INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI®

COMPUTING NORMALIZATIONS USING NEWTON POLYGONS

by

Jerry Girolamo Ianni

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2001

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

8/31/01
Date

Raymond T. Hoobler
Chair of Examining Committee

8/31/01
Date

Executive Officer

Professor Raymond T. Hoobler

Professor Carlos J. Moreno

Professor Alphonse T. Vasquez

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

COMPUTING NORMALIZATIONS USING NEWTON POLYGONS

by

Jerry Girolamo Ianni

Advisor: Professor Raymond T. Hoobler

Let A be a unique factorization domain that is finitely generated as an algebra over a field k of characteristic 0, and let K be the field of fractions of A. An algorithm is presented for computing the integral closure of A in the ring extension $L = K[X]/(f)$ where $f \in A[X]$ is monic and has no repeated roots in an algebraic closure of K. This task is accomplished by replacing the ring A with suitable complete discrete valuation rings that arise from localizations at height 1 prime ideals of A. In that setting, Henselization techniques, Newton Polygon factorizations, and Chinese Remainder Theorem decompositions are employed to compute an integrally closed separable extension that is then used to recover the desired normalization by algebraic descent. A partial implementation of the procedures used in the algorithm to MAPLE is given along with several examples.

Acknowledgements

I would like to thank my thesis advisor, Professor Raymond T. Hoobler, for sharing with me his approach to conducting mathematical research. He showed me the role of the imagination in the discovery of new results as well as the need for maintaining awareness of rigor during the process. In addition, his mathematical intuition was always quite helpful, and it also served as an energetic catalyst for my initial realization of the fundamental concepts of Commutative Algebra. Because of his guidance, I now have the ability to forge ahead with a sense of direction instead of groping forward in an aimless fashion!

I would like to thank Professors Carlos J. Moreno and Alphonse T. Vasquez for serving on my defense committee and for sharing their insights with me many times during my studies. Collectively, I would like to thank all of the faculty, staff, and students of the Mathematics Department at the CUNY Graduate Center. They cultivated a community of scholars that respected individual detachment at all times for the engagement of mathematical study. However, within that quiet context, they created a family atmosphere with much support.

I would also like to thank the Mathematics Department at the City College of New York for being my "research home away from home". They hosted the Kolchin Seminar in Differential Algebra wherein I gave several talks about the material in this thesis. The seminar coordinator, Professor William Y. Sit, was a constant source of support and helped me in my development in many ways.

I must extend my thanks to Professor Jorge A. Perez of the Mathematics Department at LaGuardia Community College. For many years, he served as my Chairperson. At all times, he provided encouragement for me to complete my dissertation.

There are so many other individuals that deserve recognition for the support that they have given to me. I am saddened that I am unable to mention all of these professors, colleagues, students, and friends by name. On the other hand, it is a beautiful manifestation of God's love to be blessed with such a problem! However, I must recognize my father, Mr. Vincent Ianni. Without his vision, support, and presence, nothing would have been possible.

Contents

Chapter 1

Introduction

1.1 Statement of the Problem and Previous Work

Let A be a unique factorization domain that is finitely generated as an algebra over a field k of characteristic 0, and let K be the field of fractions of A. Suppose that $f \in A[X]$ is monic, f has no repeated roots in an algebraic closure of K, and θ is the canonical root of f in the ring extension $L = K[X]/(f)$. Our objective is to compute the normalization of A in L.

To motivate our interest in this problem, let $B = k[y_1, \ldots, y_s]$ be a finitely generated reduced algebra over a field k of characteristic 0. Using constructive Noether Normalization Techniques, one can find elements $u_1, \ldots, u_n \in B$ which are algebraically independent and such that B is an integral extension of $A = k[u_1, \ldots, u_n]$. If $K = QF(B)$ and L is a finite extension of K, then the integral closures of A and B in L are the same.

For $L = K(\theta_1, \ldots, \theta_m)$, we can replace B with $B\left[\widetilde{\theta_1}, \ldots, \widetilde{\theta_m}\right]$ where $\widetilde{\theta_i} = c_i\theta_i$ is *integral* over B for each i. Thus, we may assume that $L = K = QF(B)$. Since A can be built up to B through monogenic extensions, we are reduced to the previous setting.

We will offer an algorithmic approach that depends on the computational nature of our conditions. For example, the assumption that f has no repeated roots in an algebraic closure of K is equivalent to the statement that there exist $a, b \in K[X]$ such that $af + bf' = 1$. Thus, $f'(\theta)$ is a unit in the ring L. This fact will be crucial in finding upper and lower module bounds for our normalization.

A. L. Chistov proved a result in 1989 which suggests that it is quite reasonable to search for a computational solution to our problem. In [Chistov], A denotes either $\mathbb{Z}$ or $\mathbb{F}_p[t]$, and K is its field of fractions. He defines the *length* $l(c)$ of a nonzero element $c \in A$ by the formulas $l(c) = (1 + \deg_t(c)) \log_2 p$ if $A = \mathbb{F}_p[t]$, and $l(c) = \min\{s \in \mathbb{Z} : |c| < 2^{s-1}\}$ if $A = \mathbb{Z}$. In both cases, he sets $l(0) = 1$. Using these definitions, he declares the *length* of a polynomial $f \in A[X]$ to be the sum of the lengths of all of its coefficients, including zero coefficients. We now state Chistov's result.

Theorem 1 *Let $f \in A[X]$ be a monic, separable polynomial, and suppose one knows the squarefree part of the discriminant d_θ of f. Then in time polynomial in the length of f one can construct an A – basis of the integral closure of the ring A in the algebra $K[X]/(f)$.*

There are several methods already known for computing the desired normalization that require assorted additional hypotheses. The most typical constraint is that A has

Krull dimension 1. The related problem of computing the ring of algebraic integers in a number field also has been studied and algorithmic procedures have been developed in that case. However, no techniques have yet been found that are efficient in all circumstances.

For example, suppose $L = \mathbb{Q}(\theta)$ is a number field where θ is a root of the monic polynomial $f \in \mathbb{Z}[X]$. Let $\mathfrak{O}_L$ denote the ring of algebraic integers in L. If $\mathfrak{O} = \mathbb{Z}[\theta]$, the idea of the Round 2 algorithm is to systematically "enlarge" $\mathfrak{O}$ until $\mathfrak{O}_L$ is obtained. For this purpose, $\mathfrak{O}$ is said to be *p-maximal* for a given prime number p if $[\mathfrak{O}_L : \mathfrak{O}]$ is not divisible by p. Then $\mathfrak{O} = \mathfrak{O}_L$ if and only if $\mathfrak{O}$ is p-maximal for each p. Using the concept of the *p-radical* I_p defined by $I_p = \{x \in \mathfrak{O} : \exists m \geq 1 \text{ such that } x^m \in p\mathfrak{O}\}$, the following enlargement criterion due to Pohst-Zassenhaus is obtained.

Theorem 2 (Cohen, 6.1.3) *Let $\mathfrak{O}$ be an order in a number field L; i.e., $[\mathfrak{O}_L : \mathfrak{O}]$ is finite. Let p be a prime number, and set $\mathfrak{O}' = \{x \in L : xI_p \subset I_p\}$. Then either $\mathfrak{O}' = \mathfrak{O}$, in which case $\mathfrak{O}$ is p-maximal, or $\mathfrak{O}' \supsetneq \mathfrak{O}$ and $p \mid [\mathfrak{O}' : \mathfrak{O}] \mid p^n$.*

A detailed treatment of the Round 2 algorithm can be found in [Cohen].

The Round 4 algorithm was developed by Zassenhaus primarily for the purpose of improving the efficiency of the Round 2 method. Experimental computations revealed that the Round 2 algorithm is relatively inefficient for polynomials of high degree with large powers of a given prime p dividing the index $[\mathfrak{O}_L : \mathfrak{O}]$. Because the power of p dividing the index $[\mathfrak{O}_L : \mathfrak{O}']$ is only guaranteed to decrease by 1, several iterations may be required to obtain $\mathfrak{O}_L$. Accordingly, Zassenhaus shifted his attention to reducing the

degree of the input polynomial. For a polynomial $f \in \mathbb{Z}[X]$, the positive generator of the ideal $\mathbb{Z} \cap ((f) + (f'))$ in $\mathbb{Z}$ is called the *reduced discriminant* $d_r(f)$ of f. In the following lemma due to Zassenhaus, $\nu_p(m)$ denotes the exponent of the exact power of p dividing $m \in \mathbb{Z}$, $d(f)$ is the discriminant of f, $\widetilde{\theta}$ is a root of $\widetilde{f}$, $\widetilde{\mathfrak{O}} = \mathbb{Z}\left[\widetilde{\theta}\right]$, and $\widetilde{L} = \mathbb{Q}\left(\widetilde{\theta}\right)$.

Lemma 3 *Let* $\kappa = \min\{\nu_p(d(f)) + 1, 2\nu_p(d_r(f))\}$ *for monic, separable polynomials* f, $\widetilde{f} \in \mathbb{Z}[X]$ *of degree* n. *If* $f \equiv \widetilde{f} \bmod (p^\kappa)$, *then the* p*-maximal overorders of* $\mathfrak{O}$ *in* L *and of* $\widetilde{\mathfrak{O}}$ *in* $\widetilde{L}$ *are isomorphic.*

The idea is to find a congruence factorization of $f \bmod (p)$ and to lift these coprime factors to a congruence factorization of $f \bmod (p^\kappa)$ using Henselization techniques. This congruence factorization is $\widetilde{f}$. In the spirit of the Chinese Remainder Theorem, one determines the p-maximal overorders for each of the subalgebras corresponding to the factors of $\widetilde{f}$ and stitches them together. A discussion of the Round 4 algorithm and its interplay with the Round 2 algorithm can be found in [Pohst1].

In Ford's Algorithm [Ford], the ring A is a complete DVR with uniformizing parameter π and quotient field K. For $f \in A[X]$ that is monic with nonzero discriminant, it is shown that it is always possible either

- to construct an integral element $\alpha \in L = K[X]/(f)$ such that $A[\alpha]$ is the normalization of A in L; or
- to factor f properly in $A[X]$ as $f = f_1 f_2$ so that $L \cong K[X]/(f_1) \times K[X]/(f_2)$ as K-algebras.

In the latter case, one iterates the algorithm on f_1 and on f_2. Ford proceeds according to the equivalent criteria given in the next theorem. The first statement is due to Berwick while the second is due to Zassenhaus. Either an element α is found such that $A[\alpha] = A[X]/(f)$ satisfies one of the criteria or an explicit factorization $f = f_1 f_2$ is found.

Theorem 4 *Suppose that A is a complete DVR with uniformizing parameter π and quotient field K. Let $f \in A[X]$ be monic with nonzero discriminant, $A_f = A[X]/(f)$, and $L = K[X]/(f)$.*

a. *A_f is the normalization of A in L if and only if there exists no decomposition $f = g^2 h_0 + \pi g h_1 + \pi^2 h_2$, with $g, h_0, h_1, h_2 \in A[X]$, g monic, and $\deg g > 0$.*

b. *Suppose $f_1, f_2, f_3, f_4 \in A[X]$ are monic where, upon reduction relative to (π), $\overline{f_1}$ is the square-free part of $\overline{f}$, $\overline{f_1}\,\overline{f_2} = \overline{f}$, $\overline{f_3} = \gcd(\overline{f_1}, \overline{f_2})$, and $\overline{f_3}^2 \overline{f_4} = \overline{f}$. Set $h = \dfrac{f - f_3^2 f_4}{\pi}$. Then A_f is the normalization of A in L if and only if $\overline{h}$ and $\overline{f_3}$ are relatively prime.*

The algorithm by Theo de Jong [Jong] assumes that R is a Noetherian, reduced ring and denotes the integral closure of R by $\widetilde{R}$. The non-normal locus NNL is defined to be the set $\{\mathfrak{p} \in Spec(R) : R_{\mathfrak{p}} \text{ is not normal}\}$. Let I be an ideal of R containing a nonzerodivisor. If $Hom_R(I, I)$ denotes the ring of R-endomorphisms defined on I, then we obtain the canonical inclusions $R \subset Hom_R(I, I) \subset \widetilde{R}$. The first inclusion is the map that sends an element of R to multiplication by this element, and the second inclusion is the map that sends $\phi \in Hom_R(I, I)$ to $\dfrac{\phi(f)}{f}$ for any element $f \in I$ that is a nonzerodivisor of R. The main result, due to Grauert and Remmert, is the following theorem.

Theorem 5 *Assume that the ideal $I \subset R$ contains a nonzerodivisor and satisfies $NNL \subset V(I)$, where $V(I) = \{\mathfrak{p} \in Spec(R) : I \subset \mathfrak{p}\}$. Suppose also that $Hom_R(I,I) = Hom_R(I,R) \cap \widetilde{R}$. Then $R = Hom_R(I,I)$ if and only if $R = \widetilde{R}$.*

Theo de Jong remarks that every radical ideal I containing a nonzerodivisor satisfies $Hom_R(I,I) = Hom_R(I,R) \cap \widetilde{R}$. The idea is to determine an ideal I with $NNL \subset V(I)$, to replace I with $\sqrt{I}$, and to compute $Hom_R\left(\sqrt{I}, \sqrt{I}\right)$. If $R = Hom_R\left(\sqrt{I}, \sqrt{I}\right)$, then stop. Otherwise, replace R with the larger ring $Hom_R\left(\sqrt{I}, \sqrt{I}\right)$ and repeat. Eventually, one obtains $\widetilde{R}$.

In the algorithm of Mark van Hoeij [Hoeij], extensive use of valuation theory and Puiseux series is made to compute a basis for the normalization of A in L as an A-module. Our algorithm also makes extensive use of valuation theory, but it dispenses with the complexities of Puiseux expansions by appealing to the simpler and more precise theory of extensions of valuations defined on *complete* discrete valuation rings. Much more will be said about this simplification later in this thesis. For now, we will outline some facts about Puiseux series and make some brief comments about the role of Puiseux expansions in determining integral elements. For proofs of these facts, the reader can consult [Ribenboim].

Proposition 6 *Let K be an arbitrary field, and let $K[[X]]$ be the ring of formal power series in the indeterminate X with coefficients from K. Then $K((X))$, the field of fractions of $K[[X]]$, is equal to the field consisting of all Laurent power series $\sum_{i \geq i_0} a_i X^i$ for any $i_0 \in \mathbb{Z}$ and $a_i \in K$.*

Proposition 7 *Let K be an arbitrary field, and let X be an indeterminate. Then $\bigcup_{n=1}^{\infty} K\left(\left(X^{\frac{1}{n}}\right)\right)$ is a field.*

Definition 8 *An element of the field $\bigcup_{n=1}^{\infty} K\left(\left(X^{\frac{1}{n}}\right)\right)$ is called a* Puiseux series.

Proposition 9 *$\bigcup_{n=1}^{\infty} K\left(\left(X^{\frac{1}{n}}\right)\right)$ is an algebraic extension of $K((X))$.*

Proposition 10 *If K is an algebraically closed field of characteristic zero, then $\bigcup_{n=1}^{\infty} K\left(\left(X^{\frac{1}{n}}\right)\right)$ is the algebraic closure of $K((X))$.*

In [Hoeij], a *Puiseux expansion* is a zero of f in $\bigcup_{n=1}^{\infty} K\left(\left(X^{\frac{1}{n}}\right)\right)$. These Puiseux expansions are used to define valuations on L. A criterion for an element to be integral is that its image under each of these valuations must be nonnegative. In essence, a finite set of "candidates" to be included in the integral basis is given in terms of θ. Then θ is replaced by each Puiseux expansion, and the images of these elements under each valuation is computed. This process can be streamlined by setting up systems of equations involving "undetermined" coefficients of the negative powers of the "candidates" and comparing them with the coefficients of the negative powers of the Puiseux expansions. An important point made by Mark van Hoeij is that the Puiseux expansions usually have infinitely many terms. However, he is able to establish a suitable bound for finite "partial sums" of the Puiseux expansions to be used instead.

Instead of emphasizing Puiseux series approximations of the root θ, we will focus on modifying the polynomial f so that the root ψ of the modified polynomial and its powers will be an integral basis. However, in the process of recovering the normalization in terms

of θ, we will discover algebraic relations between θ, ψ, and the Puiseux expansions of f. Moreover, the "intermediate" polynomials that are introduced in our sequence from f down to the final polynomial have roots that are partial Puiseux expansions.

The algorithm that will be presented in this thesis proceeds along the lines of the Round 4 number field algorithm but employs different theoretical machinery to capture the information concerning ramification and the Puiseux expansions of f. It works under the hypotheses given initially. In particular, it can handle rings of arbitrary Krull dimension.

1.2 Heuristics of the Algorithm

In order to demonstrate the fundamental ideas behind the algorithm, we will consider a simplified example involving only fields. $Tr_{L/K}(x)$ and $N_{L/K}(x)$ denote the *trace* and *norm* of an element $x \in L$ over K, respectively. The notation extends in an obvious way to *subsets*.

Definition 11 *Let A be an integral domain with quotient field K, and let L be a finite, separable field extension of K. If B is an additive subgroup of L, then we define the* complementary set *B' of B by $B' = \{x \in L \mid Tr_{L/K}(xB) \subseteq A\}$.*

Observe that B' is an A-module whenever B is an A-module (the *complementary module* of B).

Proposition 12 (Lang, pp. 58 - 59) *Let A be an integral domain with field of fractions K, and let $L = K(\theta)$ be a finite, separable field extension. Let f be the irreducible polynomial of θ over K, and let f' be its derivative. Suppose further that $f \in A[X]$ and that $B = A[\theta]$. Then $B' = \frac{B}{f'(\theta)}$, the B-fractional ideal of L generated by $\frac{1}{f'(\theta)}$.*

In the setting of the proposition, we find that the normalization of A in L is the same as that of B in L. This fact follows since B is an integral extension of A and the relation of integral closure is transitive. We denote this common normalization by $\widetilde{B}$. If $x \in \widetilde{B}$, then $xB \subseteq \widetilde{B}$. Since the trace of an element of L equals (up to sign) a coefficient of its minimal polynomial, it follows that $Tr_{L/K}(xB) \subseteq A$. So, we have obtained the following A-module bounds for $\widetilde{B}$: $B \subseteq \widetilde{B} \subseteq B'$.

Let d_θ be the *discriminant* of the polynomial f. (When there is potential for ambiguity, we will write $disc(f, X)$ instead of d_θ). Then $d_\theta = \pm N_{L/K}(f'(\theta))$. Since it is often easier to compute d_θ than $N_{L/K}(f'(\theta))$, we substitute these quantities whenever the change in sign is not important as in the following remark.

Remark 1 *By combining the proposition with the inclusion relations $B \subseteq \widetilde{B} \subseteq B'$, we see that $B = \widetilde{B}$ if $f'(\theta)$ is a unit in B. Moreover, $f'(\theta)$ is a unit in B iff d_θ is a unit in A.*

The broad idea of our approach is to iteratively transform the polynomial f so that the following occurs:

- $\widetilde{B}$ can be recovered from the normalization of A relative to the algebra defined by adjoining a root of the transformed polynomial.

- the discriminant of each transformed polynomial is "closer" to being a unit in A.

Example 13 *Using the notation that has been established, let* $A := \mathbb{Q}[t]$ *and* $f := X^2 - t^2 - t^3$. *Then* $d_\theta = 4t^2(1+t)$ *is not a unit in* A. *In the next chapter, we will discuss how to replace the ring* A *by appropriate complete discrete valuation rings that arise from localizations at height* 1 *primes of* A. *In this example, only one replacement is necessary, and the coefficient ring becomes* $A^* := \mathbb{Q}[[t]]$. *We note that* $K^* := \mathbb{Q}((t))$ *and* $L^* := K^*[X]/(f)$ *are introduced at this point as the obvious replacements for* K *and* L, *respectively. Based on consideration of the Newton Polygon for* f *(also to be discussed in the next chapter), we can predict that* f *has two roots of order 1 with respect to the uniformizing parameter* t *of* A^*. *Thus, we transform* f *by substituting* $X = tT$ *to get* $f = t^2 f_1$, *where* $f_1 = T^2 - 1 - t$. *Observe that*

$$K^*[X]/(f) = K^*[tT]/(t^2 f_1) = K^*[T]/(f_1).$$

So, $L^* \cong K^*[\psi_1]$, *where* ψ_1 *is the canonical root of* f_1 *in* $K^*[T]/(f_1)$. *From* $X = tT$, *we get the relation* $\psi_1 = \frac{\theta}{t}$. *Since* $d_{\psi_1} = 4 + t$ *is a unit in* A^*, *the normalization of* A^* *in* $K^*[\psi_1]$ *is* $A^*[\psi_1]$. *By back substitution, the normalization of* A *in* L *is* $A\left[\frac{\theta}{t}\right]$. *Alternatively, it is the* A*- module generated by* $\left\{1, \frac{\theta}{t}\right\}$.

However, the broad idea stated previously is loaded with technical obstacles! For an arbitrary Noetherian, unique factorization domain, it is not obvious how to measure how "close" an element is to being a unit. Example 13 features a replacement of the coefficient ring with a DVR. In such a ring, we can consider the *order* of an element with respect to a uniformizing parameter. We know that the element is a unit iff its order is 0. Then the issue becomes that of transforming the polynomial to bring the order of the corresponding discriminant down to 0. In the case of a *complete* DVR, the theory of Newton Polygon factorizations will allow us to achieve the polynomial transformations. But we still have to recover $\widetilde{B}$ from the normalization relative to the final transformed polynomial. Unlike the situation in Example 13, we will usually find that the iterative normalizations are *not* isomorphic. Several computational issues arise from this consideration. See below for an example that illustrates some of these nuances. Finally, after each of these "iterative" obstacles are ironed out, there remains the fact that we have only negotiated a clear path in the case of a complete DVR! Fortunately, as alluded to in Example 13, some facts and identifications from commutative algebra allow us to reduce the problem to this case in a relatively painless manner.

Example 14 *Continuing with the established notation, let* $A := \mathbb{Q}[t]$ *and* $f := X^2 - t^2X - t^3$. *Then* $d_\theta = t^3(4+t)$ *is not a unit in* A. *As in Example 13, we replace the coefficient ring* A *by* $A^* := \mathbb{Q}[[t]]$ *and introduce* K^* *and* L^*. *From the Newton Polygon for* f, *we deduce that* f *has two roots of order* $\frac{3}{2}$ *with respect to the uniformizing parameter* t *of* A^*. *We transform* f *by substituting* $X = t^{\frac{3}{2}}T$ *to get* $f = t^3 f_1$, *where*

$f_1 = T^2 - t^{\frac{1}{2}}T - 1$. *Observe that*

$$K^*[X]/(f) = K^*\left[t^{\frac{3}{2}}T\right]/(t^3 f_1) = K^*\left[t^{\frac{1}{2}}T\right]/(f_1) \subsetneq K^*\left[t^{\frac{1}{2}}\right][T]/(f_1).$$

So, the coefficient field K^* *has to be "enlarged" to* $K^*\left[t^{\frac{1}{2}}\right] = \mathbb{Q}\left(\left(t^{\frac{1}{2}}\right)\right)$ *to accommodate the iterated normalization. Moreover,* $L^* \ncong K^*\left[t^{\frac{1}{2}}\right][\psi_1]$, *where* ψ_1 *is the canonical root of* f_1 *in* $K^*\left[t^{\frac{1}{2}}\right][T]/(f_1)$. *However,* $d_{\psi_1} = 4+t$ *is a unit in* $A^*\left[t^{\frac{1}{2}}\right]$. *So, the normalization of* $A^*\left[t^{\frac{1}{2}}\right]$ *in* $K^*\left[t^{\frac{1}{2}}\right][\psi_1]$ *is* $A^*\left[t^{\frac{1}{2}}\right][\psi_1]$. But the relationship of this normalization to $\widetilde{B}$ is not clear! We will return to this example later ... .

Chapter 2

Reduction to the Case of a Complete DVR

2.1 Commutative Algebra Results

There are several results from Commutative Algebra that are used to justify various computational aspects of our algorithm. In this section, we collect these facts for future reference. The following statement is a generalization of Proposition 12 from Chapter 1.

Corollary 15 *Let A be an integral domain with field of fractions K, let $f \in A[X]$ be monic with no repeated roots in an algebraic closure of K, and let θ be the canonical root of f in the ring extension $L = K[X]/(f)$. Suppose that $B = A[\theta]$, that $f = \prod_{i=1}^{h} f_i$ where $\{f_i\}_{i=1}^{h} \subset A[X]$ is a set of monic irreducible polynomials that are pairwise relatively prime, and that $f', f_1', \ldots, f_h'$ are the derivatives of $f, f_1, \ldots, f_h$, respectively. If θ_i is the*

canonical root of f_i *in the field extension* $L_i = K[X]/(f_i)$, $B_i = A[\theta_i]$, *and* B_i' *is the complementary module of* B_i *in* L_i, *then the inverse image of* $\prod_{i=1}^{h} B_i'$ *under the canonical isomorphism* $L \cong \prod_{i=1}^{h} L_i$ *is contained in* $\frac{B}{f'(\theta)}$ *where* $B = A[\theta]$.

Corollary 16 *Let* A, B, f, K, *and* L *be as in Corollary 15, and set* $B' := \frac{B}{f'(\theta)}$ *and* $\overline{B'} := B'/B$. *Then* $Ann_B\left(\overline{B'}\right) = f'(\theta)B$ *and* $Ann_A\left(\overline{B'}\right) \supseteq N_{L/K}(f'(\theta))A$.

Proof. Observe that $B' = \frac{B}{f'(\theta)} \Rightarrow f'(\theta)c \in B$ for all $c \in B'$. So, it is clear that $Ann_B\left(\overline{B'}\right) \supseteq f'(\theta)B$. Moreover, if $r \in Ann_B\left(\overline{B'}\right)$, then it follows that $r\frac{1}{f'(\theta)} = \frac{r}{f'(\theta)} \in B$. So, $r \in f'(\theta)B$ and $Ann_B\left(\overline{B'}\right) \subseteq f'(\theta)B$. Thus, $Ann_B\left(\overline{B'}\right) = f'(\theta)B$. Now, note that $f'(\theta)$ is a factor of the element $N_{L/K}(f'(\theta)) \in A$. Thus, $N_{L/K}(f'(\theta))A \subseteq Ann_A(\overline{B'})$.

In the following two results, the "hat" denotes completion with respect to $J(A)$, the Jacobson radical of A.

Proposition 17 *Let* A *be a commutative, finitely generated integral domain over a field, and let* S *be a multiplicative subset of* A. *Then* $\left(A[\theta]'/A[\theta]\right)_S \simeq A_S[\theta]'/A_S[\theta]$ *and* $\left(\widetilde{A[\theta]}/A[\theta]\right)_S \simeq \widetilde{A_S[\theta]}/A_S[\theta]$. *Moreover,* $A_S\widehat{[\theta]'/A_S}[\theta] \simeq \widehat{A_S}[\theta]'/\widehat{A_S}[\theta]$ *and* $\widetilde{A_S[\theta]/A_S}[\theta] \simeq \widetilde{\widehat{A_S}[\theta]/\widehat{A_S}}[\theta]$.

Proof. To prove the isomorphisms involving localization at S, we need only observe that localization is exact and preserves both complementary modules and integral closures. The isomorphisms involving completions are proven using analogous properties.

Proposition 18 *Let A be a semi-local Dedekind domain, and let B, f, K, and L be as above. Then $\widehat{B'/B} = B'/B$.*

Proof. We first note that B'/B is a finitely generated A-module. Next, we see from Corollary 16 that the nontrivial ideal $I = d_\theta A \subseteq Ann_A(B'/B)$. Since A is a semi-local Dedekind domain, the ideal I is a product of finite powers of the maximal ideals of A. Thus, it is clear that I and hence, $Ann_A(B'/B)$, contain sufficiently high powers of $J(A)$. Suppose that $J(A)^n \subset Ann_A(B'/B)$. Because ideals of $A/J(A)^n$ are in one-to-one correspondence with ideals of A containing $J(A)^n$ and ideals of A have unique decompositions as products of powers of maximal ideals of A, it follows that $A/J(A)^n$ is an Artinian ring. As $B'/B \cong F/N$, where F is a finite direct sum of copies of $A/J(A)^n$ and N is a submodule of F, it follows that B'/B is an Artinian module. The punchline is that finitely generated Artinian modules are complete! This follows because there is a sufficiently high power of $J(A)$ that annihilates each generator. In particular, all limits of Cauchy sequences from B'/B are in B'/B since the tail end of each such sequence becomes constant. Thus, the completion has no additional elements; so, $\widehat{B'/B} = B'/B$.

We will now state a few results (mostly without proof) concerning integrality, valuation rings, complete DVRs, and normality.

Proposition 19 *Let A, B, and C be commutative rings such that $A \subset B \subset C$. If B is integral over A and C is integral over B, then C is integral over A.*

Proposition 20 *Let A, R, R_1, ... , R_n be commutative rings such that $A \subset R$, $A \subset R_i$ for $1 \leq i \leq n$, and $R \cong R_1 \times ... \times R_n$ via an isomorphism for which the image of A is componentwise inclusion. Then the integral closure of A in R is isomorphic to the direct product of the integral closures of A in R_i for $1 \leq i \leq n$.*

Proof. Clearly, the integral closure of the image of A in $R_1 \times \ldots \times R_n$ is isomorphic to the integral closure of A in R. We will complete the proof by showing that it is also isomorphic to the direct product of the integral closures of A in R_i for $1 \leq i \leq n$. Suppose $(r_1, \ldots, r_n)$ is integral over the image of A. Then each r_i is integral over A. Conversely, suppose that $f_i(x) \in A[x]$ are monic polynomials for which $f_i(r_i) = 0$ for $1 \leq i \leq n$. Set $f(x) = \prod_{i=1}^{n} f_i(x)$. Then $(r_1, \ldots, r_n)$ is integral over the image of A since each component is a root of $f(x)$.

Proposition 21 *A valuation ring is integrally closed.*

Proposition 22 *Let K be a field, $A \subset K$ a subring, and let B be the integral closure of A in K. Then B is the intersection of all the valuation rings of K containing A.*

Theorem 23 *Let A be a normal Noetherian domain. Then we have*

i. all the prime divisors of a nonzero principal ideal have height 1;

ii. $A = \cap_{ht\mathfrak{p}=1} A_{\mathfrak{p}}$.

Theorem 24 *Let A be a Noetherian domain. The following two conditions are necessary and sufficient for A to be normal:*

a. *for $\mathfrak{p}$ a height 1 prime ideal, $A_{\mathfrak{p}}$ is a DVR;*

b. *all the prime divisors of a nonzero principal ideal of A have height 1.*

Proposition 25 *Let A be a complete DVR, and let π be the uniformizing parameter of A. For each positive integer m, the extension ring $A[\pi^{\frac{1}{m}}]$ of A is a complete DVR with uniformizing parameter $\pi^{\frac{1}{m}}$.*

Theorem 26 (Artin) *Let A be a complete DVR, and let $f \in A[X]$ be monic. If $f_1 \equiv f \bmod \delta^2\mathfrak{m}$ where δ is the discriminant of f and $\mathfrak{m}$ is the maximal ideal of A, then $A[X]/(f) \cong A[X]/(f_1)$.*

If ν is a non-Archimedean additive valuation on a field K, we will let R_ν denote the valuation ring of ν and $\mathfrak{m}_\nu$ its maximal ideal. In particular, $R_\nu = \{x \in K : \nu(x) \geq 0\}$ and $\mathfrak{m}_\nu = \{x \in K : \nu(x) > 0\}$.

Theorem 27 (see Weiss, 2-2-10) *Suppose F is a field that is complete with respect to a non-Archimedean additive valuation ν, and let E/F be a finite extension of degree n. Then*

a. *ν has a unique extension to a non-Archimedean additive valuation $\widetilde{\nu}$ on E.*

b. *ν is discrete if and only if $\widetilde{\nu}$ is discrete.*

c. *$R_{\widetilde{\nu}}$ is the integral closure of R_ν in E.*

We now state and prove our main result, which allows us to perform an algebraic descent in the algorithm.

Theorem 28 *Let A be a complete DVR with uniformizing parameter π and field of fractions K. For each positive integer m, let $A_m := A\left[\pi^{\frac{1}{m}}\right]$ and let K_m be its field of fractions. Let $f \in A[X]$ be a monic polynomial of degree n that has no repeated roots in an algebraic closure of K, and let θ be the canonical root of f in the ring extension $L = K[X]/(f) = K[\theta]$. If $\mathfrak{B}_m = \{\beta_1, \ldots, \beta_n\} \subset K_m[\theta]$ is an A_m-basis of $\widetilde{A_m[\theta]}$ and there exist nonnegative integers $a_i < m$ such that $\pi^{\frac{a_i}{m}}\beta_i \in K[\theta]$ for $1 \leq i \leq n$, then each a_i is unique and $\mathfrak{B} = \left\{\pi^{\frac{a_1}{m}}\beta_1, \ldots, \pi^{\frac{a_n}{m}}\beta_n\right\} \subset K[\theta]$ is an A-basis of $\widetilde{A[\theta]}$.*

Proof Suppose that for some integer i such that $1 \leq i \leq n$ there exist integers c_i and d_i such that $0 \leq c_i < d_i < m$ and $\pi^{\frac{c_i}{m}}\beta_i$ and $\pi^{\frac{d_i}{m}}\beta_i$ are both in $K[\theta]$. Then we obtain the contradiction that the element $\pi^{\frac{d_i-c_i}{m}}\pi^{\frac{c_i}{m}}\beta_i = \pi^{\frac{d_i}{m}}\beta_i$ both belongs and does not belong to $K[\theta]$. So, the integers a_i are unique. Observe that a dependence relation among the elements of $\mathfrak{B}$ over K implies a dependence relation among the elements of $\mathfrak{B}_m$ over K_m, and hence over A_m. Thus, $\mathfrak{B}$ is a K-basis of $K[\theta]$. Since $\mathfrak{B}_m$ is an A_m-basis of $\widetilde{A_m[\theta]}$, it follows that the elements of $\mathfrak{B}$ belong to $\widetilde{A[\theta]}$. Thus, the free A-module generated by the elements of $\mathfrak{B}$ is a submodule of $\widetilde{A[\theta]}$. To complete the proof, suppose that $a \in \widetilde{A[\theta]}$. Then $a = \sum_{i=1}^{n} b_i\beta_i$ where each $b_i \in A_m$. Each term can be written as $\frac{b_i}{\pi^{\frac{a_i}{m}}}\left(\pi^{\frac{a_i}{m}}\beta_i\right)$, so a is a linear combination of the elements of $\mathfrak{B}$ with coefficients from K_m. Since $\mathfrak{B}$ is a K-basis of $K[\theta]$ and also linearly independent over K_m, it follows that $\frac{b_i}{\pi^{\frac{a_i}{m}}} \in K$. Since b_i has nonnegative order

relative to π and $\frac{a_i}{m} < 1$, we deduce that the order of $\frac{b_i}{\pi^{\frac{a_i}{m}}}$ relative to π is an integer greater than -1. Thus, $\frac{b_i}{\pi^{\frac{a_i}{m}}} \in A$. So, $\mathfrak{B}$ is an A-basis of $\widetilde{A[\theta]}$ in $K[\theta]$.

2.2 Newton Polygon Factorizations

Over a complete DVR, there is a relationship between the roots of a polynomial and the slopes of the line segments from an associated polygon. In this section, we state this result as well as a substitution formula that will be used in the algorithm.

Definition 29 *Let A be a complete DVR with non-Archimedean additive valuation ν. Let $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$ with $a_0 a_n \neq 0$. The* ***Newton Polygon of f with respect to ν*** *is defined to be the lower convex envelope of the set of points $S = \{(i, \nu(a_i)) \mid i = 0, \ldots, n\}$.*

Example 30 *Consider the polynomial $f := X^7 - tX^4 + t^3 \in \mathbb{Q}[[t]][X]$. With respect to the additive valuation defined by powers of the maximal ideal (t), the Newton Polygon of f has vertices at the points $(0,3), (4,1)$, and $(7,0)$. See Figure 1. Note that the slopes of the two line segments are $m = -\frac{1}{2}$ and $m = -\frac{1}{3}$. Also observe that the slopes of the segments increase from left-to-right. This fact occurs because of the convexity condition on the polygon.*

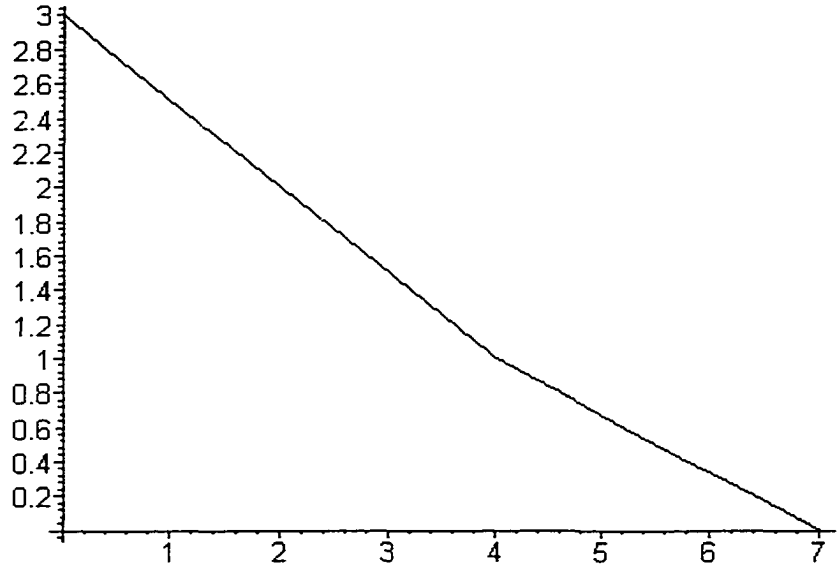

Figure 1

Theorem 31 *Suppose K is a field that is complete with respect to a non-Archimedean additive valuation ν. Let $f \in K[X]$ be as above. Suppose that $(r, \nu(a_r)) \leftrightarrow (s, \nu(a_s))$ is a line segment on the Newton Polygon of f with respect to ν with slope $-m$. Then there are precisely $s - r$ roots $\alpha_1, \alpha_2, \ldots, \alpha_{s-r}$ of f with the property that $\nu(\alpha_1) = \nu(\alpha_2) = \cdots = \nu(\alpha_{s-r}) = m$. Moreover, $\prod_{i=1}^{s-r}(X - \alpha_i) \in K[X]$, and this product divides f.*

Example 32 *Continuing to examine the polynomial from Example 30, we conclude that it has 4 roots α_i with the property that $\nu(\alpha_i) = \frac{1}{2}$ and 3 roots β_j with the property that $\nu(\beta_j) = \frac{1}{3}$. Moreover, we also can conclude that this polynomial can be factored over $\mathbb{Q}[[t]]$. Of course, its roots do not lie in the field of fractions of $\mathbb{Q}[[t]]$ since the orders are not integers. Instead, they lie in some extension field. The fractional orders tell us the ramification of the prime (t) in a minimal extension of $\mathbb{Q}[[t]]$ containing the roots. If we make the substitution $X = t^{\frac{1}{3}}T$, our polynomial becomes $f = t^{\frac{7}{3}}\left(T^7 - T^4 + t^{\frac{2}{3}}\right)$.*

The polynomial $f_1 := T^7 - T^4 + t^{\frac{2}{3}} \in \mathbb{Q}\left[\left[t^{\frac{1}{3}}\right]\right][T]$ *has Newton Polygon with vertices at the points* $(0,2), (4,0)$, *and* $(7,0)$. *See Figure 2. In contrast to Figure 1, the right-most line segment has been tilted onto the horizontal axis. Over the extension ring* $\mathbb{Q}\left[\left[t^{\frac{1}{3}}\right]\right]$, *there are* 4 *roots of order* $\frac{1}{2}$ *and* 3 *roots of order* 0.

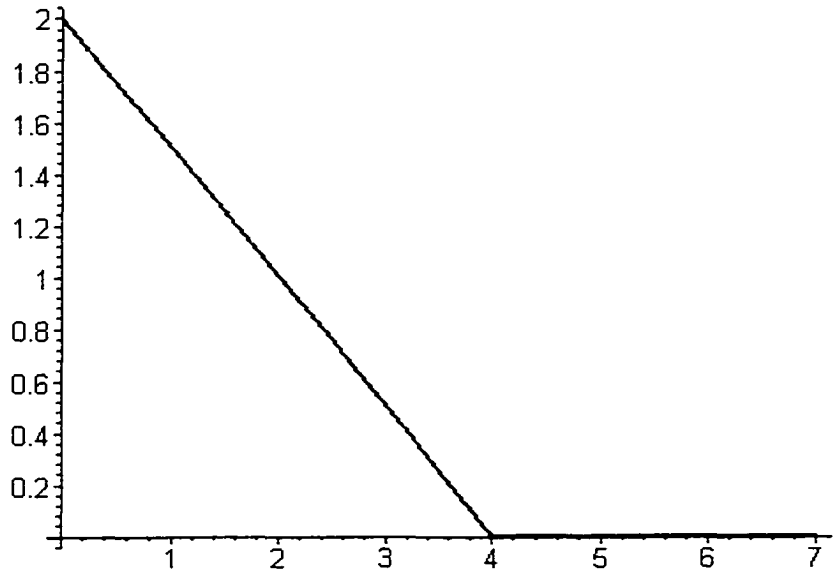

Figure 2

The following proposition shows that the phenomena of the tilting of the right-most line segment to the horizontal axis upon an appropriate variable substitution observed in Figures 1 and 2 holds in general. In particular, a polynomial with some unit roots is obtained by this process.

Proposition 33 *Let A be a complete DVR with uniformizing parameter π. Let $f \in A[X]$ be a monic polynomial of degree N with no unit roots. Let $-m$ be the slope of the right-most line segment in the Newton Polygon for f. Then upon substituting $X = \pi^m T$ into f, where $m = \frac{k}{l}$ in reduced form, we obtain $f = \pi^{mN} f_1$ where $f_1 \in A\left[\pi^{\frac{1}{l}}\right][T]$ has unit roots over $A\left[\pi^{\frac{1}{l}}\right]$. Moreover, the number of unit roots is the length of the horizontal projection of the right-most line segment from the Newton Polygon for f. Finally, $disc(f, X) = \pi^{mN(N-1)} disc(f_1, T)$.*

Proof. Suppose $f = a_0 + a_1 X + a_2 X^2 + \cdots + X^N$. Upon substituting $X = \pi^m T$ into f, we obtain $f = a_0 + a_1 \pi^m T + a_2 \pi^{2m} T^2 + \cdots + \pi^{mN} T^N = \pi^{mN} f_1$ where $f_1 = a_0 \pi^{-mN} + a_1 \pi^{-m(N-1)} T + a_2 \pi^{-m(N-2)} T^2 + \cdots + a_{N-1} \pi^{-m} T^{N-1} + T^N$. Since $m = \frac{k}{l}$ in reduced form, we observe that $f_1 \in A\left[\pi^{\frac{1}{l}}\right][T]$. By working backwards along the Newton Polygon for f, we observe that the order of a_j with respect to π is at least $m(N-j)$. Moreover, it is strictly greater than $m(N-j)$ precisely when j is not an abscissa of the right-most line segment. In this case, the coefficient of T^j has positive order. However, the order of a_j with respect to π is exactly $m(N-j)$ precisely when j is an abscissa of the right-most line segment. In this case, the coefficient of T^j has order 0. Thus, f_1 has unit roots over $A\left[\pi^{\frac{1}{l}}\right]$, and the number of unit roots is the length of the horizontal projection of the right-most line segment from the Newton Polygon for f by virtue of Theorem 31. To prove the final statement, suppose that $r_1, r_2, \ldots, r_N$ are the roots of f and that $ord(r_i) = e_i$ relative to π for $1 \leq i \leq N$. So, for each i, $r_i = u_i \pi^{e_i}$ where u_i is a unit. Since

$X = \pi^m T$, observe that the roots of f_1 are $\pi^{-m} r_i = u_i \pi^{e_i - m}$ for $1 \leq i \leq N$. Thus,

$$disc(f, X) = \prod_{1 \leq i < j \leq N} (r_i - r_j)^2 = \prod_{1 \leq i < j \leq N} (u_i \pi^{e_i} - u_j \pi^{e_j})^2$$
$$= \prod_{1 \leq i < j \leq N} \pi^{2m} (u_i \pi^{e_i - m} - u_j \pi^{e_j - m})^2 = \pi^{2m\binom{N}{2}} \prod_{1 \leq i < j \leq N} (u_i \pi^{e_i - m} - u_j \pi^{e_j - m})^2$$
$$= \pi^{mN(N-1)} disc(f_1, T).$$

2.3 Passing from DVRs to Complete DVRs and Recovering $\widetilde{B}$

We now return to the general setting. If A, f, θ, K, and L are as given in Chapter 1 and if $B = A[\theta]$, then our overall strategy for the computation of the normalization of A in L can be described with the following steps:

1. Since A is a unique factorization domain, it is normal. So, by Corollary 15 and Proposition 20, we have $B \subseteq \widetilde{B} \subseteq B'$. We will seek to identify $\widetilde{B}/B \subseteq B'/B$ since it is clear that coset representatives of $\widetilde{B}$ relative to B completely specify $\widetilde{B}$ as a B-module. We will search locally, using primes $\mathfrak{p}$ of A of height 1, for $(\widetilde{B}/B)_{\mathfrak{p}} \subseteq (B'/B)_{\mathfrak{p}}$.

2. Since $(B')_{\mathfrak{p}} = \frac{B_{\mathfrak{p}}}{f'(\theta)}$ from Proposition 17, we have $\widetilde{B}_{\mathfrak{p}} = B_{\mathfrak{p}}$ whenever $f'(\theta)$ is a unit in $B_{\mathfrak{p}}$. Since $f'(\theta)$ is a unit in $B_{\mathfrak{p}}$ whenever d_θ is a unit in $A_{\mathfrak{p}}$, we have the local normalization if $\mathfrak{p}$ is a prime of A of height 1 that does not contain d_θ.

3. At primes $\mathfrak{p}$ of A of height 1 which contain d_θ, we note that $(B'/B)_{\mathfrak{p}} = \widehat{A_{\mathfrak{p}}}[\theta]'/\widehat{A_{\mathfrak{p}}}[\theta]$ by first using Proposition 17 and then using Proposition 18.

4. Our ground ring is now reduced to the complete DVR $\widehat{A_{\mathfrak{p}}}$. So, we may now

complete the computation for this local piece by using the procedure in Chapter 3.

5. Finally, $\widetilde{B} = \bigcap \widetilde{B}_{\mathfrak{p}}$ as $\mathfrak{p}$ ranges over all the height 1 primes of A by Theorem 23**ii.**

Before moving to the technical inner workings of the algorithm in Chapters 3 and 4, it is useful to outline briefly the supporting theoretical framework for the computation mentioned in step **4.** We know that L is a direct product of fields L_i, each of which is a finite separable extension of K. By Proposition 20, our computation is further reduced to this field case. By Theorem 27, the problem becomes that of identifying the elements of nonnegative order relative to a unique discrete valuation in the field L_i. The algorithm resolves this issue by first identifying the elements of nonnegative order relative to a unique discrete valuation in a finite extension of L_i obtained by introducing fractional powers of the uniformizing parameter for $\widehat{A_{\mathfrak{p}}}$. This finite extension of L_i is determined iteratively by modifying the polynomial f in various ways to be discussed. The key point is that each of the intermediate extensions computed iteratively is also complete with respect to a unique discrete valuation by Proposition 25. The integral basis in this finite extension of L_i consists of powers of the canonical root ψ of the final polynomial obtained. Then the desired elements of nonnegative order are found by intersecting back to L_i. This intersection computation is facilitated by iteratively applying Theorem 28 and performing suitable back substitutions through all the intermediate roots so that the powers of ψ are expressed as linear combinations of powers of θ. In fact, one is able to find the elements of nonnegative order in any intermediate subfield of this finite extension of L_i using this approach!

The procedure outputs module generators for each given local piece $\widetilde{B}_{\mathfrak{p}}$ that have denominators consisting solely of powers of the corresponding uniformizing parameter $\pi_{\mathfrak{p}}$. Because A is a unique factorization domain, the canonical pullback of $\pi_{\mathfrak{p}}$ in A has order 1 at $\mathfrak{p}$ and order 0 at each of the other height 1 primes. Since these powers are units in each of the other DVRs arising from localizing at the other primes, we can conclude that each local generator is in fact a module generator for $\widetilde{B}$ over A. Thus, the final intersection in step **5.** of the strategy is executed simply by taking the union of each of the sets of module generators obtained locally! As long as there is a mechanism for computing a prime factorization of the ideal (d_θ), one can proceed to identify the height 1 primes containing d_θ and use this localization strategy.

There is a simplification that can be made based on the following result.

Proposition 34 (Weiss, 3-7-15) *Suppose that* $\{\alpha_1, \ldots, \alpha_n\}$ *and* $\{\beta_1, \ldots, \beta_n\}$ *are bases for* L/K, *and let* $M = A\alpha_1 + \cdots + A\alpha_n$ *and* $N = A\beta_1 + \cdots + A\beta_n$. *Denote the discriminants of the modules* M *and* N *by* d_M *and* d_N, *respectively. If* $M \subset N$, *then* $\frac{d_M}{d_N}$ *is the square of an element of* A. *Moreover,* $M = N$ *if and only if* $\frac{d_M}{d_N}$ *is a unit of* A.

In particular, suppose that $\mathfrak{p}$ is a prime ideal of A of height 1 that appears in the prime factorization of (d_θ) with multiplicity exactly 1. We set $M := B_{\mathfrak{p}}$, $N := \widetilde{B}_{\mathfrak{p}}$ and apply Proposition 34 over the DVR $A_{\mathfrak{p}}$. Since $\frac{d_M}{d_N}$ is a unit of $A_{\mathfrak{p}}$, it follows that $\widetilde{B}_{\mathfrak{p}} = B_{\mathfrak{p}}$. So, it is only necessary to use the procedure in Chapter 3 to compute $\widetilde{B}_{\mathfrak{p}}$ for those primes $\mathfrak{p}$ of A of height 1 that appear in the prime factorization of (d_θ) with multiplicity at least 2.

Three examples are presented in Chapter 5 for the enjoyment of the reader. The first example illustrates the process of algebraic descent with an elementary usage of Theorem 28. The second example provides a comprehensive investigation of the computation of 1 local normalization. The final example demonstrates the algorithm in its fullest generality by featuring a ground ring A of Krull dimension 2 with computations of 2 local normalizations and a final intersection according to the discussion above.

Chapter 3

The Algorithm Over a Complete DVR

3.1 The Subroutines

Throughout this chapter, A is a complete DVR with uniformizing parameter π and field of fractions K. We will denote the residue field $A/(\pi)$ by $\overline{A}$. We begin by establishing some terminology.

Definition 35 *Let R be a commutative ring. The monic polynomial $f \in R[X]$ is* ***separable over*** *R if no image $\varphi(f)$, relative to a homomorphism φ from R to a field k, has repeated roots in an algebraic closure $\overline{k}$ of k.*

Definition 36 *Let R be an integral domain, and let S be an integral extension of R.*

a. *$s \in S$ is* ***separable over*** *R if its minimal polynomial over R is separable over R.*

b. *S is a* ***separable extension of*** *R if $R \subset S$ and each $x \in S$ is separable over R.*

c. *The* ***separable closure*** *of R in S is the largest separable extension of R contained in S.*

Definition 37 *Let E be a field, and let $f \in E[X]$. A* ***separable factorization*** *of f over E is a decomposition $f = F_1 F_2^2 \cdots F_l^l$ where l is a positive integer, each F_i is separable over E, and $\gcd(F_i, F_j) = 1$ whenever $i \neq j$. The integer l is called the* ***power degree*** *of f. Note that l only depends on f.*

We now present the subroutines used in the algorithm.

- **SepProd:** Given a polynomial $f \in A[X]$, this routine calculates a factorization $\overline{f} = \overline{F}^l \overline{G}$ over $\overline{A}$ where l is a positive integer, $\overline{F}$ is separable over $\overline{A}$, and $\gcd(\overline{F}, \overline{G}) = 1$. It also computes a corresponding "partition of unity"; i.e., it computes a decomposition $1 = e_1 + e_2$ for use with the Chinese Remainder Theorem.

  - **Input:** $f \in A[X]$ and N a positive integer.
  - **Output:** A factorization $\overline{f} = \overline{F}^l \overline{G}$ where l is a positive integer and $\overline{F}$ is separable over $\overline{A}$, $\overline{a}$, and $\overline{b}$ such that $\overline{a}\,\overline{F}^l + \overline{b}\,\overline{G} = 1$.

- **Hensel:** This routine pulls back a factorization into relatively prime factors through a nilpotent extension. It also pulls back a corresponding "partition of unity."

  - **Input:** A, N a positive integer, $f \in A[X]$, $\overline{a}, \overline{b}, \overline{g}, \overline{h} \in \overline{A}[X]$ such that $\overline{f} = \overline{g}\overline{h}$, $\overline{a}\,\overline{g} + \overline{b}\,\overline{h} = 1$, $\deg(\overline{a}) < \deg(\overline{h})$, and $\deg(\overline{b}) < \deg(\overline{g})$.

- **Output:** $g_1, h_1, a_1, b_1 \in \left(A \diagup (\pi)^N\right)[X]$ such that $f = g_1 h_1$ in $\left(A \diagup (\pi)^N\right)[X]$, $a_1 g_1 + b_1 h_1 = 1$ in $\left(A \diagup (\pi)^N\right)[X]$, $\overline{a_1} = \overline{a}$ in $\overline{A}[X]$, $\overline{b_1} = \overline{b}$ in $\overline{A}[X]$, $\overline{g_1} = \overline{g}$ in $\overline{A}[X]$, $\overline{h_1} = \overline{h}$ in $\overline{A}[X]$, $\deg(a_1) < \deg(h_1)$, and $\deg(b_1) < \deg(g_1)$.

- **Root:** This routine pulls back a root of a polynomial that is separable over $\overline{A}$ through a nilpotent extension.

  - **Input:** A separable polynomial $\overline{F} \in \overline{A}[X]$ and a positive integer N.

  - **Output:** $\overline{\eta} \in \overline{A}[X] \diagup \left(\overline{F}^N\right)$, a pullback of the canonical root of $\overline{F}$ in $\overline{A}[X] \diagup \left(\overline{F}\right)$ such that $\overline{F}(\overline{\eta}) = 0$ in $\overline{A}[X] \diagup \left(\overline{F}^N\right)$.

- **Extension:** This routine constructs the separable closure A_1 of A in $\left(A \diagup \left(\pi^M\right)\right)[\theta]$ when $\overline{f} = \overline{F}^N$ for some nonlinear separable polynomial $\overline{F}$ such that $\overline{F}(0) \neq 0$.

  - **Input:** A, $f \in A[X]$, positive integers M and N, and a separable polynomial $\overline{F} \in \overline{A}[X]$ such that $\overline{f} = \overline{F}^N$ and $\overline{F}(0) \neq 0$.

  - **Output:** $A_1 := \left(A \diagup \left(\pi^M\right)\right)[\eta] \subset \left(A \diagup \left(\pi^M\right)\right)[\theta]$ with $\overline{A_1} = \overline{A}[\overline{\eta}] \subset \overline{A}\left[\overline{\theta}\right]$ (where $\overline{\eta}$ is obtained from Root and θ is a root of f) and a new $f_1 \in A_1[X]$ such that $A_1[X] \diagup (f_1) \cong \left(A \diagup \left(\pi^M\right)\right)[X] / (f)$ with $\overline{f_1} = (X - \overline{\eta})^N$.

- **Substitution:** This routine implements Proposition 33.

  - **Input:** $f \in A[X]$ where f is monic of degree N and has no unit roots and a rational number $-m$ with $m = \frac{k}{l}$ in reduced form that represents the slope of the right-most line segment in the Newton Polygon for f.

- **Output:** $f_1 \in A\left[\pi^{\frac{1}{l}}\right][T]$, a polynomial with unit roots over $A\left[\pi^{\frac{1}{l}}\right]$ such that $disc\,(f, X) = \pi^{mN(N-1)} disc\,(f_1, T)$.

3.2 The Algorithm

- **Input:** A and a monic polynomial $f \in A[X]$ with no repeated roots in an algebraic closure of K.

- **Output:** $\widetilde{B}$, the integral closure of A in $L = K[X] \diagup (f)$.

The procedure starts by applying *SepProd* to f to obtain a factorization of $\overline{f}$ as $\overline{F}^l \overline{G}$ where $\overline{F}$ is separable over $\overline{A}$, l is a positive integer, and $\gcd\left(\overline{F}, \overline{G}\right) = 1$. It also provides elements $\overline{a}, \overline{b} \in \overline{A}[X]$ such that $\overline{a}\overline{F}^l + \overline{b}\,\overline{G} = 1$ where $\deg\left(\overline{a}\right) < \deg\left(\overline{G}\right)$ and $\deg\left(\overline{b}\right) < \deg\left(\overline{F}^l\right)$. The subroutine *Hensel* is applied to the outputs of *SepProd* to obtain a factorization $F_1 G_1$ where $f - F_1 G_1 \in (\pi d_\theta^2)$, $F_1 - \overline{F}^l \in (\pi)$, and $G_1 - \overline{G} \in (\pi)$. It also finds elements $a_1, b_1 \in \left(A \diagup (\pi d_\theta^2)\right)[X]$ such that $a_1 F_1 + b_1 G_1 - 1 \in (\pi d_\theta^2)$, $a_1 - \overline{a} \in (\pi)$, and $b_1 - \overline{b} \in (\pi)$.

By Theorem 26, we can replace f with $F_1 G_1$. Over the ring $\left(A \diagup (\pi d_\theta^2)\right)[X]$, we have $a_1 F_1 + b_1 G_1 = 1$. So, we can apply the *Chinese Remainder Theorem* to decompose $\left(A \diagup (\pi d_\theta^2)\right)[X] \diagup (F_1 G_1)$ isomorphically to the direct product $\left(A \diagup (\pi d_\theta^2)\right)[X] \diagup (F_1) \times \left(A \diagup (\pi d_\theta^2)\right)[X] \diagup (G_1)$. We remark that by Corollary 16, the ideal $(\pi d_\theta^2) \subset (d_\theta)$ of A annihilates B'/B. So, we may pass back and forth abstractly between the rings A and $A \diagup (\pi d_\theta^2)$. Thus, by Proposition 20, $\widetilde{B} \cong \widetilde{B}e_1 \times \widetilde{B}e_2$ where $e_1 = b_1 G_1$, $e_2 = a_1 F_1$, $\widetilde{B}e_1$

is isomorphic to the integral closure of A in $K[X]/(F_1)$, and $\widetilde{B}e_2$ is isomorphic to the integral closure of A in $K[X]/(G_1)$.

Thus, the computation of $\widetilde{B}$ is reduced to the computation of the integral closures in the subalgebras since the idempotents e_1 and e_2 are in hand. The factor involving G_1 will be handled initially in the same way as our original f since $\overline{G}$ is not in general separable over $\overline{A}$. The factor involving F_1 is canonical, and we will now analyze the case $\overline{F_1} = \overline{F}^l$ with $\overline{F}$ separable over $\overline{A}$ in detail.

- **Case 1.** $l = 1$.

  Since the roots are distinct at the residue field level, we find that d_θ is a unit in A. Thus, $\widetilde{B} = B$ by Remark 1.

- **Case 2.** $l \neq 1$.

  We split this case into two subcases:

  - **Case 2A.** $\overline{F_1} = \overline{F}^l$ and $\overline{F}(0) \neq 0$.

    In order to introduce a linear factor we apply the subroutines *Root* and *Extension* which together produce a new $\overline{A_1} = \overline{A}[\overline{\eta}]$ where $\overline{F}(\overline{\eta}) = 0$, a lift $A_1 \subset (A/(\pi d_\theta^2))[\theta]$ of $\overline{A_1}$, and a new $\widetilde{F_1} \in A_1[X]$ such that $A_1[X]/\left(\widetilde{F_1}\right) \cong (A/(\pi d_\theta^2))[X]/(F_1)$ and $\widetilde{\overline{F_1}} = (X - \overline{\eta})^l$. Now set $X := X - \overline{\eta}$ to convert to Case 2B.

– **Case 2B.** $\overline{F_1} = X^l$.

We apply *Substitution* to get a new polynomial $\widetilde{F_1}$ with at least one unit root after removing a factor corresponding to an appropriate power of the uniformizing parameter.

Each time a pass through Case 2B occurs, we immediately compute the integral closure in each subalgebra corresponding to a pullback of a separable factor of the resulting $\widetilde{\widetilde{F_1}}$. The computation involving the other factors either iterates Case 2B or else involves Case 2A. Note the repeated uses of *SepProd* and *Hensel* as per the discussion about the original f. It is important to observe that each application of the subroutine *Substitution* produces an output polynomial $\widetilde{F_1}$ with coefficients that belong to a potentially larger ring than $A[\theta]$ because of the fractional exponent on the parameter π. Proposition 25 ensures that the ground ring remains a complete DVR. Moreover, the idempotents that are introduced by the algorithm after each pass through Case 2B will always lie in $K[\theta]$. This fact will be justified in Section 4.2. Finally, we are able to algebraically descend the integral closures to subalgebras of $\widetilde{B}$ by using Theorem 28. This manouver can always be accomplished because we can always identify suitable powers of the parameter π that will multiply each generator of the integral closure obtained at the end of the process and yield a product that belongs to $\widetilde{B}$.

To see this more clearly, suppose that θ is the canonical root of F_1 and we find that the algorithm proceeds through three consecutive cycles of Case 2A followed by Case 2B. We will denote the respective translation elements $\overline{\eta}$ by η_1, η_2, and η_3, respectively, while

the fractions $\frac{a_1}{m_1}$, $\frac{a_2}{m_2}$, and $\frac{a_3}{m_3}$ will denote the powers of π arising from the monomial substitutions, respectively. Finally, we will let ψ_1, ψ_2, and ψ_3 denote the roots of the iterated polynomials, respectively. Then we obtain the following relations:

- $\psi_1 = \dfrac{\theta - \eta_1}{\pi^{\frac{a_1}{m_1}}}$
- $\psi_2 = \dfrac{\psi_1 - \eta_2}{\pi^{\frac{a_2}{m_2}}} = \dfrac{\frac{\theta - \eta_1}{\pi^{\frac{a_1}{m_1}}} - \eta_2}{\pi^{\frac{a_2}{m_2}}} = \dfrac{\theta - \eta_1 - \eta_2 \pi^{\frac{a_1}{m_1}}}{\pi^{\frac{a_1}{m_1} + \frac{a_2}{m_2}}}$
- $\psi_3 = \dfrac{\psi_2 - \eta_3}{\pi^{\frac{a_3}{m_3}}} = \dfrac{\frac{\theta - \eta_1 - \eta_2 \pi^{\frac{a_1}{m_1}}}{\pi^{\frac{a_1}{m_1} + \frac{a_2}{m_2}}} - \eta_3}{\pi^{\frac{a_3}{m_3}}} = \dfrac{\theta - \eta_1 - \eta_2 \pi^{\frac{a_1}{m_1}} - \eta_3 \pi^{\frac{a_1}{m_1} + \frac{a_2}{m_2}}}{\pi^{\frac{a_1}{m_1} + \frac{a_2}{m_2} + \frac{a_3}{m_3}}}$

In each case, the denominator of ψ_j is a power of π. Each numerator is an element of the previous intermediate ring. By iteratively applying Theorem 28, we obtain the generators of the desired integral closure $\widetilde{B}$.

In Case 2B, the degree of the remaining polynomial drops if there is a separable factor of the transformed polynomial in the residue field. In Case 2A, either the degree of the extension drops when $\overline{F}$ is nonlinear or we obtain a polynomial that can be translated to one whose type belongs to Case 2B. Then, after an iteration of Case 2B, either the remaining polynomial has lower degree or else it admits an iteration involving Case 2A. The crucial point is that, in the *worst-case scenario* in which the procedure oscillates between Case 2A and Case 2B without a drop in either the degree of the extension or in the degree of the polynomial, there is a drop in the order of the discriminants of the iterated polynomials by Proposition 33. Thus, the oscillation will terminate with a final application of Case 2B that yields a polynomial with discriminant having order 0 or 1.

In general, each branch of this procedure stops whenever it reaches a polynomial f with discriminant having order 0 or 1.

Chapter 4

Theoretical Support for the Algorithm

4.1 Theoretical Basis for the Subroutines

We now present the proofs of the key propositions that support each of the subroutines discussed in Chapter 3. Our first result constructively justifies the *SepProd* subroutine over fields of characteristic 0. Recall that this subroutine calculates a factorization $\overline{f} = \overline{F}^{l}\overline{G}$ over $\overline{A}$ where l is a positive integer, $\overline{F}$ is separable over $\overline{A}$, and $\gcd\left(\overline{F}, \overline{G}\right) = 1$. By iterating *SepProd* on each resulting $\overline{G}$ polynomial, one eventually obtains a separable factorization of $\overline{f}$ over $\overline{A}$. The "partition of unity" is easily obtained from the *Euclidean Algorithm*.

Proposition 38 *Let F be a field of characteristic 0, and let $f \in F[X]$. Then there exist $g_1, g_2, \ldots, g_l$ in $F[X]$ such that*

a. *g_i is separable for $1 \leq i \leq l$;*

b. *$\gcd(g_i, g_j) = 1$ for $i \neq j$ and $1 \leq i, j \leq l$;*

c. *$f = g_1 g_2^2 \cdots g_l^l$;*

d. *$\gcd\left(g_i^i, \frac{f}{g_i^i}\right) = 1$ for $1 \leq i \leq l$.*

Proof. Since $F[X]$ is a unique factorization domain, it follows that $f = \prod_{i=1}^{k} p_i^{e_i}$ where each p_i is irreducible. Thus, $f' = \sum_{i=1}^{k} e_i p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_i^{e_i - 1} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k} p_i'$. Since $\gcd(p_i, p_i') = 1$, we observe that $\gcd(f, f') = \prod_{i=1}^{k} p_i^{e_i - 1}$. Thus, $\frac{f}{\gcd(f, f')} = \prod_{i=1}^{k} p_i$. We create a recursive process as follows: set $f_0 = f$, $f_1 = \gcd(f_0, f_0')$, $f_2 = \gcd(f_1, f_1'), \ldots$, $f_{i+1} = \gcd(f_i, f_i'), \ldots$. We have just seen that $\frac{f_0}{f_1} = \prod_{i=1}^{k} p_i$. Since f_1 is the same product as f_0 with all of the exponents lowered by 1, we have $\frac{f_1}{f_2} = \prod_{e_i \geq 2} p_i$. Continuing in this fashion, we deduce that $\frac{f_j}{f_{j+1}} = \prod_{e_i \geq j+1} p_i$. We now compute $f_0, f_1, \ldots$ until we come to the smallest integer l such that $f_l = 1$. From our construction, it follows that $l = \max\{e_1, \ldots, e_k\}$. Set $h_j = \frac{f_{j-1}}{f_j} = \prod_{e_i \geq j} p_i$ for $1 \leq j \leq l$ and $g_j = \frac{h_j}{h_{j+1}}$ for $1 \leq j \leq l$. Since the characteristic of F is 0, each g_j is separable over F for $1 \leq j \leq l$. Since $g_j = \prod_{e_i = j} p_i$ for $1 \leq j \leq l$, we have $f = g_1 g_2^2 \cdots g_l^l$. Finally, the statements about the greatest common divisors follow since the irreducibles are partitioned among the g_j factors.

We note, however, that separable factorizations over fields of characteristic p do not exist in general. For example, let $F = \mathbb{Z}_p(t)$. The polynomial $X^p - t \in F[X]$ is not separable over F. If b is a root of $X^p - t$ in some algebraic closure of F, then it is a repeated root since $X^p - t = X^p - b^p = (X - b)^p$. However, $X^p - t$ is irreducible over F. So, $X^p - t$ cannot possess a separable factorization over F.

Our next three results support the *Hensel* subroutine. The computational points necessary to consider for iterative usage of *Hensel* include making sure that the degree requirements on a and b relative to h and g, respectively, and the monicity requirements on g and h are satisfied. In this case, we are able to pull back through a sufficiently high power of 2 to arrive at the nilpotent extension. For greater efficiency, the pullbacks of a, b, and h are computed by using the pullback of g and performing various algebraic manipulations on lifted idempotents. We remark that other Henselization algorithms in current usage do not perform the same tasks. For example, the procedure given in [Pohst2] provides "partition of unity" factors a and b that are not pullbacks of the corresponding factors in the previous ring.

Lemma 39 *Let A be a commutative ring, let I be an ideal of A such that $I^2 = (0)$, and let $\overline{A} = A/I$. Suppose $\overline{e} \in \overline{A}$ is an idempotent element. If $e_1 \in A$ is any element such that $\overline{e_1} = \overline{e}$, then $E := 3e_1^2 - 2e_1^3$ is an idempotent element of A satisfying $\overline{E} = \overline{e}$.*

Proof. We first observe that $\overline{E} = \overline{3e_1^2 - 2e_1^3} = 3\overline{e}^2 - 2\overline{e}^3 = 3\overline{e} - 2\overline{e} = \overline{e}$ using the fact that $\overline{e}^2 = \overline{e}$. So, E is a pullback of e. Since $\overline{e_1(1 - e_1)} = \overline{e - e^2} = \overline{e} - \overline{e}^2 = 0$, it follows that $e_1(1 - e_1) \in I$. Thus,

$$E^2 - E = \left(3e_1^2 - 2e_1^3\right)^2 - \left(3e_1^2 - 2e_1^3\right) = e_1^2 (1 - e_1)^2 \left(4e_1^2 - 4e_1 - 3\right) \in I^2 = (0).$$

So, E is an idempotent element.

Lemma 40 *Let A be a commutative ring, let I be an ideal of A such that $I^2 = (0)$, and let $\overline{A} = A/I$. Let $g^* \in A[X]$ be a polynomial of degree n such that $\overline{g^*}$ is monic of degree $k \leq n$. Then there exist unique elements $g, p \in A[X]$ satisfying all of the following conditions: $g^* = g(1+p), p \in I[X], g$ is monic of degree k, and $\overline{g} = \overline{g^*}$.*

Proof. Since $\overline{g^*}$ is monic of degree k, we can partially factor x^k out of g^* to obtain $g^* = (1+p_1)x^k + \widetilde{g_1}$ where $p_1 \in I[X]$ has degree $n-k$ and $\deg(\widetilde{g_1}) \leq k-1$. Since $I^2 = (0)$, we obtain the factorization $g^* = (1+p_1)\left[x^k + (1-p_1)\widetilde{g_1}\right]$. Observe that the degree of $g_1 = x^k + (1-p_1)\widetilde{g_1}$ is at most $n-1$ and that $\overline{g_1}$ is monic of degree k. Thus, we can partially factor x^k out of g_1 and eventually obtain $g^* = (1+p_1)(1+p_2)g_2$ where $p_2 \in I[X]$ has degree at most $n-1-k$, g_2 has degree at most $n-2$, and $\overline{g_2}$ is monic of degree k. We continue in this manner until we obtain $g^* = (1+p_1)(1+p_2)\cdots(1+p_r)g_r$ where $p_1, p_2, \ldots, p_r \in I[X]$ and g_r is monic of degree k. Since $I^2 = (0)$, $\prod_{j=1}^{r}(1+p_j) = 1+p$ where $p = \sum_{j=1}^{r} p_j \in I[X]$. So, $g^* = g(1+p)$ where $g = g_r$ and p have all the desired properties since $\overline{g} = \overline{g^*}$ follows immediately from the observation that $\overline{p} = 0$.

Now, suppose that $g^* = g(1+p) = \widetilde{g}(1+\widetilde{p})$ where g and $\widetilde{g}$ are both monic of degree k and $p, \widetilde{p} \in I[X]$. Then $g = \widetilde{g}(1+\widetilde{p})(1-p) = \widetilde{g}(1+\widetilde{p}-p)$. Since g and $\widetilde{g}$

both have degree k, it follows that $\widetilde{p}-p$ is constant. Since g and $\widetilde{g}$ are both monic, we deduce that $\widetilde{p}-p=0$. Thus, $\widetilde{p}=p$ and $\widetilde{g}=g$.

Proposition 41 *Let A be a commutative ring, let I be an ideal of A such that $I^2=(0)$, and let $\overline{A}=A/I$. Let $f\in A[X]$ be monic, and let $\overline{g},\overline{h}\in\overline{A}[X]$ be monic polynomials such that $\overline{f}=\overline{g}\overline{h}$. Suppose further that $\overline{a},\overline{b}\in\overline{A}[X]$ are such that $\overline{a}\,\overline{g}+\overline{b}\,\overline{h}=1$, $\deg(\overline{a})<\deg(\overline{h})$, and $\deg(\overline{b})<\deg(\overline{g})$. Then there exist unique pullbacks $g,h,a,b\in A[X]$ of $\overline{g},\overline{h},\overline{a}$, and $\overline{b}$, respectively, such that g and h are monic, $f=gh$, $ag+bh=1$, $\deg(a)<\deg(h)$, and $\deg(b)<\deg(g)$.*

Proof. Let $\widetilde{g},\widetilde{h}\in A[X]$ be pullbacks of $\overline{g}$ and $\overline{h}$, respectively. Then $\alpha=f-\widetilde{g}\widetilde{h}\in I[X]$. We also note that if $\widetilde{a},\widetilde{b}\in A[X]$ are pullbacks of $\overline{a}$ and $\overline{b}$, respectively, then $\widetilde{a}\,\widetilde{g}+\widetilde{b}\,\widetilde{h}=1+w$ for some $w\in I[X]$. Suppose $g^*=\widetilde{g}+\widetilde{b}\alpha$ and $h^*=\widetilde{h}+\widetilde{a}\alpha$. Then since $\overline{\alpha}=0$, it is clear that $\overline{g^*}=\overline{g}$ and $\overline{h^*}=\overline{h}$. Moreover,

$$g^*h^*=\left(\widetilde{g}+\widetilde{b}\alpha\right)\left(\widetilde{h}+\widetilde{a}\alpha\right)=\widetilde{g}\widetilde{h}+\left(\widetilde{a}\,\widetilde{g}+\widetilde{b}\,\widetilde{h}\right)\alpha+\widetilde{a}\widetilde{b}\alpha^2=\widetilde{g}\widetilde{h}+\alpha=f$$

since $I^2=(0)$. From Lemma 40, we can find unique pullbacks $g,h\in A[X]$ of $\overline{g}$ and $\overline{h}$, respectively, such that $g^*=g(1+p),p\in I[X],g$ is monic, $h^*=h(1+q),q\in I[X]$, and h is monic. The relation $f=g^*h^*$ can be rewritten as $f=gh(1+p)(1+q)$. Since $\overline{f}=\overline{gh(1+p)(1+q)}$, gh is monic, $\deg(f)=\deg(g)+\deg(h)$, $\overline{f}=\overline{gh}$, and $\overline{(1+p)(1+q)}=\overline{1}$, we can deduce from the uniqueness assertion of Lemma 40 that $f=gh$. Since $\overline{f}=\overline{g}\overline{h}$ and $\overline{a}\,\overline{g}+\overline{b}\,\overline{h}=1$, the

element $\overline{\overline{e}} = \overline{\overline{a}\,\overline{g}}$ is an idempotent in $\overline{A}[X] \diagup (\overline{f})$. We can use Lemma 39 to pull back $\overline{\overline{e}}$ to an idempotent $\overline{E} \in A[X] \diagup (f)$. The representative of $\overline{E}$ of lowest degree is ag. Since g is monic, the quotient of ag with g is a and $\deg(a) < \deg(h)$. Since $\overline{b}\,\overline{h} = 1 - \overline{a}\,\overline{g}$, it follows that $bh = 1 - ag$. The quotient of bh with h is b and $\deg(b) < \deg(g)$.

Our next result supports the *Root* subroutine. The computational points within this subroutine include the use of *Taylor Series expansions* to linearize the problem and the use of the *Euclidean Algorithm* to calculate inverses that necessarily exist because f is separable.

Proposition 42 *Let E be a field, and let $f \in E[X]$ be separable over E. Then for each positive integer N, there exists $\overline{\eta} \in E[X] \diagup (f^N)$ such that $f(\overline{\eta}) = 0$ in $E[X] \diagup (f^N)$ and such that $\overline{\eta}$ is a pullback of the canonical root of f in $E[X] \diagup (f)$. In other words, $\overline{\eta} = \overline{X} + \Delta$ where $\psi_N : E[X] \diagup (f^N) \longrightarrow E[X] \diagup (f)$ is the natural map and $\Delta \in \ker \psi_N$.*

Proof. It is sufficient to prove the result when N is a power of 2. We shall do so by induction. For the base case of $N = 1$, we let $\overline{\eta} = \overline{X}$. Suppose $N = 2^j$ where j is a positive integer, and let $M = 2^{j-1}$. By hypothesis, there exists $\widetilde{\eta} \in E[X] \diagup (f^M)$ such that $f(\widetilde{\eta}) = 0$ in $E[X] \diagup (f^M)$ and such that $\widetilde{\eta}$ is a pullback of the canonical root of f in $E[X] \diagup (f)$. In other words, $\widetilde{\eta} = \overline{X} + \widetilde{\Delta}$ where

$$\psi_M : E[X] \diagup (f^M) \longrightarrow E[X] \diagup (f)$$

is the natural map and $\widetilde{\Delta} \in \ker \psi_M$. Let

$$\psi : E[X] \diagup \left(f^N\right) \longrightarrow E[X] \diagup \left(f^M\right)$$

be the natural map, and suppose that $\widehat{\eta} \in E[X] \diagup \left(f^N\right)$ is chosen such that $\psi\left(\widehat{\eta}\right) = \widetilde{\eta}$. Then

$$\psi\left(f\left(\widehat{\eta}\right)\right) = f\left(\psi\left(\widehat{\eta}\right)\right) = f\left(\widetilde{\eta}\right) = 0.$$

So, $f\left(\widehat{\eta}\right) \in \ker \psi$ and $f^2\left(\widehat{\eta}\right) = 0$. The Taylor Series expansion for f around $\widehat{\eta}$ is

$$f(T) = f\left(\widehat{\eta}\right) + f'\left(\widehat{\eta}\right)\left(T - \widehat{\eta}\right) + \frac{f''\left(\widehat{\eta}\right)\left(T - \widehat{\eta}\right)^2}{2!} + \cdots.$$

Since f is separable over E, we have $\gcd\left(f^2, f'\right) = 1$. Thus, $af^2 + bf' = 1$ for suitably chosen $a, b \in E[X]$. So, $b\left(\widehat{\eta}\right) = \dfrac{1}{f'\left(\widehat{\eta}\right)}$ in $E[X] \diagup \left(f^N\right)$ since $f^2\left(\widehat{\eta}\right) = 0$. Let $\Delta = -\dfrac{f\left(\widehat{\eta}\right)}{f'\left(\widehat{\eta}\right)}$, and consider $\overline{\eta} = \widehat{\eta} + \Delta = \widehat{\eta} - \dfrac{f\left(\widehat{\eta}\right)}{f'\left(\widehat{\eta}\right)}$. Since $\Delta \in \ker \psi$, it follows that $\Delta^r = 0$ for each integer $r \geq 2$. Thus,

$$\begin{aligned} f\left(\overline{\eta}\right) &= f\left(\widehat{\eta}\right) + f'\left(\widehat{\eta}\right)\left(\overline{\eta} - \widehat{\eta}\right) + \frac{f''\left(\widehat{\eta}\right)\left(\overline{\eta} - \widehat{\eta}\right)^2}{2!} + \cdots \\ &= f\left(\widehat{\eta}\right) + f'\left(\widehat{\eta}\right)\Delta + \frac{f''\left(\widehat{\eta}\right)\Delta^2}{2!} + \cdots \\ &= f\left(\widehat{\eta}\right) + f'\left(\widehat{\eta}\right)\Delta = f\left(\widehat{\eta}\right) + f'\left(\widehat{\eta}\right)\left(-\frac{f\left(\widehat{\eta}\right)}{f'\left(\widehat{\eta}\right)}\right) = 0. \end{aligned}$$

So, $f\left(\overline{\eta}\right) = 0$ in $E[X] \diagup \left(f^N\right)$ and $\overline{\eta}$ is a pullback of the canonical root of f in $E[X] \diagup (f)$ since $\psi_N\left(\overline{\eta}\right) = \left(\psi_M \circ \psi\right)\left(\overline{\eta}\right) = \psi_M\left(\widetilde{\eta}\right) = \psi_M\left(\overline{X} + \widetilde{\Delta}\right) = \overline{X}$.

To support the *Extension* subroutine, we will first extend the idea of Proposition 42 to obtain a pullback of the canonical root of the nonlinear separable polynomial $\overline{F}$ in an arbitrary nilpotent approximation of the subalgebra $A[X]/(f)$. We then discuss how the image of this root in the residue field gives rise to the separable closure $\overline{A_1}$ of $\overline{A}$ in $\overline{A}[\overline{\theta}]$. As a consequence, we show that $\overline{\theta}$ is a root of $\overline{f_1}$, a polynomial that is a power of a linear separable polynomial over $\overline{A_1}$. Finally, we pull back $\overline{A_1}$ and $\overline{f_1}$ to obtain the separable closure A_1 of A in $A[\theta]$ and the polynomial f_1.

Proposition 43 *Let A be a complete DVR with uniformizing parameter π and residue field $\overline{A} = A/(\pi)$. Let $f \in A[X]$ be separable over the field of fractions of A, and suppose $\overline{f} = \overline{F}^N$ where $\overline{F}$ is separable over $\overline{A}$ and N is a positive integer. Let F be any pullback of $\overline{F}$ to $A[X]$. Then for each positive integer k, if $f_{(k)}$ and $F_{(k)}$ respectively denote the reductions of f and F modulo (π^k), there exists $\eta_k \in (A/(\pi^k))[X]/(f_{(k)})$ such that $F_{(k)}(\eta_k) = 0$ in $(A/(\pi^k))[X]/(f_{(k)})$ and such that η_k is a pullback of the canonical root of $\overline{F}$ in $\overline{A}[X]/(\overline{F})$.*

Proof. It is sufficient to prove the result when k is a power of 2. We shall do so by induction. For the base case of $k = 1$, we let $\eta_1 = \overline{\eta}$ where $\overline{\eta}$ is the element provided by Proposition 42. Suppose $k = 2^j$ where j is a positive integer, and let $l = 2^{j-1}$. By hypothesis, there exists $\eta_l \in (A/(\pi^l))[X]/(f_{(l)})$ such that $F_{(l)}(\eta_l) = 0$ in $(A/(\pi^l))[X]/(f_{(l)})$ and such that η_l is a pullback of the canonical root of $\overline{F}$ in

$\overline{A}[X]/(\overline{F})$. Let

$$\psi : (A/(\pi^k))[X]/(f_{(k)}) \longrightarrow (A/(\pi^l))[X]/(f_{(l)})$$

be the natural map, and suppose that $\widehat{\eta_k} \in (A/(\pi^k))[X]/(f_{(k)})$ is chosen such that $\psi(\widehat{\eta_k}) = \eta_l$. Then

$$\psi\left(F_{(k)}(\widehat{\eta_k})\right) = F_{(l)}(\psi(\widehat{\eta_k})) = F_{(l)}(\eta_l) = 0.$$

So, $F_{(k)}(\widehat{\eta_k}) \in \ker\psi$ and $F'_{(k)}(\widehat{\eta_k}) = 0$. The Taylor Series expansion for $F_{(k)}$ around $\widehat{\eta_k}$ is

$$F_{(k)}(T) = F_{(k)}(\widehat{\eta_k}) + F'_{(k)}(\widehat{\eta_k})(T - \widehat{\eta_k}) + \frac{F''_{(k)}(\widehat{\eta_k})(T - \widehat{\eta_k})^2}{2!} + \cdots.$$

Since $\overline{F}$ is separable over $\overline{A}$, we have $\gcd\left(\overline{F}^2, \overline{F}'\right) = 1$. Thus, $a\overline{F}^2 + b\overline{F}' = 1$ for suitably chosen $a, b \in \overline{A}[X]$. By *Hensel*, we deduce that $a_{(k)}F^2_{(k)} + b_{(k)}F'_{(k)} = 1$ for appropriate pullbacks $a_{(k)}, b_{(k)} \in (A/(\pi^k))[X]$ of a and b, respectively. So, $b_{(k)}(\widehat{\eta_k}) = \dfrac{1}{F'_{(k)}(\widehat{\eta_k})}$ in $(A/(\pi^k))[X]/(f_{(k)})$ since $F^2_{(k)}(\widehat{\eta_k}) = 0$. Let $\Delta = -\dfrac{F_{(k)}(\widehat{\eta_k})}{F'_{(k)}(\widehat{\eta_k})}$, and consider $\eta_k = \widehat{\eta_k} + \Delta = \widehat{\eta_k} - \dfrac{F_{(k)}(\widehat{\eta_k})}{F'_{(k)}(\widehat{\eta_k})}$. Since $\Delta \in \ker\psi$, it follows that $\Delta^r = 0$ for each integer $r \geq 2$. Thus,

$$\begin{aligned} F_{(k)}(\eta_k) &= F_{(k)}(\widehat{\eta_k}) + F'_{(k)}(\widehat{\eta_k})(\eta_k - \widehat{\eta_k}) + \frac{F''_{(k)}(\widehat{\eta_k})(\eta_k - \widehat{\eta_k})^2}{2!} + \cdots \\ &= F_{(k)}(\widehat{\eta_k}) + F'_{(k)}(\widehat{\eta_k})\Delta + \frac{F''_{(k)}(\widehat{\eta_k})\Delta^2}{2!} + \cdots \\ &= F_{(k)}(\widehat{\eta_k}) + F'_{(k)}(\widehat{\eta_k})\Delta = F_{(k)}(\widehat{\eta_k}) + F'_{(k)}(\widehat{\eta_k})\left(-\frac{F_{(k)}(\widehat{\eta_k})}{F'_{(k)}(\widehat{\eta_k})}\right) = 0. \end{aligned}$$

So, $F_{(k)}(\eta_k) = 0$ in $\left(A \diagup \left(\pi^k\right)\right)[X] \diagup \left(f_{(k)}\right)$ and η_k is a pullback of the canonical root of $\overline{F}$ in $\overline{A}[X] \diagup \left(\overline{F}\right)$ since $\psi(\eta_k) = \eta_l$.

We observe that the element η_k constructed in Proposition 43 is also a pullback of the element $\overline{\eta}$ provided by Proposition 42. In particular, $\eta_1 = \overline{\eta}$. It is clear from the constructions given in Propositions 42 and 43 that the elements $\overline{\eta}$ and η are expressed as polynomials in the elements $\overline{\theta}$ and θ, respectively, with coefficients from $\overline{A}$ and A, respectively. We set $A_1 := A[\eta] \subset A[\theta]$. Because A_1 is separable over A, it follows that $\overline{A_1}$ is a direct product of fields. So, a map defined out of a factor of $\overline{A_1}$ is necessarily monomorphic. Thus, $\overline{A_1} = \overline{A}[\overline{\eta}] \subset \overline{A}\left[\overline{\theta}\right]$.

Since $\overline{\eta}$ is a pullback of $\overline{X}$ and $\overline{F}(\overline{\eta}) = 0 \in \overline{A}[X] \diagup \left(\overline{F}^N\right)$, we have $\overline{A_1} \cong \overline{A}[X] \diagup \left(\overline{F}\right)$. Since $\overline{f} = \overline{F}^N$, we have $\overline{A}\left[\overline{\theta}\right] \cong \overline{A}[X] \diagup \left(\overline{F}^N\right)$. From these two isomorphisms, we deduce that the ring homomorphism $\psi : \overline{A}\left[\overline{\theta}\right] \longrightarrow \overline{A_1}$ satisfies $(\ker\psi)^N = 0$ in $\overline{A}\left[\overline{\theta}\right]$. We note that $\overline{\theta} - \overline{\eta}$ is an element of $\ker\psi$ because it is a difference of two pullbacks of $\overline{X}$. So, we conclude that $\left(\overline{\theta} - \overline{\eta}\right)^N = 0$. Thus, $\overline{\theta}$ is a root of the polynomial $\overline{f_1} = (X - \overline{\eta})^N$. Since $\overline{A_1} \subset \overline{A}\left[\overline{\theta}\right]$, we can define a ring homomorphism $\varphi : \overline{A_1}[X] \longrightarrow \overline{A}\left[\overline{\theta}\right]$ by $X \longmapsto \overline{\theta}$.

Then $\ker\varphi = \left(\overline{f_1}\right)$ by a dimension count. Thus, $\overline{A_1}[X] \diagup \left(\overline{f_1}\right) \cong \overline{A}[X] \diagup \left(\overline{f}\right)$. It remains for us to pull back $\overline{f_1}$ to a polynomial $f_1 \in A_1[X]$ having θ as a root and such that $A_1[X] \diagup (f_1) \cong A[X] \diagup (f)$.

As in Propositions 42 and 43, this step is performed inductively by pulling back $\overline{f_1}$ through powers of 2 to a polynomial $f_{1(k)}$ in a sufficiently close nilpotent approximation of $A_1[X]$. For example, the first pullback will be a polynomial $f_{1(2)} \in A_{1(2)}[X] = (A \diagup (\pi^2))[\eta_2][X]$. We find $f_{1(2)}$ by letting $\widetilde{f}_{1(2)} \in A_{1(2)}[X]$ be the canonical pullback of $\overline{f_1}$. Then $\widetilde{f}_{1(2)}(\theta_2) = \pi R(\theta_2)$ where θ_2 denotes the reduction of θ modulo (π^2) and R is the canonical pullback of some polynomial in $\overline{A_1}[X]$ with degree less than N. Set $f_{1(2)} = \widetilde{f}_{1(2)} - \pi R$ and repeat.

Finally, Proposition 33 in Chapter 2 supports the *Substitution* subroutine.

4.2 Theoretical Basis for the Algorithm

Let A be a complete DVR with uniformizing parameter π and field of fractions K. Suppose that $f \in A[X]$ is monic and has no repeated roots in an algebraic closure $\overline{K}$ of K. As noted in Chapter 1, the key idea in our algorithmic process is that the discriminant d_θ of the final transformed polynomial must be a unit in some complete DVR. Since $d_\theta = \prod_{1 \le i < j \le n} (r_i - r_j)^2$ where $r_1, r_2, \ldots, r_n$ are the roots of the polynomial, it follows that d_θ cannot be a unit unless at least one of the r_i is a unit relative to the uniformizing parameter. Observe that this condition is not sufficient. For example, the polynomial $X^2 - (t+2)X + t + 1 \in Q[[t]][X]$ has the unit roots 1 and $1 + t$. However,

$d_\theta = t^2$ is *not* a unit in $Q[[t]]$. The problem in general is that the "unit parts" can be eliminated when the differences of the roots are computed.

To overcome this difficulty, the appropriate strategy initially is to examine $\overline{f} \in (A/(\pi))[X]$. If $\overline{f}$ is separable over $\overline{A}$, then the roots of f have distinct "unit parts". So, d_θ is a unit in this case. Otherwise, one appeals to Artin's Theorem (Theorem 26) to justify the approach of applying *SepProd* to obtain $\overline{f} = \overline{F}^l\overline{G}$ and then pulling back the factorization via *Hensel* to decompose the algebra $A[X]/(f)$. Observe that if $A[X]/(f) \cong A[X]/(gh) \cong A[X]/(g) \times A[X]/(h)$, then f has no repeated roots in $\overline{K}$ implies that g and h also have no repeated roots in $\overline{K}$. This point allows iteration of the algorithm on each subalgebra.

Because of Proposition 20, we focus attention on the case when $\overline{f} = \overline{F}^l$ where $\overline{F}$ is separable over $\overline{A}$ and l is a positive integer greater than 1. If $\overline{F}$ is nonlinear, then the algorithm directs us to Case 2A. The ring A is replaced by the separable extension $A[\eta]$ in $A[\theta]$, and the polynomial f is replaced by a polynomial of lower degree that can be translated to another polynomial whose analysis belongs to Case 2B. $A[\eta]$ is the integral closure of A in $K[\eta]$, and we rely on Proposition 19 to give us $\widetilde{B}$ once the normalization of A_1 is computed. Since our new polynomial has lower degree than f, we have come closer to termination because an extension of degree 1 corresponds to an integrally closed ring. We should also note that the ring $A_1 = A[\eta]$ may now be a product of complete $DVRs$. However, because η is a separable element and the overall extension $\widetilde{B}$ decomposes into a separable extension followed by a totally ramified extension or vice

versa by commutativity, we can treat η as an indeterminate and work over the complete DVR A on iteration using the minimal polynomial to reduce relations involving η. In effect, we are treating $A[\eta]$ as a complete DVR. If the algorithm breaks down, then the "minimal" polynomial F_η will split into factors.

If $\overline{F}$ is linear, then we translate f (if necessary) so that $\overline{f} = X^l$ and proceed into Case 2B. We now perform a monomial substitution based on the *Newton Polygon* for f. Upon substituting $X = \pi^{\frac{a}{m}}T$ into f, we obtain $f = \pi^{\frac{aN}{m}} f_1$ where N is the degree of f and $f_1 \in A\left[\pi^{\frac{1}{m}}\right][T]$. Then $K[X]/(f) = K\left[\pi^{\frac{a}{m}}T\right]/\left(\pi^{\frac{aN}{m}} f_1\right) \subsetneq K\left(\pi^{\frac{1}{m}}\right)[T]/(f_1)$. So, the coefficient ring A is extended to the complete DVR $A_m = A\left[\pi^{\frac{1}{m}}\right]$, and the field K is extended to the field of fractions $K_m = K\left(\pi^{\frac{1}{m}}\right)$ of A_m for the next iteration. Each pass through Case 2B produces a new polynomial f_1 with a discriminant of lower order relative to π than the discriminant of f. So, we have again come closer to termination. However, as we proceed further through the next iteration, we might introduce idempotent elements in $K_m[\theta]$. A key fact that ensures that our final normalization can be brought down to $\widetilde{B}$ is that these idempotent elements always lie in $K[\theta]$.

To see this more clearly, recall that idempotent elements arise in the algorithm in two ways. If the Newton Polygon contains line segments with different slopes, then the factorization provided by Theorem 31 introduces idempotents. Otherwise, if the Newton Polygon consists of a single horizontal line segment, idempotents are introduced when the image of the polynomial in the residue field is a product of different powers of separable factors. From Proposition 20, $\widetilde{B}$ factors as a direct product of the normalizations obtained

from the irreducible factors of f. Accordingly, let us assume that f is irreducible over K of degree d with canonical root θ. f is not necessarily irreducible over K_m. In the following discussion, $K_m(\theta)$ denotes a compositum field obtained by adjoining θ to K_m. Observe that $K_m(\theta)$ is a subfield of $K_m[\theta] := K_m \otimes_K K(\theta)$. We will show that the rank of $\widetilde{B}$ becomes too large if idempotent elements introduced in $K_m[\theta]$ do not lie in $K(\theta)$. Consider the following diagram

$$
\begin{array}{ccc}
K_m(\theta) & & \\
 & \searrow^{m_2} & \\
\mid \frac{d}{m} m_2 & & K(\theta) \\
 & & \\
K_m & & \mid d \\
 & \searrow^{m} & \\
 & & K
\end{array}
$$

We assume that $ord(\theta) = \frac{l}{m}$ in reduced form. To carry out the algorithm we need $\pi^{\frac{l}{m}}$, not θ! On the other hand, $\pi^l = u\theta^m$ where u is a unit in the unique discrete valuation ring in $K(\theta)$. Moreover, $Y^m - u \in K(\theta)$ is separable and factors precisely as $Y^m - \overline{u}$ factors over the corresponding residue field k'. Let us further assume that there is a primitive m^{th} root of unity in K. (If not, we can adjoin such a root to K and proceed with impunity.) Then the factorization is completely determined by the largest factor $m_1 \mid m$ such that $\overline{u}^{\frac{1}{m_1}}$ exists in k'. In particular, the polynomial $Y^{m_2} - u_1 \in K(\theta)[Y]$

is irreducible where $m = m_1 \cdot m_2$ and $u_1^{m_1} = u$. Note that there are m_1 possible choices for u_1. Thus $K(\theta)(u_1^{\frac{1}{m_2}})$ is a field, $K(\theta)(u_1^{\frac{1}{m_2}}) = K_m(\theta)$, and $[K_m(\theta) : K(\theta)] = m_2$. Finally, we note that the extension $K(\theta)(u_1^{\frac{1}{m_2}})$ is Galois over $K(\theta)$ with Galois group $\mathbb{Z}/m_2\mathbb{Z} \subset \mathbb{Z}/m\mathbb{Z}$. Moreover, K_m is Galois over K with Galois group $G = \mathbb{Z}/m\mathbb{Z}$. Hence,

$$K_m \otimes_K K(\theta) = K[X]/(X^m - \pi) \otimes_K K(\theta) \cong K[X]/(X^m - u) \otimes_K K(\theta) = \prod_{j=1}^{m_1} K(\theta)((\xi^j u_1)^{\frac{1}{m_2}})$$

where ξ is a primitive m_1^{st} root of unity; i.e., there are m distinct m^{th} roots of u and they may be identified with $\zeta^i (\xi^j u_1)^{\frac{1}{m_2}}$ for appropriate powers i, j where ζ is a primitive m_2^{nd} root of unity. In fact, ζ and ξ are m_1^{st}, m_2^{nd} powers of a primitive m^{th} root of unity, respectively. These comments explain how the Galois group G acts on $\prod_{j=1}^{e_1} \prod_{i=1}^{e_2} K(\theta)(\zeta^i (\xi^j u_1)^{\frac{1}{e_2}})$ via the embedding.

The algorithm proceeds in $K_m[\theta] \cong \prod_{j=1}^{m_1} K(\theta)((\xi^j u_1)^{\frac{1}{m_2}})$. Because changing a root of unity does not alter the order of the roots, idempotents that arise from line segments with different slopes are invariant under the action of G and lie in $K(\theta)$. On the other hand, if we encounter a factorization $\overline{f_1} = \overline{F}^a \cdot \overline{G}^b$ wherein $\overline{F}$ and $\overline{G}$ are invariant under the action of G, then $K_m[\theta]$ is a product of at least $2m_1$ fields because of the transitive action of the Galois group. This contradicts the fact that $K_m[\theta]$ is a product of m_1 fields. Thus, we likewise conclude that idempotents of this type must lie in $K(\theta)$.

A typical sequence of cycles through Case 2A and Case 2B might be analyzed in the following way. Let $K^{(0)} = K$, let $K^{(j)}$ denote the field

$K\left(\pi^{\frac{1}{m_1}}, \pi^{\frac{1}{m_2}}, \ldots, \pi^{\frac{1}{m_j}}\right) = K\left(\pi^{\frac{1}{\operatorname{lcm}(m_1,\ldots,m_j)}}\right)$, and let $A^{(j)}$ denote the subring $A\left[\pi^{\frac{1}{m_1}}, \pi^{\frac{1}{m_2}}, \ldots, \pi^{\frac{1}{m_j}}\right] = A\left[\pi^{\frac{1}{\operatorname{lcm}(m_1,\ldots,m_j)}}\right]$. Let $T_0 = X$, and define $T_j = \frac{T_{j-1} - \eta_j}{\pi^{\frac{a_j}{m_j}}}$ for $1 \leq j \leq r$ where $\eta_j \in A^{(j-1)}[\theta]$ and a_j and m_j are relatively prime positive integers and the monic polynomial f_r has discriminant of order 0 or 1. Let $\psi_0 = \theta$, and let ψ_j be the canonical root of f_j in $K^{(j)}[T_j] \diagup (f_j)$ for $1 \leq j \leq r$. Then $A^{(r)}[\psi_r]$ is the integral closure of A in the extension $K^{(r)}[\theta]$. More generally, $A^{(r)}[\psi_r] \cap K^{(j)}[\theta]$ is the integral closure of A in the extension $K^{(j)}[\theta]$ for $0 \leq j \leq r$. In particular, $\widetilde{B} = A^{(r)}[\psi_r] \cap K^{(0)}[\theta]$. To perform the algebraic descent of $A^{(r)}[\psi_r]$ down to $\widetilde{B}$, observe that $A^{(r)} = A_m$ and $K^{(r)} = K_m$ where $m = \operatorname{lcm}(m_1, \ldots, m_r)$. Compute the powers of ψ_r and iteratively apply Theorem 28. The appropriate powers of π that multiply the generators from $K^{(j)}[\theta]$ into $K^{(j-1)}[\theta]$ necessarily exist by examining the monomial substitution formulas!

We note that the algorithm decomposes the extension $\widetilde{B}$ into a separable extension $A[\eta_1, \ldots, \eta_r] \diagup A$ followed by a totally ramified extension since the η_j can be adjoined at once at the beginning once they have been determined.

Chapter 5

Examples

5.1 The Complete Algorithm at Work

We now complete the solution to *Example 14* from *Chapter 1*. Let $A := \mathbb{Q}[t]$ and $f := X^2 - t^2X - t^3 \in A[X]$. Then $d_\theta = t^3(4+t)$ is not a unit in A. The only prime of A of height 1 that divides d_θ with multiplicity at least 2 is (t). Replace A with the complete DVR $\mathbb{Q}[[t]]$. From the Newton Polygon for f, we find that f has two roots of order $\frac{3}{2}$ with respect to the uniformizing parameter t. Substitute $X = t^{\frac{3}{2}}T$ to get $f = t^3 f_1$, where $f_1 = T^2 - t^{\frac{1}{2}}T - 1$. Observe that the coefficient field has been enlarged to $K_2 = \mathbb{Q}\left(\left(t^{\frac{1}{2}}\right)\right)$ to accommodate the iterated normalization. Since $d_{\psi_1} = 4 + t$ is a unit in A_2, where ψ_1 is the canonical root of f_1 in $K_2[T]/(f_1)$, the normalization of $\mathbb{Q}[[t]]$ in $K_2[\psi_1]$ is $A_2[\psi_1]$. By Theorem 28, the normalization of A in $K[\theta]$ is the A-module generated by $\left\{1, \frac{\theta}{t}\right\}$ since $\psi_1 = \frac{\theta}{t^{\frac{3}{2}}}$.

As a second example, suppose again that $A := \mathbb{Q}[t]$ and let

$$f := X^{10} + 6X^8 + 14X^6 + \left(16 - t - t^2\right) X^4 + \left(9 - 2t - 2t^2\right) X^2 + 2 - t - t^2 + t^3 \in A[X].$$

The discriminant of f has the prime factorization

$$d_\theta = -1024\left(2 - t - t^2 + t^3\right) t^{14} \left(108t^6 - 3485t^5 + 364t^4 + 444t^3 - 456t^2 + 172t - 16\right)^2.$$

The primes of A of height 1 that divide d_θ with multiplicity at least 2 are (t) and $(108t^6 - 3485t^5 + 364t^4 + 444t^3 - 456t^2 + 172t - 16)$. We will compute the local normalization relative to the prime (t). So, we replace the ring A with the complete DVR $\mathbb{Q}[[t]]$. The Newton Polygon for f is a horizontal line segment with vertices at $(0,0)$ and $(10,0)$. So, f has 10 unit roots with respect to the uniformizing parameter t. Since $\overline{f} = (X^2+1)^4 (X^2+2)$ and d_θ has order 14, we replace f by gh where $f - gh \in (td_\theta^2) = (t^{29})$,

$$\begin{aligned} g = {} & X^8 + 1597865499616954782220\, X^6 t^{28} + 228690017930181778608\, X^6 t^{27} \\ & + 32799208330073920372\, X^6 t^{26} + 4714771784929081612\, X^6 t^{25} \\ & + 679391422688290726\, X^6 t^{24} + 98159618972161976\, X^6 t^{23} + 14223378386178692\, X^6 t^{22} \\ & + 2067512197755276\, X^6 t^{21} + 301581487474306\, X^6 t^{20} + 44160056451196\, X^6 t^{19} \\ & + 6493903267490\, X^6 t^{18} + 959506755782\, X^6 t^{17} + 142531476407\, X^6 t^{16} \\ & + 21300938448\, X^6 t^{15} + 3205390236\, X^6 t^{14} + 486194632\, X^6 t^{13} + 74430470\, X^6 t^{12} \\ & + 11519092\, X^6 t^{11} + 1806090\, X^6 t^{10} + 287702\, X^6 t^9 + 46743\, X^6 t^8 + 7788\, X^6 t^7 \end{aligned}$$

$$+1342\,X^6t^6+242\,X^6t^5+47\,X^6t^4+10\,X^6t^3+3\,X^6t^2+X^6t+4\,X^6$$

$$+4277323548405779551596\,X^4t^{28}+61211497421196868152\,X^4t^{27}$$

$$+87780776346995693700\,X^4t^{26}+12616616126183156348\,X^4t^{25}$$

$$+1817790363885091758\,X^4t^{24}+262598377833600328\,X^4t^{23}+38044600481885764\,X^4t^{22}$$

$$+5529192536518596\,X^4t^{21}+806368790163818\,X^4t^{20}+118049667226620\,X^4t^{19}$$

$$+17355461887034\,X^4t^{18}+2563661552614\,X^4t^{17}+380706468435\,X^4t^{16}$$

$$+56875637904\,X^4t^{15}+8555265780\,X^4t^{14}+1297057148\,X^4t^{13}+198453902\,X^4t^{12}$$

$$+30693036\,X^4t^{11}+4808514\,X^4t^{10}+765206\,X^4t^9+124163\,X^4t^8+20652\,X^4t^7$$

$$+3550\,X^4t^6+638\,X^4t^5+123\,X^4t^4+26\,X^4t^3+7\,X^4t^2+2\,X^4t+6\,X^4$$

$$+3729983466376863562172\,X^2t^{28}+533695049172392838308\,X^2t^{27}$$

$$+76520699081834324072\,X^2t^{26}+10996005693377888282\,X^2t^{25}$$

$$+1583947334317709642\,X^2t^{24}+228763081936523476\,X^2t^{23}+33133874807084272\,X^2t^{22}$$

$$+4814104470759798\,X^2t^{21}+701857154091842\,X^2t^{20}+102712989687662\,X^2t^{19}$$

$$+15094680086132\,X^2t^{18}+2228710123441\,X^2t^{17}+330797216317\,X^2t^{16}$$

$$+49390599488\,X^2t^{15}+7424343144\,X^2t^{14}+1124708462\,X^2t^{13}+171922398\,X^2t^{12}$$

$$+26559518\,X^2t^{11}+4155132\,X^2t^{10}+660065\,X^2t^9+106857\,X^2t^8+17718\,X^2t^7$$

$$+3032\,X^2t^6+541\,X^2t^5+103\,X^2t^4+21\,X^2t^3+5\,X^2t^2+X^2t+4\,X^2$$

$$+1061040591768014433392\,t^{28}+151783061291302528840\,t^{27}$$

$$+21757373996786322906\,t^{26}+3125729084314700622\,t^{25}+450128214370711342\,t^{24}$$

$$+64990446210859768\,t^{23}+9410035575935358\,t^{22}+1366707198097158\,t^{21}$$

$+199174072898992\,t^{20} + 29134924424180\,t^{19} + 4279507132217\,t^{18} + 631505657111\,t^{17}$

$+93671245709\,t^{16} + 13975565532\,t^{15} + 2099009046\,t^{14} + 317662186\,t^{13} + 48500748\,t^{12}$

$+7482108\,t^{11} + 1168529\,t^{10} + 185227\,t^9 + 29903\,t^8 + 4940\,t^7 + 841\,t^6 + 149\,t^5 + 28\,t^4$

$+6\,t^3 + t^2 + 1$, and

$h = X^2 - 1597865499616954782220\,t^{28} - 228690017930181778608\,t^{27}$

$-32799208330073920372\,t^{26} - 4714771784929081612\,t^{25} - 679391422688290726\,t^{24}$

$-98159618972161976\,t^{23} - 14223378386178692\,t^{22} - 2067512197755276\,t^{21}$

$-301581487474306\,t^{20} - 44160056451196\,t^{19} - 6493903267490\,t^{18} - 959506755782\,t^{17}$

$-142531476407\,t^{16} - 21300938448\,t^{15} - 3205390236\,t^{14} - 486194632\,t^{13}$

$-74430470\,t^{12} - 11519092\,t^{11} - 1806090\,t^{10} - 287702\,t^9 - 46743\,t^8 - 7788\,t^7 - 1342\,t^6$

$-242\,t^5 - 47\,t^4 - 10\,t^3 - 3\,t^2 - t + 2.$

Moreover, $\overline{g} = (X^2+1)^4$, $\overline{h} = X^2 + 2$, the discriminant of g has order 14, and the discriminant of h is a unit.

We now search for the normalization of $\mathbb{Q}[[t]]$ in $K[X]/(gh) \cong K[X]/(g) \times K[X]/(h)$. We have polynomials a and b such that $ag + bh = 1 \bmod (t^{29})$. So, bh is a pullback of $(1,0)$ and ag is a pullback of $(0,1)$. Let θ_g and θ_h be the canonical roots of g and h, respectively. Since h has unit discriminant, the elements $(0,1)$ and $(0,\theta_h)$ generate the normalization in the second factor. The pullbacks of these elements are ag and $ag\theta$, respectively. Both of these elements are already in $\mathbb{Q}[[t]][\theta]$.

It remains for us to find the generators of the normalization of $\mathbb{Q}[[t]]$ in the extension $K[X]/(g)$. Since $\overline{g} = (X^2+1)^4$, we find a root η of X^2+1 in $\mathbb{Q}[[t]][\theta_g]$ and form the

separable closure $\mathbb{Q}[[t]][\eta]$ of $\mathbb{Q}[[t]]$ in $\mathbb{Q}[[t]][\theta_g]$. We obtain

$$\eta = -\tfrac{1}{65536}\left(109847\,\theta_g^6 + 277823\,\theta_g^4 + 224313\,\theta_g^2 + 74257\right)\theta_g t^3$$
$$-\tfrac{1}{2048}\left(663\,\theta_g^6 + 911\,\theta_g^4 - 167\,\theta_g^2 - 415\right)\theta_g t^2 - \tfrac{7}{256}\left(\theta_g^6 - 7\,\theta_g^4 - 17\,\theta_g^2 - 9\right)\theta_g t$$
$$+1/16\left(5\,\theta_g^6 + 21\,\theta_g^4 + 35\,\theta_g^2 + 35\right)\theta_g.$$

Since $\mathbb{Q}[[t]][\eta]$ is separable over $\mathbb{Q}[[t]]$, it follows that its normalization in $\mathbb{Q}((t))(\eta)$ is itself. So, it is generated as a $\mathbb{Q}[[t]]$-module by $\{1, \eta\}$. By Proposition 19, it now suffices to find $\widetilde{B_g}$ in $\mathbb{Q}((t))(\theta_g)$ with respect to the ground ring $\mathbb{Q}[[t]][\eta]$. Afterwards, the generators for $\widetilde{B_g}$ over $\mathbb{Q}[[t]]$ are obtained by multiplying the generators over $\mathbb{Q}[[t]][\eta]$ by 1 and η. The subroutine *Extension* provides us with both η and a polynomial $F_\eta \in \mathbb{Q}[[t]][\eta][X]$ such that $\mathbb{Q}((t))(\theta_g) \cong \mathbb{Q}((t))(\eta)[X]/(F_\eta)$ and $\overline{F_\eta} = (X - \overline{\eta})^4$. By considering $F(X) := F_\eta(X + \eta)$, we obtain a polynomial that reduces to X^4. We find that

$$F_\eta = \left(3 - \tfrac{1969}{512}\,X^3\eta + \tfrac{4977}{512}\,X\eta - \tfrac{2721}{256}\,X^2\right)t^3 + \left(-\tfrac{63}{64}\,X^3\eta + 1/2 - \tfrac{79}{32}\,X^2 + \tfrac{127}{64}\,X\eta\right)t^2$$
$$+\left(-1/2\,X^2 + 1/4\,X\eta - 1/4\,X^3\eta\right)t + X^4 - 4\,X^3\eta + 4\,X\eta - 6\,X^2 + 1$$

and

$$F = X^4 + \left(-1/4\,t - \frac{1969}{512}\,t^3 - \frac{63}{64}\,t^2\right)\eta X^3 + \left(\frac{465}{512}\,t^3 + \frac{31}{64}\,t^2 + 1/4\,t\right)X^2 + 1/16\,t^3.$$

We will need to translate back later, but the use of F instead of F_η brings us to Case 2B

of the procedure and Newton Polygon factorization techniques.

In turns out that the Newton Polygon for F has vertices at $(0,3)$, $(2,1)$, and $(4,0)$. The slope of the segment ending at $(4,0)$ is $-\frac{1}{2}$. Thus, we make the substitution $X = t^{\frac{1}{2}}T$ and factor out t^2 to obtain $F\left(t^{\frac{1}{2}}T\right) = t^2 F_1(T)$. The polynomial

$$F_1 = T^4 - 1/4\sqrt{t}\eta T^3 - \frac{1969}{512}\eta t^{5/2}T^3 - \frac{63}{64}\eta t^{3/2}T^3 + \frac{465}{512}t^2T^2 + \frac{31}{64}tT^2 + 1/4\,T^2 + 1/16\,t$$

is of degree 4 and has unit roots with respect to the powers of the uniformizing parameter $t^{\frac{1}{2}}$ in the ring $A_2[\eta]$. We find ourselves in position to make a second "pass" through the procedure in the sense that we can factor $\overline{F_1}$ and pull back to obtain a separable piece for which the normalization will be readily computed. The other factor will be of lower degree than F_1 and will be amenable to the same treatment as g.

In this example, we observe that $\mathbb{Q}[[t]](\eta)[X]/(F) \subset A_2(\eta)[T]/(F_1)$ and this object is replaced by $A_2(\eta)[T]/(g^*) \times A_2(\eta)[T]/(h^*)$ where both g^* and h^* have degree 2. In this example, the discriminant of both F_1 and g^* has order 2 with respect to $\left(t^{\frac{1}{2}}\right)$ while the discriminant of h^* is a unit. We immediately obtain 2 generators for our normalization from the second factor and another 2 generators upon multiplication of these by η. The first factor requires one more Newton Polygon substitution to convert it to a factor with two unit roots. At that point, we obtain 2 generators immediately and then the last 2 generators by multiplication by η. After all of the pullbacks through the various isomorphisms are made as well as some linear translations, we obtain the following set of $\mathbb{Q}[[t]]$-module generators for $\widetilde{\mathbb{Q}[[t]][\theta]}$:

$$\left\{ \begin{array}{l} 1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \frac{2+5\theta^2+4\theta^4+6}{t}, \frac{\theta\left(2+5\theta^2+4\theta^4+6\right)}{t}, \\ -\frac{t+\theta^2 t-2-7\theta^2-9\theta^4-5\theta^6-\theta^8}{t^2}, -\frac{\theta\left(t+\theta^2 t-2-7\theta^2-9\theta^4-5\theta^6-\theta^8\right)}{t^2} \end{array} \right\}.$$

As a final example, let $A := \mathbb{Q}[s,t]$ and

$$f := X^5 + s^4X^4 - s^3t^2X^2 - s^3tX^2 + s^5t^3 \in A[X].$$

The ring A is a Noetherian, unique factorization domain of Krull dimension 2 with field of fractions $K = \mathbb{Q}(s,t)$. We will compute the normalization of A in $L = K[X]/(f) = K[\theta]$ where θ is a root of f. The discriminant of f has the prime factorization

$$\begin{aligned} d_\theta = -s^{20}t^7(&108\,t + 540\,t^2 - 16\,s^9 - 900\,s^3t^2 - 2700\,s^3t^3 + 128\,s^{12}t + 1080\,t^3 \\ &-64\,ts^9 + 1080\,t^4 - 96\,s^9t^2 + 256\,s^{12}t^2 + 2000\,s^6t^3 - 64\,s^9t^3 + 128\,s^{12}t^3 + 2000\,s^6t^4 \\ &-16\,s^9t^4 - 2585\,t^5 - 2700\,s^3t^4 - 900\,s^3t^5 - 256\,s^{15}t^2 + 108\,t^6). \end{aligned}$$

Thus, the primes of height 1 that divide d_θ with multiplicity at least 2 are (s) and (t). Our generalized algorithm instructs us to split the computation into two local computations. By localizing at (s), we find ourselves passing over to the complete DVR $\mathbb{Q}(t)[[s]]$. Likewise, by localizing at (t), we find ourselves passing over to the complete DVR $\mathbb{Q}(s)[[t]]$. We can now employ the procedure as described in Chapter 3. In the first

instance, we obtain the generating set $\left\{1, \frac{\theta}{s}, \frac{\theta^2}{s^2}, \frac{\theta^3}{s^3}, \frac{\theta^4}{s^4}\right\}$. In the second case, we obtain the generating set $\left\{1, \theta, \theta^2, \frac{\theta^2(\theta+s^4)}{t}, -\frac{\theta(s^3t-s^4\theta^2-\theta^3)}{t^2}\right\}$. The generators for $\widetilde{B}$ as an A-module are obtained simply by taking the union of these two sets.

5.2 Practical Limitations and Weaknesses

We have implemented each of the subroutines in the computer algebra system MAPLE over the complete DVR $\mathbb{Q}[[t]]$. A program that coordinates the actions of the various subroutines has not been created, so it is difficult to assess the overall efficiency of the algorithm. Moreover, our codes have been input at the top level using MAPLE worksheets rather than internally. So, the timings that are reported in the paragraphs below cannot be considered optimal. Nevertheless, it is clear that the weakest link is the subroutine *Hensel*. Our computations were performed on a Packard Bell Platinum 4400 computer. This model has an Intel Pentium II processor and operates at a speed of 266 MHz. We employed MAPLE V Release 5.

The first example in Section 5.1 only requires the use of the *SepProd* and *Substitution* subroutines, and these computations are virtually immediate. The discriminant calculation using the procedure incorporated in MAPLE is also immediate.

The second example in Section 5.1 uses all of the subroutines at least once. The first usage of *Hensel* to pull back the factorization of the degree 10 polynomial as a product of a degree 8 polynomial and a degree 2 polynomial to order 29 requires 9.414 seconds. By contrast, the computation of η and F_η only require 1.481 and 1.474 seconds,

respectively. The second usage of *Hensel* to pull back the factorization of a quartic polynomial as a product of 2 quadratic polynomials to order 5 requires 1.502 seconds. As in the first example, the computations involving the *SepProd* and *Substitution* subroutines are virtually immediate.

In the third example in Section 5.1, the computation of the local normalization of $\mathbb{Q}(t)[[s]]$ is immediate. After an initial usage of the *SepProd* and *Substitution* subroutines, the resulting polynomial has a separable image over the residue field. However, the computation of the local normalization of $\mathbb{Q}(s)[[t]]$ is quite inefficient. From *SepProd*, we find that f has the separable factorization $X^4(X+s^4)$ over the residue field. To pull back this factorization to order 15, the subroutine *Hensel* requires 88.387 seconds. Later in the computation, the quartic factor further decomposes as a product of 2 quadratic polynomials. It is only required to pull back this latter factorization to order 5. However, the subroutine *Hensel* requires 494.775 seconds! In this example, the computations of the discriminants also are not immediate. We have not investigated alternatives to the discriminant calculations, however.

The *Hensel* subroutine makes heavy use of the division algorithm. The number of terms in the intermediate dividends of each division rapidly accumulate and cause an explosion in the size of the coefficients. In the dimension 1 setting, there is a cap in the size of the exponents of the variable by the order of the nilpotent extension. However, in the dimension 2 setting, one of the variables acts as a scalar. So, the exponents can grow without bound. This complication makes the multivariable division

calculations especially cumbersome. One source of hope, at least for the dimension 1 setting, is to tighten the bound on the order of the pullback of the factorization required in Theorem 26. We have experimented with pulling factorizations back only to the order of the discriminant because Corollary 16 suggests that multiplication by terms of larger order merely drags B' into B. However, we have not yet successfully organized this intuitive idea into a theorem. Moreover, while the overwhelming majority of examples have produced identical generators using this lower order, we have come across a couple of examples that have yielded different generators. Of course, the 2 sets of generators may produce the same module. However, this verification becomes a very tedious exercise in linear algebra. For this reason, it is not clear in general that this lower order is sufficient. So, this conjecture remains open.

Appendix A

Implementation in MAPLE Over $\mathbb{Q}[[t]]$

We now present an implementation in MAPLE of each of the subroutines over $\mathbb{Q}[[t]]$.

The first one given is *SepProd*.

```
> SepProd:=proc(g::polynom,x::algebraic)
> local h,i,j,k,F,G,f,l;
> global gtilda,htilda,atilda,btilda;
### WARNING: degree(0,x) now returns -infinity
> f:=array(1..degree(g,x)+1);
> f[1]:=g; h:=g; i:=2;
### WARNING: degree(0,x) now returns -infinity
> while degree(h,x)> 0 do
```

```
> h:= evala(Gcd(h,diff(h,x)));
> f[i]:=h; i:=i+1;
> od;
> print(f,i);
> G:=array(1..i-2);
> for j from 1 to i-2 do G[j]:=f[j]/f[j+1]; od;
> F:=array(1..i-2);
> for k from 1 to i-3 do F[k]:=simplify(G[k]/G[k+1]); od;
> F[i-2]:=G[i-2];
> print(F);
> atilda:='atilda'; btilda:='btilda';
> gtilda:=F[i-2]^(i-2); htilda:=1;
> for l from 1 to i-3 do
> htilda:=htilda*F[l]^l;
> od;
> print(gtilda,htilda);
> evala(Gcdex(gtilda,htilda,x,atilda,btilda));
> print(atilda,btilda);
> end:
```

The code for *Hensel* is split into 2 subprocedures: *Henselpass* and *Hensel.*

```
> Henselpass:=proc(f::polynom,gtilda::polynom,htilda::polynom,atilda::polynom,
```

```
btilda::polynom,ntilda::integer,t::algebraic,x::algebraic)
> local g1star,g2,g3,lc,k,l,e1,e2,e11,e12;
> global alpha1,beta1,g1,h1,a1,b1,n;
> alpha1:=simplify(expand(f-gtilda*htilda));
> beta1:=simplify(expand(atilda*gtilda+btilda*htilda-1));
> k:=degree(gtilda,x);
> e1:=evala(Rem(atilda*gtilda,t^(2*ntilda),t));
> e11:=evala(Rem(e1*e1,t^(2*ntilda),t));#e1-squared
> e12:=evala(Rem(e11*e1,t^(2*ntilda),t));#e1-cubed
> e1:=3*e11-2*e12;
> e1:=evala(Rem(evala(Rem(e1,f,x)),t^(2*ntilda),t)); e2:=1-e1;
> g1star:=simplify(expand(btilda*alpha1));
> g1star:=evala(Rem(evala(Rem(g1star,f,x)),t^(2*ntilda),t));
> g1:=sort(simplify(expand(gtilda+g1star)),[x,t],plex);
> n:=2*ntilda;
> g1:=evala(Rem(evala(Rem(g1,f,x)),t^(2*ntilda),t));
> g3:=g1;
> l:=k;
> while l>=k do
> lc:=evala(Rem(evala(Quo(g3,x^k,x)),t^(2*ntilda),t));
> g2:=evala(Rem(evala(Rem(g3,x^k,x)),t^(2*ntilda),t));
```

```
> g3:=evala(Rem(x^k+(2-lc)*g2,t^(2*ntilda),t));
> l:=degree((2-lc)*g2,x);
> od;
> g1:=sort(simplify(expand(g3)),[x,t],plex);
> h1:=sort(expand(evala(Rem(evala(Quo(f,g1,x)),t^(2*ntilda),t))),[x,t],plex);
> a1:=sort(expand(evala(Rem(evala(Quo(e1,g1,x)),t^(2*ntilda),t))),[x,t],plex);
> b1:=sort(expand(evala(Rem(evala(Quo(e2,h1,x)),t^(2*ntilda),t))),[x,t],plex);
> alpha1:=sort(simplify(expand(f-g1*h1)),[t,x],plex);
> beta1:=sort(simplify(expand(a1*g1+b1*h1-1)),[t,x],plex);
> #writeline(default,"g1=");#print(g1);
> #writeline(default,"h1=");#print(h1);
> #writeline(default,"a1=");#print(a1);
> #writeline(default,"b1=");#print(b1);
> #writeline(default,"alpha1=");#print(alpha1);
> #writeline(default,"beta1=");#print(beta1);
> #writeline(default,"n=");#print(n);
> end:
> Hensel:=proc(f::polynom,gtilda::polynom,htilda::polynom,atilda::polynom,
btilda::polynom,ntilda::integer,t::algebraic,x::algebraic)
> local i,r,s;
> global a,b,g,h,alpha,beta;
```

```
> Henselpass(f,gtilda,htilda,atilda,btilda,1,t,x):
> g:=g1;h:=h1;a:=a1;b:=b1;alpha:=alpha1;beta:=beta1;
> if ntilda > 2 then
> r:=ceil(simplify(log[2](ntilda)));
> for i from 1 to r-1 do
> s:=ceil(ntilda/2^(r-i));
> g:=evala(Rem(g1,t^s,t));h:=evala(Rem(h1,t^s,t));
> a:=evala(Rem(a1,t^s,t));b:=evala(Rem(b1,t^s,t));
> Henselpass(f,g,h,a,b,s,t,x):
> od;
> g:=sort(expand(evala(Rem(g1,t^ntilda,t))),[x,t],plex);
> h:=sort(expand(evala(Rem(h1,t^ntilda,t))),[x,t],plex);
> a:=sort(expand(evala(Rem(a1,t^ntilda,t))),[x,t],plex);
> b:=sort(expand(evala(Rem(b1,t^ntilda,t))),[x,t],plex);
> alpha:=sort(simplify(expand(f-g*h)),[t,x],plex);
> beta:=sort(simplify(expand(a*g+b*h-1)),[t,x],plex);
> fi;
> writeline(default,"g=");print(g);
> writeline(default,"h=");print(h);
> #writeline(default,"a=");#print(a);
> #writeline(default,"b=");#print(b);
```

```
> #writeline(default,"alpha=");#print(alpha);
> #writeline(default,"beta=");#print(beta);
> if ntilda >= 2 then
> writeline(default,"power of lift=");print(ntilda);
> else
> writeline(default,"power of lift=");print(2);
> fi;
> end:
```

The codes for *Root* and *Extension* are split into 3 subprocedures: *Root, Rootext* and *MinPol.*

```
> Root:=proc(fbar,n::integer,indet::algebraic)
> #n is the degree of nilpotency and indet is the canonical root
> local Inv,fbarn,roottrunc,delta,eps,check1,check2,i,inv,R,a;
> global rootlift;
> D(fbar);#This is the derivative of fbar as a function.
> fbarn:=x->fbar(x)^n;#the root of fbar will be lifted to the power n
> roottrunc:=indet;
> if gcd(fbar(indet),D(fbar)(indet))=1 then
> gcdex(fbar(indet),D(fbar)(indet),indet,'a','Inv');#Inv is D(fbar)(indet) inverse
> eps:=expand(fbar(indet)*a);#previously was D(fbar)(indet)*Inv - 1.
> inv:=expand(D(fbar)(indet)*Inv*Inv);#previously was (1-eps)*Inv
```

```
> i:=1;
> while 2^(i-1)<n do
> R:=rem(fbar(roottrunc),fbar(indet)^(2^i),indet);
> delta:=expand(-R*inv);
> roottrunc:=roottrunc+delta;
> roottrunc:=rem(roottrunc,fbar(indet)^(2^i),indet);
#this is the root lifted to the power 2^i
> i:=i+1;
> eps:=expand(D(fbar)(roottrunc)*inv-1);
> inv:=expand((1-eps)*inv);
> od;
> rootlift:=sort(rem(roottrunc,fbarn(indet),indet),indet);
#this is the root lifted to the power n
> check1:=rem(expand(fbar(rootlift)),fbarn(indet),indet);
#checks that rootlift is a root of fbar
> check2:=rem(rootlift,fbar(indet),indet);#checks that rootlift is a lift of indet
> print(rootlift,check1,check2);
> else print("The input polynomial is not separable.");
> fi;
> end:
> Rootext:=proc(f,F,n::integer,m::integer,rho::algebraic,t::algebraic)
```

```
#n is power degree, m is power of lift in t, and rho is the canonical root of F
> local Fp,fm,roottrunc,check1,check2,delta,a,Fpinv,inv,eps,i,R;
> global eta;
> Root(F,n,rho);
> Fp:=D(F);
> if gcd(F(rho),Fp(rho))=1 then
> gcdex(F(rootlift),Fp(rootlift),rho,'a','Fpinv');#Fpinv is Fprime(rootlift) inverse
> inv:=Fpinv;
> fm:=(rho,t)->evala(Rem(f(rho,t),t^m,t));#the root of F will be lifted to the
power m
> roottrunc:=rootlift;#the root to be lifted is rootlift
> i:=1;
> while 2^(i-1)<m do
> eps:=evala(Rem(evala(Rem(expand(Fp(roottrunc)*inv-1),
fm(rho,t),rho)),t^(2^i),t));
> inv:=evala(Rem(evala(Rem(expand((1-eps)*inv),fm(rho,t),rho)),t^(2^i),t));
> R:=evala(Rem(evala(Rem(expand(F(roottrunc)),fm(rho,t),rho)),t^(2^i),t));
> delta:=evala(Rem(evala(Rem(expand(-R*inv),fm(rho,t),rho)),t^(2^i),t));
> roottrunc:=evala(Rem(roottrunc+delta,fm(rho,t),rho));
> roottrunc:=evala(Rem(roottrunc,t^(2^i),t));#this is the root lifted to the
power 2^i
```

```
> i:=i+1;
> od;
> roottrunc:=sort(evala(Rem(roottrunc,fm(rho,t),rho)),rho);
> eta:=sort(evala(Rem(roottrunc,t^m,t)),[rho,t],plex);#this is the root lifted to
power m
> check1:=sort(evala(Rem(evala(Rem(expand(subs(rho=eta,F(rho))),
fm(rho,t),rho)),t^m,t)),rho);
#checks that eta is a root of F
> check2:=evala(Rem(eta,t,t));#checks that eta is a lift of rootlift
> print(eta,check1,check2);
> else print("Please change the input polynomial.");
> fi;
> end:
> MinPol:=proc(f,F,eta::polynom,n::integer,m::integer,rho::algebraic,
W::algebraic,X::algebraic,t::algebraic)#n is power degree, m is power of lift in t,
X is the current indeterminate, W is placeholder for eta
> local error,Fetalift,Fetatrunc,etatail,i,check,Q;
> global Feta;
> Fetatrunc:=unapply(simplify(expand((X-W)^n),{F(W)=0}),X,W);
> i:=1;
> while 2^(i-1)<m do
```

```
> etatail:=rem(eta,t^(2^i),t);
> error:=rem(rem(Fetatrunc(rho,etatail),f(rho,t),rho),t^(2^i),t);
> Q:=simplify(expand(quo(error,t^(2^(i-1)),t)),{Fetatrunc(rho,w)=0},{rho});
> Fetalift:=simplify(Fetatrunc(rho,w)-(t^(2^(i-1)))*Q,{F(w)=0});
> Fetatrunc:=unapply(Fetalift,rho,w);
> i:=i+1;
> od;
> Fetalift:=rem(Fetatrunc(X,W),t^m,t);
> Feta:=unapply(Fetalift,W,X);
> check:=rem(rem(Feta(eta,rho),f(rho,t),rho),t^m,t);
> print(Feta(W,X),check);
> end:
```

The code for *Substitution* is split into 2 subprocedures: *NPol_Slope* and *NPol_Sub.*

```
> NPol_Slope:=proc(f::procedure,X::algebraic,t::algebraic,n::integer)
> description "This procedure takes a multivariable expression given as a
function of X and t and computes the slope of the final segment of its Newton
Polygon with respect to the parameter t. All variables other than X and t are
treated as constants. The global variable m represents the slope.";
> local a,b,i,j,list1,list2,list3,list4,slopes;
> global m,N;
> N:=degree(simplify(f(X,t^n),symbolic),X);#N is the largest abscissa among the
```

vertices

> list2:=coeffs(simplify(f(X,t^n),symbolic),X,'list1');

> list1:=[list1];#This list has the powers of X with nonzero coefficients

> list2:=[list2];#This list has the corresponding coefficients

> list1:=map(ldegree,list1);#replaces list1 by the exponents of X

> list2:=map(ldegree,list2,t);#replaces list2 by the exponents of t

> list3:=[seq([list1[i],list2[i]],i=1..nops(list1))];#creates points from list1 and list2.

However, the entries in list1 are not necessarily in ascending order!

This forces us to "reorder" the points in list3 before computing the various slopes.

> for i from 1 to nops(list3) do

> if list3[i][1]=N then j:=i; fi;

> od;#The jth point in list3 is the final point on the Newton Polygon.

> a:=list3[j];b:=list3[nops(list3)];

> list4:=subsop(nops(list3)=a,list3);

> list4[j]:=b;#Now, the final point on the polygon is the last point in list4.

So, the "backward" slopes computation can begin.

> slopes:=[seq(with(student,slope)(list4[i],list4[nops(list4)])[1],i=1..(nops(list4)-1))];

#[1] is needed for technical reasons

> m:=slopes[nops(slopes)];#The last entry in the list of slopes is used for comparison

purposes.

> for i from 1 to nops(slopes)-1 do

```
> m:=max(slopes[i],m);
> od;#This loop identifies the appropriate final slope!
> m:=m/n;#this division compensates for the scaling when changing parameters
> writeline(default,"The final slope of the Newton Polygon is");print(m);
> end:
> NPol_Sub:=proc(f::procedure,X::algebraic,t::algebraic,n::integer,T::algebraic)
> global f1;
> NPol_Slope(f,X,t,n);
> if m=0 then f1:=unapply(f(T,t),T,t);
> else f1:=unapply(simplify(expand(t^(m*N)*f(t^(-m)*T,t)),symbolic),T,t);
> fi;
> writeline(default,"The polynomial f1 with unit roots is");print(f1(T,t));
> end:
```

Bibliography

[Artin] Michael Artin, **Etale Coverings of Schemes over Hensel Rings**, American Journal of Mathematics (1966) 88, 915-934.

[Chistov] A. L. Chistov, **The Complexity of Constructing the Ring of Integers of a Global Field**, Soviet Math. Dokl. (1989) 39 No. 3, 597-600.

[Cohen] Henri Cohen, **A Course in Computational Algebraic Number Theory**, Graduate Texts in Mathematics (138), Springer-Verlag, New York, 1993.

[Ford] David J. Ford, **The Construction of Maximal Orders Over a Dedekind Domain**, Journal of Symbolic Computation (1987) 4, 69-75.

[Hoeij] Mark van Hoeij, **An Algorithm for Computing an Integral Basis in an Algebraic Function Field**, Journal of Symbolic Computation (1994) 18, 353-363.

[Jong] Theo de Jong, **An Algorithm for Computing the Integral Closure**, Journal of Symbolic Computation (1998) 26 No. 3, 273 - 277.

[Lang] Serge Lang, **Algebraic Number Theory**, Graduate Texts in Mathematics (110), Springer-Verlag, New York, 1986.

[Matsumura] Hideyuki Matsumura, **Commutative Ring Theory**, Cambridge University Press, Cambridge, 1986.

[Pohst1] Michael E. Pohst, **Computational Algebraic Number Theory**, DMV Seminar (21), Birkhäuser Verlag, Boston, 1993.

[Pohst2] Michael E. Pohst and Hans Zassenhaus, **Algorithmic Algebraic Number Theory**, Cambridge University Press, Cambridge, 1989.

[Ribenboim] Paulo Ribenboim, **The Theory of Classical Valuations**, Springer Monographs in Mathematics, Springer-Verlag, New York, 1999.

[Weiss] Edwin Weiss, **Algebraic Number Theory**, Dover Publications, Inc., Mineola, New York, 1998.