W be the ideal of $A[X]$ generated by $w_1, \ldots, w_N$.

Lemma 4.1.8. *For each $f \in A\langle X\rangle$ there is some $g \in A[X]$ such that*

$$f \equiv g \bmod WA\langle X\rangle \quad \textit{and} \quad g \textit{ is in normal form with respect to } w_1, \ldots, w_N.$$

This follows immediately from Lemma 4.1.7 and the remarks at the beginning of this subsection. In particular, each ideal of $A\langle X\rangle$ containing $w_1, \ldots, w_N$ is generated by polynomials from $A[X]$.

Lemma 4.1.9. *$WA\langle X\rangle \cap A[X] = W$.*

Proof. We proceed by induction on N. Since the case $N = 0$ is obvious, we assume $N \geqslant 1$, and let $f \in WA\langle X\rangle \cap A[X]$. Take $z_1, \ldots, z_N \in A\langle X\rangle$ such that $f = \sum_i w_i z_i$; we need to show that we can choose $z_i \in A[X]$. By Weierstrass Division take $q_1, \ldots, q_{N-1} \in A\langle X\rangle$ and $r_1, \ldots, r_{N-1} \in A\langle X'\rangle[X_N]$ such that $z_i = q_i w_N + r_i$ for $i = 1, \ldots, N-1$; then $f = \sum_{i<N} w_i r_i + w_N \left(\sum_{i<N} q_i + z_N\right)$. Hence we can reduce to the case $z_1, \ldots, z_{N-1} \in A\langle X'\rangle[X_N]$; by Corollary 2.3.6 we then also have $z_N \in A\langle X'\rangle[X_N]$. Successively applying Lemma 4.1.8 to the coefficients of z_N in $A\langle X'\rangle$ and the Weierstrass sequence $w_1, \ldots, w_{N-1} \in A[X']$ in place of f and $w_1, \ldots, w_N$, respectively, we can further reduce to the case where $z_N \in A[X]$. Hence we may replace f by $f - w_N z_N \in A[X]$ and can assume that $z_N = 0$. Now let $f_j \in A[X']$ such that $f = \sum_j f_j X_N^j$ and $z_{ij} \in A\langle X'\rangle$ such that $z_i = \sum_j z_{ij} X_N^j$; then the equation $f = \sum_{i<N} w_i z_i$ is equivalent to the equations $f_j = \sum_{i<N} w_i z_{ij}$. By inductive hypothesis, we can choose z_{ij} solving these equations in $A[X']$. □

The following generalizes Corollary 2.3.7:

Corollary 4.1.10. *Let J be an ideal of $A[X]$ containing $w_1, \ldots, w_N$. Then*

$$JA\langle X\rangle \cap A[X] = J.$$

Proof. Let $f \in JA\langle X\rangle \cap A[X]$. Then there are $f_1, \ldots, f_m \in J$ and $y_1, \ldots, y_m \in A\langle X\rangle$ (for some m) and $g \in WA\langle X\rangle$ such that $f = \sum_i y_i f_i + g$. Applying Lemma 4.1.8 successively to each y_i (in place of f) and modifying the y_i and g appropriately, we reduce to the case where $y_i \in A[X]$ for each i. Then $f - \sum_i y_i f_i = g \in WA\langle X\rangle \cap A[X] = W$ by Lemma 4.1.9. □

Weierstrass sequences in $F\langle X\rangle$

Let R, F, V be as in the previous subsection, but now let $A := F\langle V\rangle$ and $A\langle X\rangle := F\langle V, X\rangle$. Let $w_1, \ldots, w_N \in R\langle V\rangle[X]$ be a Weierstrass sequence over A, let J be an ideal of $A[X]$

containing $w_1, \dots, w_N$, and $I = JA\langle X\rangle$. Lemma 4.1.8 and Corollary 4.1.10 imply that the natural inclusion

$$A[X] = F\langle V\rangle[X] \subseteq F\langle V, X\rangle = A\langle X\rangle$$

induces an $A[X]$-algebra isomorphism $A[X]/J \xrightarrow{\cong} A\langle X\rangle/I$. In particular, I is radical (primary, prime, maximal, ...) iff J has the corresponding property.

Corollary 4.1.11. $\dim A\langle X\rangle/I \leqslant L$, *with equality if and only if* $A \cap I = \{0\}$.

Proof. By Corollary 2.3.13 we have $\dim A = L$, hence by Lemma 4.1.1 and the isomorphism above we obtain $\dim A\langle X\rangle/I \leqslant L$, with equality if $A \cap I = \{0\}$. Moreover, by Corollary 4.1.5 applied to $I \cap A[X] = J$ in place of I, we obtain $\dim A\langle X\rangle/(I, f) < L$ for each $f \in A^{\neq}$. In particular $\dim A\langle X\rangle/I = L$ implies $A \cap I = \{0\}$. □

Lemma 4.1.12. *Let* $a \in A$. *Then* $(I : a) = (J : a)A\langle X\rangle$.

Proof. Note that $I = JA\langle X\rangle \subseteq (J : a)A\langle X\rangle$. Let $f \in (I : a)$, and take $g \in A[X]$ with $f \equiv g \bmod I$ (Lemma 4.1.8). Then $ag \in I \cap A[X] = J$, hence $g \in (J : a)$, so $f \in (J : a)A\langle X\rangle$. □

Lemma 4.1.13. $\sqrt{I} = \sqrt{J}A\langle X\rangle$.

Proof. The ideal $\sqrt{J}A\langle X\rangle$ is radical, and clearly $I = JA\langle X\rangle \subseteq \sqrt{J}A\langle X\rangle \subseteq \sqrt{I}$, so $\sqrt{I} = \sqrt{J}A\langle X\rangle$. □

Constructing Weierstrass sequences

In this subsection we let I be an ideal of $F\langle X\rangle$. Here is a "non-standard" version of the familiar Noether Normalization Theorem for the restricted power series ring $\mathbb{Q}_p\langle X\rangle$ (see [14, §6.1.2]):

Proposition 4.1.14. *Suppose* $1 \notin I$. *Then there are some* $d \in \{0, \dots, N\}$ *and a polynomial automorphism* σ *of* $F\langle X\rangle$ *such that*

(1) $\sigma(I) \cap F\langle X_1, \dots, X_d\rangle = \{0\}$; *and*

(2) $\sigma(I)$ *contains a Weierstrass sequence*

$$w_1, \ldots, w_{N-d} \in R\langle X_1, \ldots, X_d\rangle[X_{d+1}, \ldots, X_N]$$

over $R\langle X_1, \ldots, X_d\rangle$.

Proof. We proceed by induction on N. If $I = \{0\}$ then we may take $d = N$ and for σ the identity on $F\langle X\rangle$. This includes the case $N = 0$, so suppose now that $N \geqslant 1$ and $I \neq \{0\}$. Take a nonzero $g \in I$, and let σ be a polynomial automorphism of $F\langle X\rangle$ such that $\sigma(g)$ is regular in X_N of some degree $s \in \mathbb{N}$. Then by Corollary 2.3.9 we have $\sigma(g) = u \cdot w$ where $u \in F\langle X\rangle^\times$ and $w \in R\langle X'\rangle[X_N]$ is a Weierstrass polynomial of degree s. Here $w \in \sigma(I)$; note that $s \geqslant 1$ since $\sigma(I) \neq F\langle X\rangle$. By inductive hypothesis applied to the ideal $I' := \sigma(I) \cap F\langle X'\rangle$ of $F\langle X'\rangle$ there is some $d \in \{0, \ldots, N-1\}$ and a polynomial automorphism σ' of $F\langle X'\rangle$ such that $\sigma'(I') \cap F\langle X_1, \ldots, X_d\rangle = \{0\}$, as well as a Weierstrass sequence

$$w_1, \ldots, w_{N-1-d} \in \sigma'(I') \cap R\langle X_1, \ldots, X_d\rangle[X_{d+1}, \ldots, X_{N-1}]$$

over $R\langle X_1, \ldots, X_d\rangle$. We extend σ' to a polynomial automorphism of $F\langle X\rangle$, also denoted by σ', such that $\sigma'(X_N) = X_N$. Then we have $(\sigma' \circ \sigma)(I) \cap F\langle X_1, \ldots, X_d\rangle = \{0\}$, and $w_1, \ldots, w_{N-1-d}, \sigma'(w)$ is a Weierstrass sequence in $(\sigma' \circ \sigma)(I)$, as required. □

By clearing denominators we obtain a version of Proposition 4.1.14 for ideals of $R\langle X\rangle$:

Corollary 4.1.15. *Let J be an ideal of $R\langle X\rangle$ with $J \cap R = \{0\}$. Then there are some $r \in R^{\neq}$, some $d \in \{0, \ldots, N\}$, and a polynomial automorphism σ of $R\langle X\rangle$ such that*

(1) $\sigma(J) \cap R\langle X_1, \ldots, X_d\rangle = \{0\}$*; and*

(2) *the ideal $\sigma(J : r) \cap R\langle X_1, \ldots, X_d\rangle[X_{d+1}, \ldots, X_N]$ contains a Weierstrass sequence over $R\langle X_1, \ldots, X_d\rangle$.*

Proof. Apply Proposition 4.1.14 to $I = JF\langle X\rangle$. □

By Corollary 4.1.11, the integer d in the previous proposition is uniquely determined: it equals $\dim I$.

Corollary 4.1.16. *If the ideal I is maximal, then the field $F\langle X\rangle/I$ is finite over its subfield F.*

4.2 Uniform Noether Normalization

In this section we formulate a uniform variant of Noether Normalization and give some of its applications. *Throughout this section we let $f_1, \dots, f_m \in D\langle C, X\rangle$, and we let R range over models of T_D.* Moreover, "formula" and "term" mean "$\mathcal{L}_D^{\mathrm{d}}$-formula" and "$\mathcal{L}_D^{\mathrm{d}}$-term," respectively, unless noted otherwise. We let $F = \mathrm{Frac}(R)$, and for $c \in R^M$ we denote again by $I(c, X)$ the ideal of $R\langle X\rangle$ generated by $f_1(c, X), \dots, f_m(c, X)$. Recall the conventions concerning polynomial automorphisms introduced in Sections 2.2 and 2.3: for each automorphism σ of $\mathbb{Z}[X]$ which maps the ideal (X) generated by the tuple of indeterminates $X = (X_1, \dots, X_N)$ to itself, we obtain an F-algebra automorphism of $F\langle X\rangle$, also denoted by σ, given by "substitution of $\sigma(X)$ for X".

Proposition 4.2.1 (Uniform Noether Normalization Theorem)**.** *There exist a quantifier-free formula $\varphi(C)$, an L-tuple of terms v ($L \in \mathbb{N}$), and a finite family*

$$\mathcal{N} = \left\{\left(\varphi^{(\lambda)}, d^{(\lambda)}, v^{(\lambda)}, w^{(\lambda)}, \sigma^{(\lambda)}\right)\right\}_{\lambda\in\Lambda}$$

where for some tuple $V = (V_1, \dots, V_L)$ of distinct new indeterminates and with λ ranging over Λ,

(1) *$\varphi^{(\lambda)} = \varphi^{(\lambda)}(C)$ is a quantifier-free formula,*

(2) *$d^{(\lambda)}$ is an element of $\{0, \dots, N\}$,*

(3) *$w^{(\lambda)}$ is a Weierstrass sequence*

$$w_1^{(\lambda)}, \dots, w_{N-d^{(\lambda)}}^{(\lambda)} \in D\langle V, X_1, \dots, X_{d^{(\lambda)}}\rangle[X_{d^{(\lambda)}+1}, \dots, X_N]$$

over $D\langle V, X_1, \dots, X_{d^{(\lambda)}}\rangle$, and

(4) *$\sigma^{(\lambda)}$ is an automorphism of $\mathbb{Z}[X]$ which maps the ideal (X) to itself,*

with the following properties, for all R and $c \in R^M$:

(N1) $R \models \varphi(c) \to \bigvee_\lambda \varphi^{(\lambda)}(c)$,

(N2) *if* $R \models \neg\varphi(c)$, *then* $I(c,X) \cap R \neq \{0\}$, *and*

(N3) *if* $R \models \varphi^{(\lambda)}(c)$, *then*

$$\sigma^{(\lambda)}\big(I(c,X)F\langle X\rangle\big) \cap F\langle X_1, \ldots, X_{d^{(\lambda)}}\rangle = \{0\}$$

and

$$w_i^{(\lambda)}\big(v(c), X\big) \in \sigma^{(\lambda)}\big(I(c,X)F\langle X\rangle\big) \quad \text{for } i = 1, \ldots, N - d^{(\lambda)}.$$

Proof. Follows from Proposition 4.1.14 by compactness, using Corollaries 3.3.10, 3.3.11, and 3.3.17. □

In particular, we see that dimension is uniformly definable in parameters:

Corollary 4.2.2. *For each $d \in \{0, \ldots, N\}$ there is a quantifier-free formula $\dim_d(C)$ such that for all R and $c \in R^M$ we have*

$$R \models \dim_d(c) \qquad \Longleftrightarrow \qquad \dim I(c,X)F\langle X\rangle = d.$$

Proof. With $\mathcal{N}$ as in the preceding proposition, let $\dim_d := \bigvee_{d^{(\lambda)}=d} \varphi^{(\lambda)}$. □

As a consequence, the dimension of $I(c,X)F\langle X\rangle$ does not change if R, F are replaced by a substructure containing c and its fraction field. We can now also prove the definability of the property of being a maximal ideal of $F\langle X\rangle$:

Corollary 4.2.3. *There is a formula $\mathrm{Max}(C)$ such that for all R and $c \in R^M$,*

$$R \models \mathrm{Max}(c) \qquad \Longleftrightarrow \qquad \textit{the ideal } I(c,X)F\langle X\rangle \textit{ of } F\langle X\rangle \textit{ is maximal.}$$

Proof. Combining Lemma 4.1.7 and Proposition 4.2.1 we obtain an L-tuple v of terms in C ($L \in \mathbb{N}$), and a finite family

$$\big\{\big(\varphi^{(\lambda)}, g^{(\lambda)}, w^{(\lambda)}, \sigma^{(\lambda)}\big)\big\}_{\lambda\in\Lambda}$$

where for some tuple $V = (V_1, \ldots, V_L)$ of distinct new indeterminates and with λ ranging over Λ,

(1) $\varphi^{(\lambda)}(C)$ is a quantifier-free formula,

(2) $g^{(\lambda)} = \big(g_1^{(\lambda)}, \ldots, g_m^{(\lambda)}\big)$ and $w^{(\lambda)} = \big(w_1^{(\lambda)}, \ldots, w_N^{(\lambda)}\big)$ are tuples of polynomials from $D\langle V\rangle[X]$, where $w^{(\lambda)}$ is a Weierstrass sequence over $D\langle V\rangle$ with respect to which each $g_i^{(\lambda)}$ is in normal form, and

(3) $\sigma^{(\lambda)}$ is an automorphism of $\mathbb{Z}[X]$ mapping the ideal (X) to itself,

with the following properties: for all R and $c \in R^M$ with $R \models \dim_0(c)$ we have $R \models \varphi^{(\lambda)}(c)$ for some $\lambda \in \Lambda$, and denoting by $J^{(\lambda)}(c, X)$ the ideal of $F[X]$ generated by the polynomials $g_i^{(\lambda)}\big(v(c), X\big)$ and $w_j^{(\lambda)}\big(v(c), X\big)$, we have

$$J^{(\lambda)}(c, X)F\langle X\rangle = \sigma^{(\lambda)}\big(I(c, X)F\langle X\rangle\big)$$

and the natural inclusion $F[X] \to F\langle X\rangle$ induces an isomorphism

$$F[X]/J^{(\lambda)}(c, X) \xrightarrow{\cong} F\langle X\rangle/J^{(\lambda)}(c, X)F\langle X\rangle.$$

Let $d_i^{(\lambda)} := \deg_{X_i} w_i^{(\lambda)}$. Note that the F-algebra $F[X]/J^{(\lambda)}(c, X)$ is finite-dimensional as an F-linear space, of dimension at most $\prod_{i=1}^N d_i^{(\lambda)}$, generated by the residue classes modulo $J^{(\lambda)}(c, X)$ of the monomials X^ν with $\nu_i < d_i^{(\lambda)}$ for $i = 1, \ldots, N$. Hence using Corollary 3.3.11 one easily obtains a formula $\psi^{(\lambda)}(C)$ such that for each R and $c \in R^M$ we have

$$R \models \psi^{(\lambda)}(c) \quad \iff \quad F\langle X\rangle/J^{(\lambda)}(c, X)F\langle X\rangle \text{ is a field.}$$

Thus $\mathrm{Max} := \dim_0 \wedge \bigvee_\lambda \big(\varphi^{(\lambda)} \wedge \psi^{(\lambda)}\big)$ does the job. □

The corresponding fact for ideals in polynomial rings over fields was shown by van den Dries [21, (1.6)–(1.10)] using a model-theoretic compactness argument:

Lemma 4.2.4. *Let $g_1(C, X), \ldots, g_n(C, X) \in \mathbb{Z}[C, X]$. Then there is a formula $\mu(C)$ in the language of rings such that for each field K and $c \in K^M$,*

$$K \models \mu(c) \qquad \iff \qquad g_1(c, X), \ldots, g_n(c, X) \text{ generate a maximal ideal of } K[X].$$

Here is an analogue for ideals of $R\langle X\rangle$:

Corollary 4.2.5. *There is a formula* $\max(C)$ *such that for all* R *and* $c \in R^M$,

$$R \models \max(c) \qquad \Longleftrightarrow \qquad \textit{the ideal } I(c, X) \textit{ of } R\langle X\rangle \textit{ is maximal.}$$

Proof. By Corollary 2.3.2, the ideal $I(c, X)$ is maximal iff it contains $\mathfrak{m}_R = t_R R$ and maps onto a maximal ideal of $\overline{R}[X]$ under the residue morphism $R\langle X\rangle \to \overline{R}[X]$. To construct our formula max, we first take $\epsilon(C, C')$ as in Corollary 3.3.10; then for all R and $c \in R^M$ we have

$$R \models \epsilon(c, t_R) \quad \Longleftrightarrow \quad I(c, X) \supseteq \mathfrak{m}_R.$$

Also, take $d \in \mathbb{N}$ as in Lemma 2.2.8 which works for each of $f_1, \dots, f_m$ (see the remarks preceding Corollary 2.2.13). Then the polynomials $\overline{f_i(c, X)} \in \overline{R}[X]$ have degree $< d$ (see (2.7)). For $i = 1, \dots, m$ write $f_i = \sum_\nu f_{i\nu}(C)X^\nu$ ($f_{i\nu} \in D\langle C\rangle$); thus $\overline{f_i(c, X)} = \sum_{|\nu|<d} \overline{f_{i\nu}(c)}X^\nu$. We introduce the tuple $f(C) := \big(f_{i\nu}(C)\big)$ of elements of $D\langle C\rangle$, where i ranges over $\{1, \dots, m\}$ and ν over the multiindices in $\mathbb{N}^N$ with $|\nu| < d$. By the lemma above we can take a formula $\overline{\mu}$ in the language of rings such that for all R and $c \in R^M$,

$$\overline{R} \models \overline{\mu}\big(\overline{f(c)}\big) \quad \Longleftrightarrow \quad \overline{f_1(c, X)}, \dots, \overline{f_m(c, X)} \text{ generate a maximal ideal of } \overline{R}[X].$$

Since $\mathfrak{m}_R = t_R R$ is uniformly definable in R, it is routine to translate $\overline{\mu}$ into a formula μ in the language of rings such that for all R and $c \in R^M$ we have

$$\overline{R} \models \overline{\mu}\big(\overline{f(c)}\big) \quad \Longleftrightarrow \quad R \models \mu\big(f(c)\big).$$

Then $\max(C) := \epsilon(C, t) \wedge \mu\big(f(C)\big)$ does the job. □

Corollary 4.2.6. *Let* $R \subseteq R^*$ *be an elementary extension of models of* T_D *with fraction fields* F, F^*, *and* $c \in R^M$. *Then*

$$I(c, X) \textit{ is maximal} \quad \Longleftrightarrow \quad I(c, X)R^*\langle X\rangle \textit{ is maximal}$$

and

$$I(c, X)F\langle X\rangle \textit{ is maximal} \quad \Longleftrightarrow \quad I(c, X)F^*\langle X\rangle \textit{ is maximal.}$$

We also have a uniform version of Proposition 4.1.4. To formulate it, let

$$g_1, \ldots, g_n, w_1, \ldots, w_{N-d} \in D\langle C, X_1, \ldots, X_d\rangle[X_{d+1}, \ldots, X_N] \qquad (d \in \{0, \ldots, N\}),$$

where $w_1, \ldots, w_{N-d}$ is a Weierstrass sequence over $D\langle C, X_1, \ldots, X_d\rangle$. Let

$$F = \mathrm{Frac}(R) \ \subseteq \ A := F\langle X_1, \ldots, X_d\rangle \ \subseteq \ K := \mathrm{Frac}(A),$$

and for $c \in R^M$ let $J(c, X)$ denote the ideal of $A[X_{d+1}, \ldots, X_N]$ generated by

$$g_1(c, X), \ldots, g_n(c, X), w_1(c, X), \ldots, w_{N-d}(c, X).$$

Corollary 4.2.7. *There are a covering family $\{\varphi^{(\lambda)}(C)\}$ of quantifier-free formulas and for each λ an element $a^{(\lambda)}$ of $D\langle C, X_1, \ldots, X_d\rangle$ such that for each R and $c \in R^M$ with $R \models \varphi^{(\lambda)}(c)$, we have*

$$J(c, X)K[X_{d+1}, \ldots, X_N] \cap A[X_{d+1}, \ldots, X_N] = \big(J(c, X) : a^{(\lambda)}(c, X_1, \ldots, X_d)\big).$$

Proof. Follow the proof of Proposition 4.1.4. □

For later use we note that the proof of Proposition 4.1.4 also indicates how to uniformly describe generators for the quotient ideal $\big(J(c, X) : a^{(\lambda)}(c, X_1, \ldots, X_d)\big)$.

Corollary 4.2.8. *Let $a(C, X_1, \ldots, X_d) \in D\langle C, X_1, \ldots, X_d\rangle$. Then there are a covering family $\{\varphi^{(\lambda)}(C)\}$ of quantifier-free formulas and for each λ elements*

$$h_1^{(\lambda)}(V, X), \ldots, h_k^{(\lambda)}(V, X) \in D\langle V, X_1, \ldots, X_d\rangle[X_{d+1}, \ldots, X_N],$$

where $V = (V_1, \ldots, V_L)$ is an L-tuple of new distinct indeterminates ($L \in \mathbb{N}$), as well as an L-tuple τ of terms in C, such that for R and $c \in R^M$ with $R \models \varphi^{(\lambda)}(c)$, the polynomials $h_1^{(\lambda)}\big(\tau(c), X\big), \ldots, h_k^{(\lambda)}\big(\tau(c), X\big)$ generate the ideal

$$\big(J(c, X) : a(c, X_1, \ldots, X_d)\big)$$

of $A[X_{d+1}, \ldots, X_N]$.

We leave the details to the reader. (Use Corollary 3.3.8.)

4.3 Uniform Noetherianity

In this section we focus on models of the analytic theory of $\mathbb{Z}_p$. Recall that an ordered abelian group Γ is said to be a $\mathbb{Z}$-*group* if it is elementarily equivalent to the ordered abelian group $\mathbb{Z}$; equivalently, if Γ has a smallest positive element and $|\Gamma/n\Gamma| = n$ for each $n \geqslant 1$. If Γ is a $\mathbb{Z}$-group, then we denote by 1 the smallest positive element of Γ, and identify $\mathbb{Z}$ with an ordered subgroup of Γ via the embedding $k \mapsto k \cdot 1 \colon \mathbb{Z} \to \Gamma$. We also recall that a henselian valued field is *p-adically closed* if its residue field is isomorphic to $\mathbb{F}_p$ and its value group is a $\mathbb{Z}$-group with smallest positive element $1 = v(p)$. A valuation ring is called *p-adically closed* if it is the valuation ring of a p-adically closed field. So the valued field $\mathbb{Q}_p$ is p-adically closed and its valuation ring $\mathbb{Z}_p$ is a p-adically closed valuation ring. By a theorem of Ax-Kochen [13] and Eršov [32] the $\mathcal{L}_{\mathrm{div}}$-theory of p-adically closed valuation rings is complete. (See also Section 6.2 below.) An analytic counterpart was proved in [23, (3.2)], based on the parametric Weierstraß Division Theorem and earlier work by Denef and van den Dries [19], who showed that the $\mathcal{L}_{\mathbb{Z}_p}$-structure $\mathbb{Z}_p$ is model complete (indeed, has quantifier elimination in an expansion of the language $\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$ by certain definable predicates). We let T_p be the $\mathcal{L}_{\mathbb{Z}_p}$-theory of *p-adically closed* valuation rings with $\mathbb{Z}_p$-structure (to be distinguished from the theory $T_{\mathbb{Z}_p} \subseteq T_p$ whose models are *all* valuation rings with $\mathbb{Z}_p$-structure; cf. Section 2.2). Note that for each model R of T_p there is a natural embedding $\mathbb{Z}_p \to R$ of $\mathcal{L}_{\mathbb{Z}_p}$-structures, via which we identify $\mathbb{Z}_p$ with a substructure of R.

Theorem 4.3.1 (van den Dries)**.** *T_p is complete.*

As a consequence one obtains (see [23, (2.4)]):

Corollary 4.3.2. *T_p has definable Skolem functions.*

We will typically use these two facts in combination, in the following way. *In the rest of this section, "formula" means "$\mathcal{L}_{\mathbb{Z}_p}$-formula" and "term" means "$\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$-term".* Let φ be a formula in a single free variable. Each ideal of $\mathbb{Z}_p$ is principal, hence if in $\mathbb{Z}_p$ the formula φ defines an ideal of $\mathbb{Z}_p$, then in each $R \models T_p$, it defines a principal ideal of R, by Theorem 4.3.1.

Moreover, using Corollary 4.3.2 we can also formulate a uniform version of this observation. For this we let C' be a new indeterminate and as usual $C = (C_1, \dots, C_M)$.

Lemma 4.3.3. *For each formula $\varphi(C, C')$ there is a formula which in each $R \models T_p$ defines the graph of a function $c \mapsto a(c)\colon R^M \to R$ with the following property: if $c \in R^M$ and $\varphi(c, C')$ defines an ideal $I(c)$ of R, then $I(c) = a(c)R$.*

In particular, definable ideals of models of T_p are principal; only very few of them are radical:

Corollary 4.3.4. *Let $R \models T_p$. Then $\mathfrak{m}_R = pR$ is the only nontrivial definable radical ideal of R.*

Proof. Clearly this holds for $R = \mathbb{Z}_p$. In general, an ideal I of R is radical if and only if the implication $a^2 \in I \Rightarrow a \in I$ holds for each $a \in R$, hence the property of being a radical ideal is uniformly definable. The claim now follows from Theorem 4.3.1. □

Remark. By the previous corollary, the property of a definable ideal of a p-adically closed valuation ring to be radical is uniformly definable, and similarly with "prime" in place of "radical." On the other hand, every proper ideal of $\mathbb{Z}_p$ is primary, hence if the property of an ideal of R to be primary was uniformly definable for all p-adically closed valuation rings, then every definable proper ideal of a p-adically closed valuation ring would be primary. But it is easy to see that none of the principal ideals of a p-adically closed valuation ring R except for the ideals $p^n R$ ($n \geqslant 1$) are primary: let $a \in R$ with $va > v(p^n)$ for all n, and set $f := p$ and $g := a/p \in R$; then $fg \in aR$, but neither $f \in \sqrt{aR}$ nor $g \in aR$, so aR is not primary.

The ring $\mathbb{Z}_p\langle X\rangle$ is noetherian: every nonempty collection of ideals of $\mathbb{Z}_p\langle X\rangle$ has a maximal element with respect to inclusion. (See Section 2.1.) The following proposition may be regarded as a uniform version of this fact for certain *definable* collections of ideals. Below we let C' be a new parametric indeterminate, we let $f_1, \dots, f_m \in \mathbb{Z}_p\langle C, C', X\rangle$, and given $R \models T_{\mathbb{Z}_p}$ and $(c, c') \in R^{M+1}$ we let

$$I(c, c', X) = \big(f_1(c, c', X), \dots, f_m(c, c', X)\big)$$

denote the ideal of $R\langle X\rangle$ generated by the $f_i(c, c', X)$.

Proposition 4.3.5. *Let $\varphi(C, C')$ be a formula and $\pi(C) := \exists C' \varphi$. Then for each $R \models T_p$ and $c \in \pi(R^M)$ there is some $c' \in R$ with $R \models \varphi(c, c')$ and*

$$I(c, c', X) = \bigcup \big\{ I(c, c'', X) : c'' \in R,\ R \models \varphi(c, c'') \big\}. \tag{4.1}$$

Moreover, there is a formula which for each $R \models T_p$ defines the graph of a function

$$c \mapsto c' \colon \pi(R^M) \to R$$

such that for each $c \in \pi(R^M)$ we have $R \models \varphi(c, c')$ and (4.1) holds.

Proof. Let C'' be another new indeterminate. By Corollary 3.3.12 there is a quantifier-free formula $\iota(C, C', C'')$ such that for all $R \models T_{\mathbb{Z}_p}$ and $c \in R^M$, $c', c'' \in R$ we have $R \models \iota(c, c', c'')$ iff $I(c, c', X) \supseteq I(c, c'', X)$. Consider the sentence

$$\mu := \forall C \Big[\pi(C) \to \exists C' \Big(\varphi(C, C') \wedge \forall C'' \big(\varphi(C, C'') \to \iota(C, C', C'') \big) \Big) \Big].$$

Noetherianity of $\mathbb{Z}_p\langle X \rangle$ and completeness of T_p yield $T_p \models \mu$. Now use the fact that T_p has definable Skolem functions. □

It may be worth explicitly stating the case $M = 0$ of the previous proposition.

Corollary 4.3.6. *Suppose $f_1, \ldots, f_m \in \mathbb{Z}_p\langle C', X \rangle$, and let $\varphi(C')$ be a formula such that $T_p \models \exists C'\, \varphi$. Then for each $R \models T_p$ there is some $c' \in R$ with $R \models \varphi(c')$ and*

$$I(c', X) = \bigcup \big\{ I(c'', X) : c'' \in R,\ R \models \varphi(c'') \big\}.$$

For notational simplicity we restricted ourselves to a single new indeterminate C' above; everything works just as well if C' is replaced by a tuple of indeterminates. Below C' continues to be a single indeterminate distinct from $C_1, \ldots, C_M$.

In the rest of this section we assume that $f_1, \ldots, f_m \in \mathbb{Z}_p\langle C, X \rangle$. Next we show a uniform version of the fact that (as a consequence of noetherianity of $\mathbb{Z}_p\langle X \rangle$) for each ideal I of $\mathbb{Z}_p\langle X \rangle$ there is some $e \in \mathbb{N}$ such that $\bigcup_n (I : p^n) = (I : p^e)$:

Proposition 4.3.7. *There is a formula which for each $R \models T_p$ defines the graph of a function $c \mapsto a(c)\colon R^M \to R$ such that for each $c \in R^M$ we have $a(c) \in R^{\neq}$ and*

$$\big(I(c,X) : a(c)\big) = \bigcup \big\{ \big(I(c,X) : b\big) : b \in R^{\neq} \big\}.$$

Proof. This follows immediately from Proposition 4.3.5, but we can also argue as follows: By Corollary 3.3.14 we can take a formula $\psi(C, C')$ such that for all $R \models T_{\mathbb{Z}_p}$ and $c \in R^M$, the formula $\psi(c, C')$ defines the ideal

$$J(c) := \big\{ c' \in R : \big(I(c,X) : c'\big) \supseteq \big(I(c,X) : b\big) \text{ for all } b \in R^{\neq} \big\}$$

of R. For $R = \mathbb{Z}_p$ and $c \in \mathbb{Z}_p^M$ we have $J(c) \neq \{0\}$. Now use Lemma 4.3.3. □

Let $R \models T_p$, $c \in R^M$, $F = \operatorname{Frac}(R)$; then

$$\bigcup \big\{ \big(I(c,X) : b\big) : b \in R^{\neq} \big\} = I(c,X)F\langle X\rangle \cap R\langle X\rangle.$$

Hence if $\alpha(C, C')$ is a formula which in each model of T_p defines a function a as in Proposition 4.3.7, then

$$R \models \forall C' \big(\alpha \to C'|1\big) \quad \iff \quad I(c,X)F\langle X\rangle \cap R\langle X\rangle = I(c,X).$$

Combining the previous proposition with Corollary 3.3.13 also yields:

Corollary 4.3.8. *There is a covering family $\big\{\psi^{(\lambda)}(C)\big\}$ and for each λ an n-tuple*

$$\big(h_1^{(\lambda)}, \dots, h_n^{(\lambda)}\big)$$

of terms $h_j^{(\lambda)}(C, C', X)$ in which the function symbol d *is not applied to subterms involving the X-variables, as well as a formula $\alpha(C, C')$, such that for each $R \models T_p$, the following holds: the formula α defines the graph of a function $c \mapsto a(c)\colon R^M \to R$, and if $c \in R^M$ satisfies $R \models \psi^{(\lambda)}(c)$, then with $F = \operatorname{Frac}(R)$ we have*

$$I(c,X)F\langle X\rangle \cap R\langle X\rangle = \big(h_1^{(\lambda)}(c, a(c), X), \dots, h_n^{(\lambda)}(c, a(c), X)\big).$$

Hence if $R \models T_p$ and I is a finitely generated ideal of $R\langle X\rangle$, then the ideal

$$IF\langle X\rangle \cap R\langle X\rangle = \bigcup \big\{ (I : a) : a \in R^{\neq} \big\}$$

of $R\langle X\rangle$ is finitely generated. For radical ideals, we have:

Corollary 4.3.9. *Let $R \models T_p$, and let I be a radical finitely generated ideal of $R\langle X\rangle$. Then $IF\langle X\rangle \cap R\langle X\rangle = (I : p)$.*

Proof. By Corollary 3.3.15, the ideal

$$J := \left\{r \in R : (I : r) \supseteq (I : b) \text{ for all } b \in R^{\neq}\right\}$$

of R is radical and definable, and by Proposition 4.3.7 we have $J \neq \{0\}$. Hence $p \in J$ by Corollary 4.3.4, and thus $IF\langle X\rangle \cap R\langle X\rangle = (I : p)$. □

Similarly to Proposition 4.3.7, using Corollary 3.3.10 instead of 3.3.14, one shows:

Proposition 4.3.10. *There is a formula which for each $R \models T_p$ defines the graph of a function $c \mapsto r(c)\colon R^M \to R$ such that for each $c \in R^M$ we have $I(c, X) \cap R = r(c)R$.*

Part II

Detecting Radical Ideals

CHAPTER 5

Radicals in Rings of Restricted Power Series

In this chapter we investigate aspects of uniformity for radicals of ideals in rings of restricted power series such as $\mathbb{Q}_p\langle X\rangle$ or $\mathbb{Z}_p\langle X\rangle$. However, in the first section we first briefly discuss the problem of uniformly computing radicals of ideals in polynomial rings. Here, we restrict to ideals of the form $I(c, X)$ of $K[X]$, K a perfect field. We treat fields of characteristic zero separately from perfect fields of positive characteristic. (In the latter case, we need to enlarge the language of rings.) In the next section, we then show that we can reduce the computation of the radical of an ideal in the ring $\mathbb{Q}_p\langle X\rangle$ to finding the radical of "simpler" ideals, some of which will be in polynomial rings of this form. In the last section, we consider the ring $\mathbb{Z}_p\langle X\rangle$. Here, the most general result is to test whether an ideal is radical, allowing us to prove Theorem A stated in the introduction.

5.1 Radicals in Polynomial Rings over Perfect Fields

We recall a few well-known facts about uniform commutative algebra in polynomial rings over fields. Let $f_1(C, X), \ldots, f_n(C, X) \in \mathbb{Z}[C, X]$. Hermann's Theorem 3.2.3 shows that given a field K and $c \in K^M$, membership in the ideal

$$I(c, X) := I_K(c, X) := \big(f_1(c, X), \ldots, f_n(c, X)\big)$$

of $K[X]$ generated by the polynomials $f_1(c, X), \ldots, f_n(c, X)$ can be described by a quantifier-free condition on c, uniformly in K. More precisely, given another polynomial $g(C, X) \in \mathbb{Z}[C, X]$ there is a quantifier-free formula $\epsilon_g(C)$ in the language $\mathcal{L}_{\text{ring}} = \{0, 1, +, -, \cdot, \}$ of rings such that for each such K, c we have

$$K \models \epsilon_g(c) \quad \Longleftrightarrow \quad g(c, X) \in I(c, X).$$

There is also an integer $D \geqslant 0$ such that for each field K and $c \in K^M$, the radical $\sqrt{I(c,X)}$ of the ideal $I(c,X)$ of $K[X]$ is generated by polynomials of degree at most D; moreover, given $f(C,X) \in \mathbb{Z}[C,X]$ there is some integer $E \geqslant 0$ such that for each field K and $c \in K^M$ with $f(c,X) \in \sqrt{I(c,X)}$, we have $f(c,X)^E \in I(c,X)$. (The first fact follows from [42]; a geometric proof is due to Kleiman [45, Corollaire 6.14]. The second fact was first shown by A. Robinson [63, p. 127]. See also Theorem 2.10 of [25].) Hence there is some $E \in \mathbb{N}$ such that

$$I(c,X) \text{ is radical} \iff \text{for all } f \in K[X] \text{ of degree at most } D\text{: } f^E \in I(c,X) \Rightarrow f \in I(c,X).$$

All this together implies that there is a universal $\mathcal{L}_{\text{ring}}$-formula $\rho(C)$ such that for each field K and $c \in K^M$ we have

$$K \models \rho(c) \iff I(c,X) \text{ is radical.}$$

The usual model-theoretic criterion for a formula to be equivalent to a quantifier-free one combined with Corollary 5.2, (1) in [8] now implies (as pointed out in the remark following that corollary):

Lemma 5.1.1. *There is a quantifier-free $\mathcal{L}_{\text{ring}}$-formula $\rho_{\text{perf}}(C)$ such that for each perfect field K and $c \in K^M$,*

$$K \models \rho_{\text{perf}}(c) \iff I(c,X) \text{ is radical.}$$

As a consequence, we obtain:

Corollary 5.1.2. *Let $\vec{g} = \big(g_1(C,X), \ldots, g_m(C,X)\big)$ be an m-tuple of polynomials from $\mathbb{Z}[C,X]$. Then there is a quantifier-free $\mathcal{L}_{\text{ring}}$-formula $\varphi_{\vec{g}}(C)$ such that for all perfect fields K and $c \in K^M$ we have*

$$K \models \varphi_{\vec{g}}(c) \iff \sqrt{I(c,X)} = \big(g_1(c,X), \ldots, g_m(c,X)\big).$$

Proof. Take $E \in \mathbb{N}$ such that for each field K, $c \in K^M$, and $j \in \{1, \ldots, m\}$ with $g_j(c,X) \in \sqrt{I(c,X)}$, we have $g_j(c,X)^E \in I(c,X)$. Next take a quantifier-free $\mathcal{L}_{\text{ring}}$-formula $\varphi_{\vec{g}}(C)$ such

that for all perfect fields K and $c \in K^M$ we have

$$K \models \varphi_{\vec{g}}(c) \quad \Longleftrightarrow \quad \begin{cases} J(c,X) := \big(g_1(c,X), \ldots, g_m(c,X)\big) \text{ is radical,} \\ f_i(c,X) \in J(c,X) \text{ for } i = 1, \ldots, n, \text{ and} \\ g_j(c,X)^E \in I(c,X) \text{ for } j = 1, \ldots, m. \end{cases}$$

Now use that if I and J are ideals in a ring, then $\sqrt{I} = J$ iff J is radical and $I \subseteq J \subseteq \sqrt{I}$. $\square$

For each finite tuple $\vec{g}$ of polynomials in $\mathbb{Z}[C,X]$ we now choose a quantifier-free $\mathcal{L}_{\text{ring}}$-formula $\varphi_{\vec{g}}(C)$ as in the corollary. Next we focus on the uniform computation of generators for $\sqrt{I(c,X)}$, for perfect fields K and $c \in K^M$. First the case of characteristic zero:

Proposition 5.1.3. *There is a finite family $\{\vec{g}_i\}_{i \in I}$ of m-tuples*

$$\vec{g}_i = \big(g_{i1}(C,X), \ldots, g_{im}(C,X)\big)$$

of polynomials from $\mathbb{Z}[C,X]$ (for some m), such that for each field K of characteristic zero we have $K \models \bigvee_{i \in I} \varphi_{\vec{g}_i}$, and if $c \in K^M$ and $i \in I$ satisfy $K \models \varphi_{\vec{g}_i}(c)$, then the ideal $\sqrt{I(c,X)}$ of $K[X]$ is generated by the polynomials $g_{i1}(c,X), \ldots, g_{im}(c,X)$.

Proof. Let K be a field of characteristic zero and $c \in K^M$ be a tuple of parameters, and let us consider the ideal $I_{\mathbb{Q}(c)}(c,X)$ of $\mathbb{Q}(c)[X]$ generated by the polynomials $f_1(c,X), \ldots, f_n(c,X)$ (with coefficients in $\mathbb{Z}[c] \subseteq \mathbb{Q}(c)$). After clearing denominators, we obtain a tuple $\vec{g} = \big(g_1(C,X), \ldots, g_m(C,X)\big)$ of polynomials from $\mathbb{Z}[C,X]$ (for some m) such that the radical of $I_{\mathbb{Q}(c)}(c,X)$ is generated by the $g_j(c,X)$. Since the field $\mathbb{Q}(c)$ is perfect, the polynomials $g_j(c,X)$ then also generate the radical of the ideal $I(c,X) = I_K(c,X)$ of $K[X]$ generated by $f_1(c,X), \ldots, f_n(c,X)$. (See, e.g., [8, Corollary 5.2].) So for each field K of characteristic zero and $c \in K^M$ there is a tuple $\vec{g}$ as above satisfying $K \models \varphi_{\vec{g}}(c)$. The claim now follows by compactness. $\square$

Next we turn to the case of positive characteristic. Fix a prime p and expand $\mathcal{L}_{\text{ring}}$ by a unary function symbol $(\,\cdot\,)^{1/p}$ to the language $\mathcal{L}_{\text{ring},p}$. We view each perfect field of characteristic p as an $\mathcal{L}_{\text{ring},p}$-structure in the natural way.

Proposition 5.1.4. *There is a finite family $\{\vec{g}_i\}_{i\in I}$ of m-tuples*

$$\vec{g}_i = \big(g_{i1}(C,X),\dots,g_{im}(C,X)\big)$$

of polynomials from $\mathbb{Z}[C,X]$ (for some m) and some $k\in\mathbb{N}$ such that for each perfect field K of characteristic p we have $K\models\bigvee_{i\in I}\varphi_{\vec{g}_i}$, and if $c\in K^M$ and $i\in I$ satisfy $K\models\varphi_{\vec{g}_i}(c)$, then the polynomials $g_{i1}(c^{1/p^k},X),\dots,g_{im}(c^{1/p^k},X)\in K[X]$ generate the ideal $\sqrt{I(c,X)}$ of $K[X]$.

Proof. Let K be a perfect field of characteristic p and $c\in K^M$. We want to argue as in the proof of the proposition above, with the subfield $\mathbb{F}_p(c)$ of K generated by the entries of the coefficient tuple c in place of $\mathbb{Q}(c)$; however, our field K may be an inseparable extension of $\mathbb{F}_p(c)$, and so we use its perfect closure $\mathbb{F}_p(c)^{1/p^\infty}$ (inside K) instead. Therefore we obtain a tuple $\vec{g}$ and some $k\in\mathbb{N}$ such that $\sqrt{I(c,X)}$ is generated by $g_1(c^{1/p^k},X),\dots,g_m(c^{1/p^k},X)$. Now use compactness again. □

We note that for finite prime fields, we may take $k=0$ and $g_{ij}\in\mathbb{Z}[X]$: since $\mathbb{F}_p^M$ is finite, a case distinction over all choices of parameters $c\in\mathbb{F}_p^M$ will do. Hence:

Corollary 5.1.5. *There exist a finite family $\{\vec{g}_i\}_{i\in I}$ of m-tuples $\vec{g}_i=(g_{i1},\dots,g_{im})$ of polynomials from $\mathbb{Z}[X]$ (for some m) and some $k\in\mathbb{N}$ such that $\mathbb{F}_p\models\bigvee_{i\in I}\varphi_{\vec{g}_i}$, and if $c\in\mathbb{F}_p^M$ and $i\in I$ satisfy $K\models\varphi_{\vec{g}_i}(c)$, then the images of $g_{i1},\dots,g_{im}$ under the natural surjection $\mathbb{Z}[X]\to\mathbb{F}_p[X]$ generate the ideal $\sqrt{I(c,X)}$ of $\mathbb{F}_p[X]$.*

We now return to the setting of restricted power series. Thus let D be a noetherian domain which is t-adically complete with respect to a fixed prime element t of D as in Section 2.1. Let $T_{D,p}$ be the $\mathcal{L}_D$-theory of valuation rings with D-structure R whose residue field $\overline{R}=R/t_RR$ is the field $\mathbb{F}_p$. We also let $f_1(C,X),\dots,f_n(C,X)\in D\langle C,X\rangle$, and as in earlier sections, given $R\models T_{D,p}$ and $c\in R^M$ we let

$$I(c,X) := \big(f_1(c,X),\dots,f_n(c,X)\big)$$

be the ideal of $R\langle X\rangle$ generated by its elements $f_1(c,X),\dots,f_n(c,X)$. We now have:

Proposition 5.1.6. *There are finite families $\{\varphi_i\}_{i\in I}$ and $\{\vec{g}_i\}_{i\in I}$, where each $\varphi_i(C)$ is a quantifier-free $\mathcal{L}_D$-formula and $\vec{g}_i = (g_{i1}, \ldots, g_{im})$ is a vector of m-tuples from $\mathbb{Z}[X]$ (for some m), such that for each $R \models T_{D,p}$ and $c \in R^M$ we have:*

(1) *$R \models \varphi_i(c)$ for some $i \in I$, and*

(2) *if $R \models \varphi_i(c)$ where $i \in I$, then in $R\langle X\rangle$ we have*

$$\sqrt{\big(I(c,X), p\big)} = \big(g_{i1}(X), \ldots, g_{im}(X),\, p\big).$$

Proof. By the results (on uniform Weierstrass) from Section 2.2 we can take some $d \in \mathbb{N}$ such that for each $R \models T_D$ and $c \in R^M$ the polynomials $\overline{f_i(c,X)} \in \overline{R}[X]$ $(i = 1, \ldots, n)$ have degree at most d. (See proof of Corollary 4.2.5.) Thus the preceding corollary yields a finite family $\{\vec{g}_i\}_{i\in I}$ of m-tuples $\vec{g}_i = (g_{i1}, \ldots, g_{im})$ of polynomials from $\mathbb{Z}[X]$ such that for all $R \models T_{D,p}$ and $c \in R^M$, we have $\overline{R} \models \bigvee_{i\in I} \varphi_{\vec{g}_i}$, and if $c \in R^M$ and $i \in I$ satisfy $\overline{R} \models \varphi_{\vec{g}_i}(\overline{c})$, then the images of $g_{i1}, \ldots, g_{im}$ under the natural morphism $R[X] \to \overline{R}[X]$ generate the radical of the ideal of $\overline{R}[X]$ generated by $\overline{f_1(c,X)}, \ldots, \overline{f_n(c,X)}$. Now for each $i \in I$ take a quantifier-free $\mathcal{L}_D$-formula $\varphi_i(C)$ such that for $R \models T_D$ and $c \in R^M$ we have $R \models \varphi_i(c) \iff \overline{R} \models \varphi_{\vec{g}_i}(\overline{c})$. Then $\{\varphi_i\}$ and $\{\vec{g}_i\}$ have the desired properties. □

5.2 Radicals in $\mathbb{Q}_p\langle X\rangle$

To determine generators for the radical $\sqrt{I}$ of an ideal I of $\mathbb{Q}_p\langle X\rangle$, we follow a "divide-and-conquer" strategy for computing radicals in polynomial rings over fields indicated in [35]. This is based on the following elementary observation:

Lemma 5.2.1. *Let A be a ring, I be an ideal of A, and $a \in A$ such that $(I : a) = (I : a^2)$. Then $I = (I : a) \cap (I, a)$ and hence $\sqrt{I} = \sqrt{(I : a)} \cap \sqrt{(I, a)}$.*

Proof. Let $f \in (I : a) \cap (I, a)$, so $af \in I$ and $f = g + ah$ $(g \in I,\ h \in A)$. Then $a^2h = af - ag \in I$, so $h \in (I : a^2) = (I : a)$ and thus $f \in I$ as required. □

Let now I be an ideal of $\mathbb{Q}_p\langle X\rangle$, specified by finitely many generating elements. We first use Noether Normalization to obtain some $d \leqslant N$ and a *finite* ring embedding

$$A \;:=\; \mathbb{Q}_p\langle X_1, \ldots, X_d\rangle \;\to\; \mathbb{Q}_p\langle X\rangle/I \;\cong\; A[Y]/J$$

where $Y = (Y_1, \ldots, Y_{N-d})$ is a tuple of indeterminates and J is an ideal of the polynomial ring $A[Y]$ which contains a Weierstrass sequence over A; so it is enough to be able to compute generators for the radical $\sqrt{J}$ of J. To do so we construct some nonzero $a \in A$ such that

$$JK[Y] \cap A[Y] = (J : a) \qquad \text{where } K = \mathrm{Frac}(A).$$

Then by the lemma above

$$\sqrt{J} = \sqrt{(J : a)} \cap \sqrt{(J, a)}.$$

Generators for the radical $\sqrt{JK[Y]}$ of the ideal $JK[Y]$ of the polynomial ring $K[Y]$ over the perfect field K can be explicitly computed, as discussed in Section 5.1 above. From these generators we then obtain generators for $\sqrt{JK[Y]} \cap A[Y] = \sqrt{(J : a)}$. The ideal (J, a) of $A[Y]$ has smaller dimension than J; this allows us to compute generators for $\sqrt{(J, a)}$ by an appeal to induction on dimension. It now remains to compute generators for the intersection ideal $\sqrt{(J : a)} \cap \sqrt{(J, a)}$.

We now make these considerations uniform in the coefficients of given generators for the ideal I; the required subroutines have already been developed in the previous sections, and it only remains to put everything together. We let D be as in Section 2.1, and we let $f_1(C, X), \ldots, f_m(C, X) \in D\langle C, X\rangle$. Given $R \models T_D$ and $c \in R^M$ we let

$$I(c, X) := \big(f_1(c, X), \ldots, f_m(c, X)\big)$$

be the ideal of $R\langle X\rangle$ generated by $f_1(c, X), \ldots, f_m(c, X)$. In the rest of this section we let R range over models of the $\mathcal{L}_D$-theory $T_{D,0}$ of valuation rings with D-structure R such that $F = \mathrm{Frac}(R)$ has characteristic zero, and c over R^M. "Formula" will mean "$\mathcal{L}_D^{\mathrm{d}}$-formula" and "term" will mean "$\mathcal{L}_D^{\mathrm{d}}$-term."

Theorem 5.2.2. *There are a covering family* $\big\{\mathrm{rad}^{(\lambda)}(C)\big\}_{\lambda\in\Lambda}$ *of quantifier-free formulas as well as for each* $\lambda \in \Lambda$ *terms*

$$g_1^{(\lambda)}(C, X), \ldots, g_n^{(\lambda)}(C, X) \qquad (\textit{for some } n)$$

in which the function symbol d *is not applied to subterms involving the* X*-variables, such that if* $R \models \mathrm{rad}^{(\lambda)}(c)$*, then*

$$\sqrt{I(c,X)F\langle X\rangle} = \big(g_1^{(\lambda)}(c,X),\dots,g_n^{(\lambda)}(c,X)\big). \tag{5.1}$$

To prove this theorem, thanks to Corollary 4.2.2, it is enough to show, for $d = 0,\dots,N$, the existence of a covering family $\big\{\mathrm{rad}_d^{(\lambda)}\big\}$ of quantifier-free formulas as well as terms $g_j^{(\lambda)}$ as in the statement of Theorem 5.2.2 such that (5.1) holds provided $R \models \mathrm{rad}_d^{(\lambda)}(c)$ and $\dim I(c,X)F\langle X\rangle = d$. We show this by induction on d: but first some general reductions based on Proposition 4.2.1 (uniform Noether Normalization) that are valid for each d. With $\mathcal{N}$ as in this proposition, we may focus on a particular member of $\mathcal{N}$. In other words, after replacing $f_1,\dots,f_m$ by their images under a suitable polynomial automorphism of $D\langle C,X\rangle$ and enlarging this list and the tuple C of parametric variables if necessary, we can assume that the f_i already contain a Weierstrass sequence over $D\langle C,X_1,\dots,X_d\rangle$. For notational convenience relabel $(X_{d+1},\dots,X_N)$ as $Y = (Y_1,\dots,Y_{N-d})$. By Lemma 4.1.6 we can moreover assume that all f_i are polynomials from $D\langle C,X_1,\dots,X_d\rangle[Y]$. Thus for all R and c, letting $A := F\langle X_1,\dots,X_d\rangle$, the restricted power series $f_i(c,X)$ are elements of the subring $A[Y]$ of $F\langle X\rangle$. According to Corollary 4.2.7, we now take a covering family $\big\{\varphi^{(\lambda)}(C)\big\}$ of quantifier-free formulas and for each λ an element $a^{(\lambda)}$ of $D\langle C,X_1,\dots,X_d\rangle$ such that if $R \models \varphi^{(\lambda)}(c)$, with

$$A = F\langle X_1,\dots,X_d\rangle, \qquad K = \mathrm{Frac}(A), \qquad a = a^{(\lambda)}(c,X_1,\dots,X_d)$$

and J denoting the ideal of $A[Y]$ generated by the $f_i(c,X)$, we have

$$JK[Y] \cap A[Y] = (J : a).$$

Let $I = I(c,X)F\langle X\rangle$; then by Lemmas 4.1.12, 4.1.13, and 5.2.1, we have

$$\sqrt{I} = \sqrt{(I:a)} \cap \sqrt{(I,a)} \quad \text{where} \quad \sqrt{(I:a)} = \sqrt{(J:a)}F\langle X\rangle. \tag{5.2}$$

Refining our covering family suitably, by Proposition 5.1.3 we can also assume that for each λ we have

$$h_1^{(\lambda)}(C,X),\dots,h_k^{(\lambda)}(C,X) \in D\langle C,X_1,\dots,X_d\rangle[Y] \qquad (\text{for some } k \in \mathbb{N})$$

such that if $R \models \varphi^{(\lambda)}(c)$, then with J, K as above,

$$\sqrt{JK[Y]} = \big(h_1^{(\lambda)}(c, X), \ldots, h_k^{(\lambda)}(c, X)\big).$$

Further refining $\{\varphi^{(\lambda)}\}$, by Corollaries 4.2.7 and 4.2.8 we can also assume that for each λ we have polynomials

$$\widetilde{h}_1^{(\lambda)}(V, X), \ldots, \widetilde{h}_k^{(\lambda)}(V, X) \in D\langle V, X_1, \ldots, X_d\rangle[Y],$$

where $V = (V_1, \ldots, V_L)$ is a tuple of new distinct indeterminates ($L \in \mathbb{N}$), and an L-tuple τ of terms in C, such that if $R \models \varphi^{(\lambda)}(c)$, then with A, J, K as before,

$$\sqrt{(J : a)} = \sqrt{JK[Y]} \cap A[Y] = \Big(\widetilde{h}_1^{(\lambda)}\big(\tau(c), X\big), \ldots, \widetilde{h}_k^{(\lambda)}\big(\tau(c), X\big)\Big).$$

By Corollary 4.1.11, for $R \models \varphi^{(\lambda)}(c)$ such that $\dim I = d$, we have $\dim(I, a) < d$ for $a := a^{(\lambda)}(c, X_1, \ldots, X_d)$. In order to finish the proof of Theorem 5.2.2, it remains to appeal to the inductive hypothesis applied with $f_1, \ldots, f_m, a^{(\lambda)}$ in place of $f_1, \ldots, f_m$, as well to Corollary 3.3.13 and (5.2). □

We note an immediate consequence of Theorem 5.2.2, obtained using Corollary 3.3.12:

Corollary 5.2.3. *There is a quantifier-free formula* $\mathrm{rad}(C)$ *such that for all* R *and* c*, we have* $R \models \mathrm{rad}(c)$ *iff the ideal* $I(c, X)F\langle X\rangle$ *is radical.*

In particular, if $R \subseteq R^*$ is an extension of models of T_D and $F^* = \mathrm{Frac}(R^*)$, then the ideal $I(c, X)F\langle X\rangle$ of $F\langle X\rangle$ is radical iff the ideal $I(c, X)F^*\langle X\rangle$ of $F^*\langle X\rangle$ is. The uniformity with respect to R inherent to Theorem 5.2.2 and model-theoretic compactness also easily yield an analogue of A. Robinsons result ([63, p. 127] or [25, (2.10)(ii)]) for $F\langle X\rangle$:

Corollary 5.2.4. *There is some integer* $E \geqslant 1$ *such that for all* R*,* c *and* $f \in F\langle X\rangle$*:*

$$f \in \sqrt{I(c, X)F\langle X\rangle} \quad \Longrightarrow \quad f^E \in I(c, X)F\langle X\rangle.$$

Proof. Take $\mathrm{rad}^{(\lambda)}$ and $g_i^{(\lambda)}$ as in Theorem 5.2.2. By compactness we obtain an integer $D \geqslant 1$ such that for all R and c with $R \models \mathrm{rad}^{(\lambda)}(c)$ we have $g_i^{(\lambda)}(c, X)^D \in I(c, X)F\langle X\rangle$. Recall the

familiar multinomial formula: for $e \in \mathbb{N}$ we have

$$(Y_1 + \cdots + Y_n)^e = \sum_{e_1+\cdots+e_n=e} \binom{e}{e_1, \ldots, e_n} Y_1^{e_1} \cdots Y_n^{e_n},$$

where $Y_1, \ldots, Y_n$ are distinct indeterminates over $\mathbb{Z}$ and $\binom{e}{e_1,\ldots,e_n} = \frac{e!}{e_1! \cdots e_n!}$ for all $(e_1, \ldots, e_n) \in \mathbb{N}^n$ with $e_1 + \cdots + e_n = e$. Hence $E := nD$ has the required property. □

5.3 Radical ideals in $\mathbb{Z}_p\langle X \rangle$

We now turn our attention to analogous questions for ideals of $\mathbb{Z}_p\langle X \rangle$. We should not expect a result like Theorem 5.2.2, which holds uniformly for all models of the elementary theory $T_{D,0}$: although a non-noetherian p-adically closed valuation ring may have many radical ideals, only few of them are definable (Corollary 4.3.4). So the best we can hope for is to define the property of being a radical ideal, and this is what we show in the next proposition. We let $f_1(C, X), \ldots, f_m(C, X) \in \mathbb{Z}_p\langle C, X \rangle$, and given $R \models T_{\mathbb{Z}_p}$ and $c \in R^M$ we let $I(c, X)$ denote the ideal of $R\langle X \rangle$ generated by $f_1(c, X), \ldots, f_m(c, X)$.

Proposition 5.3.1. *There is an $\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$-formula $\mathrm{rad}_p(C)$ such that for all $R \models T_p$ and $c \in R^M$, we have $R \models \mathrm{rad}_p(c)$ iff the ideal $I(c, X)$ of $R\langle X \rangle$ is radical.*

The proof rests on the following criterion for an ideal of a ring to be radical.

Lemma 5.3.2. *Let A be a ring, I be an ideal of A, and $a \in A$. Then I is radical if and only if $(I : a)$ is radical and $(I : a) \cap \sqrt{(I, a)} \subseteq I$.*

Proof. Suppose I is radical. If $f \in A$ satisfies $af^2 \in I$, then $(af)^2 \in I$ and thus $af \in I$; hence $(I : a)$ is radical. By Lemma 5.2.1 we have

$$(I : a) \cap \sqrt{(I, a)} \subseteq \sqrt{(I : a)} \cap \sqrt{(I, a)} = \sqrt{I} = I.$$

This shows the forward direction; the converse also follows from Lemma 5.2.1. □

Example. Suppose $A = \mathbb{Z}_p\langle X \rangle$ where X is a single indeterminate, and

$$I = (X^2 + p)\mathbb{Z}_p\langle X \rangle = \big\{(X^2 + p)g : g \in \mathbb{Z}_p\langle X \rangle\big\}.$$

Then the ideal $I = (I : p)$ of $\mathbb{Z}_p\langle X\rangle$ is radical, but $(I, p) = (X^2, p)$ is not. Hence in the previous lemma we cannot replace the condition "$(I : a) \cap \sqrt{(I, a)} \subseteq I$" by "$(I, a)$ is radical".

Corollary 5.3.3. *Let $R \models T_p$ with fraction field F and I be a finitely generated ideal of $R\langle X\rangle$. Then I is radical if and only if*

(1) *the ideal $IF\langle X\rangle$ of $F\langle X\rangle$ is radical,*

(2) *$IF\langle X\rangle \cap R\langle X\rangle = (I : p)$, and*

(3) *$(I : p) \cap \sqrt{(I, p)} \subseteq I$.*

Proof. If the conditions (1)–(3) hold, then I is radical by Lemma 5.3.2 for $a = p$. Conversely, suppose I is radical. Then clearly (1) holds, and (2), (3) follow from Corollary 4.3.9 and Lemma 5.3.2. □

Proof of Proposition 5.3.1. First, let $\varphi_1(C) := \mathrm{rad}(C)$ be as in Corollary 5.2.3. Next, take $\psi^{(\lambda)}(C)$, $h_j^{(\lambda)}(C, C', X)$, and $\alpha(C, C')$ as in Corollary 4.3.8, and let $\epsilon_j^{(\lambda)}(C, C') := \epsilon_{p\, h_j^{(\lambda)}}(C, C')$ be as explained after Corollary 3.3.9 applied to $g = p\, h_j^{(\lambda)}$. Set

$$\varphi_2(C) := \bigvee_\lambda \left(\psi^{(\lambda)}(C) \wedge \forall C' \left(\alpha(C, C') \to \bigwedge_j \epsilon_j^{(\lambda)}(C, C') \right) \right).$$

Then for all $R \models T_p$ and $c \in R^M$ we have

$$R \models \varphi_2(c) \quad \Longleftrightarrow \quad I(c, X)F\langle X\rangle \cap R\langle X\rangle = \big(I(c, X) : p\big).$$

By Corollaries 3.3.12, 3.3.13, and Proposition 5.1.6 there is a quantifier-free $\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$-formula $\varphi_3(C)$ such that for all $R \models T_p$ and $c \in R^M$,

$$R \models \varphi_3(c) \quad \Longleftrightarrow \quad \big(I(c, X) : p\big) \cap \sqrt{\big(I(c, X), p\big)} \subseteq I(c, X).$$

Then $\mathrm{rad}_p := \varphi_1 \wedge \varphi_2 \wedge \varphi_3$ has the required property, by Corollary 5.3.3. □

Combining Proposition 5.3.1 with model completeness of T_p yields:

Corollary 5.3.4. *If $R \subseteq R^*$ is an extension of models of T_p and $c \in R^M$, then the ideal $I(c, X)$ of $R\langle X\rangle$ is radical iff the ideal $I(c, X)R^*\langle X\rangle$ of $R^*\langle X\rangle$ is radical.*

Although a uniform description of the generators of the radical of an ideal of $\mathbb{Z}_p\langle X\rangle$ depending on parameters is impossible, we do have the following test for being radical:

Corollary 5.3.5. *There exist a finite family $\{f_\lambda\}_{\lambda\in\Lambda}$ of power series in $\mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new indeterminates, $L \in \mathbb{N}$, as well as some integer $E \geqslant 1$ and an $\mathcal{L}_{\mathbb{Z}_p}$-formula $\alpha(C, X)$ which for all $R \models T_p$ defines the graph of a map $c \mapsto a(c)\colon R^M \to R^L$, with the following properties, for $R \models T_p$, $c \in R^M$:*

$$I = I(c, X) \text{ is radical} \quad\Longleftrightarrow\quad \text{for all } \lambda, \text{ if } f_\lambda\big(a(c), X\big)^E \in I \text{ then } f_\lambda\big(a(c), X\big) \in I.$$

Proof. Given an integer $E \geqslant 1$, a power series $f \in \mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new indeterminates ($L \in \mathbb{N}$), and a formula $\alpha(C, V)$ which defines, in each $R \models T_p$, the graph of a map $c \mapsto a(c)\colon R^M \to R^L$, let $\rho(C) = \rho_{E,f,\alpha}(C)$ be an $\mathcal{L}_{\mathbb{Z}_p}$-formula such that for $R \models T_{\mathbb{Z}_p}$ and $c \in R^M$, with $I = I(c, X)$ we have

$$R \models \rho(c) \iff f\big(a(c), X\big)^E \notin I \text{ or } f\big(a(c), X\big) \in I.$$

(Such a formula ρ exists by Corollary 3.3.9.) Let also rad_p be as in Proposition 5.3.1. Suppose the conclusion of the corollary fails. Then by compactness we obtain some $R^* \models T_p$ and $c^* \in (R^*)^M$ such that $R^* \models \rho_{E,f,\alpha}(c^*)$ for all choices of E, f, α, yet $R^* \models \neg\,\mathrm{rad}_p(c^*)$. Let now R be the definable closure of c^* in R^*. Then R is an elementary substructure of R^*, so $R^* \models \neg\,\mathrm{rad}_p(c^*)$, hence the ideal $I(c^*, X)$ of $R^*\langle X\rangle$ is not radical. However, we also have $R \models \rho_{E,f,\alpha}(c^*)$ for all choices of E, f, and α, and this says that $I(c^*, X)$ *is* radical, a contradiction. □

Part III

Defining Primality

CHAPTER 6

Newton, Hensel, and Dedekind

In this chapter, we establish several algebraic results and methods that will be useful in our study of prime ideals. We show that for $R \models T_D$, the ring $R\langle X\rangle$ introduced in Section 2.2 is henselian with respect to its prime ideal $\mathfrak{m}_R R\langle X\rangle$ (6.1.6); this may be made uniform (6.1.7). We then use the method of Newton diagrams to compute approximate zeroes of polynomials (6.1.11), and apply it to parametrize the zeros of polynomials with bounded discriminant over $R\langle X\rangle$ where R is a model of T_p and X is a single indeterminate (6.1.15). The principle of Ax-Kochen and Eršov gives conditions for two valued fields to be elementarily equivalent (6.2.4). In the last section of this chapter we use this principle in combination with a generalization of a result of Dedekind (6.2.5) to give a bound on the discriminant of a polynomial describing an integral extension of a finitely ramified valuation ring (6.2.7), extending a classical theorem of Hensel (6.2.1); this will be used in the next chapter.

6.1 The Newton-Hensel Lemma

The p-adic integers are a henselian ring; they satisfy Hensel's Lemma, which may be proved by an application of Newton's method of finding solutions to polynomial equations. In this section we use the process of Newton diagrams towards finding roots of one-variable polynomials in broader generality: for certain *semi-valuations* on restricted power series rings over nonstandard models of T_p. This leads to a parametrization of the roots of polynomials with bounded discriminant over special classes of rings.

Throughout this section we let Y be a single indeterminate.

The discriminant

Let A be a ring. Given $P, Q \in A[Y]$, we denote by $\operatorname{res}(P, Q)$ the *resultant* of P and Q. (See [49, IV, §8].) Let now $P \in A[Y]$ be monic of degree $n \geqslant 1$. The *discriminant* of P is

$$\Delta(P) := (-1)^{n(n-1)/2} \operatorname{res}(P, P') \in A;$$

Note that $\Delta(P)$ is a linear combination of P and P':

$$\Delta(P) \in A[Y]P + A[Y]P'.$$

If P factors as $P = \prod_{i=1}^{n}(Y - b_i)$ where $b_1, \ldots, b_n \in A$, then

$$\Delta(P) = (-1)^{n(n-1)/2} \prod_{i \neq j} (b_i - b_j).$$

Hence if $A = K$ is a field, then P is separable (that is, has n distinct zeros in an algebraic closure of K) iff $\Delta(P) \neq 0$. We record some further basic properties of the discriminant to be used later.

Lemma 6.1.1. *If $Q \in A[Y]$ is another monic polynomial, then*

$$\Delta(PQ) = \Delta(P)\Delta(Q) \operatorname{res}(P, Q)^2.$$

Next let $\varphi\colon A \to B$ be a ring morphism, and extend φ to a ring morphism $A[Y] \to B[Y]$, also denoted by φ, such that $\varphi(Y) = Y$; then $\varphi(\Delta(P)) = \Delta(\varphi(P))$.

Suppose now that A is an integral domain. Then the definition of $\Delta(P)$ can be naturally extended to the case where $P \in A[Y]^{\neq}$ is not necessarily monic: Suppose

$$P = a_0 Y^n + a_1 Y^{n-1} + \cdots + a_n \in A[Y] \qquad (a_0, \ldots, a_n \in A,\ a_0 \neq 0).$$

Then $\operatorname{res}(P, P')$ is divisible by a_0 [49, IV, Proposition 8.5], and one sets

$$\Delta(P) := (-1)^{n(n-1)/2} \operatorname{res}(P, P')/a_0.$$

If $P = a_0 \prod_{i=1}^{n}(Y - b_i)$ where $b_1, \ldots, b_n \in A$, then

$$\Delta(P) = (-1)^{n(n-1)/2} a_0^{2(n-1)} \prod_{i \neq j} (b_i - b_j).$$

This implies the following well-known transformation formulas for $\Delta(P)$:

Lemma 6.1.2. *Let $a, b \in A$ be nonzero. Then*

$$\Delta\big(aP(Y)\big) = a^{2(n-1)}\Delta\big(P(Y)\big), \qquad \Delta\big(P(bY)\big) = b^{n(n-1)}\Delta\big(P(Y)\big).$$

Let

$$\widetilde{P}(Y) := a_0^{n-1}P(a_0^{-1}Y) = Y^n + \sum_{i=0}^{n-1} a_{n-i}a_0^{n-1-i}Y^i \in A[Y].$$

An element y of an integral domain extending A is a zero of P iff $a_0 y$ is a zero of $\widetilde{P}$, and $\Delta(\widetilde{P}) = a_0^{(n-1)(n-2)}\Delta(P)$.

Henselian pairs

We now consider pairs $(A, \mathfrak{m})$ where A is a ring and $\mathfrak{m}$ is a proper ideal of A (i.e., $1 \notin \mathfrak{m}$). We set $\overline{A} := A/\mathfrak{m}$, and we extend the residue morphism $a \mapsto \overline{a} := a + \mathfrak{m}\colon A \to \overline{A}$ to a ring morphism $P \mapsto \overline{P}\colon A[Y] \to \overline{A}[Y]$ such that $\overline{Y} = Y$. A polynomial $P \in A[Y]$ such that $\overline{P} = 1 + Y$ is said to be **henselian** in $(A, \mathfrak{m})$. Note that if $P \in A[Y]$ is henselian in $(A, \mathfrak{m})$ then $\overline{P'} = 1$, and if $a \in A$ is a zero of P then $a \equiv -1 \bmod \mathfrak{m}$. Moreover:

Lemma 6.1.3. *Suppose A is an integral domain, and let $P \in A[Y]$ be henselian in $(A, \mathfrak{m})$. Then P has at most one zero in A.*

Proof. Let $a, b \in A$ be zeros of P; then $b - a \in \mathfrak{m}$. Write $P(Y) = Q(Y) \cdot (Y - a)$ where $Q \in A[Y]$; then $0 = P(b) = Q(b) \cdot (b - a)$, so it is enough to show $Q(b) \neq 0$. Now $P'(Y) = Q'(Y) \cdot (Y - a) + Q(Y)$ yields $P'(b) = Q'(b) \cdot (b - a) + Q(b)$ and so $\overline{Q(b)} = \overline{P'(b)} = 1$, hence $Q(b) \neq 0$ as required. □

Remark. We have

$$\mathfrak{m} \subseteq \operatorname{rad}(A) \quad \iff \quad 1 + \mathfrak{m} \subseteq A^\times \quad \iff \quad A^\times = \big\{a \in A : \overline{a} \in \overline{A}^\times\big\}.$$

In particular, the previous lemma goes through if instead of assuming that A is an integral domain we assume that $\mathfrak{m} \subseteq \operatorname{rad}(A)$.

We say that $(A, \mathfrak{m})$ is **henselian**, or that the ring A is **henselian with respect to** $\mathfrak{m}$, if every henselian polynomial in $(A, \mathfrak{m})$ has a zero in A. If A is complete and separated in its

$\mathfrak{m}$-adic topology (that is, the natural morphism $A \to \varprojlim A/\mathfrak{m}^n$ is an isomorphism), then A is henselian with respect to $\mathfrak{m}$ (Hensel's Lemma; see, e.g., [22, (2.9)]). A valued field with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{m}$ of $\mathcal{O}$ is henselian if (by definition) the pair $(\mathcal{O}, \mathfrak{m})$ is henselian.

Lemma 6.1.4. *The pair $(A, \mathfrak{m})$ is henselian if and only if*

(1) $1 + \mathfrak{m} \subseteq A^\times$, *and*

(2) *for each $P \in A[Y]$, $a \in A$ and $h \in \mathfrak{m}$ such that $P(a) = hP'(a)^2$, there is some $z \in A$ such that $P(z) = 0$ and $z \equiv a \bmod P'(a)hA$.*

Proof. Suppose $(A, \mathfrak{m})$ is henselian, and let $a \in \mathfrak{m}$; then the polynomial $(1+a)Y + 1 \in A[Y]$ is henselian in $(A, \mathfrak{m})$ and hence has a zero in A, showing that $1 + a \in A^\times$. Let $P \in A[Y]$, $a \in A$, $h \in \mathfrak{m}$ such that $P(a) = hP'(a)^2$. By Taylor expansion write

$$\begin{aligned} P(a+Y) &= P(a) + P'(a)Y + (\text{terms in } Y^n \text{ for } n \geqslant 2) \\ &= hP'(a)^2 + P'(a)Y + (\text{terms in } Y^n \text{ for } n \geqslant 2). \end{aligned}$$

Now substitute $hP'(a)Y$ for Y:

$$P\big(a + hP'(a)Y\big) = hP'(a)^2 Q(Y)$$

where $Q(Y) \in A[Y]$ is henselian in $(A, \mathfrak{m})$, hence has a zero $y \in A$. Then $z := a + hP'(a)y$ is a zero of P with $z \equiv a \bmod P'(a)hA$. This shows that if $(A, \mathfrak{m})$ is henselian, then (1) and (2) hold. Conversely, suppose (1), (2) hold, and let $P \in A[Y]$ be henselian in $(A, \mathfrak{m})$. Then with $a := -1$ we have $P(a) \in \mathfrak{m}$ and $P'(a) \in 1 + \mathfrak{m} \subseteq A^\times$, hence $P(a) = hP'(a)^2$ with $h \in \mathfrak{m}$, so P has a zero in A. □

Remark. If A is an integral domain and P, a, h are as in part (2) of the lemma, then there is at most one $z \in A$ such that $P(z) = 0$ and $z \equiv a \bmod P'(a)hA$.

We refer to [16, 37, 38] for further characterizations of henselian pairs.

Lemma 6.1.5. *Suppose $1 + \mathfrak{m} \subseteq A^\times$, and let $P \in A[Y]$ and $a \in A$, $h \in \mathfrak{m}$ such that $P(a) = \Delta(P)^2 h$. Then $P'(a)$ divides $\Delta(P)$ in A.*

Proof. Take $F, G \in A[Y]$ with $\Delta(P) = FP + GP'$. Then

$$\Delta(P) = F(a)P(a) + G(a)P'(a) = \Delta(P)^2 f + G(a)P'(a) \quad \text{where } f := F(a)h \in \mathfrak{m},$$

and hence

$$G(a)P'(a) = \Delta(P)\big(1 - \Delta(P)f\big)$$

where $1 - \Delta(P)f$ is a unit in A, thus $P'(a)|\Delta(P)$. □

The Newton-Hensel Lemma for $R\langle X\rangle$

Let R be a model of T_D.

Lemma 6.1.6. *The pair $\big(R\langle X\rangle, t_R R\langle X\rangle\big)$ is henselian.*

Proof. Let $P(X, Y) \in R\langle X\rangle[Y]$ be henselian; we need to find some $y \in R\langle X\rangle$ such that $P(X, y) = 0$. Our assumption implies that P is regular in Y of degree 1, so by Weierstrass Preparation in $R\langle X, Y\rangle$ (Corollary 2.3.5) there is a unit u of $R\langle X, Y\rangle$ and a monic polynomial $w \in R\langle X\rangle[Y]$ of degree 1 such that $P = w \cdot u$. Now $w = Y - y$ where $y \in R\langle X\rangle$, and y has the required property. □

Remark. We note in passing that as a consequence of the previous lemma and [54], the fraction field of the integral domain $R\langle X\rangle$ is large. (A field K is said to be *large* if it is existentially closed in the Laurent series field $K(\!(t)\!)$; see [55]).

Using compactness we obtain a uniform variant of Lemma 6.1.6. For this, let $P \in D\langle C, X\rangle[Y]$ and $a \in D\langle C, X\rangle$. Below $P'(C, X, Y) \in D\langle C, X\rangle[Y]$ denotes the derivative of P with respect to Y. Note that for $R \models T_D$, $c \in R^M$ we have $\Delta\big(P(C, X, Y)\big)(c, X) = \Delta\big(P(c, X, Y)\big)$.

Corollary 6.1.7. *There exist a finite family $\{y_i\}_{i\in I}$ of elements of $D\langle V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new indeterminates (for some $L \in \mathbb{N}$), and an L-tuple v of $\mathcal{L}_D^{\mathrm{d}}$-terms in C, such that if $R \models T_D$, $c \in R^M$ and*

$$P\big(c, X, a(c, X)\big) \equiv 0 \mod \Delta\big(P(c, X, Y)\big)^2 t_R, \tag{6.1}$$

then for some $i \in I$ we have

$$P\big(c, X, y_i\big(v(c), X\big)\big) = 0$$

and

$$y_i\big(v(c), X\big) \equiv a(c, X) \mod P'\big(c, X, a(c, X)\big)t_R.$$

Proof. Suppose not. Then compactness and Corollary 3.3.9 yield $R \models T_D$ and $c \in R^M$ such that (6.1) holds, but with R_0 denoting the $\mathcal{L}_D^{\mathrm{d}}$-substructure of R generated by c, there is no $y \in R_0\langle X\rangle$ such that $P(c, X, y) = 0$ and $y \equiv a(c, X) \bmod P'\big(c, X, a(c, X)\big)t_R$. This contradicts the henselianity of $\big(R_0\langle X\rangle, t_R R_0\langle X\rangle\big)$, by Lemmas 6.1.4 and 6.1.5. □

Newton diagrams

In this subsection we develop the rudiments of a Newton diagram process for solving polynomial equations over integral domains equipped with a semi-valuation, used in the next subsection. For this we fix an integral domain A, and we let a, b, y, z range over A. We let p be a prime element of A. Given $a \in p^d A \setminus p^{d+1}A$ we set $v_p(a) := d$, and for $a \in p^\infty A := \bigcap_{d\in\mathbb{N}} p^d A$ we set $v_p(a) := \infty > \mathbb{N}$. We declare $\infty + d = d + \infty = \infty$ for $d \in \mathbb{N} \cup \{\infty\}$. The map $v = v_p \colon A \to \mathbb{N} \cup \{\infty\}$ is a semi-valuation on A, that is,

(S1) $v(0) = \infty$,

(S2) $v(ab) = va + vb$,

(S3) $v(a + b) \geqslant \min\{va, vb\}$.

Here (S2), (S3) imply as usual that $v(a + b) = \min\{va, vb\}$ if $va \neq vb$. We say that a is **finite** if $va < \infty$ (equivalently, $a \notin p^\infty A$). We set $\overline{A} := A/pA$, with residue morphism $a \mapsto \overline{a} \colon A \to \overline{A}$. (Below we will apply this to $A = R\langle X\rangle$ where $R \models T_p$, so $\overline{A} \cong \mathbb{F}_p[X]$.) We define $y \sim z :\Longleftrightarrow v(y - z) > vy$. If $y \sim z$ then $vy = vz < \infty$, and $\sim$ is an equivalence relation on the set of finite elements of A.

We also fix a polynomial

$$P = P_0 + P_1 Y + \cdots + P_n Y^n \qquad (P_0, \ldots, P_n \in A,\ P_n \neq 0)$$

over A. Let $v(P) := \min_i v(P_i)$. We also call P finite if $v(P) < \infty$, that is, if $P_i \notin p^\infty A$ for some i. In this case, with $d = v(P)$ we have $p^{-d}P \in A[Y]$ and the polynomial

$$D_P := \sum_i \overline{P_i/p^d}\, Y^i \in \overline{A}[Y]$$

is nonzero. Note that if a and P are finite then so is

$$P_{\times a} := P(aY) = \sum_i P_i a^i\, Y^i, \text{ hence}$$
$$D_{P_{\times a}} = \sum_i \overline{P_i a^i/p^e}\, Y^i \qquad \text{where } e = v(P_{\times a}).$$

Moreover, if P is finite, then so is

$$P_{+a} := P(a+Y) = \sum_i \left(\sum_{j \geqslant i} \binom{j}{i} P_j a^{j-i} \right) Y^i$$

with $v(P_{+a}) = v(P)$: to see this note that the displayed formula for the coefficients of $P(a+Y)$ implies $v(P_{+a}) \geqslant v(P)$, and since $P = (P_{+a})_{+b}$ with $b := -a$ we also obtain $v(P_{+a}) \leqslant v(P)$.

Definition 6.1.8. We call y an **approximate zero** of P if

$$v\big(P(y)\big) > \min_i v(P_i y^i) \qquad \text{(in particular } n \geqslant 1 \text{ and } P, y \text{ are finite).}$$

In the rest of this section P is assumed to be finite. Note that then y is an approximate zero of P iff y is finite and $D_{P_{\times a}}(\overline{y/a}) = 0$ where $a = p^d$, $d = vy$. In this case the polynomial $D_{P_{\times a}} \in \overline{A}[Y]$ is not homogeneous (since $\overline{y/a} \neq 0$), hence there are at least two $i \in \{0, \dots, n\}$ such that $v(P_i y^i) = \min_j v(P_j y^j)$. If y is an approximate zero of P and $y \sim z$, then z is an approximate zero of P. If $P(y) = 0$ and y is finite then y is an approximate zero of P.

Lemma 6.1.9. *Let y be finite such that $v\big(P(y)\big) > v(P) + n\, vy$. Then y is an approximate zero of P.*

Proof. Take $i \in \{0, \dots, n\}$ such that $v(P_i) = v(P)$. Then $v(P_i y^i) = v(P) + i\, vy \leqslant v(P) + n\, vy < v\big(P(y)\big)$. □

In the plane given by $\mathbb{Z} \times \mathbb{Q}$, for $\beta, \delta \in \mathbb{Q}$ we define the line $L_\beta = \delta$ to be the set

$$\big\{(i, \alpha) \in \mathbb{Z} \times \mathbb{Q} : \alpha + i\beta = \delta\big\}.$$

Given any two points $(i_1, \alpha_1), (i_2, \alpha_2) \in \mathbb{Z} \times \mathbb{Q}$, with $i_1 \neq i_2$, there is exactly one line which contains both points: $L_\beta = \delta$, for $\beta = -\frac{\alpha_2 - \alpha_1}{i_2 - i_1}$, $\delta = \alpha_1 + i_1\beta$. Call β the antislope of this line, which has geometric slope $-\beta$ in the $\mathbb{Z} \times \mathbb{Q}$ plane. Now, define the **Newton diagram** of P to be the finite, nonempty set

$$\mathcal{N}(P) = \big\{\big(i, v(P_i)\big) : i = 0, \ldots, n,\ P_i \text{ finite}\big\} \subseteq \mathbb{Z} \times \mathbb{N}.$$

Connect points in the Newton diagram by drawing edges: lines as above, containing at least two points of $\mathcal{N}(P)$, such that all points of $\mathcal{N}(P)$ lie on or above the line. Define the antislopes of $\mathcal{N}(P)$ to be the antislopes of all its edges. If y is an approximate zero of P, then $\mathcal{N}(P)$ has an antislope $d = vy$, and $\overline{y/p^d} \neq 0$ is a zero of the polynomial $D_{P_{\times p^d}} \in \overline{A}[Y]$. Conversely, suppose $d \in \mathbb{N}$ is an antislope of $\mathcal{N}(P)$, and $c \in \overline{A}^{\neq}$ is a zero of $D_{P_{\times p^d}}$. Then P has an approximate zero y with $vy = d$ and $\overline{y/p^d} = c$. Hence we have a bijection between equivalence classes of approximate zeros of P and pairs (d, c) where d is an antislope of $\mathcal{N}(P)$ and $c \neq 0$ is a zero of $D_{P_{\times p^d}}$. Moreover, if an edge of $\mathcal{N}(P)$ with antislope $d \in \mathbb{N}$ has left endpoint $\big(i, v(P_i)\big) \in \mathcal{N}(P)$ and right endpoint $\big(j, v(P_j)\big) \in \mathcal{N}(P)$, then the polynomial $D_{P_{\times p^d}}$ has the form $D_{P_{\times p^d}} = Y^i Q(Y)$ where Q has degree $j - i$ and $Q(0) \neq 0$. Therefore we obtain:

Lemma 6.1.10. *P has, up to equivalence, at most n approximate zeros.*

These observations lead to a crucial fact:

Proposition 6.1.11. *Let $d \in \mathbb{N}$ and $d' := v(P) + nd$. Then there are $y_1, \ldots, y_m \in A$, for some m, such that for every y with $v\big(P(y)\big) \geqslant d'$ we have $y \equiv y_i \bmod p^d A$ for some $i \in \{1, \ldots, m\}$.*

Proof. By induction on $e = 0, \ldots, d$ we show the existence of $y_1, \ldots, y_m \in A$ satisfying the conclusion of the proposition for every $y \in p^{d-e}A$ with $v\big(P(y)\big) > d'$. For $e = 0$ we may take $m = 1$, $y_1 = 0$, so suppose $e > 0$. Let $f_1, \ldots, f_k$ be all approximate zeros of P, up to equivalence, which are in $p^{d-e}A$. By inductive hypothesis let $z_1, \ldots, z_l \in A$ be such that for every $i = 1, \ldots, k$ and $z \in p^{d-e+1}A$ with $v\big(P_{+f_i}(z)\big) \geqslant v(P_{+f_i}) + nd$ we have $z \equiv z_j \bmod p^d A$ for some $j \in \{1, \ldots, l\}$. Suppose y satisfies $v\big(P(y)\big) \geqslant d'$ and $vy = d - e$. Then y is an

approximate zero of P, by Lemma 6.1.9, hence we can take some $i \in \{1, \dots, k\}$ with $y \sim f_i$ and set $z := y - f_i$. Then $v\big(P_{+f_i}(z)\big) = v\big(P(y)\big) \geqslant d' = v(P_{+f_i}) + nd$ and $vz \geqslant d - e + 1$, hence $z \equiv z_j \bmod p^d A$ and thus $y \equiv f_i + z_j \bmod p^d A$, for some $j \in \{1, \dots, l\}$. Hence $f_i + z_j$ $(i = 1, \dots, k,\ j = 1, \dots, l)$ satisfy the conditions required of $y_1, \dots, y_m$. □

Let now A^* be an integral domain extending A such that p remains a prime element of A^* and $pA^* \cap A = pA$. Then $p^d A^* \cap A = p^d A$ for each $d \in \mathbb{N}$, the p-adic semi-valuation of A^* extends that of A, and the natural inclusion $A \to A^*$ induces a ring embedding $\overline{A} = A/pA \to \overline{A^*} := A^*/pA^*$, via which we identify $\overline{A}$ as a subring of $\overline{A^*}$. Every approximate zero y of P remains an approximate zero of P when viewed as polynomial with coefficients from A^*. Moreover, if $\overline{A}$ is algebraically closed in $\overline{A^*}$, then every approximate zero of P in A^* is equivalent to an approximate zero of P in A. Hence the proof of the previous proposition also shows:

Corollary 6.1.12. *In the context of Proposition 6.1.11 we can choose $y_1, \dots, y_m$ with the following additional property: for every element y^* of an integral domain A^* extending A such that pA^* is a prime ideal of A^* with $pA^* \cap A = pA$ and $\overline{A}$ is algebraically closed in $\overline{A^*}$, if $P(y^*) \in p^{d'} A^*$ then $y^* \equiv y_i \bmod p^d A^*$ for some $i \in \{1, \dots, m\}$.*

Application to $R\langle X\rangle$

Suppose now that $R \models T_p$; the material in the previous section then applies to $A = R\langle X\rangle$ equipped with the p-adic semi-valuation. For each $d \in \mathbb{N}$, the natural ring morphism $\mathbb{Z} \to R$ induces an isomorphism $\mathbb{Z}/p^d\mathbb{Z} \to R/p^d R$. Hence by the discussion on reduction mod p^d in Section 2.3 we have:

Lemma 6.1.13. *Let $d \in \mathbb{N}$ and $f \in \mathbb{Z}_p\langle C, X\rangle$. Then there are $f_1, \dots, f_m \in \mathbb{Z}[X]$, for some m, such that for each $R \models T_p$ and $c \in R^M$ we have $f(c, X) \equiv f_i \bmod p^d R\langle X\rangle$ for some $i \in \{1, \dots, m\}$.*

Let now

$$P := P_n Y^n + P_{n-1} Y^{n-1} + \cdots + P_0 \in \mathbb{Z}_p\langle C, X\rangle[Y] \qquad (P_i \in \mathbb{Z}_p\langle C, X\rangle) \tag{6.2}$$

and fix some $d \in \mathbb{N}$.

Lemma 6.1.14. *There is a finite set $\mathcal{Z} = \mathcal{Z}_d \subseteq \mathbb{Z}[X]$ with the following property: for each model R of T_p, each $c \in R^M$ with $v\big(P(c,X,Y)\big) = 0$ and each $y \in R\langle X\rangle$ with $P(c,X,y) = 0$, we have $y \equiv z \bmod p^d R\langle X\rangle$ for some $z \in \mathcal{Z}$.*

Proof. Suppose not. Then by compactness there is a family $\{R_i\}_{i\in I}$ of models of T_p and a non-principal ultrafilter $\mathcal{U}$ on I as well as some $c^* \in (R^*)^M$, where $R^* := \prod_i R_i/\mathcal{U}$, such that $v\big(P(c^*,X,Y)\big) = 0$, and a zero $y^* \in R\langle X\rangle^* := \prod_i R_i\langle X\rangle/\mathcal{U}$ of the polynomial $P(c^*,X,Y) \in R^*\langle X\rangle[Y]$, such that $y^* \not\equiv z \bmod p^d R\langle X\rangle^*$ for each $z \in \mathbb{Z}[X]$. Here we view $R^*\langle X\rangle$ as an R^*-subalgebra of $R\langle X\rangle^*$ as described in Section 3.3. Then p is a prime element of $R\langle X\rangle^*$ with $pR\langle X\rangle^* \cap R^*\langle X\rangle = pR^*\langle X\rangle$, hence the inclusion $R^*\langle X\rangle \to R\langle X\rangle^*$ induces an embedding

$$\iota\colon R^*\langle X\rangle/pR^*\langle X\rangle \to R\langle X\rangle^*/pR\langle X\rangle^*.$$

The compositions of the natural morphisms

$$R_i\langle X\rangle \to R_i\langle X\rangle/pR_i\langle X\rangle \xrightarrow{\cong} \mathbb{F}_p[X]$$

induce a surjective morphism

$$R\langle X\rangle^* = \textstyle\prod_i R_i\langle X\rangle/\mathcal{U} \to \mathbb{F}_p[X]^* := \prod_i \mathbb{F}_p[X]/\mathcal{U}$$

whose kernel is $pR\langle X\rangle^*$, and hence an isomorphism $R\langle X\rangle^*/pR\langle X\rangle^* \xrightarrow{\cong} \mathbb{F}_p[X]^*$, and one easily checks that this isomorphism fits into a commutative diagram

$$\begin{array}{ccc} R\langle X\rangle^*/pR\langle X\rangle^* & \xrightarrow{\cong} & \mathbb{F}_p[X]^* \\ \uparrow{\scriptstyle \iota} & & \uparrow{\scriptstyle \delta} \\ R^*\langle X\rangle/pR^*\langle X\rangle & \xrightarrow{\cong} & \mathbb{F}_p[X] \end{array}$$

where δ is the diagonal embedding. Hence $R^*\langle X\rangle/pR^*\langle X\rangle$, identified with its image under ι, is algebraically closed in $R\langle X\rangle^*/pR\langle X\rangle^*$. Thus Corollary 6.1.12 applies to $A = R^*\langle X\rangle$ and $A^* = R\langle X\rangle^*$ equipped with their p-adic semi-valuations and the finite polynomial $P(c^*,X,Y) \in A[Y]$ in place of P, and so we obtain some $y \in R^*\langle X\rangle$ such that $y \equiv y^* \bmod p^d R\langle X\rangle^*$. By Lemma 6.1.13 there is some $z \in \mathbb{Z}[X]$ such that $z \equiv y \bmod p^d R^*\langle X\rangle$. Hence $y^* \equiv z \bmod p^d R\langle X\rangle^*$, a contradiction. □

Parametrizing zeros of polynomials with bounded discriminant

In this subsection we assume that $N = 1$, so $X = X_1$ is a single indeterminate. We let P be as in (6.2), and we fix a constant $\beta \in \mathbb{N}$. Our first goal is to show:

Proposition 6.1.15. *There are a finite family $\{y^{(\lambda)}\}_{\lambda\in\Lambda}$ of elements of $\mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \dots, V_L)$ is an L-tuple of new indeterminates ($L \in \mathbb{N}$), as well as an $\mathcal{L}_{\mathbb{Z}_p}$-formula $\alpha(C, V)$, satisfying the following properties: for $R \models T_p$, the formula α defines the graph of a map $c \mapsto a(c)\colon R^M \to R^L$, and if $c \in R^M$ and $y(X) \in R\langle X\rangle$ satisfy*

$$v\big(\Delta(P, c, X, Y)\big) \leqslant \beta \quad \text{and} \quad P\big(c, X, y(X)\big) = 0,$$

then $y(X) = y^{(\lambda)}\big(a(c), X\big)$ for some $\lambda \in \Lambda$.

This follows by a familiar compactness argument from the lemma below. (See also the proof of Theorems 3.3.1 and 3.3.3.) For this lemma we fix a family $\{R_i\}_{i\in I}$ of models of T_p and a non-principal ultrafilter $\mathcal{U}$ on I and we let $R\langle X\rangle^* := \prod_{i\in I} R_i\langle X\rangle/\mathcal{U}$. We also let R be a definably closed substructure of the p-adically closed valuation ring with $\mathbb{Z}_p$-structure $R^* := \prod_{i\in I} R_i/\mathcal{U}$, and we let $Q \in R\langle X\rangle[Y]$.

Lemma 6.1.16. *If $v\big(\Delta(Q)\big) \leqslant \beta$, then all zeros of Q in $R\langle X\rangle^*$ are in $R\langle X\rangle$.*

Proof. Note that $v\big(\Delta(Q)\big) \leqslant \beta$ implies $Q \neq 0$. We show the lemma by induction on $\deg_Y Q$, with the case $\deg_Y Q = 0$ being trivial. Suppose that $v\big(\Delta(Q)\big) \leqslant \beta$ and Q has a zero in $R\langle X\rangle^*$. It suffices to show that then Q has a zero $y \in R\langle X\rangle$: then $Q(Y) = Q_1(Y)\cdot(Y - y)$ in $R\langle X\rangle[Y]$ with $v\big(\Delta(Q_1)\big) \leqslant \beta$ by Lemma 6.1.1, so the inductive hypothesis applies to Q_1 in place of Q. Let $y^* \in R\langle X\rangle^*$ with $Q(y^*) = 0$. Taking $r \in R$ with $v(r) = v(Q)$ and replacing Q by $r^{-1}Q \in R\langle X\rangle[Y]$ and using Lemma 6.1.2 we may assume that $v(Q) = 0$. Let $d \in \mathbb{N}$, $u \in R\langle X\rangle$ be a unit, and $w \in R[X]$ be monic such that $\Delta(Q)^2 = p^d uw$. By Lemma 6.1.14 we can take some $y \in \mathbb{Z}[X]$ such that $y \equiv y^* \bmod p^{d+1}R\langle X\rangle^*$. We have

$$Q(y) \equiv Q(y^*) \equiv 0 \bmod p^{d+1}R\langle X\rangle^*.$$

Let $a \in R\langle X\rangle^*$ with $Q(y) = ap^{d+1}$, and note that $a \in R\langle X\rangle$. Let also $z^* \in R\langle X\rangle^*$; then by Taylor expansion in $R\langle X\rangle^*[Y]$ we have

$$Q(y + p^{d+1}z^*) = Q(y) + Q'(y)p^{d+1}z^* + \cdots + \frac{Q^{(i)}(y)}{i!}(p^{d+1}z^*)^i + \cdots .$$

and hence

$$Q(y + p^{d+1}z^*) \equiv 0 \bmod p\Delta(Q)^2 \quad \iff \quad \widehat{Q}(z^*) \equiv 0 \bmod w$$

where

$$\widehat{Q}(Z) := a + Q'(y)Z + \cdots + \frac{Q^{(i)}(y)}{i!}p^{(i-1)(d+1)}Z^i + \cdots \in R\langle X\rangle[Z].$$

Weierstrass Division by w yields an R^*-algebra isomorphism

$$R\langle X\rangle^*/wR\langle X\rangle^* \cong (R^*)^e \qquad \text{where } e := \deg w.$$

Thus there are some m and polynomials $A_i \in R[Z_0, \ldots, Z_{e-1}]$, $i = 1, \ldots, m$, such that if $z_0^*, \ldots, z_{e-1}^* \in R^*$ satisfy

$$z^* \equiv z_0^* + z_1^*X + \cdots + z_{e-1}^*X^{e-1} \mod wR\langle X\rangle^*,$$

then

$$\widehat{Q}(z^*) \equiv 0 \bmod w \quad \iff \quad A_i(z_0^*, \ldots, z_{e-1}^*) = 0 \text{ for } i = 1, \ldots, m.$$

Taking z^* so that $y^* = y + p^{d+1}z^*$ yields a solution $(z_0^*, \ldots, z_{e-1}^*) \in (R^*)^e$ of the system of polynomial equations on the right; since R is an elementary substructure of R^*, there is also $(z_0, \ldots, z_{e-1}) \in R^e$ solving this system, and then with

$$z := z_0 + z_1X + \cdots + z_{e-1}X^{e-1} \in R[X]$$

we have $Q(y + p^{d+1}z) \equiv 0 \bmod p\Delta(Q)^2$ in $R\langle X\rangle$. Now Corollary 6.1.7 implies that Q has a zero in $R\langle X\rangle$. □

We also need a more general version of the previous proposition for uniformly describing the zeros of $P(c, X, Y) \in R\langle X\rangle[Y]$ in the fraction field of $R\langle X\rangle$:

Proposition 6.1.17. *There are $\{y^{(\lambda)}\}$ and α as in Proposition 6.1.15 with the following properties: for $R \models T_p$, the formula α defines the graph of a map $c \mapsto a(c)\colon R^M \to R^L$, and if $c \in R^M$ satisfies*

$$v\big(\Delta(P, c, X, Y)\big) \leqslant \beta, \quad P_0(c, X) \neq 0, \quad v\big(P_0(c, X)\big) \leqslant v\big(P_i(c, X)\big) \text{ for all } i,$$

then for each $y(X) \in \mathrm{Frac}\big(R\langle X\rangle\big)$ with $P\big(c, X, y(X)\big) = 0$ there is some λ with

$$y(X) \cdot P_0(c, X) = y^{(\lambda)}\big(a(c), X\big).$$

Again, this follows from a lemma about $R\langle X\rangle^*$, where $R\langle X\rangle^*$, $R\langle X\rangle$, are as above and $Q = Q_0 Y^n + Q_1 Y^{n-1} + \cdots + Q_n$ where $Q_0, \ldots, Q_n \in R\langle X\rangle$.

Lemma 6.1.18. *Suppose $v(Q_0) \leqslant v(Q_i)$ for $i = 0, \ldots, n$ and $v\big(\Delta(Q)\big) \leqslant \beta$. Then all zeros of Q in $\mathrm{Frac}\big(R\langle X\rangle^*\big)$ are of the form y/Q_0 where $y \in R\langle X\rangle$.*

Proof. As in the proof of Lemma 6.1.16 we reduce to the case $v(Q_0) = 0$. Let $\widetilde{Q} \in R\langle X\rangle[Y]$ be the monic polynomial introduced after Lemma 6.1.2 with P in place of Q. Then we have $v\big(\Delta(\widetilde{Q})\big) \leqslant \beta$, and by Corollary 2.3.12, every zero of $\widetilde{Q}$ in $\mathrm{Frac}\big(R\langle X\rangle^*\big)$ lies in $R\langle X\rangle^*$. Now apply Lemma 6.1.16 to $\widetilde{Q}$ in place of Q. □

6.2 Valuation-Theoretic Preliminaries

The results of Ax-Kochen and Eršov show that, with appropriate assumptions, two valued fields are elementarily equivalent if and only if both their residue fields and value groups are elementarily equivalent. We apply this to bound the discriminants of an important class of polynomials over valuation rings. This will be used later, e.g., to parametrize zeros of these polynomials in certain general settings.

A uniform bound on the valuation of the discriminant

Let A be a Dedekind domain with fraction field K, and let L be a separable field extension of K of finite degree $n = [L : K]$. Let B be the integral closure of A in L, and let $\mathfrak{P}$ range

over all non-zero prime ideals of B. We recall the definition and some basic properties of the *different* $\mathfrak{D}_{B|A}$ of B over A (cf. [71, III, §3]). This is the inverse of the fractional ideal

$$\mathfrak{D}_{B|A}^{-1} = \big\{x \in L : \mathrm{Tr}_{L|K}(xB) \subseteq A\big\}$$

of B, where $\mathrm{Tr}_{L|K}\colon L \to K$ is the trace of the field extension $L|K$. The different of B over A is actually a non-zero ideal of B, so $\mathfrak{D}_{B|A} = \prod_{\mathfrak{P}} \mathfrak{P}^{d_{\mathfrak{P}}}$ where $d_{\mathfrak{P}} \in \mathbb{N}$, with $d_{\mathfrak{P}} = 0$ for all but finitely many $\mathfrak{P}$. In the next proposition we fix $\mathfrak{P}$ and denote by $\mathfrak{p}$ the maximal ideal $\mathfrak{P} \cap A$ of A. We identify the residue field $\boldsymbol{k}_{A_{\mathfrak{p}}} := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ of the DVR $A_{\mathfrak{p}}$ with a subfield of the residue field $\boldsymbol{k}_{B_{\mathfrak{P}}} := B_{\mathfrak{P}}/\mathfrak{P}B_{\mathfrak{P}}$ of $B_{\mathfrak{P}}$ in the natural way; then the *residue degree* $f_{\mathfrak{P}} := [\boldsymbol{k}_{B_{\mathfrak{P}}} : \boldsymbol{k}_{A_{\mathfrak{p}}}]$ of $\mathfrak{P}$ is finite. Let $v_{\mathfrak{p}}$ be the normalized discrete valuation on K with valuation ring $A_{\mathfrak{p}}$, and let $\pi \in A$ be a uniformizing element. Let also $v_{\mathfrak{P}}$ be the normalized discrete valuation on L with valuation ring $B_{\mathfrak{P}}$, and let $e_{\mathfrak{P}} := v_{\mathfrak{P}}(\pi)$ be the *ramification index* of $\mathfrak{P}$, so $v_{\mathfrak{P}}(\pi) = e_{\mathfrak{P}} \cdot v_{\mathfrak{p}}(\pi)$. The following bound, for $A = \mathbb{Z}$, was conjectured by Dedekind [18] and first shown by Hensel [41] (see also [68]):

Proposition 6.2.1. *Suppose that K has characteristic zero. Then*

$$d_{\mathfrak{P}} \leqslant e_{\mathfrak{P}} - 1 + e_{\mathfrak{P}} \cdot v_{\mathfrak{p}}(n).$$

Proof. We may replace A, B by $A_{\mathfrak{p}}$, $B_{\mathfrak{P}}$, respectively, and can thus assume that both A and B are DVRs. Set $x := 1/(n\pi) \in K$. Since B is a valuation ring, we have $xB \subseteq \mathfrak{D}_{B|A}^{-1}$ or $xB \supseteq \mathfrak{D}_{B|A}^{-1}$; but $\mathrm{Tr}_{L|K}(x) = 1/\pi \notin A$, hence the first possibility is excluded. Thus $\mathfrak{D}_{B|A}$ strictly contains the ideal $n\pi B$ of B, therefore

$$d_{\mathfrak{P}} < v_{\mathfrak{P}}(n\pi) = e_{\mathfrak{P}} \cdot v_{\mathfrak{p}}(n\pi) = e_{\mathfrak{P}} \cdot \big(v_{\mathfrak{p}}(n) + 1\big),$$

and the claim follows. □

Remark. In later sections we only need this proposition in the case where the residue field extension $\boldsymbol{k}_{B_{\mathfrak{P}}}|\boldsymbol{k}_{A_{\mathfrak{p}}}$ is separable; in this situation see also [71, III, remark (1) after Proposition 13].

See [71, I, §5] for the definition of the *norm map* $\mathrm{N}_{L|K}$, and [71, III, §3] for the *discriminant* $\mathfrak{d}_{B|A}$ of B over A. We recall that $\mathfrak{d}_{B|A} = \mathrm{N}_{L|K}(\mathfrak{D}_{B|A})$ (see [71, III, Proposition 6]). In

the rest of this subsection we assume that A is a DVR with maximal ideal $\mathfrak{p}$ and K has characteristic zero, and we let $v = v_{\mathfrak{p}}$.

Corollary 6.2.2. $v(\mathfrak{d}_{B|A}) \leqslant n - 1 + nv(n)$.

Proof. We have $\mathrm{N}_{L|K}(\mathfrak{D}_{B|A}) = \prod_{\mathfrak{P}} \mathfrak{p}^{d_{\mathfrak{P}} f_{\mathfrak{P}}}$ and hence by the proposition above:

$$v(\mathfrak{d}_{B|A}) = \sum_{\mathfrak{P}} d_{\mathfrak{P}} f_{\mathfrak{P}} \leqslant \sum_{\mathfrak{P}} \big(e_{\mathfrak{P}} - 1 + e_{\mathfrak{P}} \cdot v(n)\big) \cdot f_{\mathfrak{P}}.$$

Now use that $\sum_{\mathfrak{P}} e_{\mathfrak{P}} f_{\mathfrak{P}} \leqslant n$ (see also (6.3) below). □

Now let $y \in L$ be a primitive element of $L|K$, and let $P \in K[Y]$ be the minimum polynomial of y over K. Replacing P, y by $a^n P(a^{-1}Y)$, ay for suitable $a \in A^{\neq}$, we can assume that $P(Y) \in A[Y]$ and $y \in B$. In this case, if $B = A[y]$, then $\mathfrak{d}_{B|A} = \Delta(P)A$ (see [71, III, §6]), and hence from the previous corollary we obtain:

Corollary 6.2.3. *If $B = A[y]$, then $v\big(\Delta(P)\big) \leqslant n - 1 + nv(n)$.*

Note that if A has characteristic $(0, p)$, then $v(n) = v_p(n) \cdot v(p)$, where v_p denotes the p-adic valuation on $\mathbb{Q}$.

The Ax-Kochen-Eršov Principle

Let K be a valued field. Below we denote the valuation ring of K by $\mathcal{O}$, the value group of K by Γ, and the residue field of K by $\boldsymbol{k}$. If we want to stress the dependence on K we write $\mathcal{O}_K$, Γ_K, $\boldsymbol{k}_K$ instead of $\mathcal{O}$, Γ, $\boldsymbol{k}$, respectively. We always denote the valuation of K by $v\colon K^\times \to \Gamma$. One says that K is *finitely ramified* if the set $\{\gamma \in \Gamma : 0 < \gamma \leqslant vn\}$ is finite for all $n \geqslant 1$. If $\Gamma \neq \{0\}$, then this clearly implies that K has characteristic zero. If $\boldsymbol{k}$ has characteristic $p > 0$, then K is finitely ramified iff there are only finitely many $\gamma \in \Gamma$ with $0 < \gamma \leqslant vp$, and we define the (*absolute*) *ramification index* of K (see [46, p. 390]) to be the number of $\gamma \in \Gamma$ with $0 < \gamma \leqslant vp$. If $\boldsymbol{k}$ has characteristic zero, then K is finitely ramified, and we define the ramification index of K to be 1. If K has ramification index 1, then K is said to be *unramified*. We view a valued field as a structure in the expansion $\mathcal{L}_{\mathrm{val}}$ of the language of rings by a unary predicate symbol, interpreted as the valuation ring.

Theorem 6.2.4. *Let K, L be finitely ramified henselian valued fields of the same ramification index. Then $K \equiv L$ if and only if $\boldsymbol{k} \equiv \boldsymbol{k}_L$ and $\Gamma \equiv \Gamma_L$.*

The equicharacteristic zero case was shown independently by Ax-Kochen [13] and Eršov [32], and the general case by Eršov [33] and Ziegler [74]; the unramified case was also treated by Kochen [46].

A generalization of Dedekind's Criterion

Let A be an integral domain with fraction field K and $P \in A[Y]$ be monic of degree $n \geqslant 1$ and irreducible over K. The natural inclusions $A \subseteq A[Y] \subseteq K[Y]$ induce ring embeddings

$$A \to A[y] := A[Y]/PA[Y] \to L := K[Y]/PK[Y] \qquad (y := Y + PA[Y])$$

via which we identify A with a subring of $A[y]$ and $A[y]$ with a subring of the field L as usual. Here L is the fraction field of $A[y]$. Some ad hoc terminology: call the polynomial P **integrally closed** (over A) if $A[y]$ is integrally closed in L (that is, if $A[y]$ is the integral closure of A in L). Suppose now that K is a valued field and $A = \mathcal{O}$. We extend the residue morphism $a \mapsto \overline{a}\colon \mathcal{O} \to \boldsymbol{k}$ to a ring morphism $P \mapsto \overline{P}\colon \mathcal{O}[Y] \to \boldsymbol{k}[Y]$ such that $\overline{Y} = Y$. The next theorem describes when P is integrally closed over $\mathcal{O}$; this was shown independently by Eršov [34] and Khanduja-Kumar [44], and generalizes a well-known criterion of Dedekind [17]:

Theorem 6.2.5. *Let $Q_1, \dots, Q_m \in \mathcal{O}[Y]$ be monic and $e_1, \dots, e_m \geqslant 1$ be integers such that $\overline{Q_1}, \dots, \overline{Q_m} \in \boldsymbol{k}[Y]$ are pairwise distinct and irreducible and $\overline{P} = \overline{Q_1}^{e_1} \cdots \overline{Q_m}^{e_m}$. Set $R := P - Q_1^{e_1} \cdots Q_m^{e_m}$. Then P is integrally closed if and only if one of the following conditions holds:*

(1) *$e_1 = \cdots = e_m = 1$; or*

(2) *there is some i such that $e_i > 1$, Γ has a smallest positive element $v\pi$, and $\overline{Q_i}$ does not divide $\overline{R/\pi}$ for each i with $e_i > 1$.*

In particular, the property of P to be integrally closed is first-order expressible in its coefficients.

Polynomials with large discriminant

In this subsection K is a valued field whose value group Γ is a $\mathbb{Z}$-group, and $P \in \mathcal{O}[Y]$ is monic. As a consequence of Corollary 6.2.3 and Theorem 6.2.5, the Ax-Kochen-Eršov Principle yields:

Corollary 6.2.6. *Suppose that K is henselian and finitely ramified of characteristic $(0, p)$. If P is integrally closed, then*

$$v\big(\Delta(P)\big) \leqslant n - 1 + n \cdot v_p(n) \cdot v(p) \qquad \textit{where } n = \deg P.$$

Proof. By Corollary 6.2.3 this is clear if $\mathcal{O}$ is a DVR. Next suppose that K is henselian. Choose a complete DVR $\mathcal{O}'$ of characteristic zero with the same residue field $\boldsymbol{k}$ and the same absolute ramification index as $\mathcal{O}$. If K is unramified and $\boldsymbol{k}$ is perfect, this is the ring of Witt vectors over $\boldsymbol{k}$ (see [71, II, §5 and §6]), otherwise it's something a bit more complicated; in any case, the existence of such an $\mathcal{O}'$ was shown by Hasse-Schmidt [40] and Teichmüller [73]. Theorem 6.2.4 yields $\mathcal{O} \equiv \mathcal{O}'$, and so the claim follows from Corollary 6.2.3 and Theorem 6.2.5. □

A weaker bound holds if we drop the henselian assumption:

Proposition 6.2.7. *There is a constant $C(n, p)$ such that if K is finitely ramified of characteristic $(0, p)$ and P is integrally closed of degree n, then*

$$v\big(\Delta(P)\big) \leqslant n - 1 + C(n, p)v(p).$$

Proof. We claim that

$$C(n, p) = n \max\left\{\sum_i v_p(n_i) : n_i \geqslant 1, \sum_i n_i = n\right\}$$

has the required property. To see this let $\mathcal{O}^{\mathrm{h}}$ be the henselization of $\mathcal{O}$. Suppose P is integrally closed, and let $Q_1, \dots, Q_m, e_1, \dots, e_m, R$ be as in the previous theorem. Then by [44, Lemma 2.1] we have $P = P_1 \cdots P_m$ for distinct monic irreducible polynomials $P_1, \dots, P_m \in \mathcal{O}^{\mathrm{h}}[Y]$. Each $\overline{P_i}$ is a power of an irreducible polynomial in $\boldsymbol{k}[Y]$, by Hensel's

Lemma; hence after reordering we may assume $\overline{P_i} = \overline{Q_i}^{e_i}$ for $i = 1, \dots, m$. We claim that $P_1, \dots, P_m$ are integrally closed over $\mathcal{O}^{\mathrm{h}}$. This is clear if $e_1 = \cdots = e_m = 1$. Suppose otherwise. Then with $\pi \in \mathcal{O}$ such that $v\pi$ is the smallest positive element of Γ, we have $\overline{Q_i} \nmid \overline{R/\pi}$ for each i with $e_i > 1$. By [44, Lemma 3.2] we then also have $\overline{Q_i} \nmid \overline{R_i/\pi}$ where $R_i := P_i - Q_i^{e_i} \in \mathcal{O}^{\mathrm{h}}[Y]$. Together with the theorem this implies the claim. Now by Lemma 6.1.1 we have $\Delta(P) = u \prod_i \Delta(P_i)$ where u is a unit in $\mathcal{O}^{\mathrm{h}}$, since $\overline{P_i}$, $\overline{P_j}$ are coprime for $i \neq j$. Hence by Corollary 6.2.6,

$$v\big(\Delta(P)\big) = \sum_i v\big(\Delta(P_i)\big) \leqslant \sum_i \big(n_i - 1 + n_i v(n_i)\big) \leqslant n - 1 + C(n,p)v(p)$$

as required. □

In a similar way as Proposition 6.2.7 one shows:

Proposition 6.2.8. *If $\boldsymbol{k}$ has characteristic zero and P is integrally closed, then $v\big(\Delta(P)\big) \leqslant n - 1$ where $n = \deg P$.*

We say that our monic polynomial $P \in \mathcal{O}[Y]$ (assumed to be neither integrally closed nor even irreducible) has **large discriminant** if $v\big(\Delta(P)\big)$ satisfies the inequality in Proposition 6.2.7 if $\boldsymbol{k}$ has characteristic p, respectively Proposition 6.2.8 if $\boldsymbol{k}$ has characteristic zero. Every polynomial with large discriminant is separable, and by Lemma 6.1.1, every one of its monic factors in $\mathcal{O}[Y]$ has large discriminant itself. Also, if L is a valued field extension of K, then $P \in \mathcal{O}[Y]$ has large discriminant iff it has large discriminant when viewed as an element of $\mathcal{O}_L[Y]$.

Defectlessness and monogenicity of the integral closure

Let K be a valued field and $L|K$ be a finite field extension. Let $v_1, \dots, v_m$ be the distinct extensions of the valuation v of K to a valuation on L, with respective value groups Γ_i and residue fields $\boldsymbol{k}_i$. Then the fundamental inequality holds:

$$\sum_{i=1}^{m} e_i f_i \leqslant n, \tag{6.3}$$

where $n = [L : K]$ is the degree of the extension, $e_i = [\Gamma_{v_i} : \Gamma]$ are the respective ramification indices, and $f_i = [\boldsymbol{k}_i : \boldsymbol{k}]$ are the respective inertia degrees. One says that the extension $L|K$ is *defectless* if equality holds in (6.3), and the valued field K is said to be defectless if each finite-degree field extension of K is defectless. We recall a few basic facts about this notion. First, by [31, (18.2)], a valued field of characteristic zero is defectless if and only if its henselization is. (F.-V. Kuhlmann has generalized this to positive characteristic.) Suppose now that our valued field K is henselian. Then necessarily $m = 1$ in the above, hence a finite valued field extension $L|K$ is defectless if and only if $[L : K] = [\Gamma_L : \Gamma]\cdot[\boldsymbol{k}_L : \boldsymbol{k}]$. By a theorem of Ostrowski (see, e.g., [30, Theorem 17.2.1]), the quotient $[L : K]/\big([\Gamma_L : \Gamma] \cdot [\boldsymbol{k}_L : \boldsymbol{k}]\big)$ is always an integer, and equals 1 if $\operatorname{char} \boldsymbol{k} = 0$ (and is a power of $\operatorname{char} \boldsymbol{k}$ otherwise). In particular,

(D1) every henselian valued field of equicharacteristic zero is defectless.

It is also well-known that each finite separable extension of a discrete valued field is defectless (see, e.g., [31, (18.7)] or [30, Corollary 17.4.4]). Thus

(D2) every discrete valued field of characteristic zero is defectless.

As observed by Prestel-Roquette [58, proof of Lemma 2.9], (D1) and (D2) together with a coarsening/specialization argument quite easily imply:

Lemma 6.2.9. *Every finitely ramified valued field is defectless.*

Given a ring A, an A-algebra B is said to be **monogenic** if it is generated by a single element: $B = A[y]$ for some $y \in B$.

Proposition 6.2.10. *Suppose the value group of K is a $\mathbb{Z}$-group and its residue field is perfect and infinite. Then the integral closure of $\mathcal{O}$ in a defectless finite field extension of K is monogenic.*

This is a special case of [44, Theorem 1.2].

CHAPTER 7

Prime Ideals

In this chapter we consider primality of ideals in polynomial and power series rings. Since being prime is equivalent to being both primary and radical, it suffices to construct a formula for defining primariness, by our previous results on radicality. First, we recall a definable test for being primary (and thus prime) in polynomial rings over perfect fields (7.1.2) from [8]. We then present a set of universal axioms for valued fields of characteristic $(0, p)$ whose value group is a $\mathbb{Z}$-group and whose residue field is infinite and perfect; these axioms are strong enough to ensure analogous properties hold in substructures. Within this framework we then show that testing for primary (prime) ideals can be reduced to the uniform parametrization of zeros of polynomials with large discriminant (7.1.5). (Here the results from Section 6.2 of the previous chapter are crucial.)

We may expand the ring $\mathbb{Q}_p\langle X\rangle$ by adding p^nth roots of X for each n. The fraction field of the ensuing ring, $\mathbb{Q}_p\langle X^{1/p^\infty}\rangle$, has a perfect infinite residue field with respect to the natural (Gauss) valuation. The results of Section 7.1 thus allow us to define primary and prime ideals in rings of the form $\mathrm{Frac}\big(\mathbb{Q}_p\langle X\rangle\big)[Y]$ (7.2.11). Finally, in the last section we give conditions for primariness and primality of one-dimensional ideals of $\mathbb{Q}_p\langle X\rangle$ (7.3.1). This can be generalized to restricted power series over $\mathbb{Z}_p$ (7.3.6). All of this also works with $\mathbb{Z}_p$, $\mathbb{Q}_p$ replaced by a model R of T_p and $F = \mathrm{Frac}(R)$, respectively. Combining these results yields Theorem B from the introduction.

7.1 Prime Ideals in Polynomial Rings over Perfect Fields

In this section we work in the setting of Section 5.1. As usual $X = (X_1, \ldots, X_N)$ and $C = (C_1, \ldots, C_M)$; we also let Y be a single new indeterminate. As in that section we let $f_1(C, X), \ldots, f_m(C, X) \in \mathbb{Z}[C, X]$, and given a field K and $c \in K^M$, we let

$$I(c, X) = I_K(c, X) = \big(f_1(c, X), \ldots, f_m(c, X)\big)$$

be the ideal of $K[X]$ generated by $f_1(c, X), \ldots, f_m(c, X) \in K[X]$. We recall the definition of the language $\mathcal{L}_0$ from [8, Section 5]: This is the expansion of the language $\mathcal{L}_{\text{ring}} = \{0, 1, +, -, \cdot, \}$ of rings by n-ary relation symbols Z_n, one for each $n \geqslant 1$. Let also T_0 be the $\mathcal{L}_0$-theory of fields together with axioms, for each $n \geqslant 1$, which express that for every model K of T_0 and $b = (b_1, \ldots, b_n) \in K^n$,

$$K \models Z_n(b) \quad \iff \quad Y^n + b_1 Y^{n-1} + \cdots + b_n \in K[Y] \text{ is separable and has a zero in } K.$$

In [8, Corollary 5.5], it is shown that the property of the ideal $I(c, X)$ to be primary can be defined by a quantifier-free $\mathcal{L}_0$-formula (uniformly over all models K of T_0):

Proposition 7.1.1. *There is a quantifier-free $\mathcal{L}_0$-formula* $\text{primary}_0(C)$ *such that for all $K \models T_0$ and $c \in K^M$ we have*

$$K \models \text{primary}_0(c) \qquad \iff \qquad I(c, X) \text{ is primary.}$$

Combining this proposition with Lemma 5.1.1 yields:

Corollary 7.1.2. *There is a quantifier-free $\mathcal{L}_0$-formula* $\text{prime}_0(C)$ *such that for all $K \models T_0$ whose underlying field is perfect and all $c \in K^M$ we have*

$$K \models \text{prime}_0(c) \qquad \iff \qquad I(c, X) \text{ is prime.}$$

Let K be a valued field. In the rest of this section we use the results of Section 6.2 to describe a situation where defining the property of ideals in $K[X]$ to be primary essentially only requires us to know which monic $P \in \mathcal{O}[Y]$ with large discriminant have zeros in $\mathcal{O}$. For this, let $\mathcal{L}^*$ be the language $\mathcal{L}_{\text{val}}$ of valued fields augmented by

(1) constant symbols π and ξ, as well as

(2) unary function symbols ρ, $^{-1}$, and δ_n (one for each $n \geqslant 1$).

Fix an integer $e \geqslant 1$ and let $T^* = T^*(e,p)$ be the $\mathcal{L}^*$-theory of valued fields of characteristic $(0,p)$ whose value group is a $\mathbb{Z}$-group together with axioms which say that for every model of T^* with underlying valued field K and $\mathfrak{m}$ = maximal ideal of the valuation ring $\mathcal{O}$ of K, we have

(T1) $v\pi$ is the smallest positive element of $\Gamma = v(K^\times)$ and $vp = e\, v\pi$;

(T2) $\xi \in \mathcal{O}$ and $\xi^{p^n} \not\equiv \xi \bmod \mathfrak{m}$ for all $n \geqslant 1$ (so the ξ^{p^n} represent infinitely many distinct elements of the residue field $\boldsymbol{k} = \mathcal{O}/\mathfrak{m}$ of K);

(T3) $\rho(a)^p \in a + \mathfrak{m}$ for all $a \in \mathcal{O}$ (so the Frobenius morphism $x \mapsto x^p \colon \boldsymbol{k} \to \boldsymbol{k}$ is onto, hence $\boldsymbol{k}$ is perfect);

(T4) $a^{-1} \cdot a = 1$ for $a \in K^\times$ and $0^{-1} = 0$;

(T5) for all $n \geqslant 1$ and $a \in K^\times$, if $va \in n\Gamma$ then $va = n\, v\big(\delta_n(a)\big)$.

Note that these axioms are rather weak; for example, we do not require that ρ is an automorphism of the field K, or that δ_n restricts to an endomorphism of the multiplicative group $K^\times$ of K. However, it will be crucial that axioms (T1)–(T5) are universal, and hence any substructure of a model K of T^* is a finitely ramified valued field of characteristic $(0,p)$ with absolute ramification index e (by (T1) and (T4)) and infinite perfect residue field (thanks to conditions (T2) and (T3)), whose value group is a pure subgroup of $\Gamma = v(K^\times)$ (by (T5)) with the same smallest positive element $v\pi$, and hence is a $\mathbb{Z}$-group. We now let $\mathcal{L}_0^*$ be the expansion of $\mathcal{L}^*$ by m-ary relation symbols Z_m^* (one for each $m \geqslant 1$), and we let T_0^* be T^* together with axioms which express that for all models K of T_0^*, $m \geqslant 1$, and $a = (a_1, \dots, a_m) \in \mathcal{O}^m$ we have

$$K \models Z_m^*(a) \quad \Longleftrightarrow$$

$$Y^m + a_1 Y^{m-1} + \cdots + a_m \in \mathcal{O}[Y] \text{ has large discriminant and a zero in } \mathcal{O}.$$

Lemma 7.1.3. *Every $\mathcal{L}_{\mathrm{ring}}$-formula*

$$\varphi(x_1, \ldots, x_n) = \exists y(y^n + x_1 y^{n-1} + \cdots + x_n = 0)$$

is equivalent, in T_0^*, to a quantifier-free $\mathcal{L}_0^*$-formula.

Proof. We verify that condition (2) in [8, Lemma 5.3] holds (in the case where $\mathcal{L} = \mathcal{L}^*$). Let E_1 and E_2 be models of T_0^* with common substructure K. Let $Q \in K[Y]$ be monic of degree $n \geqslant 1$, and suppose Q has a zero in E_1; we need to show that Q has a zero in E_2. We can assume that Q is irreducible over K. Take $b \in \mathcal{O}$, $b \neq 0$, such that $bQ \in \mathcal{O}[Y]$ and set $\widetilde{Q}(Y) := b^n Q(b^{-1}Y) \in \mathcal{O}[Y]$. Then an element y in a field extension of K is a zero of Q iff *by* is a zero of $\widetilde{Q}$. Hence we can replace Q by $\widetilde{Q}$ and assume $Q \in \mathcal{O}[Y]$. Let now B be the integral closure of $\mathcal{O}$ in the field extension $L := K[Y]/QK[Y]$ of K. Then the $\mathcal{O}$-algebra B is monogenic by Lemma 6.2.9 and Proposition 6.2.10, so $B = \mathcal{O}[z]$ for some $z \in B$. Take a monic $P \in \mathcal{O}[Z]$ such that $B \cong \mathcal{O}[Z]/P\mathcal{O}[Z]$. Then P is irreducible (since the subring B of the field L is an integral domain) and integrally closed, hence has large discriminant by Corollary 6.2.6. Now our zero of Q in E_1 (actually, in $\mathcal{O}_{E_1}$) gives rise to a K-algebra morphism

$$L = K[Y]/QK[Y] \to E_1,$$

and by restriction to B we obtain an $\mathcal{O}$-algebra morphism $B \to E_1$. Hence P has a zero in E_1. So with

$$P = Y^m + a_1 Y^{m-1} + \cdots + a_m \qquad (a = (a_1, \ldots, a_m) \in \mathcal{O}^m,\ m \geqslant 1)$$

we have $E_1 \models Z_m^*(a)$ and hence $E_2 \models Z_m^*(a)$, since K is an $\mathcal{L}_0^*$-substructure of both E_1 and E_2. This means that P has a zero in E_2. Thus we have an $\mathcal{O}$-algebra morphism $B \to E_2$. By restriction to $\mathcal{O}[y] \cong \mathcal{O}[Y]/Q\mathcal{O}[Y]$ we obtain an $\mathcal{O}$-algebra morphism $\mathcal{O}[y] \to E_2$, and hence a zero of Q in E_2, as required. □

Recall that a nonzero polynomial $P(Y) \in K[Y]$ over a field K is separable if and only if it is relatively prime in $K[Y]$ to its derivative $P'(Y)$; this condition can be checked using Euclid's Algorithm for polynomials, leading to the following:

Lemma 7.1.4. *There is a quantifier-free $\mathcal{L}_{\mathrm{ring}}$-formula $\mathrm{sep}(x_1, \dots, x_n)$ such that for each field K and $a_1, \dots, a_n \in K$:*

$$K \models \mathrm{sep}(a_1, \dots, a_n) \quad \iff \quad Y^n + a_1 Y^{n-1} + \cdots + a_n \text{ is separable.}$$

Combining the previous two lemmas with Proposition 7.1.1 and its corollary yields:

Corollary 7.1.5. *There are quantifier-free $\mathcal{L}_0^*$-formulas $\mathrm{primary}_0^*$ and prime_0^* such that for all models K of T_0^* and $c \in K^M$ we have*

$$K \models \mathrm{primary}_0^*(c) \quad \iff \quad I(c, X) \text{ is primary,}$$
$$K \models \mathrm{prime}_0^*(c) \quad \iff \quad I(c, X) \text{ is prime.}$$

However, for the purposes of the next section, it is convenient to show something a bit stronger than Lemma 7.1.3. Thus, let now $\mathcal{L}_1^*$ be the expansion of $\mathcal{L}^*$ by Skolem functions for the zeros of polynomials with large discriminant, and let T_1^* be T^* augmented by defining axioms for these new function symbols. More precisely, we let $\mathcal{L}_1^* = \mathcal{L}^* \cup \{r_{mn} : 1 \leqslant n \leqslant m\}$ where the r_{mn} are new n-ary function symbols and $T_1^* = T^* \cup \{\sigma_m : m \geqslant 1\}$ where σ_m is an $\mathcal{L}_1^*$-sentence which expresses that for each model K of T_1^*,

$$K \models \sigma_m \iff \begin{cases} \text{for all } a = (a_1, \dots, a_m) \in \mathcal{O}^m \text{ and all } y \in \mathcal{O} \text{ such that } P = \\ Y^m + a_1 Y^{m-1} + \cdots + a_m \text{ has large discriminant and } P(y) = 0, \\ \text{there is some } n \in \{1, \dots, m\} \text{ with } y = r_{mn}(a). \end{cases}$$

Note that T_1^* is universally axiomatizable. We now show that zeros of polynomials in models of T_1^* are uniformly parametrized by $\mathcal{L}_1^*$-terms; in the next lemma and its corollary we fix $n \geqslant 1$.

Lemma 7.1.6. *There is a finite family $\{\tau_i^n\}_{i \in I}$ of $\mathcal{L}_1^*$-terms $\tau_i^n(x_1, \dots, x_n)$ such that for all $K \models T_1^*$ and $b = (b_1, \dots, b_n) \in K^n$, if*

$$Q(Y) = Y^n + b_1 Y^{n-1} + \cdots + b_{n-1} Y + b_n$$

has a zero in K, then $Q\big(\tau_i^n(b)\big) = 0$ for some $i \in I$.

Proof. The proof is similar to that of Lemma 7.1.3. Let $E \models T_1^*$ and $Q(Y) \in E[Y]$ be monic and have a zero in E. Let K be the $\mathcal{L}_1^*$-substructure of E generated by the coefficients of Q; by compactness it suffices to show that then Q has a zero in K. Note that K contains all zeros $y \in E$ of monic polynomials in $\mathcal{O}[Y]$ with large discriminant. We now argue in a similar way as in the proof of Lemma 7.1.3. First, we can assume that Q is irreducible and has coefficients in $\mathcal{O}$. Next, we let B be the integral closure of $\mathcal{O}$ in $L := K[Y]/QK[Y]$. The $\mathcal{O}$-algebra B being monogenic, take a monic $P \in \mathcal{O}[Z]$ such that $B \cong \mathcal{O}[Z]/P\mathcal{O}[Z]$. Then P is irreducible and integrally closed, hence has large discriminant by Corollary 6.2.6. Our zero of Q in E gives rise to a K-algebra morphism $L = K[Y]/QK[Y] \to E$, and by restriction to B we obtain an $\mathcal{O}$-algebra morphism $B \to E$. Hence P has a zero in E, and this zero lies in K. Thus we have an $\mathcal{O}$-algebra morphism $B \to K$. By restriction to $\mathcal{O}[y] \cong \mathcal{O}[Y]/Q\mathcal{O}[Y]$ we obtain an $\mathcal{O}$-algebra morphism $\mathcal{O}[y] \to K$, and hence a zero of Q in K, as required. $\square$

A standard resolvent argument yields a strengthening of the previous lemma (not used later):

Corollary 7.1.7. *There is a finite family $\{\tau_i^n\}_{i\in I}$ of $\mathcal{L}_1^*$-terms $\tau_i^n(x_1, \dots, x_n)$ such that for all $K \models T_1^*$ and $b = (b_1, \dots, b_n) \in K^n$, if*

$$Q(Y) = Y^n + b_1 Y^{n-1} + \cdots + b_{n-1}Y + b_n \in K[Y]$$

is separable, then the $\tau_i^n(b) \in K$ $(i \in I)$ contain the coefficients of all monic irreducible factors of Q in $K[Y]$.

Proof. Let $U_1, \dots, U_n, V_1, \dots, V_n, Z$ be distinct indeterminates. Let S be the set of all elementary symmetric polynomials in all finite subsets of $\{U_1, \dots, U_n\}$, and let $\sigma_1, \dots, \sigma_n \in S$ be the elementary symmetric polynomials in $U = (U_1, \dots, U_n)$:

$$Y^n + \sigma_1(U)Y^{n-1} + \cdots + \sigma_n(U) = \prod_{i=1}^{n}(Y - U_i).$$

Then for each $\sigma \in S$ there is a unique polynomial $h_\sigma \in \mathbb{Z}[V] = \mathbb{Z}[V_1, \dots, V_n]$ such that $\sigma = h_\sigma(\sigma_1, \dots, \sigma_n)$ (see [49, IV, §6]). Put

$$R(V, Z) := \prod_{\sigma\in S} \big(Z - h_\sigma(V)\big) \in \mathbb{Z}[V, Z].$$

Let K be a field and $Q(Y) = Y^n + b_1 Y^{n-1} + \cdots + b_n$ ($b_i \in K$) be separable, and let $r_1, \ldots, r_n$ be the distinct roots of Q in a given splitting field of Q over K. Then $b_i = \sigma_i(r_1, \ldots, r_n)$ for $i = 1, \ldots, n$, so with $b = (b_1, \ldots, b_n)$ and $r = (r_1, \ldots, r_n)$,

$$R(b, Z) = \prod_{\sigma \in S} \big(Z - \sigma(r)\big).$$

The coefficients of each monic factor of Q in $K[Y]$ are elementary symmetric polynomials in some of the r_i (in a splitting field of P), and hence are zeros of $R(b, Z) \in K[Z]$. Thus the claim follows from the previous lemma. □

7.2 Solving Polynomial Equations in $\mathbb{Q}_p\langle X\rangle$

In this section we let X be a single indeterminate. Turn the fraction field K of $\mathbb{Q}_p\langle X\rangle$ into a valued field with the Gauss valuation (see Section 2.3); its residue field is $\mathbb{F}_p(X)$. Our first goal is to describe a certain extension of K to a valued field whose residue field is the perfect closure of $\mathbb{F}_p(X)$. This construction applies more generally to $K = \mathrm{Frac}(F\langle X\rangle)$ where F is the fraction field of a model R of $T_{\mathbb{Z}_p}$ equipped with the Gauss valuation $v\colon K^\times \to \Gamma$.

The ring $\mathbb{Q}_p\langle X^{1/p^\infty}\rangle$

Let $R \models T_{\mathbb{Z}_p}$ and $F = \mathrm{Frac}(R)$. We let X^{1/p^n} be distinct new indeterminates (one for each $n \geqslant 1$), and also let $X^{1/p^0} := X$, and for $\nu \in \mathbb{N}$ we let $X^{\nu/p^n} := (X^{1/p^n})^\nu$. We have an F-algebra isomorphism

$$f(X) = \sum_\nu f_\nu X^\nu \mapsto f(X^{1/p^n}) := \sum_\nu f_\nu X^{\nu/p^n} \colon F\langle X\rangle \to F\langle X^{1/p^n}\rangle.$$

We let $R\langle X^{1/p^n}\rangle$ be the image of the R-subalgebra $R\langle X\rangle$ of $F\langle X\rangle$ under this isomorphism. View $F\langle X^{1/p^n}\rangle$ as a subring of $F\langle X^{1/p^{n+1}}\rangle$ via the embedding $F\langle X^{1/p^n}\rangle \to F\langle X^{1/p^{n+1}}\rangle$ which makes the diagram

$$\begin{array}{ccc} F\langle X^{1/p^n}\rangle & \longrightarrow & F\langle X^{1/p^{n+1}}\rangle \\ \cong\uparrow & & \cong\uparrow \\ F\langle X\rangle & \xrightarrow{f(X)\mapsto f(X^p)} & F\langle X\rangle \end{array}$$

commute, where the vertical isomorphisms are $f(X) \mapsto f(X^{1/p^n})$, respectively $f(X) \mapsto f(X^{1/p^{n+1}})$. With this identification we have

$$F\langle X^{1/p^n}\rangle = \left\{ f = \sum_\nu f_\nu X^{\nu/p^{n+1}} \in F\langle X^{1/p^{n+1}}\rangle : f_\nu = 0 \text{ for all } \nu \notin p\mathbb{N} \right\}.$$

Moreover, $R\langle X^{1/p^n}\rangle$ is an R-subalgebra of $R\langle X^{1/p^{n+1}}\rangle$ and $\mathrm{Frac}\big(F\langle X^{1/p^n}\rangle\big)$ is a subfield of $\mathrm{Frac}\big(F\langle X^{1/p^{n+1}}\rangle\big)$. Note that

$$F\langle X^{1/p^n}\rangle = \bigoplus_{0\leqslant\nu<p^n} F\langle X\rangle\, X^{\nu/p^n} \qquad \text{(internal direct sum of } F\langle X\rangle\text{-submodules)},$$

hence the ring extension $F\langle X\rangle \subseteq F\langle X^{1/p^n}\rangle$ is faithfully flat. We let

$$F\langle X^{1/p^\infty}\rangle := \bigcup_n F\langle X^{1/p^n}\rangle,$$

and we similarly introduce $R\langle X^{1/p^\infty}\rangle$ and $R[X^{1/p^\infty}]$. Note that $F\langle X^{1/p^\infty}\rangle$ is an integrally closed domain, but $F\langle X^{1/p^\infty}\rangle$ is not noetherian (its ideal generated by all X^{1/p^n} is not finitely generated). The ring extensions $F\langle X^{1/p^n}\rangle \subseteq F\langle X^{1/p^\infty}\rangle$ are faithfully flat. Let ρ_n be the unique F-algebra isomorphism $F\langle X^{1/p^n}\rangle \to F\langle X^{1/p^{n+1}}\rangle$ making the diagram

$$\begin{array}{ccc} F\langle X^{1/p^n}\rangle & \xrightarrow{\ \rho_n\ } & F\langle X^{1/p^{n+1}}\rangle \\ \cong\uparrow & \nearrow_{\cong} & \\ F\langle X\rangle & & \end{array}$$

commute, which we suggestively denote by $f(X^{1/p^n}) \mapsto f(X^{1/p^{n+1}})$. The ρ_n extend to a common endomorphism ρ of $F\langle X^{1/p^\infty}\rangle$, and one verifies easily that ρ is an automorphism of $F\langle X^{1/p^\infty}\rangle$. Now set

$$K := \mathrm{Frac}\big(F\langle X^{1/p^\infty}\rangle\big) = \bigcup_n \mathrm{Frac}\big(F\langle X^{1/p^n}\rangle\big).$$

We call $f \in R[X^{1/p^\infty}]$ **monic** if $f = g(X^{1/p^n})$ for some n and some monic $g \in R[X]$. Lemma 2.3.14 implies the following useful description of the elements of K:

Lemma 7.2.1. *Let $f \in K^\times$. Then there is a unique tuple (a, u, g, h) where $a \in F^\times$, $u \in 1 + t_R R\langle X^{1/p^\infty}\rangle$, and $g, h \in R[X^{1/p^\infty}]$ are monic and coprime in $F[X^{1/p^\infty}]$, such that $f = a\,u\,\dfrac{g}{h}$.*

Equip $F\langle X^{1/p^n}\rangle$ with the valuation $F\langle X^{1/p^n}\rangle^{\neq} \to \Gamma$ given by $f(X^{1/p^n}) \mapsto v\big(f(X)\big)$; we call this the Gauss valuation on $F\langle X^{1/p^n}\rangle$. The Gauss valuation on $F\langle X^{1/p^{n+1}}\rangle$ then extends that on $F\langle X^{1/p^n}\rangle$, and we equip K with the common extension of the Gauss valuations on the subrings $F\langle X^{1/p^n}\rangle$ of $F\langle X^{1/p^\infty}\rangle$ to a valuation $v\colon K^\times \to \Gamma$. The valuation ring of this valuation on K is

$$\mathcal{O} = \left\{\frac{f}{g} : f, g \in F\langle X^{1/p^\infty}\rangle,\ vf \geqslant 0 = vg\right\},$$

and its residue field is

$$\mathbb{F}_p(X^{1/p^\infty}) := \bigcup_n \mathbb{F}_p(X^{1/p^n}) \quad (= \text{the perfect closure of } \mathbb{F}_p(X)).$$

For each $f \in K^\times$ we have $v(f) = v\big(\rho(f)\big)$.

Lemma 7.2.2. *Let $P \in F\langle X\rangle[Y]^{\neq}$ be of degree $d \geqslant 1$. Then every zero of P in K lies in the subfield* $\mathrm{Frac}\big(F\langle X^{1/p^n}\rangle\big)$ *where $n = v_p(d!)$.*

Proof. Let $\mathrm{P}(F) := \bigcup_{m\geqslant 1} F(\!(X^{1/m})\!)$ be the field of Puiseux series over F. It is well-known that every zero $y \in \mathrm{P}(F)$ of a polynomial from $F(\!(X)\!)[Y]$ of degree d lies in the subfield $F(\!(X^{1/d!})\!)$ of $\mathrm{P}(F)$. (This is a consequence of the Newton diagram method applied to the X-adic valuation on $F(\!(X)\!)$, see, for example, [1, Lecture 12].) Since we may view K as a subfield of $\mathrm{P}(F)$ in a natural way, this yields the claim. □

The fraction field of $\mathbb{Q}_p\langle X^{1/p^\infty}\rangle$ as an $\mathcal{L}_1^*$-structure

Here $\mathcal{L}_1^*$ is the language introduced in Section 6.2. Let $R \models T_p$, and let F and K be as in the previous section. We expand the valued field K (viewed as an $\mathcal{L}_{\mathrm{val}}$-structure as usual) into an $\mathcal{L}_1^*$-structure. Before we describe this expansion, for each $n \geqslant 1$ we fix a formula which in every $R \models T_p$, $F = \mathrm{Frac}(R)$, defines the graph of a function $\delta_n\colon F \to F$ such that for each $a \in F$ with $va \in n\Gamma$ and $b = \delta_n(a)$ we have $v(b^n) = va$. (Cf. Corollary 4.3.2.) We now describe the $\mathcal{L}_1^*$-structure with underlying valued field K: First, interpret π as p and ξ as X. Interpret ρ as the unique extension of the automorphism of $F\langle X^{1/p^\infty}\rangle$ defined in the previous section and denoted there by the same symbol; then $\overline{\rho(f)}^p = \overline{f}$ for $f \in \mathcal{O}$. We interpret the unary function symbol $^{-1}$ of $\mathcal{L}_1^*$ such that $f^{-1}\cdot f = 1$ for $f \in K^\times$ and $0^{-1} = 0$.

Given $f \in K$, if $vf \in n\Gamma$, then we take (a, u, g, h) as in Lemma 7.2.1 and set $\delta_n(f) := \delta_n(a)$; otherwise we set $\delta_n(f) := 0$. Finally, suppose $a = (a_1, \dots, a_m) \in \mathcal{O}^m$ $(m \geqslant 1)$ and consider the polynomial

$$P = Y^m + a_1 Y^{m-1} + \cdots + a_m \in \mathcal{O}[Y].$$

If P has large discriminant, then we choose elements $r_{mn}(a)$ of $\mathcal{O}$ (where $n = 1, \dots, m$) such that each zero of P in $\mathcal{O}$ is among them, and if $r_{mn}(a)$ is not a zero of P, then $r_{mn}(a) = 0$. If P does not have large discriminant, then we set $r_{mn}(a) := 0$ for $n = 1, \dots, m$. The following is now obvious:

Lemma 7.2.3. *K is a model of the $\mathcal{L}_1^*$-theory $T_1^* = T_1^*(1, p)$.*

In the following, whenever we refer to "the $\mathcal{L}_1^*$-structure K" we mean K turned into an $\mathcal{L}_1^*$-structure in the way indicated above. (This expansion of the valued field K is not quite uniquely determined by R: for given $n \geqslant 1$ the choice of $r_{mn}(a)$ is only unique up to permutation.)

Parametrizing elements of $\mathbb{Q}_p\langle X^{1/p^\infty}\rangle$

Let as usual $C = (C_1, \dots, C_M)$. Given

$$f(C, X) = \sum_\nu f_\nu(C) X^\nu \in \mathbb{Z}_p\langle C, X\rangle$$

and $R \models T_{\mathbb{Z}_p}$, $c \in R^M$, as well as some n, we let

$$f(c, X^{1/p^n}) := \sum_\nu f_\nu(c) X^{\nu/p^n} \in R\langle X^{1/p^n}\rangle.$$

The map

$$f(C, X) \mapsto f(c, X^{1/p^n}) \colon \mathbb{Z}_p\langle C, X\rangle \to R\langle X^{1/p^n}\rangle$$

is a $\mathbb{Z}_p$-algebra morphism. We prove a version of Proposition 6.1.17 for parametrizing zeros of polynomials with large discriminant in K:

Lemma 7.2.4. *Let $f_1, \dots, f_n, g \in \mathbb{Z}_p\langle C, X\rangle$ and $k \in \mathbb{N}$ be given. Then there are finitely many elements $y^{(\lambda)}$ of $\mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \dots, V_L)$ is a tuple of new indeterminates $(L \in \mathbb{N})$,*

as well as some integer $l \geqslant k$ *and some* $\mathcal{L}_{\mathbb{Z}_p}$*-formula* $\alpha(C, V)$*, such that for each* $R \models T_p$ *and* $c \in R^M$*, the following holds:*

(1) α *defines the graph of a function* $c \mapsto a(c)\colon R^M \to R^L$*, and*

(2) *if* $0 = v\big(g(c, X)\big) \leqslant v\big(f_i(c, X)\big)$ *for* $i = 1, \ldots, n$ *and the polynomial*

$$P(Y) := Y^n + \sum_{i=0}^{n} \big(f_i(c, X^{1/p^k})/g(c, X^{1/p^k})\big)Y^{n-i} \in \mathcal{O}[Y]$$

has large discriminant, then for each $y \in K$ *with* $P(y) = 0$ *there is some* λ *such that*

$$y \cdot g(c, X^{1/p^k}) = y^{(\lambda)}\big(a(c), X^{1/p^l}\big).$$

Proof. Thanks to Lemma 7.2.2 and the automorphism ρ of the valued field K we may take some $l \geqslant k$ such that $\mathrm{Frac}\big(R\langle X^{1/p^l}\rangle\big)$ contains every zero $y \in K$ of a polynomial P as in (2). The claim now follows from Proposition 6.1.17 applied to the polynomial

$$g(C, X^{p^{l-k}})Y^n + \sum_{i=0} f_{n-i}(C, X^{p^{l-k}})Y^i \in \mathbb{Z}_p\langle C, X\rangle[Y]$$

in place of P. □

In the next proposition we let $f_1, \ldots, f_m, g \in \mathbb{Z}_p\langle C, X\rangle$ and $\tau(y_1, \ldots, y_m)$ be an $\mathcal{L}_1^*$-term, and we assume that some n is given.

Proposition 7.2.5. *There exist finitely many pairs* $\big(p^{(\lambda)}, q^{(\lambda)}\big)$ *of power series from* $\mathbb{Z}_p\langle V, X\rangle$*, where* $V = (V_1, \ldots, V_L)$ *is a tuple of new indeterminates* $(L \in \mathbb{N})$*, and some* $k \in \mathbb{N}$ *and some* $\mathcal{L}_{\mathbb{Z}_p}$*-formula* $\alpha(C, V)$*, such that for each* $R \models T_p$ *and* $c \in R^M$*, the following holds:*

(1) α *defines the graph of a function* $c \mapsto a(c)\colon R^M \to R^L$*, and*

(2) *if* $g(c, X) \neq 0$ *then for some* λ *we have* $q^{(\lambda)}\big(a(c), X\big) \neq 0$ *and*

$$\tau\big(f_1(c, X^{1/p^n})/g(c, X^{1/p^n}), \ldots, f_m(c, X^{1/p^n})/g(c, X^{1/p^n})\big) = p^{(\lambda)}\big(a(c), X^{1/p^k}\big) \,/\, q^{(\lambda)}\big(a(c), X^{1/p^k}\big)$$

where on the right τ *is evaluated in the* $\mathcal{L}_1^*$*-structure* $K = \mathrm{Frac}\big(R\langle X^{1/p^\infty}\rangle\big)$*.*

Proof. Easy induction on the construction of τ, using Corollary 2.3.15 and the preceding lemma. □

In the next lemma and its corollaries we let $f, g \in \mathbb{Z}_p\langle C, X\rangle$ and n be given.

Lemma 7.2.6. *There are finitely many $\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$-terms $y^{(\lambda)}(C, X)$ in which the function symbol* d *is not applied to subterms involving the X-variables, as well as $\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$-terms $d^{(\lambda)}(C)$, such that for all $R \models T_{\mathbb{Z}_p}$, $c \in R^M$, and $F = \mathrm{Frac}(R)$, we have*

$$f(c, X^{1/p^n}) \in g(c, X^{1/p^n})F\langle X^{1/p^\infty}\rangle \iff$$
$$d^{(\lambda)}(c) \neq 0 \text{ and } f(c, X^{1/p^n}) \cdot d^{(\lambda)}(c) = g(c, X^{1/p^n}) \cdot y^{(\lambda)}(c, X^{1/p^n}) \text{ for some } \lambda.$$

Proof. Let R, c, F be as in the statement of the lemma. Then by faithful flatness of $F\langle X^{1/p^\infty}\rangle$ over its subring $F\langle X^{1/p^n}\rangle$ we have

$$\begin{aligned} f(c, X^{1/p^n}) \in g(c, X^{1/p^n})F\langle X^{1/p^\infty}\rangle &\iff f(c, X^{1/p^n}) \in g(c, X^{1/p^n})F\langle X^{1/p^n}\rangle \\ &\iff f(c, X) \in g(c, X)F\langle X\rangle, \end{aligned}$$

and the lemma thus follows from (a very simple case of) Theorem 3.3.7. □

Corollary 7.2.7. *There are $\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$-terms $z^{(\lambda)}(C, X)$ and $d^{(\lambda)}(C)$ as in the previous lemma such that for all $R \models T_{\mathbb{Z}_p}$, $c \in R^M$, and $F = \mathrm{Frac}(R)$, we have*

$$f(c, X^{1/p^n}) \in g(c, X^{1/p^n})F\langle X\rangle \iff$$
$$d^{(\lambda)}(c) \neq 0 \text{ and } f(c, X^{1/p^n}) \cdot d^{(\lambda)}(c) = g(c, X^{1/p^n}) \cdot z^{(\lambda)}(c, X) \text{ for some } \lambda.$$

Proof. Take $y^{(\lambda)}$, $d^{(\lambda)}$ as in the previous lemma. Then $y^{(\lambda)}(C, X) = f^{(\lambda)}\big(\tau(C), X\big)$ where $f^{(\lambda)} \in \mathbb{Z}_p\langle V, X\rangle$, $V = (V_1, \ldots, V_L)$, $L \in \mathbb{N}$, and τ is an L-tuple of $\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$-terms in the tuple of variables C. Write

$$f^{(\lambda)}(V, X) = \sum_\nu f^{(\lambda)}_\nu(V)X^\nu \qquad (f^{(\lambda)}_\nu \in \mathbb{Z}_p\langle V\rangle)$$

and set

$$g^{(\lambda)}(V, X) := \sum_{\nu \in p^n\mathbb{N}} f^{(\lambda)}_\nu(V)X^\nu \in \mathbb{Z}_p\langle V, X\rangle.$$

Then $z^{(\lambda)}(C, X) := g^{(\lambda)}\big(\tau(C), X\big)$ has the required property. □

The following consequence is not used later:

Corollary 7.2.8. *There is a quantifier-free $\mathcal{L}_{\mathbb{Z}_p}$-formula $\varphi(C)$ such that for all $R \models T_{\mathbb{Z}_p}$, $c \in R^M$, we have $R \models \varphi(c)$ iff $f(c, X^{1/p^n}) \in R\langle X\rangle$.*

This follows easily from the previous corollary in the case $g = 1$. (Alternatively, we may apply the discussion at the beginning of the subsection on parametric Weierstraß Preparation of Section 2.2 to $\mathcal{F} = \{f_\nu(C) : \nu \notin p^n\mathbb{N}\}$, which also shows that φ may be taken to be a quantifier-free $\mathcal{L}_{\mathbb{Z}_p}$-formula.)

Parametrizing zeros of polynomials in $\mathbb{Q}_p\langle X\rangle$

Suppose that $n \geqslant 1$ and let

$$P(C, X, Y) = a_0(C, X)Y^n + a_1(C, X)Y^{n-1} + \cdots + a_n(C, X) \in \mathbb{Z}_p\langle C, X\rangle[Y],$$

where Y is a single indeterminate. Combining Lemma 7.1.6 with the previous proposition yields a uniform parametrization of the zeros of the polynomial $P(c, X, Y) \in R\langle X\rangle[Y]$ in the field $\mathrm{Frac}\big(R\langle X^{1/p^\infty}\rangle\big)$:

Corollary 7.2.9. *There is a finite family $\big\{(p^{(\lambda)}, q^{(\lambda)})\big\}_{\lambda\in\Lambda}$ of pairs of elements of $\mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new indeterminates ($L \in \mathbb{N}$), as well as some $k \in \mathbb{N}$ and some $\mathcal{L}_{\mathbb{Z}_p}$-formula $\alpha(C, V)$, such that for each $R \models T_p$ and $c \in R^M$ with $a_0(c, X) \neq 0$ the following holds:*

(1) *α defines the graph of a function $a\colon R^M \to R^L$, and*

(2) *for each $y \in \mathrm{Frac}\big(R\langle X^{1/p^\infty}\rangle\big)$ with $P(c, X, y) = 0$ there is some $\lambda \in \Lambda$ with*

$$q^{(\lambda)}\big(a(c), X\big) \neq 0 \quad \text{and} \quad y = p^{(\lambda)}\big(a(c), X^{1/p^k}\big) \,/\, q^{(\lambda)}\big(a(c), X^{1/p^k}\big).$$

If we are only interested in those zeros of the polynomial $P(c, X, Y)$ which lie in the subfield $\mathrm{Frac}\big(R\langle X\rangle\big)$ of $\mathrm{Frac}\big(R\langle X^{1/p^\infty}\rangle\big)$, we can use the following corollary:

Corollary 7.2.10. *There are finitely many $y^{(\lambda)} \in \mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new indeterminates, for some $L \in \mathbb{N}$, and an $\mathcal{L}_{\mathbb{Z}_p}$-formula $\alpha(C, V)$, such that for each $R \models T_p$ and $c \in R^M$ with $a_0(c, X) \neq 0$,*

(1) *α defines the graph of a function $a\colon R^M \to R^L$, and*

(2) *if $y \in \mathrm{Frac}\big(R\langle X\rangle\big)$ and $P(c, X, y) = 0$, then $y = y^{(\lambda)}\big(a(c), X\big)/a_0(c, X)$ for some λ.*

Proof. Let

$$\widetilde{P}(C, X, Y) := Y^n + \sum_{i=0}^{n-1} a_{n-i}(C, X)\, a_0(C, X)^{n-1-i}\, Y^i \in \mathbb{Z}_p\langle C, X\rangle[Y].$$

Then

$$\widetilde{P}\big(C, X, a_0(C, X)Y\big) = a_0(C, X)^{n-1} \cdot P(C, X, Y).$$

By Corollary 2.3.12 all zeros of the monic polynomial $\widetilde{P}(c, X, Y) \in R\langle X\rangle[Y]$ in the fraction field of $R\langle X\rangle$ are contained in its subring $R\langle X\rangle$. Hence the claim now follows from Corollary 7.2.7 and Corollary 7.2.9 applied to $\widetilde{P}$ in place of P. □

In particular, there is an $\mathcal{L}_{\mathbb{Z}_p}$-formula defining the existence of some $y \in \mathrm{Frac}\big(R\langle X\rangle\big)$ satisfying $P(c, X, y) = 0$. Together with Proposition 7.1.1 and its corollary and Lemma 7.1.4 in the previous section, this implies the definability of prime and primary ideals in polynomial rings $\mathrm{Frac}\big(R\langle X\rangle\big)[Y]$, where Y is a finite tuple of indeterminates. We let

$$F_1(C, X, Y), \ldots, F_m(C, X, Y) \in \mathbb{Z}_p\langle C, X\rangle[Y].$$

Corollary 7.2.11. *There are $\mathcal{L}_{\mathbb{Z}_p}$-formulas* $\mathrm{Primary}(C)$ *and* $\mathrm{Prime}(C)$ *such that for $R \models T_p$ and $c \in R^M$, denoting by I the ideal of* $\mathrm{Frac}\big(R\langle X\rangle\big)[Y]$ *generated by the polynomials $F_1(c, X, Y), \ldots, F_m(c, X, Y) \in R\langle X\rangle[Y]$, we have:*

$$R \models \mathrm{Primary}(c) \iff I \text{ is primary,}$$
$$R \models \mathrm{Prime}(c) \iff I \text{ is prime.}$$

An open question

Let $R \subseteq R^*$ be p-adically closed valuation rings with $\mathbb{Z}_p$-structure. By Corollary 7.2.10, the ring $R\langle X\rangle$ is algebraically closed in $R^*\langle X\rangle$. This raises the following natural question, which we will not pursue here:

Question 7.2.12. *Does $R\langle X\rangle \subseteq R^*\langle X\rangle$ have the specialization property?*

Here a ring extension $A \subseteq B$ has the *specialization property* if for each finitely generated subalgebra B' of the A-algebra B there is an A-algebra morphism $B' \to A$. (This implies that A is algebraically closed in B.) Most known instances of the specialization property in the literature assume that A is noetherian, or more. For example, if A is noetherian and henselian with respect to an ideal $\mathfrak{m}$, then the natural morphism $A \to \widehat{A}$ to the $\mathfrak{m}$-adic completion $\widehat{A} = \varprojlim A/\mathfrak{m}^n$ of A is injective (by Lemma 6.1.4 and Krull's Intersection Theorem [11, Corollary 10.18]), so we can identify A with a subring of $\widehat{A}$; if we assume in addition that the ring A is excellent (cf. [52, Chapter 13]), then $A \subseteq \widehat{A}$ has the specialization property. This follows from the generalized Néron Desingularization of Popescu [56, 57], cf. [65, Theorem 2.27].

7.3 Prime Ideals in Rings of Restricted Power Series

Let $f_1(C, X), \dots, f_m(C, X) \in \mathbb{Z}_p\langle C, X\rangle$. For $R \models T_{\mathbb{Z}_p}$ we let $F = \mathrm{Frac}(R)$, and given $c \in R^M$ we let as usual $I(c, X)$ denote the ideal of $R\langle X\rangle$ generated by $f_1(c, X), \dots, f_m(c, X)$.

Primary ideals in $F\langle X\rangle$

Our goal in this subsection is to prove the following:

Theorem 7.3.1. *There are $\mathcal{L}_{\mathbb{Z}_p}$-formulas* $\mathrm{primary}(C)$ *and* $\mathrm{prime}(C)$ *such that for all $R \models T_p$ and $c \in R$, if* $\dim I(c, X)F\langle X\rangle \leqslant 1$*, then*

$$R \models \mathrm{primary}(c) \iff I(c, X)F\langle X\rangle \text{ is primary,}$$
$$R \models \mathrm{prime}(c) \iff I(c, X)F\langle X\rangle \text{ is prime.}$$

We recall that by Corollary 4.2.2 the condition "$\dim I(c, X)F\langle X\rangle \leqslant 1$" is also definable (in fact, uniformly in all models of $T_{\mathbb{Z}_p}$). We also note that it suffices to prove the existence of a formula primary with the stated property, since then, with rad as in Corollary 5.2.3, $\mathrm{prime} := \mathrm{primary} \wedge \mathrm{rad}$ defines the property of generating a prime ideal. For the proof of

Theorem 7.3.1 we use the following criterion:

Lemma 7.3.2. *Let A be an integral domain with fraction field K, and let I be an ideal of $A[Y]$ with $A \cap I = \{0\}$. Then I is primary if and only if $IK[Y] \cap A[Y] = I$ and $IK[Y]$ is a primary ideal of $K[Y]$.*

Proof. Note that $A \cap \sqrt{I} = \{0\}$ since A is reduced. Suppose I is primary. Given $f \in IK[Y] \cap A[Y]$, take $a \in A^{\neq}$ with $af \in I$; then $a \notin \sqrt{I}$ and hence $f \in I$. This shows $IK[Y] \cap A[Y] = I$. Further, let $f, g \in K[Y]$ with $fg \in IK[Y]$; we need to show that $f \in IK[Y]$ or $g \in \sqrt{IK[Y]}$. After multiplying f, g by suitable elements of $A^{\neq}$ we can assume $f, g \in A[Y]$, and then $fg \in IK[Y] \cap A[Y] = I$ and so $f \in I$ or $g \in \sqrt{I}$. This shows the forward direction; the backward direction is obvious. □

Proof of Theorem 7.3.1. Fix $d \in \{0, 1\}$. It suffices to show the existence of a formula $\mathrm{primary}_d(C)$ satisfying the conclusion of the theorem for all $R \models T_p$ and $c \in R$ with $\dim I(c, X)F\langle X\rangle = d$. As at the beginning of the proof of Theorem 5.2.2, by employing a case distinction using uniform Noether Normalization we reduce to the case that the f_i are polynomials in $\mathbb{Z}_p\langle C, X_1, \ldots, X_d\rangle[X_{d+1}, \ldots, X_N]$ and contain a Weierstrass sequence over $\mathbb{Z}_p\langle C, X_1, \ldots, X_d\rangle$. Then for $R \models T_p$ and $c \in R^M$, the ideal $I(c, X)F\langle X\rangle$ of $F\langle X\rangle$ is primary iff the $f_i(c, X)$ generate a primary ideal of the polynomial ring $F\langle X_1, \ldots, X_d\rangle[X_{d+1}, \ldots, X_N]$; see the remarks preceding Corollary 4.1.11. Hence in the case $d = 0$ we are already done by Proposition 7.1.1. So suppose $d = 1$, and relabel the indeterminates X_1 as X and $(X_2, \ldots, X_N)$ as $Y = (Y_1, \ldots, Y_{N-1})$; thus $f_i = f_i(C, X, Y) \in \mathbb{Z}_p\langle C, X\rangle[Y]$. Corollary 4.2.8 yields a covering family $\{\varphi^{(\lambda)}(C)\}$ of quantifier-free $\mathcal{L}^{\mathrm{d}}_{\mathbb{Z}_p}$-formulas and for each λ elements

$$h_1^{(\lambda)}(V, X, Y), \ldots, h_k^{(\lambda)}(V, X, Y) \in \mathbb{Z}_p\langle V, X\rangle[Y] \qquad (k \in \mathbb{N}),$$

where $V = (V_1, \ldots, V_L)$ is a tuple of new distinct indeterminates ($L \in \mathbb{N}$), and an L-tuple τ of terms in C, such that for $R \models T_{\mathbb{Z}_p}$ and $c \in R^M$ with $R \models \varphi^{(\lambda)}(c)$, setting

$$A = F\langle X\rangle, \qquad K = \mathrm{Frac}(A), \qquad J = \big(f_1(c, X, Y), \ldots, f_m(c, X, Y)\big) \subseteq A[Y],$$

we have

$$JK[Y] \cap A[Y] = \Big(h_1^{(\lambda)}\big(\tau(c), X, Y\big), \ldots, h_k^{(\lambda)}\big(\tau(c), X, Y\big)\Big).$$

Note that then

$$I := I(c, X, Y)F\langle X, Y\rangle = JF\langle X, Y\rangle$$

and so $I \cap A[Y] = J$. Hence by Corollary 3.3.11 we can take a quantifier-free $\mathcal{L}_{\mathbb{Z}_p}^{\mathrm{d}}$-formula $\psi^{(\lambda)}(C)$ such that for all $R \models T_{\mathbb{Z}_p}$ and $c \in R^M$, with A, J, K as above,

$$R \models \psi^{(\lambda)}(c) \quad \Longleftrightarrow \quad JK[Y] \cap A[Y] = J.$$

Let Primary(C) be as in Corollary 7.2.11. Then

$$\text{primary}_1 := \text{Primary} \wedge \bigvee_{\lambda} \big(\varphi^{(\lambda)} \wedge \psi^{(\lambda)}\big)$$

has the required property, by Lemma 7.3.2. □

Now that Theorem 7.3.1 is established, we can show that the formulas postulated in its statement can be taken to be of a particularly simple shape. (One can think of this as the analogue of [25, (2.10), parts (i) and (iv)]; for the property of being a prime ideal this formulation first appears in Chapter 4, §3 of [20].)

Corollary 7.3.3. *There are a finite family $\big\{(f_\lambda, g_\lambda)\big\}$ of pairs of power series in $\mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new indeterminates, $L \in \mathbb{N}$, as well as some integer $E \geqslant 1$ and an $\mathcal{L}_{\mathbb{Z}_p}$-formula $\alpha(C, X)$ which for all $R \models T_p$ defines the graph of a map $c \mapsto a(c)\colon R^M \to R^L$, with the following properties, for $R \models T_p$, $c \in R^M$ and $I := I(c, X)F\langle X\rangle$ with $\dim I \leqslant 1$:*

(1) *I is primary iff $1 \notin I$ and for all λ,*

$$f_\lambda\big(a(c), X\big) \cdot g_\lambda\big(a(c), X\big) \in I \;\Rightarrow\; f_\lambda\big(a(c), X\big) \in I \text{ or } g_\lambda\big(a(c), X\big)^E \in I;$$

(2) *I is prime iff $1 \notin I$ and for all λ,*

$$f_\lambda\big(a(c), X\big) \cdot g_\lambda\big(a(c), X\big) \in I \;\Rightarrow\; f_\lambda\big(a(c), X\big) \in I \text{ or } g_\lambda\big(a(c), X\big) \in I.$$

Proof. Take an integer $E \geqslant 1$ as in Corollary 5.2.4. Given power series $f, g \in \mathbb{Z}_p\langle V, X\rangle$, where $V = (V_1, \ldots, V_L)$ is a tuple of new indeterminates ($L \in \mathbb{N}$) and a formula $\alpha(C, V)$ which defines, in each $R \models T_p$, the graph of a map $c \mapsto a(c)\colon R^M \to R^L$, let $\pi(C) = \pi_{f,g,\alpha}(C)$ be an $\mathcal{L}_{\mathbb{Z}_p}$-formula such that for $R \models T_{\mathbb{Z}_p}$ and $c \in R^M$, with $I = I(c, X)F\langle X\rangle$ we have

$$R \models \pi(c) \iff f\big(a(c), X\big)\, g\big(a(c), X\big) \notin I \text{ or } f\big(a(c), X\big) \in I \text{ or } g\big(a(c), X\big)^E \in I.$$

(Such a formula π exists by Corollaries 3.3.11 and 5.2.4.) Let primary(C) be as in the theorem above and let $\dim_d$ be as in Corollary 4.2.2. Suppose the conclusion of the corollary fails. Then by compactness we obtain some $R^* \models T_p$ and $c^* \in (R^*)^M$ such that $R^* \models \pi_{f,g,\alpha}(c^*)$ for all choices of f, g, α, yet $R^* \models \dim_0(c^*) \vee \dim_1(c^*) \vee \big(\neg\,\text{primary}(c^*)\big)$. As at the end of the proof of Corollary 5.3.5, this leads to contradiction. This shows (1), and (2) is proved in a similar way. □

As another consequence of Theorem 7.3.1 and various earlier results we obtain the uniform parametrizability of primary decompositions for one-dimensional ideals:

Corollary 7.3.4. *There are a finite family $\big\{(\vec{f}_{1,\lambda}, \ldots, \vec{f}_{n,\lambda})\big\}$ where each $\vec{f}_{i,\lambda}$ is an m-tuple of power series in $\mathbb{Z}_p\langle V, X\rangle$, for some m, n and tuple $V = (V_1, \ldots, V_L)$ of new indeterminates ($L \in \mathbb{N}$), as well as an $\mathcal{L}_{\mathbb{Z}_p}$-formula $\alpha(C, X)$ which for all $R \models T_p$ defines the graph of a map $c \mapsto a(c)\colon R^M \to R^L$, such that for $R \models T_p$, $c \in R^M$ and $I := I(c, X)F\langle X\rangle$, the following holds: if $\dim I \leqslant 1$, then for some λ the ideals generated by the power series in $\vec{f}_{i,\lambda}\big(a(c), X\big) \in R\langle X\rangle^m$ $(i = 1, \ldots, n)$ are an irredundant primary decomposition of I.*

Proof. Given m-tuples $\vec{f}_1, \ldots, \vec{f}_n$ of power series in $\mathbb{Z}_p\langle V, X\rangle$ there is an $\mathcal{L}_{\mathbb{Z}_p}$-formula $\Pi(C, V)$ such that for $R \models T_p$, $c, a \in R^M$ and $I := I(c, X)F\langle X\rangle$ and

$$J_i := \text{ the ideal of } F\langle X\rangle \text{ generated by the power series in } \vec{f}_i\big(a, X\big) \quad (i = 1, \ldots, n)$$

we have

$$R \models \Pi(c, a) \iff \begin{cases} \dim I > 1 \text{ or } J_1, \ldots, J_n \text{ is an irredundant pri-} \\ \text{mary decomposition of } I. \end{cases}$$

Such a formula Π exists thanks to Theorems 5.2.2, 7.3.1 and Corollaries 3.3.11, 3.3.13, 4.2.2. Now for each $R \models T_p$ the ring $F\langle X\rangle$ is noetherian (Corollary 2.3.11), hence every one of its ideals has an irredundant primary decomposition; in particular, if $c \in R^M$ then $R \models \Pi(c, a)$ for some choice of $\vec{f_1}, \ldots, \vec{f_n}$ and some $a \in R^L$; thus the claim follows by compactness and definability of Skolem functions in T_p (Corollary 4.3.2). □

Prime ideals in $R\langle X\rangle$

Our analysis of prime ideals in $R\langle X\rangle$ rests on the following:

Lemma 7.3.5. *Let $R \models T_p$ and I be a finitely generated ideal of $R\langle X\rangle$. Then I is prime if and only if*

(1) *$p \in I$, and the image of I under the natural surjection*

$$R\langle X\rangle \to R\langle X\rangle/pR\langle X\rangle \cong \mathbb{F}_p[X]$$

is prime; or

(2) *$p \notin I$, $IF\langle X\rangle \cap R\langle X\rangle = I$, and the ideal $IF\langle X\rangle$ of $F\langle X\rangle$ is prime.*

Proof. This is clear if $p \in I$, so suppose that $p \notin I$. In this case, if I is prime then $I = (I : p) = IF\langle X\rangle \cap R\langle X\rangle$ by Corollary 4.3.9, and it follows that $IF\langle X\rangle$ is prime. Conversely, it is clear that if (2) holds, then I is prime. □

As a consequence we can reduce primality testing for ideals of $\mathbb{Z}_p\langle X\rangle$ to the case of ideals of $\mathbb{Q}_p\langle X\rangle$:

Corollary 7.3.6. *Let $\varphi(C)$ and $\mathrm{prime}(C)$ be $\mathcal{L}_{\mathbb{Z}_p}$-formulas such that for each $R \models T_p$ and $c \in R^M$ with $R \models \varphi(c)$ we have $R \models \mathrm{prime}(c)$ iff $I(c, X)F\langle X\rangle$ is prime. Then there is an $\mathcal{L}_{\mathbb{Z}_p}$-formula $\mathrm{prime}_p(C)$ such that for $R \models T_p$ and $c \in R^M$ with $R \models \varphi(c)$ we have $R \models \mathrm{prime}_p(c)$ iff $I(c, X)$ is prime.*

Proof. Thanks to Lemma 2.2.8 and (2.7) we can take a (quantifier-free) $\mathcal{L}_{\mathrm{div}}$-formula $\varphi_1(C)$ such that for all $R \models T_{\mathbb{Z}_p}$ and $c \in R^M$ we have

$$R \models \varphi_1(c) \quad \Longleftrightarrow \quad \overline{f_1(c,X)}, \ldots, \overline{f_N(c,X)} \text{ generate a prime ideal of } \mathbb{F}_p[X].$$

Let $\varphi_2(C)$ be an $\mathcal{L}_{\mathbb{Z}_p}$-formula such that for all $R \models T_p$ and $c \in R^M$ we have

$$R \models \varphi_2(c) \quad \Longleftrightarrow \quad I(c,X)F\langle X\rangle \cap R\langle X\rangle = I(c,X).$$

(See the remarks following Proposition 4.3.7.) Then with $\epsilon_p(C)$ as described after Corollary 3.3.9, the formula

$$\mathrm{prime}_p := (\epsilon_p \wedge \varphi_1) \vee (\neg\epsilon_p \wedge \varphi_2 \wedge \mathrm{prime})$$

has the required property. □

Combining Theorem 7.3.1 with the preceding corollary yields:

Corollary 7.3.7. *There is an $\mathcal{L}_{\mathbb{Z}_p}$-formula which in each $R \models T_p$ defines the set of all $c \in R^M$ such that $\dim I(c,X)F\langle X\rangle \leqslant 1$ and $I(c,X)$ is prime.*

Similarly to Corollary 7.3.3, this implies the following uniform characterization of prime ideals. (For the property of being a radical ideal of $R\langle X\rangle$ we already noted a similar result in Corollary 5.3.5.)

Corollary 7.3.8. *There are $\{f_\lambda\}$, $\{g_\lambda\}$, α as in Corollary 7.3.3 such that for $R \models T_p$, $c \in R^M$, and $I = I(c,X)$:*

$$I \text{ is prime} \quad \Longleftrightarrow \quad \begin{cases} 1 \notin I \text{ and for all } \lambda, \text{ if } f_\lambda\big(a(c),X\big) \cdot g_\lambda\big(a(c),X\big) \in I, \\ \text{then } f_\lambda\big(a(c),X\big) \in I \text{ or } g_\lambda\big(a(c),X\big) \in I. \end{cases}$$

Remark 7.3.9. Suppose $f_1, \ldots, f_n \in \mathbb{Z}[C,X] \subseteq \mathbb{Z}_p\langle C,X\rangle$. In [8, Corollary 5.12] it is shown that for $R = \mathbb{Z}_p$ the set of all $c \in R^M$ such that the ideal of $R[X]$ generated by $f_1(c,X), \ldots, f_n(c,X)$ is prime is definable by a formula $\pi(C)$ in the language of rings; however, in contrast to Corollary 7.3.7, no such formula $\pi(C)$ does the job uniformly for an arbitrary p-adically closed valuation ring R; see [8, example following 5.12] and [10].

REFERENCES

[1] S. Abhyankar, *Algebraic Geometry for Scientists and Engineers,* Mathematical Surveys and Monographs, vol. 35, American Mathematical Society, Providence, RI, 1990.

[2] W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases,* Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.

[3] M. E. Alonso, T. Mora, M. Raimondo, *On the complexity of algebraic power series,* in: S. Sakata (ed.), *Applied Algebra, Algebraic Algorithms and Error-correcting Codes* (*Tokyo, 1990*), pp. 197–207, Lecture Notes in Comput. Sci., vol. 508, Springer, Berlin, 1991.

[4] M. E. Alonso, T. Mora, M. Raimondo, *Local decomposition algorithms,* in: S. Sakata (ed.), *Applied Algebra, Algebraic Algorithms and Error-correcting Codes* (*Tokyo, 1990*), pp. 208–221, Lecture Notes in Comput. Sci., vol. 508, Springer, Berlin, 1991.

[5] M. E. Alonso, T. Mora, M. Raimondo, *A computational model for algebraic power series,* J. Pure Appl. Algebra **77** (1992), no. 1, 1–38.

[6] M. Aschenbrenner, *Ideal Membership in Polynomial Rings over the Integers*, Ph.D. thesis, University of Illinois at Urbana-Champaign, 2001.

[7] M. Aschenbrenner, *Ideal membership in polynomial rings over the integers,* J. Amer. Math. Soc. **17** (2004), 407–441.

[8] M. Aschenbrenner, *Bounds and definability in polynomial rings*, Quart. J. Math. **56** (2005), 263–300.

[9] M. Aschenbrenner, *An effective Weierstrass Division Theorem*, manuscript.

[10] M. Aschenbrenner, *Erratum to "Ideal membership in polynomial rings over the integers",* preprint, 2018.

[11] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Reading, Mass.-London-Don Mills, Ont., 1969.

[12] T. Becker, V. Weispfenning, *Gröbner Bases*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993.

[13] J. Ax, S. Kochen, *Diophantine problems over local fields,* III, Ann. of Math. **83** (1966), 437–456.

[14] S. Bosch, U. Güntzer, R. Remmert, *Non-Archimedean Analysis. A Systematic Approach to Rigid Analytic Geometry*, Grundlehren der Mathematischen Wissenschaften, vol. 261, Springer-Verlag, Berlin, 1984.

[15] Y. F. Çelikler, *Dimension theory and parameterized normalization for D-semianalytic sets over non-Archimedean fields,* J. Symbolic Logic **70** (2005), no. 2, 593–618.

[16] E. Crépeaux, *Une caractérisation des couples henséliens,* Enseignement Math. **13** (1968), 273–279.

[17] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen,* Abhandl. Kgl. Ges. Wiss. Göttingen **23** (1878), 1–23.

[18] R. Dedekind, *Über die Diskriminanten endlicher Körper,* Abhandl. Kgl. Ges. Wiss. Göttingen **29** (1882), 1–56.

[19] J. Denef, L. van den Dries, *p-adic and real subanalytic sets,* Ann. Math. **128** (1988), 79–138.

[20] L. van den Dries, *Model Theory of Fields*, Ph.D. thesis, R.U. Utrecht, 1978.

[21] L. van den Dries, *Algorithms and bounds for polynomial rings,* in: M. Boffa et al. (eds.), *Logic Colloquium '78,* pp. 147–157, Studies in Logic and the Foundations of Mathematics, vol. 97, North-Holland Publishing Co., Amsterdam, 1979.

[22] L. van den Dries, *A specialization theorem for p-adic power series converging on the closed unit disc,* J. Algebra **73** (1981), no. 2, 613–623.

[23] L. van den Dries, *Analytic Ax-Kochen-Ersov theorems,* in: *Proceedings of the International Conference on Algebra, Part 3* (*Novosibirsk, 1989*), pp. 379–398, Contemp. Math. **131**, Part 3, Amer. Math. Soc., Providence, RI, 1992.

[24] L. van den Dries, D. Haskell, D. Macpherson, *One-dimensional p-adic subanalytic sets,* J. London Math. Soc. (2) **59** (1999), 1–20.

[25] L. van den Dries, K. Schmidt, *Bounds in the theory of polynomial rings over fields,* Invent. math. **76** (1984), 77–91.

[26] L. van den Dries, A. J. Wilkie, *Gromov's theorem on groups of polynomial growth and elementary logic,* J. Algebra **89** (1984), 349–374.

[27] B. Dwork, A. van der Poorten, *The Eisenstein constant,* Duke Math. J. **65** (1992), 23–43l.

[28] B. Dwork, A. van der Poorten, *Correction to "The Eisenstein constant"*, Duke Math. J. **76** (1994), 669–672.

[29] P. C. Eklof, *Resolution of singularities in prime characteristic for almost all primes,* Trans. Amer. Math. Soc. **146** (1969), 429–438.

[30] I. Efrat, *Valuations, Orderings, and Milnor K-theory,* Mathematical Surveys and Monographs, vol. 124, American Mathematical Society, Providence, RI, 2006.

[31] O. Endler, *Valuation Theory,* Springer-Verlag, Berlin, 1972.

[32] Ju. L. Eršov, *On the elementary theory of maximal normed fields*, Soviet Math. Dokl. **6** (1965), 1390–1393.

[33] Ju. L. Eršov, *On the elementary theory of maximal valued fields,* III, Algebra i Logika Sem. **6** (1967), no. 3, 31–38.

[34] Ju. L. Eršov, *The Dedekind criterion for arbitrary valuation rings*, Dokl. Akad. Nauk **410** (2006), no. 2, 158–160.

[35] P. Gianni, B. Trager, G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals,* J. Symbolic Comput. **6** (1988), no. 2-3, 149–167.

[36] C. Gomez, *Definability in p-adic Power Series Rings,* Ph.D. thesis, University of California at Berkeley, 2000.

[37] S. Greco, *Algebras over nonlocal Hensel rings,* J. Algebra **8** (1968), 45–59.

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

[39] M. Harrison-Trainor, J. Klys, R. Moosa, *Nonstandard methods for bounds in differential polynomial rings,* J. Algebra **360** (2012), 71–86.

[40] H. Hasse, F. K. Schmidt, *Die Struktur diskret bewerteter Körper,* J. Reine Angew. Math. **170** (1933), 4–63.

[41] K. Hensel, *Über die Entwicklung der algebraischen Zahlen in Potenzreihen,* Math. Ann. **55** (1902), 301–336.

[42] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788.

[43] G. Hermann, *The question of finitely many steps in polynomial ideal theory*, SIGSAM Bulletin **32** (1998), no. 3, 8–30 (translation of [42]).

[44] S. Khanduja, M. Kumar, *On Dedekind criterion and simple extensions of valuation rings,* Comm. Algebra **38** (2010), no. 2, 684–696.

[45] S. Kleiman, *Les théorèmes de finitude pour le foncteur de Picard,* in: P. Berthelot, A. Grothendieck, L. Illusie (eds.), *Théorie des Intersections et Théorème de Riemann-Roch. Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967* (*SGA 6*), pp. 616–666, Lecture Notes in Mathematics, vol. 225, Springer-Verlag, Berlin-New York, 1971.

[46] S. Kochen, *The model theory of local fields,* in: G. H. Müller et al. (eds.), *Proceedings of the International Summer Institute and Logic Colloquium, Kiel, 1974,* pp. 384–425, Lecture Notes in Mathematics, vol. 499, Springer-Verlag, Berlin-New York, 1975.

[47] W. M. Lambert, Jr., *Effectiveness, Elementary Definability, and Prime Polynomial Ideals,* PhD Thesis, University of California, Los Angeles, 1965.

[48] W. M. Lambert, Jr. *A notion of effectiveness in arbitrary structures*, J. Symbolic Logic **33** (1968), 577–602.

[49] S. Lang, *Algebra,* 3rd ed., Addison-Wesley Publishing Company, Reading, MA, 1993.

[50] L. Lipshitz, Z. Robinson, *Rings of separated power series and quasi-affinoid geometry,* Astérisque **264** (2000).

[51] S. Łojasiewicz, *Ensembles semi-analytiques*, Inst. Hautes Études Sci., Bures-sur-Yvette, 1964.

[52] H. Matsumura, *Commutative Algebra,* 2nd ed., W. A. Benjamin, Reading, MA, 1980.

[53] R. Mechik, *Sur la constante d'Eisenstein,* Ann. Math. Blaise Pascal **15** (2008), no. 1, 87–108.

[54] F. Pop, *Henselian implies large,* Ann. Math. **172** (2010), 2183–2195.

[55] F. Pop, *Little survey on large fields—old & new,* in: A. Campillo et al. (eds.), *Valuation Theory in Interaction,* pp. 432–463, EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich, 2014.

[56] D. Popescu, *General Néron desingularization,* Nagoya Math. J. **100** (1985), 97–126.

[57] D. Popescu, *General Néron desingularization and approximation,* Nagoya Math. J. **104** (1986), 85–115.

[58] A. Prestel, P. Roquette, *Formally p-adic Fields*, Lecture Notes in Mathematics, vol. 1050, Springer-Verlag, Berlin-New York, 1984.

[59] B. Renschuch, *Beiträge zur konstruktiven Theorie der Polynomideale.* XVII/1. *Zur Hentzelt/Noether/Hermannschen Theorie der endlich vielen Schritte,* Wiss. Z. Pädagog. Hochsch. "Karl Liebknecht" Potsdam **24** (1980), no. 1, 87–99.

[60] B. Renschuch, *Beiträge zur konstruktiven Theorie der Polynomideale.* XVII/2. *Zur Hentzelt/Noether/Hermannschen Theorie der endlich vielen Schritte,* Wiss. Z. Pädagog. Hochsch. "Karl Liebknecht" Potsdam **25** (1981), no. 1, 125–136.

[61] M. Reufel, *Konstruktionsverfahren bei Moduln über Polynomringen,* Math. Z. **90** (1965), 231–250.

[62] A. Robinson, *Théorie Métamathematique des Idéaux,* Coll. de Logique Mathématique, Gauthier-Villars, Paris, 1955.

[63] A. Robinson, *Introduction to Model Theory and to the Metamathematics of Algebra,* Studies in Logic and the Foundations of Math., North-Holland, Amsterdam, 1965.

[64] A. Robinson, *On bounds in the theory of polynomial ideals,* in: Ju. L. Eršov et al. (eds.), *Selected Questions of Algebra and Logic. A Collection Dedicated to the Memory of A. I. Mal′cev,* pp. 245–252, Izdat. "Nauka" Sibirsk. Otdel., Novosibirsk, 1973.

[65] G. Rond, *Artin Approximation,* J. Singul. **17** (2018), 108–192.

[66] T. Sander, *Effektive Algebraische Geometrie über nicht algebraisch abgeschlossenen Körpern,* PhD Thesis, Universität Dortmund, 1996.

[67] M. P. F. du Sautoy, *Finitely generated groups, p-adic analytic groups and Poincaré series,* Ann. of Math. (2) **137** (1993), no. 3, 639–670.

[68] I. Schur, *Einige Bemerkungen über die Diskriminante eines algebraischen Zahlkörpers,* J. Reine Angew. Math. **167** (1932), 264–269.

[69] A. Seidenberg, *On the length of a Hilbert ascending chain,* Proc. Amer. Math. Soc. **29** (1971), 443–450.

[70] A. Seidenberg, *Constructions in algebra,* Trans. Amer. Math. Soc. **197** (1974), 273–313.

[71] J.-P. Serre, *Local Fields,* Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.

[72] H. Stützer, *Die elementare Formulierbarkeit von Dimension und Grad algebraischer Mannigfaltigkeiten,* Arch. Math. (Basel) **28** (1977), no. 3, 270–273.

[73] O. Teichmüller, *Diskret bewertete Körper mit unvollkommenem Restklassenkörper,* J. Reine Angew. Math. **176** (1937), 141–152.

[74] M. Ziegler, *Die elementare Theorie der henselschen Körper,* PhD thesis, Universität zu Köln, 1972.