RAMIFICATION OF VALUATIONS

STEVEN DALE CUTKOSKY AND OLIVIER PILTANT

1. Introduction

The ramification theory of valuations was developed classically in finite extensions of rings of algebraic integers, and for mappings of algebraic curves. In these cases, the corresponding homomorphisms of local rings of points are ramified maps $R \rightarrow S$ of discrete (rank 1) valuation rings, $R = V$ and $S = V^*$. These valuation rings are local Dedekind domains. Suppose that (y) is the maximal ideal of R, (x) is the maximal ideal of S. We have an expression

$$y = x^e \delta \tag{1}$$

where $\delta \in S$ is a unit. If the value groups are $\Gamma^* \cong \mathbf{Z}$ and $\Gamma \cong \mathbf{Z}$ we have a natural isomorphism $\Gamma^*/\Gamma \cong \mathbf{Z}_e$. This theme is developed into the beautiful theory of ramification of discrete (rank 1) valuation rings. If R contains a field k, we observe that $\hat{R} \rightarrow \hat{S}$ is the finite extension $R/m_R[[y]] \rightarrow S/m_S[[x]]$. Suppose that k has characteristic zero, and let k' be an algebraic closure of S/m_S. Then we have an action of the finite Abelian group $\mathrm{Hom}(\Gamma^*/\Gamma, (k')^\times) \cong \Gamma^*/\Gamma$ on $\hat{S} \otimes_{S/m_S} k'$, and the invariant ring is

$$\left(\hat{S} \otimes_{S/m_S} k'\right)^{\Gamma^*/\Gamma} \cong \hat{R} \otimes_{R/m_R} k' \tag{2}$$

The theory of valuation rings in arbitrary fields, and the ramification theory of valuations was initiated by Krull.

Suppose that R is a local domain. A monoidal transform $R \rightarrow R_1$ is a birational extension of local domains such that $R_1 = R[\frac{P}{x}]_m$ where P is a regular prime ideal of R, $0 \neq x \in P$ and m is a prime ideal of $R[\frac{P}{x}]$ such that $m \cap R = m_R$. If $P = m_R$, $R \rightarrow R_1$ is called a quadratic transform.

If R is regular, and $R \rightarrow R_1$ is a monoidal transform, then there exists a regular system of parameters $(x_1, \ldots, x_n)$ of R and $r \leq n$ such that

$$R_1 = R\left[\frac{x_2}{x_1}, \ldots, \frac{x_r}{x_1}\right]_m.$$

Suppose that ν is a valuation of the quotient field R which dominates R. Then $R \rightarrow R_1$ is a monoidal transform along ν if ν dominates R_1.

Suppose that K is an algebraic function field. If K has dimension ≥ 2, then K has non Noetherian valuation rings. However, whenever there is a sufficiently strong theory of resolution of singularities, the valuation rings of K can be written as unions of algebraic regular local rings with quotient field K. When k has characteristic zero, this follows from Zariski's Theorem on local uniformization along a valuation [21]. A stronger version of this theorem is proven in Theorem 6.2.

The first author was partially supported by NSF.

The second author was supported by CNRS and Ecole Polytechnique.

In Chapters 2 to 6, we assume K has characteristic zero. Suppose that K^* is a finite extension of K, V^* is a valuation ring of K^*.

We show in Theorem 6.1 and Theorem 6.3 that we can express $V \to V^*$ as $V = \cup R_i$, $V^* = \cup S_i$ so that R_i and S_i are algebraic normal local rings with quotient fields K and K^* respectively, S_i is regular and obtained from a fixed S_0 by a product of monoidal transforms along ν, R_i has toric singularities, and S_i lies above R_i. If k' is an algebraic closure of V^*/m_{V^*}, then there is an action of the finite Abelian group Γ^*/Γ on $\hat{S}_i \otimes_{S_i/m_{S_i}} k'$ such that

$$\left(\hat{S}_i \otimes_{S_i/m_{S_i}} k'\right)^{\Gamma^*/\Gamma} \cong \hat{R}_i \otimes_{R_i/m_{R_i}} k'$$

and these actions are compatible with inclusion of the S_i. We thus obtain the strongest possible generalization of the classical theory of equations (1) and (2) to algebraic function fields of arbitrary dimension and characteristic zero. Such a statement was unanticipated by previous work. It can be viewed as a relative local uniformization theorem.

We also interpret the invariants of ramification of valuations and of the Galois theory of ramification of valuations, to show that they also generalize from the classical case of local Dedekind domains in the best possible way (Theorem 5.2 and Remark 6.4).

The first author's proof of the "Weak simultaneous resolution conjecture" is the main step in this construction. Abhyankar's "Weak simultaneous resolution local conjecture" (page 144 [6]), asserts that if we start with an algebraic regular local ring S^* with quotient field K^* which is dominated by V^*, then there exists a sequence of monoidal transforms $S^* \to S$ along V^* (blowups of regular primes, localized at the center of V^*) such that there exists an algebraic normal local ring R with quotient field K such that S lies above R. Abhyankar has proven this theorem for two dimensional function fields in all characteristics. It is a key step in his proof of resolution of singularities of surface singularities in char ≥ 0. We have proven in [11] that the "Weak simultaneous resolution local conjecture" is true in function fields of arbitrary dimension and characteristic 0. We prove a stronger version of the Weak simultaneous resolution local conjecture in Theorem 4.2. This theorem is a corollary of the local monomialization theorem of [10]. The subtlety of the conjecture can be understood by the fact that the "Global weak simultaneous local conjecture" (page 144 [6]) is false, even in characteristic zero [12].

Suppose that k is a field of characteristic zero, S^* is an algebraic regular local ring with quotient field K^* which is dominated by V^* and R^* is an algebraic regular local ring with quotient field K which is dominated by S^*. The local monomialization theorem [10] proves that there then exist sequences of monoidal transforms $R^* \to R_0$ and $S^* \to S$ such that V^* dominates S, S dominates R_0 and there are regular parameters $(x_1, ..., x_n)$ in R_0, $(y_1, ..., y_n)$ in S, units $\delta_1, \ldots, \delta_n \in S$ and a matrix $A = (a_{ij})$ of nonnegative integers such that $\det(A) \neq 0$ and

$$\begin{aligned} x_1 &= y_1^{a_{11}} \cdots y_n^{a_{1n}} \delta_1 \\ &\vdots \\ x_n &= y_1^{a_{n1}} \cdots y_n^{a_{nn}} \delta_n. \end{aligned}$$

The difficulty in obtaining this result is to achieve the condition $\det(A) \neq 0$.

A refinement of this Theorem is possible, giving a description of A depending on invariants of V^*, which we call Strong Monomialization. This is proven in Theorem 4.8. A further refinement is obtained in Theorem 4.9. Theorem 4.9 is necessary to prove Theorems 6.1 and 6.3.

Several hard facts make it difficult to extend the classical theory of equations (1) and (2) to algebraic function fields of positive characteristic. First, the local uniformization theorem has been proven sofar in characteristic $p > 0$ only when K has dimension two ([1]), and when K has dimension three and $p \neq 2, 3, 5$ ([5]). Also, equation (2) implies that the induced inclusion of function fields

$$QF\left(\hat{R} \otimes_{R/m_R} k'\right) \subset QF\left(\hat{S} \otimes_{S/m_S} k'\right)$$

is cyclic Galois, whereas it need not even be Galois in positive characteristic (examples 2.1.5 and 2.1.6 [8]). Moreover, even in the Galois case, the local inertia group of (2) is not in general Abelian (example 2.1.7 [8]). In particular, it is not in general isomorphic to Γ^*/Γ.

In Chapter 7 we study the ramification in surfaces over a field of positive characteristic. Most of this chapter is devoted to getting a right formulation of (1) in dimension two. Suppose that K^*/K is a finite, separable extension of two dimensional algebraic function fields, over an algebraically closed field k of characteristic $p > 0$. Suppose that V^* is a valuation ring of K^* and $V = V^* \cap K$. Let Γ^* be the value group of V^*, Γ be the value group of V. We further consider a birational extension of algebraic regular local rings $R \to S$ where R has quotient field K, S has quotient field K^*, and V^* dominates R and S.

In Theorem 7.3, we prove that Strong Monomialization holds whenever Γ^* is finitely generated. Since K^* is a two dimensional algebraic function field, this includes all valuations of K^* except those which are nondiscrete and rational.

We now restrict to the case where Γ^* is nondiscrete and rational.

Simultaneous Resolution is the statement that there exists a commutative diagram of algebraic regular local rings

$$\begin{array}{ccc} R' & \to & S' \\ \uparrow & & \uparrow \\ R & \to & S \end{array}$$

such that the vertical arrows are products of monoidal transforms along V^*, and $R' \to S'$ is the localization of a finite map. Proving Simultaneous Resolution is extremely useful for applications to local uniformization since it implies that local uniformization "goes up" in a field extension ([1]).

In the case where k had characteristic zero, Simultaneous Resolution held along V^*. This is proven for rational valuations in algebraic function fields of dimension 2 and characteristic zero by Abhyankar (Theorem 2 [3]) and follows for rational valuations in algebraic function fields of arbitrary dimension and characteristic 0 from Strong Monomialization in characteristic 0 (Theorem 4.8). An example of Abhyankar (Theorem 12 [3]) shows that Simultaneous Resolution is in general false for valuations of rational rank larger than 1. A direct consequence of (2) of Theorem 7.33 is that Simultaneous Resolution is true in dimension two and characteristic $p > 0$ whenever the nondiscrete rational group Γ is not p-divisible.

One essential new invariant to be considered in characteristic $p > 0$ is the defect of V^* over V which is a power of p (cf. Definition 7.1). V^*/V is defectless if k has characteristic zero. We prove that V^*/V is defectless (in characteristic $p > 0$) if Γ^* is finitely generated ((3) of Theorem 7.3, see also [15]). In Theorem 7.33 we obtain stable forms for mappings $R' \to S'$ where S' is a product of quadratic transforms along V^* and $R \to R'$ is the maximal factorization by quadratic transforms of $R \to S'$. The ramification index and defect of V^* over V can be computed from the equations defining these mappings. In Theorem 7.35 we prove that Strong Monomialization holds whenever V^*/V is defectless.

In Theorem 7.38 we give an example of an extension of two dimensional algebraic function fields with valuations V^*/V such that V^*/V has positive defect, and Strong Monomialization does not hold.

2. NOTATIONS

We will denote the maximal ideal of a local ring R by m_R. We will denote the quotient field of a domain R by $QF(R)$. Suppose that $R \subset S$ is an inclusion of local rings. We will say that R dominates S if $m_S \cap R = m_R$. Suppose that K is an algebraic function field over a field k. We will say that a subring R of K is algebraic if R is essentially of finite type over k. Suppose that K^* is a finite extension of an algebraic function field K, R is a local ring with $QF(K)$ and S is a local ring with $QF(K^*)$. We will say that S lies over R and R lies below S if S is a localization at a maximal ideal of the integral closure of R in K^*. If R is a local ring, $\hat{R}$ will denote the completion of R at its maximal ideal. If M is a finite field extension of a field L, we will denote the group of L-automorphisms of M by $\mathrm{Gal}(M/L)$.

Good introductions to the valuation theory which we require in this paper can be found in Chapter VI of [22] and in [4]. A valuation ν of K will be called a k-valuation if $\nu(k) = 0$. We will denote by V_ν the associated valuation ring, which necessarily contains k. A valuation ring V of K will be called a k-valuation ring if $k \subset V$. The residue field V/m_V of a valuation ring V will be denoted by $k(\nu)$. The value group of a valuation ν will be denoted by Γ_ν. If X is an integral k-scheme with function field K, then a point $p \in X$ is called a center of the valuation ν (or the valuation ring V_ν) if V_ν dominates $\mathcal{O}_{X,p}$. If R is a subring of V_ν then the center of ν (the center of V_ν) on R is the prime ideal $R \cap m_{V_\nu}$.

Suppose that R is a local domain. A monoidal transform $R \to R_1$ is a birational extension of local domains such that $R_1 = R[\frac{P}{x}]_m$ where P is a regular prime ideal of R, $0 \neq x \in P$ and m is a prime ideal of $R[\frac{P}{x}]$ such that $m \cap R = m_R$. $R \to R_1$ is called a quadratic transform if $P = m_R$.

If R is regular, and $R \to R_1$ is a monoidal transform, then there exists a regular system of parameters $(x_1, \ldots, x_n)$ in R and $r \leq n$ such that

$$R_1 = R\left[\frac{x_2}{x_1}, \ldots, \frac{x_r}{x_1}\right]_m.$$

Suppose that ν is a valuation of the quotient field R with valuation ring V_ν which dominates R. Then $R \to R_1$ is a monoidal transform along ν (along V_ν) if ν dominates R_1.

3. CONVENTIONS ON VALUATIONS

We recall some classical invariants of valuations (Chapter VI, [22], [4]), and establish some notations which we will follow.

Suppose that K is a field of algebraic functions over a field k, and ν is a k-valuation of K with valuation ring V and value group Γ.

The primes of V are a finite chain

$$0 = p_0 \subset \cdots \subset p_r = m_V \subset V.$$

The rank of V is the length r of this chain. $r \leq \mathrm{trdeg}_k K < \infty$ by Corollary, page 50, Section 11, Chapter VI, [22]. The isolated subgroups of the value group Γ of V are

$$0 = \Delta_r \subset \cdots \subset \Delta_0 = \Gamma.$$

The Δ_i are defined as follows. Set $U_i = \{\nu(a) \mid a \in p_i\}$. Δ_i is the complement of U_i and $-U_i$ in Γ. For $i < j$, $(V/p_i)_{p_j}$ is a rank $j-i$ valuation ring with value group Δ_i/Δ_j and with quotient field $(V/p_i)_{p_i}$. V is said to be composite with the valuations $(V/p_i)_{p_j}$. Set

$$\lambda_i = \mathrm{trdeg}_k(V/p_i)_{p_i}$$

for $0 \le i \le r$. The rational rank of $(V/p_{i-1})_{p_i}$ is

$$s_i = \mathrm{ratrank}(V/p_{i-1})_{p_i} := \dim_{\mathbf{Q}}(\Delta_{i-1}/\Delta_i) \otimes \mathbf{Q}$$

for $1 \le i \le r$. s_i and λ_i are $< \infty$ by Theorem 1 [2] or by Proposition 2, Appendix 2 [22].

Now suppose that K^* is a finite extension of K, and ν^* is an extension of ν to K^*. Let V^* be the valuation ring of ν^*, and let Γ^* be the value group. The primes of V^* are a finite chain

$$0 = p_0^* \subset \cdots \subset p_r^* \subset V^*$$

with $p_i^* \cap V = p_i$, $0 \le i \le r$, and with isolated subgroups

$$0 = \Delta_r^* \subset \cdots \subset \Delta_0^* = \Gamma^*$$

which have the property that $\Delta_i^* \cap \Gamma = \Delta_i$ for $0 \le i \le r$ and Δ_i^*/Δ_i is a finite (Abelian) group for $0 \le i \le r$ (Section 11, Chapter VI [22]). We further have that

$$\mathrm{trdeg}_k(V^*/p_i^*)_{p_i^*} = \mathrm{trdeg}_k(V/p_i)_{p_i} = \lambda_i$$

for $0 \le i \le r$ and

$$\mathrm{ratrank}(V^*/p_{i-1}^*)_{p_i^*} = \mathrm{ratrank}(V/p_{i-1})_{p_i} = s_i$$

for $1 \le i \le r$. Set $t_i = \lambda_{i-1} - \lambda_i$ for $1 \le i \le r$.

The ramification index of ν^* relative to ν is defined to be (page 53, Section 11, Chapter VI, [22])

$$e = [\Gamma^* : \Gamma]. \tag{3}$$

The residue degree of ν^* with respect to ν is defined to be (page 53, Section 11, Chapter VI)

$$f = [V^*/m_{V^*} : V/m_V]. \tag{4}$$

4. Ramification of valuations in algebraic function fields

Theorem 4.1. *(Local Monomialization)(Theorem 1.1* [10]*) Let k be a field of characteristic zero, K an algebraic function field over k, K^* a finite algebraic extension of K, ν^* a k-valuation of K^*. Suppose that S^* is an algebraic regular local ring with quotient field K^* which is dominated by ν^* and R^* is an algebraic regular local ring with quotient field K which is dominated by S^*. Then there exist sequences of monoidal transforms $R^* \to R_0$ and $S^* \to S$ such that ν^* dominates S, S dominates R_0 and there are regular parameters $(x_1, ..., x_n)$ in R_0, $(y_1, ..., y_n)$ in S, units $\delta_1, \ldots, \delta_n \in S$ and a matrix $A = (a_{ij})$ of nonnegative integers such that $det(A) \neq 0$ and*

$$\begin{array}{rcl} x_1 & = & y_1^{a_{11}} \cdots y_n^{a_{1n}} \delta_1 \\ & \vdots & \\ x_n & = & y_1^{a_{n1}} \cdots y_n^{a_{nn}} \delta_n. \end{array} \tag{5}$$

The standard theorems on resolution of singularities allow one to easily find R_0 and S such that (5) holds, but, in general, we will not have the essential condition $\det(a_{ij}) \neq 0$. The difficulty in the proof of this Theorem is to achieve the condition $\det(a_{ij}) \neq 0$.

Let α_i be the images of δ_i in S/m_S for $1 \le i \le n$. Let $C = (a_{ij})^{-1}$, a matrix with rational coefficients. Define regular parameters $(\overline{y}_1, \dots, \overline{y}_n)$ in $\hat{S}$ by

$$\overline{y}_i = \left(\frac{\delta_1}{\alpha_1}\right)^{c_{i1}} \cdots \left(\frac{\delta_n}{\alpha_n}\right)^{c_{in}} y_i$$

for $1 \le i \le n$. We thus have relations

$$x_i = \alpha_i \overline{y}_1^{a_{i1}} \cdots \overline{y}_n^{a_{in}} \tag{6}$$

with $\alpha_i \in S/m_S$ for $1 \le i \le n$ in

$$\hat{R}_0 = R_0/m_{R_0}[[x_1, \dots, x_n]] \to \hat{S} = S/m_S[[\overline{y}_1, \dots, \overline{y}_n]].$$

Theorem 4.2. *Let k be a field of characteristic zero, K an algebraic function field over k, K^* a finite algebraic extension of K, ν^* a k-valuation of K^*. Suppose that S^* is an algebraic local ring with quotient field K^* which is dominated by ν^* and R^* is an algebraic local ring with quotient field K which is dominated by S^*. Then there exists a commutative diagram*

$$\begin{array}{ccccccc} R_0 & \to & R & \to & S & \subset & V_{\nu^*} \\ \uparrow & & & & \uparrow & & \\ R^* & & \to & & S^* & & \end{array} \tag{7}$$

where $S^* \to S$ and $R^* \to R_0$ are sequences of monoidal transforms along ν^* such that $R_0 \to S$ have regular parameters of the form of the conclusions of Theorem 4.1, R is an algebraic normal local ring with toric singularities which is the localization of the blowup of an ideal in R_0, and the regular local ring S is the localization at a maximal ideal of the integral closure of R in K^*.

Proof. By resolution of singularities [14] (c.f. Theorem 2.6, Theorem 2.9 [10]), we first reduce to the case where R^* and S^* are regular, and then construct, by the local monomialization theorem, Theorem 4.1 a sequence of monoidal transforms along ν^*

$$\begin{array}{ccccc} R_0 & \to & S & \subset & V_{\nu^*} \\ \uparrow & & \uparrow & & \\ R* & \to & S^* & & \end{array} \tag{8}$$

so that R_0 is a regular local ring with regular parameters $(x_1, \dots, x_n)$, S is a regular local ring with regular parameters $(y_1, \dots, y_n)$, there are units $\delta_1, \dots, \delta_n$ in S, and a matrix of natural numbers $A = (a_{ij})$ with nonzero determinant d such that

$$x_i = \delta_i y_1^{a_{i1}} \cdots y_n^{a_{in}}$$

for $1 \le i \le n$. After possibly reindexing the y_i we may assume that $d > 0$. Let (b_{ij}) be the adjoint matrix of A. Set

$$f_i = \prod_{j=1}^n x_j^{b_{ij}} = (\prod_{j=1}^n \delta_j^{b_{ij}}) y_i^d$$

for $1 \le i \le n$. Let R be the integral closure of $R_0[f_1, \dots, f_n]$ in K, localized at the center of ν^*. Since $\sqrt{m_R S} = m_S$, Zariski's Main Theorem (10.9 [5]) shows that R is an algebraic normal local ring with quotient field K such that S lies above R.

We thus have a sequence of the form (7). □

As an immediate consequence, we obtain a proof in characteristic zero of the "weak simultaneous resolution local conjecture". which is stated explicitly on page 144 of [6], and is implicit in [3]. Abhyankar proves this for algebraic function fields of dimension two and any characteristic in [1] and [4]. In the paper [11], we have given a direct proof of this result, also as a consequence of Theorem 4.1.

Corollary 4.3. *(Theorem 1.1 [11]) Let k be a field of characteristic zero, K an algebraic function field over k, K^* a finite algebraic extension of K, ν^* a k-valuation of K^*, and S^* an algebraic regular local ring with quotient field K^* which is dominated by ν^*. Then for some sequence of monoidal transforms $S^* \to S$ along ν^*, there exists a normal algebraic local ring R with quotient field K, such that the regular local ring S is the localization at a maximal ideal of the integral closure of R in K^*.*

Proof. There exists a normal algebraic local ring R^* with quotient field K such that ν^* dominates R^* (take R^* to be the local ring of the center of ν^* on a normal projective model of K). There exists a finite type k-algebra T such that the integral closure of R^* in K^* is a localization of T, and T is generated over k by $g_1, \dots, g_m \in V^*$ such that $\nu^*(g_i) \geq 0$ for all i. There exists a sequence of monoidal transforms $S^* \to S_1$ along ν^* such that $T \subset S_1$ (Theorem 2.7 [10]). S_1 dominates R. After replacing S^* with S_1, we can assume that S^* dominates R^*. Theorem 4.2 applies to this situation, so we can construct a diagram of the form (7). □

The sequence of monoidal transforms $S^* \to S$ is necessary in Theorem 4.2 and Corollary 4.3 as can be seen by the following simple example which was communicated to us by William Heinzer. Let x, y be algebraically independent over a field k, and let $S^* = k[x^3, x^2y]_{(x^3,x^2y)}$. Consider the automorphism of $K^* = k(x, y)$ over k that maps x to y and y to x. The image of S^* is the 2 dimensional regular local ring S' where $S' = k[y^3, y^2x]$ localized at (y^3, y^2x). Regarding S^* and S' as subrings of the formal power series $k[[x, y]]$, we see that the intersection of S^* and S' is k. Hence if K is the fixed field of the above automorphism, so that $K = k(x + y, xy)$, we have $S^* \cap K = S' \cap K = k$.

When K^* is Galois over K, it is not difficult to construct using Galois theory and resolution of singularities a regular local ring S with quotient field K^* and a normal local ring R with quotient field K such that S lies over R (Theorem 7 [3], Theorem 6.2), although even in the Galois case the full statements of Theorem 4.2 and Corollary 4.3 do not follow from these results (Theorem 7 [3], Theorem 6.2). The general case of non Galois extensions is much more subtle, and not as well behaved, as can be seen from Theorem 3.1 of [12]. This Theorem shows that a generically finite morphism of projective surfaces cannot in general be birationally modified to produce a proper morphism from a nonsingular surface to a normal surface. Theorem 3.1 [12] is thus a counterexample to Abhyankar's "weak simultaneous resolution global conjecture", which is stated explicitely on page 144 of [6] and is implicit in [3].

The following lemma prepares the proof of our higher dimensional version of (2) in the introduction.

Lemma 4.4. *Suppose that $k_1 \to k_2$ is a finite extension of fields of characteristic zero, $A = (a_{ij})$ is an $n \times n$ matrix of natural numbers with $det(A) \neq 0$ and*

$$L = k_1(x_1, \dots, x_n) \to L_1 = k_2(x_1, \dots, x_n) \to L^* = k_2(\overline{y}_1, \dots, \overline{y}_n)$$

are inclusions of rational function fields, given by

$$x_i = \alpha_i \overline{y}_1^{a_{i1}} \cdots \overline{y}_n^{a_{in}}$$

with $\alpha_i \in k_2$ for $1 \leq i \leq n$. Then

1. $[L^* : L] = \mid det(A) \mid [k_2 : k_1]$.
2. *L^* is Galois over L if and only if the following conditions hold: k_2 is Galois over k_1 and there is a primitive e^{th} root of unity in k_2 where*

$$e = lcm\{ord(b) \mid b \in \mathbf{Z}^n/A\mathbf{Z}^n\}.$$

(3) *If L^* is Galois over L, then there is a natural exact sequence*

$$0 \to Gal(L^*/L_1) \cong \mathbf{Z}^n/A\mathbf{Z}^n \to Gal(L^*/L) \to Gal(k_2/k_1) \to 0. \quad (9)$$

Proof. Let $0 \neq d = \mid det(A) \mid$. Set $\overline{x}_i = \frac{x_i}{\alpha_i} \in L_1$ for $1 \leq i \leq n$. If $v = (v_1, \ldots, v_n) \in \mathbf{Z}^n$, we will write

$$\overline{y}^v = \overline{y}_1^{v_1} \cdots \overline{y}_n^{v_n}.$$

Let $e_1, \ldots, e_d \in \mathbf{Z}^n$ be representatives of distinct cosets of $\mathbf{Z}^n/A^t\mathbf{Z}^n$. We will show that $\{\overline{y}^{e_1}, \ldots, \overline{y}^{e_d}\}$ is a basis of L^* over L_1.

Suppose that there is a relation

$$\sum_{i=1}^m f_i(\overline{x})\overline{y}^{e_i} = 0$$

with $f_i(\overline{x}) \in L_1$. After clearing denominators, we may assume that each $f_i(\overline{x}) \in k_2[\overline{x}_1, \ldots, \overline{x}_n]$,

$$f_i(\overline{x}) = \sum_I \alpha_{i,I}\overline{x}^I$$

with $\alpha_{i,I} \in k_2$.

$$0 = \sum_{i,I} \alpha_{i,I}\overline{y}^{A^tI+e_i}$$

$A^tI + e_i = A^tJ + e_j$ implies $e_i = e_j$, and thus $I = J$ so $\alpha_{i,I} = 0$ for all i, I, and $\overline{y}^{e_1}, \ldots, \overline{y}^{e_d}$ are linearly independent over L.

Set $B = (b_{ij}) = dA^{-1} = \pm\mathrm{adj}(A)$.

$$\overline{y}_i^d = \overline{x}_1^{b_{i1}} \cdots \overline{x}_n^{b_{in}} \in L_1$$

for $1 \leq i \leq n$ so that the monomials

$$\overline{y}_1^{i_1} \cdots \overline{y}_n^{i_n} \quad 0 \leq i_j \leq d-1$$

generate L^* over L_1 which thus implies $\overline{y}^{e_1}, \ldots, \overline{y}^{e_d}$ generate L^* over L_1. Thus

$$[L^* : L_1] = \mid \mathbf{Z}^n/A^t\mathbf{Z}^n \mid = d$$

and 1. of the Lemma follows.

Now suppose that $k_1 = k_2$ contains a primitive d^{th} root of unity ω. Then $\overline{x}_i \in L$, and $\overline{y}_i^d \in L$ for $1 \leq i \leq n$.

$\sigma \in \mathrm{Gal}(L^*/L)$ implies $\sigma(\overline{y}_i^d) = \overline{y}_i^d$ for $1 \leq i \leq n$ so that $\sigma(\overline{y}_i) = \omega^{c_i}\overline{y}_i$ for some $c_i \in \mathbf{Z}$.

Given $c = (c_1, \ldots, c_n) \in \mathbf{Z}^n$, define a k_2 algebra automorphism $\sigma_c : L^* \to L^*$ by $\sigma_c(\overline{y}_i) = \omega^{c_i}\overline{y}_i$. σ_c is an L automorphism if and only if $Ac \in d\mathbf{Z}^n$. Thus

$$\mathrm{Gal}(L^*/L) \cong \{c \in \mathbf{Z}^n \mid Ac \in d\mathbf{Z}^n\}/d\mathbf{Z}^n.$$

Define a group homomorphism

$$\Psi : \mathbf{Z}^n/A\mathbf{Z}^n \to \mathrm{Gal}(L^*/L)$$

by $\Psi(c) = Bc$, where $B = dA^{-1} = \pm\mathrm{adj}(A)$. Ψ is well defined and an isomorphism. Thus $\mid \mathrm{Gal}(L^*/L) \mid = d$. By 1. of this Lemma, L^* is Galois over L.

Now consider the general case, with no restrictions on k_1 and k_2. Let ω be a primitive d^{th} root of unity in some extension field of k_2. Set $k' = k_2(\omega)$. Set $L_0 = k'(\overline{x}_1, \ldots, \overline{x}_n)$, $L' = k'(\overline{y}_1, \ldots, \overline{y}_n)$. By the argument for $k_1 = k_2$, we know that L'/L_0 is Galois with $\mathrm{Gal}(L'/L_0) \cong \mathbf{Z}^n/A\mathbf{Z}^n$.

Suppose that L^*/L is Galois. Then there is a natural homomorphism

$$\mathrm{Gal}(L'/L_0) \to \mathrm{Gal}(L^*/L)$$

which is an inclusion since L' is the join of L_0 and L^*. If $\sigma\in \mathrm{Gal}(L'/L_0)$ then for $1\le i\le n$, $\frac{\sigma(\overline{y}_i)}{\overline{y}_i}=\omega^{\lambda_i}\in k_2$ for some $\lambda_i\in\mathbf{Z}$. $\sigma^e=Id$ and $\omega^{\lambda_i e}=1$ and $\frac{d}{e}\mid\lambda_i$ for $1\le i\le n$. There exists $\sigma\in\mathrm{Gal}(L'/L_0)$ of order e. If $\frac{\sigma(y_i)}{y_i}=\omega^{\lambda_i}$ for $1\le i\le n$, we then have $\gcd(\lambda_1,\ldots,\lambda_n)=\frac{d}{e}$ and thus $\omega^{\frac{d}{e}}\in k_2$ which is a primitive e^{th} root of unity.

L^*/L Galois implies the fixed field of the image of $\mathrm{Gal}(L^*/L)$ in $\mathrm{Gal}(k_2/k_1)$ by the natural morphism is k_1. Thus k_2/k_1 is Galois and the diagram (9) is short exact.

Now suppose that k_2/k_1 is Galois and k_2 contains a primitive e^{th} root of unity. Then there is a natural inclusion

$$\mathbf{Z}^n/A\mathbf{Z}^n\cong\mathrm{Gal}(L^*/L_1)\rightarrow\mathrm{Gal}(L^*/L).$$

To show that L^*/L is Galois, is thus suffices to show that any $\sigma\in\mathrm{Gal}(k_2/k_1)$ extends to an L automorphism of L^*. σ extends to an L automorphism of L_1 such that $\sigma(x_i)=x_i$ for all i. Since L^* is Galois over L_1, σ extends to an L automorphism of L^*. □

Remark 4.5. *With the assumptions of Lemma 4.4, assume that L^* is Galois over L. Then $Gal(L^*/L)$ acts faithfully on $T=k_2[\overline{y}_1,\ldots,\overline{y}_n]$ by $k_1[x_1,\ldots,x_n]$ automorphisms, and we have natural inclusions of invariant rings*

$$k_1[x_1,\ldots,x_n]\subset T^{Gal(L^*/L)}\subset T^{\mathbf{Z}^n/A\mathbf{Z}^n}\subset T. \tag{10}$$

Suppose that $\tau\in k_2$ is a primitive e^{th} root of unity, $d=\mid det(A)\mid$. To $c\in\mathbf{Z}^n/A\mathbf{Z}^n$ the corresponding k_2-algebra automorphism σ_c of T is defined by

$$\sigma_c(\overline{y}_i)=\tau^{<B_i,c>\frac{e}{d}}\overline{y}_i$$

for $1\le i\le n$, where B_i is the i^{th} row of $dA^{-1}=\pm adj(A)$.

Theorem 4.6. *Suppose that*

$$R_0\rightarrow R\rightarrow S\subset V_{\nu^*}$$

is a sequence of the form of (7) of Theorem 4.2. Let k' be an algebraic closure of S/m_S. Then

$$\hat{R}\otimes_{R/m_R}k'\cong(\hat{S}\otimes_{S/M_S}k')^{\mathbf{Z}^n/A\mathbf{Z}^n}$$

by the faithful action of $\mathbf{Z}^n/A\mathbf{Z}^n$ on $\hat{S}\otimes_{S/m_S}k'$ of Remark 4.5. If

$$\hat{R}\otimes_{S/m_S}k'\cong k'[[x^{e_1},\ldots,x^{e_r}]],$$

then

$$R\cong R_0[x^{e_1},\ldots,x^{e_r}]_P,$$

where $P=(x^{e_1},\ldots,x^{e_r})$. In particular, R has normal toric singularities.

Proof. Set $k_1=R_0/m_{R_0}$, $k_2=S/m_S$. From (6) we see that there are regular parameters $\overline{y}_1,\ldots,\overline{y}_n$ in $\hat{S}$ and $\alpha_i\in k_2$ such that

$$x_i=\alpha_i\overline{y}_1^{a_{i1}}\cdots\overline{y}_n^{a_{in}}$$

for $1\le i\le n$. Let $d=\mid\det(A)\mid>0$. Set $F=\mathbf{Z}^n/A\mathbf{Z}^n$.

Set $\overline{x}_i=\frac{x_i}{\alpha_i}$, $1\le i\le n$. By Lemma 4.4, $k'(\overline{y}_1,\ldots,\overline{y}_n)$ is Galois over $k'(\overline{x}_1,\ldots,\overline{x}_n)$ with Galois group F. By Remark 4.5, we have an expansion

$$k'[\overline{y}_1,\ldots,\overline{y}_n]^F=k'[\overline{y}^{c_1},\ldots,\overline{y}^{c_r}]$$

where $c_i\in\mathbf{N}^r$ and $\overline{y}^{c_i}=\overline{x}^{e_i}$ with $e_i\in\mathbf{Z}^n$, and these invariants include $\overline{x}_1,\ldots,\overline{x}_n$.

$$k'[\overline{y}^{c_1},\ldots,\overline{y}^{c_r}]=k'[x^{e_1},\ldots,x^{e_r}]$$

is normal, and thus $k_1[x^{e_1},\ldots,x^{e_r}]$ is normal. We have $x^{e_i}=\epsilon_i y^{c_i}$ in K^* where $\epsilon_i\in S$ are units. $R_0[x^{e_1},\ldots,x^{e_r}]$ has a maximal ideal $m=(x^{e_1},\ldots,x^{e_r})$. Set $R_1=R_0[x^{e_1},\ldots,x^{e_r}]_m$. $R_1/m_{R_1}=R_0/m_{R_0}$. We have $R_0\subset R_1\subset S$. $\hat{R}_1=k_1[[x^{e_1},\ldots,x^{e_r}]]$ is normal (Theorem 32, Section 13, Chapter VIII [22]), so R_1 is normal since $\hat{R}_1\cap K=R_1$ (by Lemma 2, [1]). Since $\sqrt{m_{R_1}S}=m_S$, R_1 lies below S by Zariski's Main Theorem (10.9 [5]). Thus $R_1=S\cap K=R$ by Proposition 1 (iv) [1]. $\square$

Theorem 4.7. *Suppose that assumptions are as in Theorem 4.2. Let k' be an algebraic closure of V^*/m_{V^*}. Then there exists a sequence*

$$R_0\rightarrow R\rightarrow S\subset V_{\nu^*}$$

of the form of (7) of Theorem 4.2, with the following property. Suppose that there is a commutative diagram

$$\begin{array}{lllllll} R_0(1) & \rightarrow & R(1) & \rightarrow & S(1) & \subset V_{\nu^*}\\ \uparrow & & \uparrow & & \uparrow & \\ R_0 & \rightarrow & R & \rightarrow & S & \end{array}$$

such that the top row is also a sequence of the form of (7) of Theorem 4.2, so that there are regular parameters $(x_1(1),\ldots,x_n(1))$ in $R_0(1)$, $(y_1(1),\ldots,y_n(1))$ in $S(1)$, units $\delta_i(1)\in S(1)$ and a matrix $A(1)$ of natural numbers (with nontrivial determinant) such that

$$x_i(1)=y_1(1)^{a_{i1}(1)}\cdots y_n(1)^{a_{in}(1)}\delta_i(1)$$

for $1\le i\le n$. Then

$$\mathbf{Z}^n/A\mathbf{Z}^n\cong\mathbf{Z}^n/A(1)\mathbf{Z}^n.$$

Let L be the quotient field of $\hat{R}\otimes_{R/m_R}k'$, M be the quotient field of $\hat{S}\otimes_{S/M_S}k'$, L_1 be the quotient field of $\hat{R}(1)\otimes_{R(1)/m_{R(1)}}k'$, M_1 be the quotient field of $\hat{S}(1)\otimes_{S(1)/M_{S(1)}}k'$. Then there are natural restriction maps of Galois groups

$$Gal(M_1/L_1)\rightarrow Gal(M/L)\tag{11}$$

which are isomorphisms.

Proof. Let

$$R_0\rightarrow R\rightarrow S\subset V_{\nu^*}$$

be a sequence of the form of (7) of Theorem 4.2. Let

$$\begin{array}{lllllll} R_0(1) & \rightarrow & R(1) & \rightarrow & S(1) & \subset V_{\nu^*}\\ \uparrow & & \uparrow & & \uparrow & \\ R_0 & \rightarrow & R & \rightarrow & S & \end{array}$$

be a commutative diagram such that the top row is also a sequence of the form of (7) of Theorem 4.2.

There exist ideals $I\subset R$ and $J\subset S$, $f\in I$, $g\in J$, maximal ideals m_1 in $R[\frac{I}{f}]$ and n_1 in $S[\frac{J}{g}]$ such that $R(1)=R[\frac{I}{f}]_{m_1}$, $S(1)=S[\frac{J}{g}]_{n_1}$.

Let $\overline{R}=\hat{R}\otimes_{R/m_R}k'$, $\overline{S}=\hat{S}\otimes_{S/M_S}k'$, $\overline{R}_1=\hat{R}(1)\otimes_{R(1)/m_{R(1)}}k'$,

$$\overline{S}_1=\hat{S}(1)\otimes_{S(1)/M_{S(1)}}k'.$$

We have natural inclusions $\overline{R}[\frac{I}{f}]\rightarrow\overline{R}_1$ and $\overline{S}[\frac{J}{g}]\rightarrow\overline{S}_1$. Let $\overline{m}=\overline{R}[\frac{I}{f}]\cap m_{\overline{R}_1}$, $\overline{n}=\overline{S}[\frac{J}{g}]\cap m_{\overline{S}_1}$. Let $\tilde{R}=\overline{R}[\frac{I}{f}]_{\overline{m}}$, $\tilde{S}=\overline{S}[\frac{J}{g}]_{\overline{n}}$. We have a commutative diagram of inclusions of local rings

$$\begin{array}{ccc} \overline{R}_1 & \rightarrow & \overline{S}_1 \\ \uparrow & & \uparrow \\ \tilde{R} & \rightarrow & \tilde{S} \\ \uparrow & & \uparrow \\ \overline{R} & \rightarrow & \overline{S} \end{array}.$$

By construction, $\overline{R}_1 = \hat{\tilde{R}}$ and $\overline{S}_1 = \hat{\tilde{S}}$. Let $L = \mathrm{QF}(\overline{R})$, $M = \mathrm{QF}(\overline{S})$, $L_1 = \mathrm{QF}(\overline{R}_1)$, $M_1 = \mathrm{QF}(\overline{S}_1)$. $\tilde{R}$ and $\tilde{S}$ are normal local rings, since $\tilde{R} = \overline{R}_1 \cap L$ and $\tilde{S} = \overline{S}_1 \cap M$, by Lemma 2 [1].

By Theorem 4.6, M is Galois over L and M_1 is Galois over L_1. There is a natural isomorphism (the notation G^s is defined in Section 4)

$$\mathrm{Gal}(M_1/L_1) \cong G^s(\tilde{S}/\tilde{R})$$

by Lemma 7 [1]. (The proof of this Lemma generalizes without difficulty to fields of the form of M and L). In particular, there is a 1-1 restriction homomorphism

$$\mathrm{Gal}(M_1/L_1) \rightarrow \mathrm{Gal}(M/L).$$

If this map is not an isomorphism, we can replace $R_0 \rightarrow S$ with $R_0(1) \rightarrow S(1)$. After repeating this process a finite number of times, we will find an extension $R_0 \rightarrow S$ such that the conclusions of the Theorem hold. □

Theorem 4.8. *(Strong Monomialization) Let k be a field of characteristic zero, K an algebraic function field over k, K^* a finite algebraic extension of K, ν^* a k-valuation of K^*. Suppose that S^* is an algebraic local ring with quotient field K^* which is dominated by ν^* and R^* is an algebraic local ring with quotient field K which is dominated by S^*. Let notation be as in Section 3 for $V = V_\nu$, $V^* = V_{\nu^*}$. Then there exists a commutative diagram*

$$\begin{array}{ccccc} R_0 & \rightarrow & S & \subset & V^* \\ \uparrow & & \uparrow & & \\ R^* & \rightarrow & S^* & & \end{array} \tag{12}$$

such that $R^* \rightarrow R_0$ and $S^* \rightarrow S$ are sequences of monoidal transforms such that V^* dominates S, S dominates R_0 and there are regular parameters $(x_1, ..., x_n)$ in R_0, $(y_1, ..., y_n)$ in S such that

$$\begin{array}{l} p_i \cap R_0 = (x_1, \ldots, x_{t_1+\cdots+t_i}) \\ p_i^* \cap S = (y_1, \ldots, y_{t_1+\cdots+t_i}) \end{array}$$

for $1 \le i \le r$ and there are relations

$$
\begin{aligned}
x_1 &= y_1^{g_{11}(1)} \cdots y_{s_1}^{g_{1s_1}(1)} y_{t_1+1}^{h_{1,t_1+1}(1)} \cdots y_m^{h_{1m}(1)} \delta_{11}\\
&\vdots\\
x_{s_1} &= y_1^{g_{s_1 1}(1)} \cdots y_{s_1}^{g_{s_1 s_1}(1)} y_{t_1+1}^{h_{s_1,t_1+1}(1)} \cdots y_m^{h_{s_1 m}(1)} \delta_{1s_1}\\
x_{s_1+1} &= y_{s_1+1} y_{t_1+1}^{h_{s_1+1,t_1+1}(1)} \cdots y_m^{h_{s_1+1,m}(1)} \delta_{1,s_1+1}\\
&\vdots\\
x_{t_1} &= y_{t_1} y_{t_1+1}^{h_{t_1,t_1+1}(1)} \cdots y_n^{h_{t_1 n}(1)} \delta_{1t_1}\\
x_{t_1+1} &= y_{t_1+1}^{g_{11}(2)} \cdots y_{t_1+s_2}^{g_{1s_2}(2)} y_{t_1+t_2+1}^{h_{1,t_1+t_2+1}(2)} \cdots y_m^{h_{1m}(2)} \delta_{21}\\
&\vdots\\
x_{t_1+s_2} &= y_{t_1+1}^{g_{s_2 1}(2)} \cdots y_{t_1+s_2}^{g_{s_2 s_2}(2)} y_{t_1+t_2+1}^{h_{s_2,t_1+t_2+1}(2)} \cdots y_n^{h_{s_2 n}(2)} \delta_{2s_2}\\
x_{t_1+s_2+1} &= y_{t_1+s_2+1} y_{t_1+t_2+1}^{h_{s_2+1,t_1+t_2+1}(2)} \cdots w_m^{h_{s_2+1,m}(2)} \delta_{2,s_2+1}\\
&\vdots\\
x_{t_1+t_2} &= y_{t_1+t_2} y_{t_1+t_2+1}^{h_{t_2,t_1+t_2+1}(2)} \cdots y_m^{h_{t_2 m}(2)} \delta_{2t_2}\\
&\vdots\\
x_{t_1+\cdots+t_{r-1}+1} &= y_{t_1+\cdots+t_{r-1}+1}^{g_{11}(r)} \cdots y_{t_1+\cdots+t_{r-1}+s_r}^{g_{1s_r}(r)} \delta_{r1}\\
&\vdots\\
x_{t_1+\cdots+t_{r-1}+s_r} &= y_{t_1+\cdots+t_{r-1}+1}^{g_{s_r 1}(r)} \cdots y_{t_1+\cdots+t_{r-1}+s_r}^{g_{s_r s_r}(r)} \delta_{rs_r}\\
x_{t_1+\cdots+t_{r-1}+s_r+1} &= x_{t_1+\cdots+t_{r-1}+s_r+1} \delta_{r,s_r+1}\\
&\vdots\\
x_{t_1+\cdots+t_r} &= y_{t_1+\cdots+t_r} \delta_{rt_r}
\end{aligned}
$$

where $m = t_1 + \cdots + t_{r-1} + s_r$ and for $1 \le i \le r$,

$$
det \begin{pmatrix} g_{11}(i) & \cdots & g_{1s_i}(i) \\ \vdots & & \vdots \\ g_{s_i 1}(i) & \cdots & g_{s_i s_i}(i) \end{pmatrix} \ne 0,
$$

δ_{ij} are units in S, $h_{jk}(i)$ are natural numbers such that for $1 \le l \le k \le r-1$,

$$
h_{i,j}(l) = 0 \text{ if } 1 \le i \le t_l \text{ and } t_1 + \cdots + t_k + s_{k+1} < j \le t_1 + \cdots + t_{k+1}.
$$

Let

$$
T = \{ j \mid t_1 + \cdots + t_k < j \le t_1 + \cdots + t_k + s_{k+1} \text{ for some } 0 \le k \le r-1 \}.
$$

Then $\{\nu^*(y_j) \mid j \in T\}$ is a rational basis of $\Gamma^* \otimes \mathbf{Q}$, $\{\nu^*(x_j) \mid j \in T\}$ is a rational basis of $\Gamma \otimes \mathbf{Q}$.

Theorem 4.8 can be visualized as follows. For $1 \le i \le r$ there are $t_i \times t_i$ matrices

$$
M_i = \begin{pmatrix} (g_{jk}(i)) & 0 \\ 0 & I_{t_i - s_i} \end{pmatrix}
$$

corresponding to the composite valuation rings $(V/p_{i-1})_{p_i}$, such that

$$
A = \begin{pmatrix} M_1 & *0 & *0 & \cdots & *0 \\ & M_2 & *0 & \cdots & *0 \\ & & M_3 & \cdots & *0 \\ & 0 & & \cdots & *0 \\ & & & & M_r \end{pmatrix}. \qquad (13)
$$

The smbols“$*0$” in (13) denote $t_i \times t_j$ matrices whose last $t_j - s_j$columns are identically zero.

Proof. For valuations V of rank 1 this is immediate from Theorem 5.1 [10].

Suppose that V has rank $r > 1$ and that the Theorem is true for valuations of rank less than r. To reach the conclusions of the Theorem, we need only modify the proof of Theorem 5.3 [10] by observing that we can assume by induction that the upper $\lambda \times \lambda$ matrix of exponents of (131) in the proof of Theorem 5.1 [10] has the desired form, and notice that we actually have $e_{ij} = 0$ if $j > \lambda + s_r$ in (131). We can then construct a sequence of monoidal transforms $\overline{S}(m') \rightarrow \overline{S}(m'+1)$ along ν^* by choosing

$$t > \max\{a_{ij}, g_{ij}(r)\}$$

and defining

$$\overline{y}_i(m') = \begin{cases} \overline{y}_{\lambda+1}(m'+1)^t \cdots \overline{y}_{\lambda+s_r}(m'+1)^t \overline{y}_i(m'+1) & 1 \le i \le \lambda \\ \overline{y}_i(m'+1) & \lambda+1 \le i \le n \end{cases}$$

We then obtain the conclusions of Theorem 4.8. □

Theorem 4.9. *With the assumptions of Theorem 4.8, further suppose that* $u_j \in V^*$*,* $1 \le j \le \bar{l}$*, and* $v_j \in V$*,* $1 \le j \le \overline{m}$*. Then there exists a commutative diagram*

$$\begin{array}{ccccc} R_0 & \rightarrow & S & \subset & V^* \\ \uparrow & & \uparrow & & \\ R^* & \rightarrow & S^* & & \end{array}$$

such that the conclusions of Theorem 4.8 hold and

(1) $v_j = x_1^{b_{j1}} \cdots x_n^{b_{jn}} \delta_j \in R_0$ *for* $1 \le j \le \overline{m}$*, where* $\delta_j \in R_0$ *is a unit, and* $b_{ji} = 0$ *if* $t_1 + \cdots + t_l + s_l < i \le i_1 + \cdots + t_{l+1}$ *for some* l*.*

(2) $u_j = y_1^{d_{j1}} \cdots y_n^{d_{jn}} \epsilon_j \in S$ *for* $1 \le j \le \bar{l}$*, where* $\epsilon_j \in S$ *is a unit, and* $d_{ji} = 0$ *if* $t_1 + \cdots + t_l + s_l < i \le t_1 + \cdots + t_{l+1}$ *for some* l*.*

Proof. First assume that ν has rank 1. As in the beginning of the proof of Theorem 5.1 [10], first construct a sequence of monoidal transforms $R^* \rightarrow R_1$ along ν such that $R_1/m_1 \rightarrow V/m_V$ is algebraic, and there are regular parameters $(x_1(1), \ldots, x_n(1))$ in R_1 such that $\nu(x_1(1)), \ldots, \nu(x_s(1))$ are a basis of $\Gamma \otimes \mathbf{Q}$. For $1 \le i \le \overline{m}$, write $v_i = \frac{f_i}{g_i}$ with $f_i, g_i \in R_1$. By Theorem 4.8 [10] (with $S = R$, $l = n$, $m = n$) applied to $f = f_i$ or $f = g_i$ in (60) and by (2) of Theorem 4.10 [10] (with $S = R$, $l = n$) we can perform a sequence of monoidal transforms along ν $R_1 \rightarrow R_2$ where R_2 has regular parameters $(x_1(2), \ldots, x_n(2))$ such that $\nu(y_1(2)), \ldots, \nu(y_s(2))$ are a basis of $\Gamma \otimes \mathbf{Q}$ and

$$\begin{aligned} f_i &= x_1(2)^{\overline{c}_{i1}} \cdots x_s(2)^{\overline{c}_{is}} \overline{\alpha}_i \\ g_i &= x_1(2)^{\overline{d}_{i1}} \cdots x_s(2)^{\overline{d}_{is}} \overline{\beta}_i \end{aligned}$$

where $\overline{\alpha}_i$, $\overline{\beta}_i$ are units in R_2. We remark that (A3) on page 83 [10] implies $\nu(m(U(t))$ of (64) in Theorem 4.8 [10] is a constant which does not depend on N for $N \ge N_0$. Now by (25) of Lemma 4.2 [10], applied to the pair f_i, g_i we can perform a further sequence of monoidal transforms $R_2 \rightarrow R_3$ along ν to achieve that $v_i \in R_3$ for $1 \le i \le \overline{m}$, and there exist regular parameters $(x_1(3), \ldots, x_n(3))$ in R_3 such that $\nu(x_1(3)), \ldots, \nu(x_s(3))$ are a basis of $\Gamma \otimes \mathbf{Q}$,

$$v_i = x_1(3)^{\tilde{d}_{i1}} \cdots x_s(3)^{\tilde{d}_{is}} \epsilon_i$$

for $1 \le i \le \overline{m}$ where $\tilde{d}_{i1}, \ldots, \tilde{d}_{is}$ are natural numbers, ϵ_i are units in R_3.

Let $S^* \to S_2$ be a sequence of monoidal transforms along ν^* so that S_2 dominates R_3. As in the proof of Theorem 5.1 [10], we can perform a sequence of monoidal transforms $S_2 \to S_3$ along ν^* so that $u_i \in S_3$ for all i, S_2 has a regular system of parameters $(y_1(3),\dots,y_n(3))$ such that

$$x_i = y_1(3)^{c_{i1}} \cdots y_s(3)^{c_{is}} \phi_i$$

$1 \le i \le s$, ϕ_i are units in S_2, $(y_1(3),\dots,y_s(3))$ is a basis of $\Gamma^* \otimes \mathbf{Q}$ and $\det(c_{ij}) \ne 0$.

By Theorem 5.1 [10], we can perform a sequence of monoidal transforms

$$\begin{array}{ccc} R_4 & \to & S_4 \\ \uparrow & & \uparrow \\ R_3 & \to & S_3 \end{array}$$

so that R_4 has regular parameters $(x_1(4),\dots,x_n(4))$, S_4 has regular parameters $(y_1(4),\dots,y_n(4))$ such that

$$\begin{array}{ll} x_1(4) & = y_1(4)^{e_{11}} \cdots y_s(4)^{e_{1s}} \delta_1 \\ & \vdots \\ x_s(4) & = y_1(4)^{e_{s1}} \cdots y_s(4)^{e_{ss}} \delta_s \\ x_{s+1}(4) & = y_{s+1}(4) \\ & \vdots \\ x_n(4) & = y_n(4) \end{array}$$

where $\det(e_{ij}) \ne 0$, $\delta_1,\dots,\delta_s$ are units in S_4, $(\nu(x_1(4)),\dots,\nu(x_s(4)))$ is a rational basis of $\Gamma \otimes \mathbf{Q}$. We further have

$$v_i = x_1(4)^{d_{i1}} \cdots x_s(4)^{d_{is}} \epsilon_i$$

$1 \le i \le \overline{m}$, $\epsilon_i \in R_4$ units (since the monoidal transforms used in the proof of Theorem 5.1 [10] preserve this form) and $u_i \in S_4$, $1 \le i \le \overline{l}$.

Now by (60) of Theorem 4.8 and (2) of Theorem 4.10 [10], with $l = n$ and $m = n$, applied to $R_4 \to S_4$ and $f = u_1 \cdots u_{\overline{l}}$, we achieve a commutative diagram

$$\begin{array}{ccc} R' & \to & S' \\ \uparrow & & \uparrow \\ R_4 & \to & S_4 \end{array}$$

where the vertical arrows are sequences of monoidal transforms along ν^* such that the conclusions of the Theorem hold in $R' \to S'$.

Now assume that V has rank $r > 1$. For the general case of rank $r > 1$ we must modify the proof of Theorem 5.3 [10]. We assume (by induction) that the Theorem is true for valuations of rank $< r$.

We first construct (as in the proof of Theorem 5.3 [10]) sequences of monoidal transforms

$$\begin{array}{ccc} R(1) & \to & S(1) \\ \uparrow & & \uparrow \\ R^* & \to & S^* \end{array}$$

along ν^* such that if $p_i(1) = p_i \cap R(1)$, $q_i(1) = q_i \cap S(1)$ then

$$\mathrm{trdeg}_{(R(1)/p_i(1))_{p_i(1)}} (V^*/p_i)_{p_i} = 0$$

for $1 \le i \le r$ and (using the induction assumption) that the conclusions of the Theorem hold for $R(1)_{p_{r-1}(1)} \to S(1)_{q_{r-1}(1)}$. Set

$$\lambda = t_1 + \cdots + t_{r-1}.$$

As in the proof of Theorem 5.3 [10], we can construct sequences of monoidal transforms

$$\begin{array}{lll} R'' & \rightarrow & S'' \\ \uparrow & & \uparrow \\ R(1) & \rightarrow & S(1) \end{array}$$

along ν^* such that if $q''_{r-1}=p_{r-1}\cap S''$, $p''_{r-1}=p_{r-1}\cap R''$, then $R(1)_{p_{r-1}(1)}=R''_{p''_{r-1}}$, $S(1)_{q_{r-1}(1)}=S''_{q''_{r-1}}$, there exist regular parameters $(x''_1,\ldots,x''_n)$ in R'', $(y''_1,\ldots,y''_n)$ in S'' such that, as in (129) of the proof of Theorem 5.3 [10],

$$\begin{array}{ll} x''_1 & =\psi_1(y''_1)^{g_{11}(1)}\cdots(y''_{s_1})^{g_{1,s_1}(1)}(y''_{t_1+1})^{h_{1,t_1+1}(1)}\cdots(y''_\lambda)^{h_{1\lambda}(1)}\\ & \vdots\\ x''_\lambda & =\psi_\lambda y''_\lambda \end{array}$$

with $\psi_1,\cdots,\psi_\lambda\in S''-q''_{r-1}$, and

$$u_j=\overline{\gamma}_j(y''_1)^{\overline{e}_{j1}}\cdots(y''_\lambda)^{\overline{e}_{j\lambda}} \tag{14}$$

$1\le j\le\overline{l}$ with $\overline{\gamma}_j\in S''-q''_{r-1}$ and

$$v_j=\gamma_j(x''_1)^{e_{j1}}\cdots(x''_\lambda)^{e_{j\lambda}} \tag{15}$$

$1\le j\le\overline{m}$ with $\gamma_j\in R''-p''_{r-1}$.

We further have that the exponents of $y''_1,\ldots,y''_\lambda$ (respectively $x''_1,\ldots,x''_\lambda$) in (14) (respectively (15)) are of the form of the conclusions of the Theorem (by our induction assumption on the rank), or $u_j=\overline{\gamma}_j$, $v_j=\gamma_j$.

We now construct a sequence of monoidal transforms along ν^* (as in the proof of Theorem 5.3 [10]).

$$\begin{array}{lll} R(m') & \rightarrow & \overline{S}(m') \\ \uparrow & & \uparrow \\ R'' & \rightarrow & S'' \end{array}$$

so that there exist regular parameters $(\overline{y}_1(m'),\ldots,\overline{y}_n(m'))$ in $\overline{S}(m')$, $(x_1(m'),\ldots,x_n(m'))$ in $R(m')$ such that (as in (131) of page 121 of the proof of Theorem 5.3 [10])

$$\begin{array}{ll} x_1(m') & =\overline{y}_1(m')^{g_{11}(1)}\cdots\overline{y}_{s_1}(m')^{g_{1s_1}(1)}\overline{y}_{t_1+1}(m')^{h_{1,t_1+1}(1)}\cdots\overline{y}_\lambda(m')^{h_{1\lambda}(1)}\\ & \quad\cdot\overline{y}_{\lambda+1}(m')^{e_{1,\lambda+1}}\cdots\overline{y}_{\lambda+s_r}(m')^{e_{1,\lambda+s_r}}\psi_1\\ & \vdots\\ x_\lambda(m') & =\overline{y}_\lambda(m')\overline{y}_{\lambda+1}(m')^{e_{\lambda,\lambda+1}}\cdots\overline{y}_{\lambda+s_r}(m')^{e_{\lambda,\lambda+s_r}}\psi_\lambda\\ x_{\lambda+1}(m') & =\overline{y}_{\lambda+1}(m')^{g_{11}(r)}\cdots\overline{y}_{\lambda+s_r}(m')^{g_{s_rs_r}(r)}\delta_{\lambda+1}+f_1^{\lambda+1}\overline{y}_1(m')+\cdots+f_\lambda^{\lambda+1}\overline{y}_\lambda(m')\\ \vdots & \\ x_n(m') & =\overline{y}_n(m')\delta_n+f_1^n\overline{y}_1(m')+\cdots+f_\lambda^n\overline{y}_\lambda(m') \end{array}$$

where δ_i are units in $\overline{S}(m')$, $f_i^j\in\overline{S}(m')$ for $1\le i\le\lambda$,

$$\psi_i=u'_i\overline{y}_{\lambda+1}(m')^{a_{i,\lambda+1}}\cdots\overline{y}_{\lambda+s_r}(m')^{a_{i,\lambda+s_r}}+h_1^i\overline{y}_1(m')+\cdots+h_\lambda^i\overline{y}_\lambda(m')$$

where u'_i are units in $\overline{S}(m')$, and we further have

$$v_j=\alpha_jx_1(m')^{e_{j1}}\cdots x_\lambda(m')^{e_{j\lambda}}$$

$1\le j\le\overline{m}$, where $e_{ji}=0$ if $t_1+\cdots+t_l+s_l<i\le t_1+\cdots+t_{l+1}$ for some l.

$$u_j=\beta_j\overline{y}_1(m')^{f_{j1}}\cdots\overline{y}_\lambda(m')^{f_{j\lambda}}$$

$1\le j\le\overline{l}$, where $f_{ji}=0$ if $t_1+\cdots+t_l+s_l<i\le t_1+\cdots+t_{l+1}$ for some l,

$$\alpha_j = \overline{\alpha}_j x_{\lambda+1}(m')^{\overline{a}_{j,\lambda+1}} \cdots x_{\lambda+s_r}(m')^{\overline{a}_{j,\lambda+s_r}} + \overline{h}_1^j x_1(m') + \cdots + \overline{h}_\lambda^j x_\lambda(m'), \tag{16}$$

where $\overline{\alpha}_j$ are units in $R(m')$, $\overline{h}_i^j \in R(m')$ and

$$\beta_j = \overline{\beta}_j \overline{y}_{\lambda+1}(m')^{\tilde{a}_{j,\lambda+1}} \cdots \overline{y}_{\lambda+s_r}(m')^{\tilde{a}_{j,\lambda+s_r}} + \tilde{h}_1^j \overline{y}_1(m') + \cdots + \tilde{h}_\lambda^j \overline{y}_1(m') + \cdots + \tilde{h}_\lambda^j \overline{y}_\lambda(m') \tag{17}$$

where $\overline{\beta}_j$ are units in $\overline{S}(m')$, $\tilde{h}_i^j \in \overline{S}(m')$.

Set $t_1 = \max\{\overline{a}_{ji}\}$ in (16). Define a sequence of monoidal transforms along V $\overline{R}(m') \to \overline{R}(m'+1)$ where $\overline{R}(m'+1)$ has regular parameters $(\overline{x}_1(m'+1), \dots, \overline{x}_n(m'+1))$ defined by by

$$\overline{x}_i(m') = \begin{cases} \overline{x}_{\lambda+1}(m'+1)^{t_1} \cdots \overline{x}_{\lambda+s_r}(m'+1)^{t_1} \overline{x}_i(m'+1) & 1 \le i \le \lambda \\ \overline{x}_i(m'+1) & \lambda+1 \le i \le n \end{cases}$$

Set $t_2 = \max\{\tilde{a}_{ji}, g_{ij}(r), a_{ij}, t_1\}$. Now perform a sequence of monoidal transforms along ν^*, $\overline{S}(m') \to \overline{S}(m'+1)$ where $\overline{S}(m'+1)$ has regular parameters $(\overline{y}_1(m'+1), \dots, \overline{y}_n(m'+1))$ defined by

$$\overline{y}_i(m') = \begin{cases} \overline{y}_{\lambda+1}(m'+1)^{t_2} \cdots \overline{y}_{\lambda+s_r}(m'+1)^{t_2} \overline{y}_i(m'+1) & 1 \le i \le \lambda \\ \overline{y}_i(m'+1) & \lambda+1 \le i \le n \end{cases}$$

Then $\overline{S}(m'+1)$ dominates $\overline{R}(m'+1)$ and the conclusions of the Theorem hold in $\overline{R}(m'+1) \to \overline{S}(m'+1)$. □

Theorem 4.10. *Suppose that assumptions are as in Theorem 4.2. Let k' be an algebraic closure of V^*/m_{V^*}. Then there exists a sequence*

$$R_0 \to R \to S \subset V_{\nu^*}$$

of the form of (7) of Theorem 4.2, which satisfies the conclusions of Theorem 4.7, and with the following property. Suppose that there is a commutative diagram

$$\begin{array}{ccccccc} R_0(1) & \to & R(1) & \to & S(1) & \subset V_{\nu^*} \\ \uparrow & & \uparrow & & \uparrow & \\ R_0 & \to & R & \to & S & \end{array}$$

such that the top row is also a sequence of the form of (7) of Theorem 4.2, so that there are regular parameters $(x_1(1), \dots, x_n(1))$ in $R_0(1)$, $(y_1(1), \dots, y_n(1))$ in $S(1)$, units $\delta_i(1) \in S(1)$ and a matrix $A(1)$ of natural numbers (with nontrivial determinant) such that

$$x_i(1) = y_1(1)^{a_{i1}(1)} \cdots y_n(1)^{a_{in}(1)} \delta_i(1)$$

for $1 \le i \le n$. Then there is an isomorphism of Abelian groups

$$\mathbf{Z}^n / A(1)\mathbf{Z}^n \cong \Gamma^*/\Gamma.$$

Γ^*/Γ acts faithfully on $\hat{S}(1) \otimes_{S(1)/m_{S(1)}} k'$ by k'-algebra automorphisms, and there is an isomorphism

$$(\hat{S}(1) \otimes_{S(1)/m_{S(1)}} k')^{\Gamma^*/\Gamma} \cong \hat{R}(1) \otimes_{R(1)/m_{R(1)}} k'.$$

Proof. There exist $u_1, \dots, u_{\overline{l}} \in V^*$ such that Γ^*/Γ is generated by $\nu^*(u_1,), \dots, \nu^*(u_{\overline{l}})$. By Theorem 4.9 and Theorem 4.7, there exists a sequence $R_0 \to R \to S$ of the form of (7) of Theorem 4.2 such that the conclusions of Theorem 4.7 hold, and there are units $\beta_i \in S$ and natural numbers e_{ij} such that with the notation of Theorem 4.9 (and Theorem 4.8),

$$u_i = \beta_i \prod_{j \in T} y_j^{e_{ij}}$$

for $1 \le i \le \bar{l}$.

Observe that $\mathbf{Z}^n/A\mathbf{Z}^n \cong \mathbf{Z}^n/A^t\mathbf{Z}^n$ since A and A^t have the same invariant factors. We will prove that $\mathbf{Z}^n/A^t\mathbf{Z}^n \cong \Gamma^*/\Gamma$. Then the conclusions of the Theorem will follow from Theorem 4.7 and 4.6.

We have a group homomorphism

$$\Psi : \mathbf{Z}^n \to \Gamma^*/\Gamma$$

defined by

$$(b_1, \dots, b_n) \mapsto b_1\nu^*(y_1) + \cdots + b_n\nu^*(y_n).$$

Ψ is onto since $\{\nu^*(u_i) \mid 1 \le i \le \bar{l}\}$ generate Γ^*/Γ. By definition of A, $\Psi(A^t\mathbf{Z}^n) \subset \Gamma$. Let $\{e_i\}$ be the standard basis of $\mathbf{Z}^n$.

Suppose that $\Psi(\sum \lambda_m e_m) = 0$. Then

$$\sum \lambda_m \nu^*(y_m) = \nu(f)$$

for some $f \in K$. By Theorem 4.9, there exists a diagram

$$\begin{array}{lcl} R_0(1) & \to & S(1) \\ \uparrow & & \uparrow \\ R_0 & \to & S \end{array}$$

such that $f \in R_0(1)$ satisfies

$$f = \prod_{l \in T} x_l(1)^{b_l}\delta,$$

b_l natural numbers, $\delta \in R_0(1)$ a unit, and

$$y_i = \prod_{l \in T} y_l(1)^{c_{il}}\epsilon_i$$

for $1 \le i \le n$, c_{il} natural numbers, $\epsilon_i \in S(1)$ units.

$$\begin{array}{ll} \nu^*(\prod y_m^{\lambda_m}) & = \nu^*(\prod_{l \in T} y_l(1)^{\sum \lambda_m c_{ml}}) = \nu^*(f) \\ & = \nu^*(\prod x_m(1)^{b_m}) = \nu^*\left(\prod_m(\prod_{l \in T} y_l(1)^{a_{ml}(1)})^{b_m}\right) \end{array}$$

implies

$$\sum_m \lambda_m c_{ml} = \sum_m a_{ml} b_m$$

for all $l \in T$ since $\{\nu^*(y_l(1)) \mid l \in T\}$ are linearly independent. Thus

$$\prod y_m^{\lambda_m} = f\tilde{\delta}$$

where $\tilde{\delta} \in S(1)$ is a unit.

Set $R(0) = R$, $S(0) = S$. For $j = 0, 1$, let $K(j) = \mathrm{QF}(\hat{R}(j) \otimes_{R(j)/m_{R(j)}} k')$, $L(j) = \mathrm{QF}(\hat{S}(j) \otimes_{S(j)/m_{S(j)}} k')$. With notations as in (6), set

$$\overline{R}(j) := \hat{R}(j) \otimes_{R(j)/m_{R(j)}} k' \cong k'[[\overline{x}_1(j), \dots, \overline{x}_n(j)]]$$

and

$$\overline{S}(j) := \hat{S}(j) \otimes_{S(j)/m_{S(j)}} k' \cong k'[[\overline{y}_1(j), \dots, \overline{y}_n(j)]]$$

where

$$\overline{x}_i(j) = \overline{y}_1(j)^{a_{i1}(j)} \cdots \overline{y}_n(j)^{a_{in}(j)}$$

for $1 \le i \le n$. Let $A_T(j)$ be the $\mid T \mid \times \mid T \mid$ submatrix of $A(j)$ which is the matrix of exponents of

$$\overline{x}_i(j) = \prod_{l \in T, l \ge \lambda_k} \overline{y}_l(j)^{a_{il}(j)}$$

for $\lambda_k = t_1 + \cdots t_k$, $\lambda_k < i \le \lambda_k + s_{k+1}$.

We have a commutative diagram

$$\begin{array}{ccc} K(1) & \rightarrow & L(1) \\ \uparrow & & \uparrow \\ K(0) & \rightarrow & L(0) \end{array}$$

where the horizontal arrows are finite Galois, with respective Galois groups

$$G_1 \cong \mathbf{Z}^{|T|}/A_T(1)\mathbf{Z}^{|T|}$$

and

$$G \cong \mathbf{Z}^{|T|}/A_T(0)\mathbf{Z}^{|T|}.$$

We have

$$\prod \overline{y}_m(0)^{\lambda_m} = f\overline{\delta}$$

where $\overline{\delta} \in \overline{S}(1)$ is a unit.

Suppose that $\sigma \in G \cong G_1$. Then

$$\frac{\sigma(\prod \overline{y}_m(0)^{\lambda_m})}{\sigma(\overline{\delta})} = \frac{\prod \overline{y}_m(0)^{\lambda_m}}{\overline{\delta}}.$$

We can write $\overline{\delta} = c + h$ with $c \in k'$, $h \in m_{\overline{S}(1)}$. Thus $\sigma(\overline{\delta}) \equiv \overline{\delta} \mod m_{\overline{S}(1)}$.

$$\sigma(\prod \overline{y}_m(0)^{\lambda_m}) = \omega \prod \overline{y}_m(0)^{\lambda_m}$$

for some d^{th} root of unity $\omega \in k'$, with $d = \mid G \mid$. Thus

$$\frac{\sigma(\overline{\delta})}{\overline{\delta}} = 1$$

and

$$\sigma(\prod \overline{y}_m(0)^{\lambda_m}) = \prod \overline{y}_m(0)^{\lambda_m}$$

implies $\prod \overline{y}_m(0)^{\lambda_m} \in K(0)$, and

$$\prod \overline{y}_m(0)^{\lambda_m} = \prod \overline{x}_m(0)^{d_m}$$

for some $d_m \in \mathbf{Z}$. Thus $\sum \lambda_m e_m \in A^t\mathbf{Z}^n$. In particular,

$$\mathbf{Z}^n/A^t\mathbf{Z}^n \cong \Gamma^*/\Gamma.$$

□

5. Ramification in Galois extensions

Let k be a field of characteristic zero, K an algebraic function field over k, K^* a finite Galois extension of K with Galois group $G = \mathrm{Gal}(K^*/K)$, ν^* a k-valuation of K^*, with value group Γ^*. Let ν be the restriction of ν^* to K, and let Γ be the value group of ν.

Let V^* be the valuation ring of ν^* and V be the valuation ring of ν.

Suppose that R is a normal local ring with quotient field K and S is a normal local ring with quotient field K^* which lies above R. We can then define the splitting groups and inertia groups

$$G^s(S/R) = \{g \in G \mid g(S) = S\},$$

$$G^i(S/R) = \{g \in G^s(S/R) \mid g(u) \equiv u \mod m_S \text{ for all } u \in S\}.$$

$$G^i(S/R) \subset G^s(S/R) \subset G.$$

$G^i(S/R)$ is a normal subgroup of $G^s(S/R)$ (Theorem 1.48 [4]). The splitting field K^s of S over R is the fixed field of $G^s(S/R)$. The inertia field K^i of S over R is the fixed field of $G^i(S/R)$. We have a corresponding sequence of fields

$$K \to K^s \to K^i \to K^*.$$

K^s is the smallest subfield of K^* such that S is the only local ring lying above $S \cap K^s$ (Proposition 1.46 [4]). We have a sequence

$$R \to R^s \to R^i \to S \tag{18}$$

where $R^s = S \cap K^s$ is the localization of the integral closure of R in K^s at the center of ν^*. $R^i = S \cap K^i$ is the localization of the integral closure of R in K^i at the center of ν^*. $R \to R^s$ is unramified, with $R/m_R = R^s/m_{R^s}$, $R^s \to R^i$ is unramified, R^i/m_{R^i} is Galois over R^s/m_{R^s} with Galois group $G^s(S/R)/G^i(S/R)$ (by Theorem 1.48 [4]). We will write $G^s(\nu^*/\nu) = G^s(V^*/V)$, $G^i(\nu^*/\nu) = G^i(V^*/V)$.

Since we are in characteristic zero, by Theorem 3 [16] or Corollary, Section 12, Chapter VI [22], there is an isomorphism

$$G^i(\nu^*/\nu) \cong \Gamma^*/\Gamma. \tag{19}$$

Lemma 5.1. *Let assumptions be as in Theorem 4.2. Suppose that K^* is Galois over K. Let $t_1, \dots, t_f \in k(\nu^*)$ be a $k(\nu)$ basis. Then there exists an algebraic regular local ring R' with quotient field K which is dominated by ν such that if R is an algebraic normal local ring dominated by ν, $R' \subset R$, S is the localization of the integral closure of R in K^* at the center of ν^*, then $R/m_R \to k(\nu)$ is algebraic, $G^s(S/R) = G^s(\nu^*/\nu)$ and $G^i(S/R) = G^i(\nu^*/\nu)$. Further, $[S/m_S : R/m_R] = f$, and $\{t_1, \dots, t_f\}$ is a basis of S/m_S over R/m_R, where $f = [k(\nu^*) : k(\nu)]$ is the residue degree of ν^* with respect to ν.*

Proof. Let $V^* = V_1, V_2, \dots, V_n$ be the distinct valuation rings of K^* lying over V. Then $T = \cap_{i=1}^n V_i$ is the integral closure of V in K^* (by Propositions 2.36 and 2.38 [4]). Let $m_i = m_{V_i} \cap T$ be the maximal ideals of T. By the Chinese remainder theorem, there exists $u \in T$ such that $u \in m_1$ and $u \notin m_i$ for $i = 2, \dots, n$. Let

$$u^m + a_1 u^{m-1} + \cdots + a_m = 0$$

be the equation of integral dependence of u over V. Let $R_0 \subset K$ be an algebraic regular local ring with quotient field K which is dominated by ν. As a consequence of resolution of singularities (cf. Theorem 2.7 [10]) there exists a sequence of monoidal transforms $R_0 \to R_1$ along ν such that $a_i \in R_1$ for $1 \le i \le n$.

Let $\{w_1, \dots, w_r\}$ be a transcendence basis of $k(\nu) = V/m_V$ over k. $r < \infty$ by Theorem 1 [7] or Appendix 2 [22]. Let $\overline{w}_1, \dots, \overline{w}_r$ be lifts of the w_i to V. $\overline{w}_i \in V$ implies there exists a sequence of monoidal transforms $R_1 \to R_2$ along ν such that $\overline{w}_i \in R_2$ for all i (Theorem 2.7 [10]).

Suppose that R is an algebraic normal local ring with quotient field K such that $R_2 \subset R$ and R is dominated by ν. Let W be the integral closure of R in K^*. $u \in W \cap m_{V^*}$ and $u \notin W \cap m_{V_i}$ for $2 \le i \le n$. Let S be the localization of W at the center of ν^*. $g \in G^s(S/R)$ implies $u \in g(m_{V^*})$ and consequently $g(V^*) = V^*$, so that $g \in G^s(\nu^*/\nu)$. Thus $G^s(S/R) \subset G^s(\nu^*/\nu)$. By Proposition 1.50 [4], $G^s(S/R) = G^s(\nu^*/\nu)$.

$R_2 \subset R$ implies $k(w_1, \dots, w_r) \subset R/m_R$ so that $k(\nu)$ is algebraic over R/m_R.

$k(\nu^*)$ is finite over $k(\nu)$ by Corollary 2, Section 6, Chapter VI [22] (although $k(\nu)$ need not be finite over $k(w_1, \dots, w_r)$). Let $t_1, \dots, t_f \in k(\nu^*)$ be a $k(\nu)$ basis. Let $\overline{t}_i$

be lifts of the t_i to T. Let

$$\overline{t}_i^{m_i} + a_{1i}\overline{t}_i^{m_i-1} + \cdots + a_{m_i i} = 0, \quad 1 \le i \le f$$

be equations of integral dependence of $\overline{t}_i$ over V. There exists a sequence of monoidal transforms $R_2 \rightarrow R'$ along ν such that $a_{ji} \in R'$ for all i, j.

Now suppose that R is an algebraic normal local ring such that $R' \subset R$ and R is dominated by ν. Let S be the localization at the center of ν^* of the integral closure of R in K^*.

$R_2 \subset R$ implies $G^s(S/R) = G^s(\nu^*/\nu)$. $G^i(\nu^*/\nu) \subset G^i(S/R)$ by Proposition 1.50 [4]. By Theorem 1.48 [4] S/m_S is Galois over R/m_R and $k(\nu^*)$ is Galois over $k(\nu)$. We have an exact diagram

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & G^i(S/R) & \leftarrow & G^i(\nu^*/\nu) & \leftarrow & 0 \\
 & & \downarrow & & \downarrow & & \\
 & & G^s(S/R) & = & G^s(\nu^*/\nu) & & \\
 & & \downarrow & & \downarrow & & \\
0 & \leftarrow & \mathrm{Gal}(S/m_S/R/m_R) & \leftarrow & \mathrm{Gal}(k(\nu^*)/k(\nu)) & & \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

By construction, $\overline{t}_i \in S$ for all i which implies that $t_1, \ldots, t_f \in S/m_S$. $t_1, \ldots, t_f$ are necessarily linearly independent over R/m_R. Thus

$$f \le [S/m_S : R/m_R] =\mid \mathrm{Gal}(S/m_S/R/m_R) \mid .$$

$$f =\mid \mathrm{Gal}(k(\nu^*)/k(\nu)) \mid = \mid \mathrm{Gal}(S/m_S/R/m_R) \mid [G^i(S/R) : G^i(\nu^*/\nu)]$$

implies $G^i(S/R) = G^i(\nu^*/\nu)$, and $t_1, \ldots, t_f$ is a R/m_R basis of S/m_S. □

Theorem 5.2. *Let assumptions be as in Theorem 4.2. Suppose that K^* is Galois over K. Let $t_1, \ldots, t_f \in k(\nu^*)$ be a $k(\nu)$ basis. Suppose that*

$$R_0 \rightarrow R \rightarrow S$$

is a sequence of the form of (7) of Theorem 1 such that the R' of Lemma 5.1 is contained in R_0. Set $k_1 = R_0/m_{R_0}$, $k_2 = S/m_S$. Then $QF(\hat{S})$ is Galois over $QF(\hat{R})$, with Galois group $G^s(\nu^*/\nu)$, k_2 is Galois over k_1 with Galois group $G^s(\nu^*/\nu)/G^i(\nu^*/\nu)$. With the notation of (6) and Theorem 4.6, the completion of the sequence of (18)

$$\hat{R}_0 \rightarrow \hat{R} = \hat{R}^s \rightarrow \hat{R}^i \rightarrow \hat{S}$$

is

$$\begin{array}{l} \hat{R}_0 = k_1[[x_1, \ldots, x_n]] \rightarrow \hat{R} = (\hat{S})^{G^s(\nu^*/\nu)} = k_1[[x^{e_1}, \ldots, x^{e_r}]] \rightarrow \\ (\hat{S})^{G^i(\nu^*/\nu)} = k_2[[x^{e_1}, \ldots, x^{e_r}]] \rightarrow \hat{S} = k_2[[\overline{y}_1, \ldots, \overline{y}_n]] \end{array} .$$

with

$$x_i = \alpha_i \overline{y}_1^{a_{i1}} \cdots \overline{y}_n^{a_{in}}$$

$\alpha_i \in k_2$ for $1 \le i \le n$. There is an exact sequence

$$0 \rightarrow G^i(\nu^*/\nu) \cong \mathbf{Z}^n/A\mathbf{Z}^n \rightarrow G^s(\nu^*/\nu) \cong \mathrm{Gal}(QF(\hat{S})/QF(\hat{R}) \rightarrow \mathrm{Gal}(k_2/k_1) \rightarrow 0.$$

$f = [S/m_S : R/m_R]$, $e =\mid det(A) \mid$, $[QF(\hat{S}) : QF(\hat{R})] = ef$ and $\{t_1, \ldots, t_f\}$ is a basis of $k_2 = S/m_S$ over $k_1 = R/m_R$ where $e = [\Gamma^*/\Gamma]$ is the ramification index of ν^* with respect to ν, $f = [k(\nu^*) : k(\nu)]$ is the residue degree of ν^* with respect to ν.

Proof. $QF(\hat{S})$ is Galois over $QF(\hat{R}) = QF(\hat{R}^s)$ with Galois group $G^s(S/R)$ by Lemma 7 a), b) [1] and $QF(\hat{S})$ is Galois over $QF(\hat{R}^i)$ with Galois group $G^i(S/R)$ by Proposition 1.49 [4] and Lemma 7 a), b) [1] applied to $K \subset K^i \subset K^*$ and $R \subset R^i \subset S$. $R/m_R = R_0/m_{R_0}$ by Theorem 4.6. With the notations of (6) and Theorem 4.6, $\hat{R}_0 = k_1[[x_1, \ldots, x_n]]$, $\hat{R}^s = k_1[[x^{e_1}, \ldots, x^{e_r}]]$, $\hat{R}^i = k_2[[x^{e_1}, \ldots, x^{e_r}]]$, $\hat{S} = k_2[[\overline{y}_1, \ldots, \overline{y}_n]]$. S/m_S is Galois over $R/m_R = R^s/m_{R^s}$ implies k_2 is Galois over k_1.

With the notations of Lemma 4.4, set

$$L = k_1(x_1, \ldots, x_n) \subset L_1 = k_2(x_1, \ldots, x_n) \subset L^* = k_2(\overline{y}_1, \ldots, \overline{y}_n).$$

We have that L^*/L is Galois with $\mathrm{Gal}(L^*/L) = \mathrm{Hom}_{\hat{R}}(\hat{S}, \hat{S}) = G^s(S/R)$. We further have that L^*/L_1 is Galois with $\mathrm{Gal}(L^*/L_1) = \mathrm{Hom}_{\hat{R}^i}(\hat{S}, \hat{S}) = G^i(S/R)$.

By Lemma 5.1, $G^s(S/R) = G^s(\nu^*/\nu)$, $G^i(S/R) = G^i(\nu^*/\nu)$ and $[S/m_S : R/m_R] = f$. By (19) and Lemma 4.4, $e = \mid \det(A) \mid$ and $[QF(\hat{S}) : QF(\hat{R})] = ef$. ☐

Lemma 5.3. *Let k be a field of characteristic zero, K an algebraic function field over k, K^* a finite algebraic extension of K, ν^* a k-valuation of K^*, $\nu = \nu^* \mid K$. Suppose that S_0 is an algebraic normal local ring with quotient field K^* such that S_0 is dominated by ν^*. Then there exists an algebraic regular local ring R' with quotient field K which is dominated by ν such that if R is an algebraic normal local ring with quotient field K, S is an algebraic regular local ring with quotient field K^* such that R contains R' and S is dominated by V^*, R is dominated by S, then S contains S_0.*

Proof. There exists a sequence of monoidal transforms $S_0 \rightarrow S_1$ along ν^* such that S_1 dominates an algebraic regular local ring R_1 with quotient field K. Let U_1 be the integral closure of R_1 in K^*. There exists $f_1, \ldots, f_m \in K^*$ (with $\nu^*(f_i) \geq 0$ for all i) such that S_1 is a localization of $U_1[f_1, \ldots, f_m]$.

Let T be the integral closure of V in K^*, so that V^* is the localization of T at $T \cap m_{V^*}$. Thus for $1 \leq i \leq m$, $f_i = \frac{b_i}{c_i}$ with $b_i, c_i \in T$, $\nu^*(b_i) \geq 0, \nu^*(c_i) = 0$.

Let

$$\begin{array}{l} b_i^{m_i} + d_{i1} b_i^{m_i - 1} + \cdots + d_{i,m_i} = 0 \\ c_i^{n_i} + e_{i1} c_i^{n_i - 1} + \cdots + e_{in_i} = 0, \end{array}$$

$1 \leq i \leq m$, be equations of integral dependence of b_i, c_i over V, so that all $d_{ij}, e_{ij} \in V$.

There exists a sequence of monoidal transforms $R_1 \rightarrow R'$ along ν such that all $d_{ij}, e_{ij} \in R'$.

Suppose that R, S are as in the statement of the Lemma, so that R contains R'. Then $U_1[b_1, \ldots, b_m, c_1, \ldots, c_m]$ is contained in S. $c_i \in S$ and $\nu^*(c_i) = 0$ implies $c_i \notin m_{V^*} \cap S = m_S$ and c_i is a unit in S. Thus $f_i \in S$ for $1 \leq i \leq m$, and $S_1 \subset S$. ☐

6. Extensions of valuation rings are toric

Theorem 6.1. *Suppose that the assumptions of Theorem 4.2 hold. Let $g_1, \ldots, g_f$ be a basis of V^*/m_{V^*} over V/m_V. Then there exists an algebraic regular local ring R' with quotient field K which is dominated by V, such that if $R_0 \rightarrow R \rightarrow S$ is of the form of (7) of Theorem 4.2 and $R' \subset R_0$, then the conclusions of Theorem 4.10 hold for $R_0 \rightarrow R \rightarrow S$. Further, with the notations of (3) and (4),*

$$[S/m_S : R/m_R] = f, \ \mid det(A) \mid = e, \ [QF(\hat{S}) : QF(\hat{R})] = ef$$

and $\{g_1, \ldots, g_f\}$ is a basis of S/m_S over $R/m_R = R_0/m_{R_0}$.

Proof. As in the proof of Lemma 5.1, there exists an algebraic regular local ring R_1 with quotient field K which is dominated by ν such that if R is an algebraic regular local ring with quotient field K such that $R_1 \subset R$ and R is dominated by ν, then

$g_1, \dots, g_f \in S/m_S$, where S is the localization of the integral closure of R in K^* at the center of ν^*. This argument does not require that K^*/K be Galois.

Let K' be a Galois closure of K^* over K, ν' be an extension of ν^* to K'. By Lemma 5.1, there exists an algebraic regular local ring S_0 with quotient field K^* which is dominated by ν^* such that if S is a normal algebraic local ring of K^* which contains S_0 and S' is the localization of the integral closure of S in K' at the center of ν', then $G^s(S'/S) = G^s(\nu'/\nu)$ and $G^i(S'/S) = G^i(\nu'/\nu)$. By Lemma 5.3 and Lemma 5.1, there exists an algebraic regular local ring R'' which is dominated by ν and has quotient field K, such that if R is an algebraic local ring with quotient field K which is dominated by ν, $R'' \subset R$, and S lies above R in K^* and is dominated by ν^*, S' lies above R in K' and is dominated by ν', then

$$\begin{array}{ll} G^s(S'/R) = G^s(\nu'/\nu) & G^i(S'/R) = G^i(\nu'/\nu), \\ G^s(S'/S) = G^s(\nu'/\nu^*) & G^i(S'/S) = G^i(\nu'/\nu^*) \end{array}.$$

By Theorem 4.10 and Lemma 5.3, there exists an algebraic regular local ring R' with quotient field K which contains R'' and is dominated by ν^* such that if $R_0 \rightarrow R \rightarrow S$ is a sequence of the form (7), then the conclusions of Theorem 4.10 hold. Since $R'' \subset R_0$, we further have

$$\begin{aligned} [S/m_S : R/m_R] &= [S'/m_{S'} : R/m_R]/[S'/m_{S'} : S/m_S] \\ &= [G^s(S'/R) : G^i(S'/R)]/[G^s(S'/S) : G^i(S'/S)] \\ &= [G^s(\nu'/\nu) : G^i(\nu'/\nu)]/[G^s(\nu'/\nu^*) : G^i(\nu'/\nu^*)] \\ &= [k(\nu') : k(\nu)]/[k(\nu') : k(\nu^*)] = [k(\nu^*) : k(\nu)] = f \end{aligned}$$

Since $g_1, \dots, g_f \in S/m_S$, we have that $g_1, \dots, g_f$ is an R/m_R basis of S/m_S. Since the conclusions of Theorem 4.10 hold (and by (19)), $e = \mid \det(A) \mid$. By Theorem 4.6, $\hat{R} \rightarrow \hat{S}$ is the completion of the finite extension

$$k_1[x^{e_1}, \dots, x^{e_r}] \rightarrow k_2[\overline{y}_1, \dots, \overline{y}_n]$$

where $k_1 = R/m_R$, $k_2 = S/m_S$, so that with the notation of Lemma 4.4, $[QF(\hat{S}) : QF(\hat{R})] = [L^* : L]$. By Lemma 4.4,

$$[QF(\hat{S}) : QF(\hat{R})] = [S/m_S : R/m_R] \mid \det(A) \mid = fe.$$

□

Theorem 6.2 is essentially proven by Zariski in [21]. Certainly the expression of V as a union of algebraic regular local rings follows easily from the results of [21]. The remaining statements follow easily from Zariski's results when V has rank 1, and can be deduced with some effort for higher rank.

Theorem 6.2. *Let k be a field of characteristic zero, K an algebraic function field over k, V a k-valuation ring of K. Then there exists a partially ordered set I and algebraic regular local rings $\{R(i) \mid i \in I\}$ with quotient field K which are dominated by V such that*

$$V = \lim_{\rightarrow} R(j) = \cup_{j \in I} R(j)$$

and such that, with the notations on V defined in Section 3, $R(j)$ has regular parameters $(x_1(j), \dots, x_n(j))$ such that

(1) *$p_i(j) = p_i \cap R(j) = (x_1(j), \dots, x_{t_1+\cdots+t_i}(j))$ for $1 \le i \le r$ and*

$$\{\nu(x_{t_1+\cdots+t_{i-1}+1}(j)), \dots, \nu(x_{t_1+\ldots+t_{i-1}+s_i}(j))\}$$

is a rational basis of $(\Delta_{i-1}/\Delta_i) \otimes \mathbf{Q}$ for $1 \le i \le r$.

(2) *Let*

$$T = \{j \mid t_1 + \cdots + t_k < j \leq t_1 + \cdots + t_k + s_{k+1} \text{ for some } 0 \leq k \leq r-1\}.$$

If $j < k \in I$ *then there are relations*

$$x_i(j) = \prod_{c \in T, c > t_1 + \cdots + t_a} x_c(k)^{d_{ic}} \delta_i \tag{20}$$

where d_{ic} *are natural numbers and* $\delta_i \in R(k)$ *is a unit for* $i = t_1 + \cdots + t_a + b \in T$ *with* $1 \leq b \leq s_{a+1}$*. If* $D(j,k)$ *is the* $\mid T \mid \times \mid T \mid$ *matrix* (d_{ic}) *of (20) then* $det(D(j,k)) \neq 0$.

(3) *For* $j \in I$*, let* Λ_j *be the free* $\mathbf{Z}$*-module* $\Lambda_j = \sum_{i \in T} \nu(x_i(j))\mathbf{Z}$*. Then*

$$\Gamma = \lim_{\rightarrow} \Lambda_j = \cup_{j \in I} \Lambda_j.$$

Proof. Let R^* be an algebraic regular local ring such that V dominates R^*. By Theorem 4.8 (with $S^* = R^*$) there exists a sequence of monoidal transforms $R^* \to R(0)$ along V such that 1. of this theorem holds on $R(0)$.

Suppose that m is a positive integer and $f = (f_1, \ldots, f_m) \in V^m$. We will construct a sequence of monoidal transforms $R_0 \to R(f)$ along V such that $f_1, \ldots, f_m \in R(f)$, 1. of this theorem holds for $R(f)$ and 2. of this theorem holds for $R_0 \to R(f)$. We will further have $\nu(f) \in \Lambda_f$.

By Theorem 4.9, with the R^*, S^* of the statement of Theorem 4.9 set as $R^* = S^* = R(0)$, and $v_i = x_i(0)$ if $i \in T$, and $v_{|T|+1} = f_1, \ldots, v_{|T|+m} = f_m$, there exists a sequence of monoidal transforms $R(0) \to R(f)$ along V such that 1. of this theorem holds for $R(f)$, 2. of this theorem holds for $R(0) \to R(f)$, $f \in R(f)$ and $\nu(f) \in \Lambda_f$. Det$D(0,f) \neq 0$ since $\{\nu(x_i(0) \mid i \in T\}$ and $\{\nu(x_i(f)) \mid i \in T\}$ are two bases of $\Gamma \otimes \mathbf{Q}$.

Let $I = \sqcup_{m \in \mathbf{N}_+} V^m$ be the disjoint union. For $f \in I$ we construct $R(f)$ as above. If $f = 0$ we let $R(0)$ be the $R(0)$ constructed above. Define a partial order on I by $f \leq g$ if $R(f) \subset R(g)$.

Suppose that $R(\alpha) \subset R(\beta)$. We have $R(0) \subset R(\alpha) \subset R(\beta)$.

$$x_i(0) = \prod_{j \in T} x_j(\alpha)^{c_{ij}} \delta_i$$

for $i \in T$ with δ_i a unit in $R(\alpha)$ and

$$x_i(0) = \prod_{j \in T} x_j(\beta)^{d_{ij}} \epsilon_i$$

for $i \in T$ with ϵ_i a unit in $R(\beta)$. Thus in $R(\beta)$ there are factorizations

$$x_i(\alpha) = \prod_{j \in T} x_j(\beta)^{e_{ij}} \lambda_i$$

for $i \in T$ and λ_i a unit in $R(\beta)$. We have $\det(D(\alpha,\beta)) \neq 0$ since 1. holds for $R(\alpha)$ and $R(\beta)$. Thus 2. holds for $R(\alpha) \to R(\beta)$. To show that $V = \lim_{\rightarrow} R(j)$, we must verify that I is a directed set. That is, for $\alpha, \beta \in I$, there exists $\gamma \in I$ such that $R(\alpha) \subset R(\gamma)$ and $R(\beta) \subset R(\gamma)$.

There exists $f_1, \ldots, f_m \in V$ such that if $A = k[f_1, \ldots, f_m]$, $m = A \cap m_{V_1}$ then $R(\alpha) = A_m$. There exists $g_1, \ldots, g_n \in V$ such that if $B = k[g_1, \ldots, g_n]$, $n = B \cap m_{V_1}$ then $R(\beta) = B_n$. Set $\gamma = (f_1, \ldots, f_m, g_1, \ldots, g_n)$. By construction, $A, B \subset R(\gamma)$. Since $m_V \cap R(\gamma) = m_\gamma$ is the maximal ideal of $R(\gamma)$, we have $R(\alpha)$, $R(\beta) \subset R(\gamma)$.

3. holds by our construction,since $\nu(f) \in \Lambda_f$ if $f \in V$. □

Theorem 6.3. *Let k be a field of characteristic zero, K an algebraic function field over k, K^* a finite algebraic extension of K, V^* a k-valuation ring of K^*, $V = V^* \cap K$. Let*

$$e = [\Gamma^*/\Gamma]$$

be the ramification index of V^* relative to V,

$$f = [V^*/m_{V^*} : V/m_V]$$

be the residue degree of V^* relative to V, and let τ be a primitive element of V^*/m_{V^*} over V/m_V. Then there exists a partially ordered set I and algebraic regular local rings $\{S(i) \mid i \in I\}$ with quotient field K^* which are dominated by V^* such that with the notations on V^* defined in Section 3, $S(j)$ has regular parameters $(y_1(j), \dots, y_n(j))$ such that

(1) $p_i^*(j) = p_i^* \cap S(j) = (y_1(j), \dots, y_{t_1+\cdots+t_i}(j))$ *for* $1 \le i \le r$ *and*

$$\{\nu^*(y_{t_1+\cdots+t_{i-1}+1}(j)), \dots, \nu^*(y_{t_1+\dots+t_{i-1}+s_i}(j)\}$$

is a rational basis of $(\Delta_{i-1}^*/\Delta_i^*) \otimes \mathbf{Q}$ *for* $1 \le i \le r$.

(2) *For all $k \in I$ there exist algebraic regular local rings $R_0(k)$ with quotient field K which are dominated by V such that there exist factorizations*

$$R_0(k) \to R(k) \to S(k)$$

of the form of (7) so that there are regular parameters $(x_1(k), ..., x_n(k))$ in $R_0(k)$, units $\delta_1(k), \dots, \delta_n(k) \in S(k)$ and a matrix $A(k) = (a_{ij}(k))$ of non-negative integers such that $det(A(k)) \ne 0$ and

$$\begin{array}{rcl} x_1(k) & = & y_1(k)^{a_{11}(k)} \cdots y_n(k)^{a_{1n}(k)} \delta_1(k) \\ & \vdots & \\ x_n(k) & = & y_1^{a_{n1}(k)} \cdots y_n^{a_{nn}(k)} \delta_n(k) \end{array} \tag{21}$$

has the form of the conclusions of Theorem 4.8. Furthermore, there are isomorphisms of abelian groups

$$\Gamma^*/\Gamma \cong \mathbf{Z}^n/A(k)\mathbf{Z}^n,$$

and

$$[S(k)/m_{S(k)} : R(k)/m_{R(k)}] = f, \ \mid det(A(k)) \mid = e, \ [QF(\hat{S}(k)) : QF(\hat{R}(k))] = ef$$

and $S(k)/m_{S(k)} = R(k)/m_{R(k)}[\tau]$.

(3) *Let*

$$T = \{j \mid t_1 + \cdots + t_k < j \le t_1 + \cdots + t_k + s_{k+1} \text{ for some } 0 \le k \le r-1\},$$

k' be an algebraic closure of V^*/m_{V^*}. Suppose that $j < k \in I$.

(a) *There are relations*

$$y_i(j) = \prod_{c \in T, c > t_1 + \cdots + t_a} y_c(k)^{d_{ic}} \epsilon_i \tag{22}$$

where d_{ic} are natural numbers and $\epsilon_i \in S(k)$ is a unit for $i = t_1 + \cdots + t_a + b \in T$ with $1 \le b \le s_{a+1}$. Let $D(j,k)$ be the $\mid T \mid \times \mid T \mid$ matrix of (22). Then $det(D(j,k)) \ne 0$

(b) *There exists a commutative diagram*

$$\begin{array}{ccc} R(k) & \to & S(k) \\ \uparrow & & \uparrow \\ R(j) & \to & S(j) \end{array} \tag{23}$$

(c) *Further, we have actions of* Γ^*/Γ *on* $\hat S(j)\otimes_{S(j)/m_{S(j)}}k'$ *such that*

$$(\hat S(j)\otimes_{S(j)/m_{S(j)}}k')^{\Gamma^*/\Gamma}\cong \hat R(j)\otimes_{R(j)/m_{R(j)}}k'$$

for all j*, and this action is compatible with restriction in the diagram (23).*

(4)

$$V^*=\lim_{\rightarrow} S(j)=\cup_{j\in I}S(j)$$

and

$$V=\lim_{\rightarrow} R(j)=\cup_{j\in I}R(j).$$

For $j\in I$*, let* Λ_j *be the free* $\mathbf{Z}$ *module* $\Lambda_j=\sum_{i\in T}\nu(x_i(j))\mathbf{Z}$*, and let* Ω_j *be the free* $\mathbf{Z}$ *module* $\Omega_j=\sum_{i\in T}\nu^*(y_i(j))\mathbf{Z}$*. Then*

$$\Gamma=\lim_{\rightarrow}\Lambda_j=\cup_{j\in I}\Lambda_j$$

and

$$\Gamma^*=\lim_{\rightarrow}\Omega_j=\cup_{j\in I}\Omega_j$$

Proof. Suppose that R' is the regular local ring of Theorem 6.1. By Theorem 6.1, there exists a sequence of local rings

$$R_0(0)\rightarrow R(0)\rightarrow S(0)$$

such that $R'\subset R_0(0)$ and the conclusions of Theorem 6.1 hold for this sequence. In particular, 1. and 2. of the theorem hold for $R_0(0)\rightarrow R(0)\rightarrow S(0)$.

Suppose that m is a positive integer, $f=(f_1,\dots,f_m)\in(V^*)^m$. Set $u_i=y_i(0)$, $1\le i\le n$. Set $u_{n+i}=f_i$ for $1\le i\le m$. If $f_i\in V^*\cap K=V$, also set $v_i=f_i$.

By Theorem 4.9 and Theorem 6.1, with the R^*, S^* in the assumptions of Theorem 4.9 set as $R^*=R_0(0)$, $S^*=S(0)$, and with the $\{u_i\}$ and $\{v_i\}$ as defined above, there exists a commutative diagram

$$\begin{array}{ccccc} R_0(f) & \rightarrow & R(f) & \rightarrow & S(f)\\ \uparrow & & & & \uparrow\\ R_0(0) & \rightarrow & & & \tilde S \end{array}$$

such that the vertical arrows are sequences of monoidal transforms along V^*, 1. and 2. of this theorem hold for

$$R_0(f)\rightarrow R(f)\rightarrow S(f)$$

and 3. (a) of this theorem holds for

$$\begin{array}{ccc} R(f) & \rightarrow & S(f)\\ \uparrow & & \uparrow\\ R(0) & \rightarrow & S(0) \end{array}.$$

$\det(D(0,f))\ne 0$ since 1. holds for $S(0)$ and $S(f)$. Define a partial ordering on $I=\sqcup_{m\in\mathbf{N}_+}(V^*)^m$ by $f\le g$ if $S(f)\subset S(g)$. We will associate to $0\in V^*$ the sequence $R_0(0)\rightarrow R(0)\rightarrow S(0)$ constructed in the beginning of the proof. Suppose that $\alpha\le\beta$. We have

$$S(0)\subset S(\alpha)\subset S(\beta)$$

so the proof of 2. of Theorem 6.2 shows that 3. (a) of this Theorem holds for α,β. 3. (b) holds since

$$R(\alpha)=S(\alpha)\cap K\subset S(\beta)\cap K=R(\beta).$$

3. (c) is immediate, since the conclusions of Theorem 6.1 hold. In particular, (11) holds.

Finally, we will establish 4. of the Theorem. By construction, $V^* = \cup_{j\in I} S(j)$. If $f \in V$, we have $f \in S(f) \cap K = R(f)$, thus $V = \cup_{j\in I} R(j)$. By construction, $\cup_{j\in I}\Omega_j = \Gamma^*$, since $\nu^*(f) \in \Omega_f$ for $f \in V^*$. We also have $\cup_{j\in I}\Lambda_j = \Gamma$, since $\nu(f) \in \Lambda_f$ for $f \in V$. I is a directed set as shown in the proof of Theorem 6.2. □

Remark 6.4. *If K^* is Galois over K, then 3. (c) of Theorem 6.3 can be strengthened to the conclusions of Theorem 5.2.*

7. Ramification in function fields of surfaces of positive characteristic.

In this section, k is an algebraically closed field of characteristic $p > 0$, and K^*/K is a finite and *separable* extension of function fields of transcendence degree two over k. Let ν be a k-valuation of K, with valuation ring V and value group Γ, and ν^* be an extension of ν to K^*, with valuation ring V^* and value group Γ^*.

It follows from the local uniformization theorem ([1] top of p.492) that there exists an algebraic regular local ring S (resp. R) with quotient field K^* (resp. K) which is dominated by ν^* (resp. ν).

Let $S < S_1 < \cdots < S_s < \cdots$ be the quadratic sequence along V^* and $R < R_1 < \cdots < R_r < \cdots$ be the quadratic sequence along V. A basic result ([1] lemma 10) is that $V^* = \bigcup_{j>0} S_j$ and $V = \bigcup_{i>0} R_i$. This local result on elimination of indeterminacies implies that there exists a pair of regular local rings (R, S) as before with S furthermore dominating R. These notations will be kept all along this section.

Abhyankar's inequality ([22] proposition 1 p.330) states that

$$\mathrm{ratrank}(V) + \mathrm{trdeg}_k(V/m_V) \leq \mathrm{trdeg}_k K = 2.$$

Moreover, Γ (and Γ^*) are finitely generated except possibly when $\mathrm{ratrank}(V) = 1$ and $\mathrm{trdeg}_k(V/m_V) = 0$ (thus $V/m_V \simeq k$ since k is algebraically closed). In case Γ is not finitely generated, Γ is thus isomorphic to a nondiscrete subgroup of $\mathbf{Q}$.

In section 7.2, it is proved that most of the characteristic zero results of the previous sections extend in a satisfactory way to valuation rings with finitely generated value group in function fields of surfaces of positive characteristic.

The case of valuation rings whose value group is isomorphic to a nondiscrete subgroup of $\mathbf{Q}$ is much more subtle and is the purpose of all remaining subsections. It is well known that this case is also the hard part in the proof of the local uniformization theorem: most of the content of [1] is indeed devoted to the local uniformization of valuations whose value group is isomorphic to a nondiscrete subgroup of $\mathbf{Q}$. Basically, we prove that the pair (R, S) can be replaced by another pair (R', S') from which the ramification index and the defect of ν^* relative to ν can be read off (theorem 7.33).

In theorem 7.35, we prove that most of the characteristic zero statements in the previous sections extend to finite and separable extensions of function fields of transcendence degree two over k whenever V^*/V is *defectless* (see definition in section 7.1). On the other hand, we prove that the conclusion of the stronger form of the monomialization theorem (theorem 4.8) may be false when V^*/V has nontrivial defect (theorem 7.38). We do not know if the weaker form of the monomialization theorem (theorem 4.1) holds in this case.

Notations. We freely use the following notation: if A is a commutative ring which is a UFD, $f \in A$ is a nonunit and $g \in A$, then the largest power of f which divides g is denoted by $\mathrm{ord}_f(g)$.

7.1. **Ramification theory of local rings.** In this section, we recall the definition of ramification groups as can be found in pp. 50-82 of [22].

Suppose that R is a normal local ring with quotient field K which is dominated by V, and R^* is a normal local ring with quotient field K^* which lies above R and is dominated by V^*. Let $f(R^*/R)$ be the degree of the residue extension $\frac{R^*}{m_{R^*}}/\frac{R}{m_R}$. In case K^* is a finite Galois extension of K with Galois group $G = \mathrm{Gal}(K^*/K)$, one can consider the splitting and inertia groups of R^* over R as in section 5.

Notice that in case $\mathrm{trdeg}_k(R/m_R) = 0$, we have $R/m_R \cong k$, since k is algebraically closed. Consequently,

$$G^i(R^*/R) = G^s(R^*/R)$$

by theorem 1.48 [4]. In particular, this holds when R is a two dimensional algebraic normal local ring or when R is a valuation ring V such that $\mathrm{trdeg}_k(V/m_V) = 0$.

The inertia group $G^i(V^*/V)$ has a natural normal subgroup $G^r(V^*/V)$, called the *ramification group* of V^* over V, and defined by

$$G^r(V^*/V) := \{g \in G^i(V^*/V) \mid \nu^*\left(\frac{g(x)}{x} - 1\right) > 0 \text{ for all } x \in K^*/\{0\}\} \subseteq G^i(V^*/V).$$

It is proved in theorems 24 and 25 of [22] that $G^r(V^*/V)$ is the unique p-Sylow subgroup of $G^i(V^*/V)$ and that

$$G^i(V^*/V)/G^r(V^*/V) \simeq (\Gamma^*/\Gamma)_{(p)} \text{ (:= the prime to } p \text{ part of } \Gamma^*/\Gamma). \tag{24}$$

Let $p^{w_0(V^*/V)}$ be the order of the *wild* part of Γ^*/Γ, that is

$$\mid \Gamma^*/\Gamma \mid = p^{w_0(V^*/V)} \mid (\Gamma^*/\Gamma)_{(p)} \mid .$$

By the corollary on p.78 of [22], we have

$$\mid G^r(V^*/V) \mid = p^{w_0(V^*/V)+\delta_0(V^*/V)}, \tag{25}$$

where $\delta_0(V^*/V) \geq 0$. The previous considerations yield the formula

$$\mid G^s(V^*/V) \mid = f(V^*/V)p^{\delta_0(V^*/V)} \mid \Gamma^*/\Gamma \mid .$$

Finally, one extends the definition of the integer $\delta_0(V^*/V)$ to an arbitrary finite and separable extension K^* of K by taking a Galois closure K'/K of K^*/K, choosing an extension V' of V to K' which dominates V^* and letting

$$\delta_0(V^*/V) := \delta_0(V'/V) - \delta_0(V'/V^*) \geq 0. \tag{26}$$

It is easily checked using multiplicativity of ramification index, residue degree and degree of field extensions that

$$[K_s^* : K_s] = f(V^*/V)p^{\delta_0(V^*/V)} \mid \Gamma^*/\Gamma \mid,$$

where K_s (resp. K_s^*) denotes the splitting field of V' over V (resp. over V^*).

Definition 7.1. *With notations as above, the integer* $p^{\delta_0(V^*/V)}$ *is called the defect of* V^* *over* V. *The extension of valuation rings* V^*/V *is said to be defectless if* $\delta_0(V^*/V) = 0$.
Finally, V^*/V *is said to be tamely ramified if* p *does not divide* $e(V^*/V)$ *and* V^*/V *is defectless. If* K^*/K *is Galois,* V^*/V *is tamely ramified if and only if* $G^r(V^*/V) = (1)$.

We conclude this section by stating the following extension of lemma 2 of [13].

Proposition 7.2. *Let* $R \subset S$ *be an inclusion of two dimensional algebraic regular local rings over* k, *with* $K^*/K := QF(S)/QF(R)$ *finite and separable. Let* S^* *be the unique two dimensional algebraic normal local ring over* k *lying above* R *with* $QF(S^*) = K^*$ *and* $S^* \subset S$. *Assume that* R *has a r.s.p.* (u, v), S *has a r.s.p.* (x, y), *and there is an expression*

$$\begin{array}{rcl} u & = & x^a f_u \\ v & = & x^b f_v, \end{array}$$

where $a, b > 0$, x *does not divide* $f_u f_v$. *Assume moreover that either (1) or (2) below holds.*

(1) f_u *is a unit in* S *and* f_v *is not a unit in* S.
(2) $f_u = \gamma y^c$, $f_v = \gamma' y^d$, *where* $\gamma, \gamma' \in S$ *are units and* $ad - bc \neq 0$.

Then there exists a diagram

$$\begin{array}{ccc} S^* & \to & S \\ \uparrow & & \uparrow \\ R & \to & R_0 \end{array} \tag{27}$$

of local inclusions with the following properties: R_0 *is a two dimensional algebraic normal local ring over* k, *with* $QF(R_0) = K$ *such that* S *lies above* R_0. *Let* $\overline{\nu}$ *be the natural valuation of the DVR* $\frac{S}{(x)}$. *Then we have*

$$[\hat{S} : \hat{R}_0] := [QF(\hat{S}) : QF(\hat{R}_0)] = ad,$$

with $d := \overline{\nu}(f_v \bmod x)$ *in case (1) and*

$$[\hat{S} : \hat{R}_0] := [QF(\hat{S}) : QF(\hat{R}_0)] = \mid ad - bc \mid,$$

in case (2).

Proof. We review the proof of lemma 2 of [13] and point out the appropriate changes.

First assume that assumption (1) holds. Let $\delta :=$ g.c.d(a, b), and $\varphi := \dfrac{v^{\frac{a}{\delta}}}{u^{\frac{b}{\delta}}}$. We have $\varphi \in S$ and φ is not a unit in S.

Let $I \subset R$ be the integral closure of the ideal $(u^{\frac{b}{\delta}}, v^{\frac{a}{\delta}})$. Then I is a *simple* complete m_R-primary ideal (p.385, appendix 5 of [22]). There are local inclusions

$$R \subset R_0 := \overline{R}_{\mathcal{P}} \subset S,$$

where $\overline{R} := R[\frac{I}{u^{\frac{b}{\delta}}}]$ and $\mathcal{P} := m_S \cap \overline{R}$. R_0 is normal by Zariski's theory of complete ideals ([22] appendix 5). By construction, $\varphi \in \overline{R}$ and neither is a unit nor is divisible by x in S. This implies that $\mathrm{ht}((x) \cap \overline{R}) = 1$. Clearly, (27) holds.

Let $W^* := S_{(x)}$ and $W := \overline{R}_{(x) \cap \overline{R}}$. Then W and W^* are divisorial valuation rings and $W^* \cap K = W$. The argument in the proof of lemma 2 of [13] now shows that the ramification index $e(W^*/W)$ of W^*/W is δ and that there is an inclusion

$$\frac{\overline{R}}{(x) \cap \overline{R}} = k[\overline{\varphi}] \subset \frac{S}{(x)}, \tag{28}$$

where $\overline{\varphi}$ is the image of φ in the ring to the left. We claim that W has a unique extension $\hat{W}$ to $QF(\hat{R}_0)$, $\hat{W}$ has a unique extension $\hat{W}^*$ to $QF(\hat{S})$, and that

$$e(\hat{W}^*/\hat{W}) = \delta,\ f(\hat{W}^*/\hat{W}) = \frac{ad}{\delta}.$$

Notice that this implies proposition 7.2, since we then get

$$[\hat{S} : \hat{R}_0] = e(\hat{W}^*/\hat{W})f(\hat{W}^*/\hat{W}) = ad$$

by [22] theorem 20 p.60 and remark at the bottom of p.63.

To prove that the extension of W to $QF(\hat{R}_0)$ is unique, it must be proved that the prime $(x) \cap R_0$ does not split in $\hat{R}_0$. By proposition 21.3 and following remark of [17], the reduced exceptional divisor of the blow-up $\overline{X} := \mathrm{Proj}(\bigoplus_{n\geq 0} I^n) \rightarrow \mathrm{Spec}R$ is an irreducible curve $F \simeq \mathbf{P}^1_k$. In particular, $\frac{R_0}{(x)\cap R_0}$ is a *regular* algebraic local ring (of dimension one) and therefore $(x) \cap R_0$ does not split in $\hat{R}_0$.

To prove that the extension of $\hat{W}$ to $QF(\hat{S})$ is unique, it is sufficient to prove that (x) is the unique height one prime (f) of S such that $(f) \cap R_0 = (x) \cap R_0$, since (x) does not split in $\hat{S}$. Let (f) be a height one prime of S containing $(x) \cap R_0$. Then $m_R \supseteq (f) \cap R = (x) \cap R = m_R$. In particular, f divides u in S. Assumption (1) now implies that $(f) = (x)$. This proves that (x) is the unique height one prime of S such that $(f) \cap R_0 = (x) \cap R_0$.

By (28), we get

$$f(\hat{W}^*/\hat{W}) = \left[QF(\frac{\hat{S}}{(x)}) : QF(\frac{\hat{R}_0}{(x)\cap R_0}) \right] = [\ k[[y]] : k[[\overline{\varphi}]]\ ] = \overline{\nu}(\overline{\varphi}) = \frac{ad}{\delta}.$$

But $e(\hat{W}^*/\hat{W}) = e(W^*/W) = \delta$ since algebraic local rings are analytically unramified, and this concludes the proof under assumption (1).

We now sketch the proof under assumption (2). One reduces to assumption (1) if $c = 0$ or $d = 0$, so assume $c > 0, d > 0$. By possibly exchanging x and y, it can also be assumed that $ad - bc > 0$. Let $\delta := \mathrm{g.c.d}(a, b)$ and $\delta' := \mathrm{g.c.d}(c, d)$. Let $I \subset R$ (resp. $I' \subset R$) be the integral closure of the ideal $(u^{\frac{b}{\delta}}, v^{\frac{a}{\delta}})$ (resp. $(u^{\frac{d}{\delta'}}, v^{\frac{c}{\delta'}})$). Then each of I, I' is a *simple* complete ideal and $I \neq I'$. We have

$$IS = (x^{\frac{ab}{\delta}} y^{\frac{bc}{\delta}}) = (u^{\frac{b}{\delta}})S,$$

and

$$I'S = (x^{\frac{bc}{\delta'}} y^{\frac{cd}{\delta'}}) = (v^{\frac{c}{\delta'}})S.$$

In particular, $II'S$ is a principal ideal. There are local inclusions

$$R \subset R_0 := \overline{R}_{\mathcal{P}} \subset S,$$

where $\overline{R} := R[\frac{II'}{u^{\frac{b}{\delta}} v^{\frac{c}{\delta'}}}]$ and $\mathcal{P} := m_S \cap \overline{R}$. As in the proof in case 1, we have $\mathrm{ht}((x) \cap \overline{R}) = \mathrm{ht}((y) \cap \overline{R}) = 1$, so that by construction (27) holds.

One introduces the divisorial valuation rings $W^* := S_{(x)}$ and $W := \overline{R}_{(x)\cap\overline{R}}$ as in case (1). Then W has a unique extension $\hat{W}$ to $QF(\hat{R}_0)$, $\hat{W}$ has a unique extension $\hat{W}^*$ to $QF(\hat{S})$, and we have

$$e(\hat{W}^*/\hat{W}) = \delta,\ f(\hat{W}^*/\hat{W}) = \frac{ad - bc}{\delta}.$$

One concludes as before, by noticing that

$$[\hat{S} : \hat{R}_0] = e(\hat{W}^*/\hat{W})f(\hat{W}^*/\hat{W}) = ad - bc.$$

□

7.2. **Valuation rings with finitely generated value group.** In this section, we prove that theorem 4.8 extends to positive characteristic and dimension two if V^* has finitely generated value group (theorem 7.3). We also prove that, in this case, V^*/V is defectless.

First consider the case when V^* is *divisorial*. By definition, this means that $\mathrm{ratrank}(V) = \mathrm{trdeg}_k(V/m_V) = 1$. By proposition 4.4 [2], ν and ν^* are discrete, and V (resp. V^*) itself is an iterated quadratic transform of R (resp. S). Let x (resp. y) be a regular parameter of V (resp. V^*). There is a relation

$$x = \gamma y^e,$$

where $\gamma \in V^*$ is a unit, and $e \geq 1$. Clearly,

$$\Gamma^*/\ \Gamma \simeq \mathbf{Z}/e\mathbf{Z}.$$

From now on, till the end of this section, it is assumed that V is *not* divisorial, that is, $\mathrm{trdeg}_k(V/m_V) = 0$. Since k is algebraically closed, this implies that $V/m_V \simeq k$. The main result is

Theorem 7.3. *Assume that $V/m_V \simeq k$ and that Γ is finitely generated. The following holds.*

(1) *There exist iterated quadratic transforms R' of R along ν and S' of S along ν^* with $R' \subset S'$, such that R' has a r.s.p. (u, v), S' has a r.s.p. (x, y), and there is a relation*
$$\begin{array}{rcl} u & = & \gamma x^a y^c \\ v & = & \delta x^b y^d, \end{array}$$
where $\gamma, \delta \in S'$ are units, $a, b, c, d \geq 0$ and $ad - bc \neq 0$. Moreover, $\Gamma^*/\ \Gamma \simeq \mathbf{Z}^2/A\mathbf{Z}^2$, where
$$A = \left(\begin{array}{cc} a & c \\ b & d \end{array} \right).$$

(2) *If ν has rank two, there exist R' and S' as in (1) and such that*
$$A = \left(\begin{array}{cc} a & b \\ 0 & d \end{array} \right).$$
If ν is discrete, there exist R' and S' as in (1) and such that
$$A = \left(\begin{array}{cc} 1 & 0 \\ 0 & d \end{array} \right).$$

(3) *The extension of valuation rings V^*/V is defectless.*

Proof. First assume that ν has rational rank two. Theorem 4.7 of [2], implies that there exists an iterated quadratic transform R' of R along ν, with r.s.p. (u, v) such that $\Gamma = \mathbf{Z}\nu(u) + \mathbf{Z}\nu(v)$ (and $\nu(v) = (0, 1)_\Gamma$ if $\Gamma \simeq \mathbf{Z}^2$ with lexicographical ordering). There exists an iterated quadratic transform S_1 of S along ν^* such that $R' \subset S_1$.

Apply again theorem 4.7 of [2] to the algebraic regular local ring of dimension two S_1, and $f := uv \in S_1$. Then there exists an iterated quadratic transform S' of S_1 along ν^*, with r.s.p. (x, y) such that $\Gamma^* = \mathbf{Z}\nu^*(x) + \mathbf{Z}\nu^*(y)$ (and $\nu^*(y) = (0, 1)_{\Gamma^*}$ if $\Gamma^* \simeq \mathbf{Z}^2$ with lexicographical ordering) and

$$uv = \overline{\gamma} x^m y^n,$$

where $\overline{\gamma} \in S'$ is a unit and $m, n \geq 0$. Since S' is a UFD, we have $u = \gamma x^a y^c$, $v = \delta x^b y^d$, where $\gamma, \delta \in S'$ are units and $a, b, c, d \geq 0$, $a + b = m$, $c + d = n$ (and $b = 0$

if Γ^* is lexicographically ordered). Since $\nu^*(u)$ and $\nu^*(v)$ are rationally independent, we have $ad-bc\neq 0$. Moreover,

$$\Gamma^*/\ \Gamma = \mathbf{Z}^2/(\mathbf{Z}\nu^*(u)+\mathbf{Z}\nu^*(v)) \simeq \mathbf{Z}^2/A\mathbf{Z}^2.$$

This proves (1) and (2) if ν has rational rank two.

Assume now that ν is discrete. Since R is two dimensional and regular, there is a 1-1 correspondence between iterated quadratic transforms of R and iterated quadratic transforms of $\hat{R}$. By [19] theorem 3.1 and case 4.2 p.154, ν has a unique extension $\hat{\nu}$ to $\hat{K} := QF(\hat{R})$, and $\hat{\nu}$ has value group $\mathbf{Z}\oplus\Gamma$ with lexicographical ordering. By Zariski's subspace theorem ([5] theorem 10.13), the natural map $\hat{R}\to\hat{S}$ is an inclusion. Similarly, let $\hat{\nu}^*$ be the unique extension of ν^* to $\hat{K}^* := QF(\hat{S})$.

Since $\hat{\nu}^*$ and $\hat{\nu}$ have rank two, it follows from the above construction that there exists an iterated quadratic transform S'_1 of $\hat{S}$ along $\hat{\nu}^*$ (corresponding to an iterated quadratic transform S_1 of S along ν) and an iterated quadratic transform R'_1 of $\hat{R}$ along $\hat{\nu}$ (corresponding to an R_1) with the following property: S'_1 has a r.s.p. (x_1,y_1) with $y_1\in S_1$, such that we have $\hat{\nu}^*(y_1)=(0,1)$, $\hat{\nu}^*(x_1)=(1,h)$ in $\mathbf{Z}\oplus\Gamma^*$, R'_1 has a r.s.p. (u_1,v_1) with $v_1\in R_1$, such that $\hat{\nu}(v_1)=(0,1)$, $\hat{\nu}(u_1)=(1,g)$ in $\mathbf{Z}\oplus\Gamma$, and there is a relation:

$$\begin{array}{rcl} u_1 &=& \gamma_1 x_1^{a_1}y_1^{c_1}\\ v_1 &=& \delta_1 y_1^{d_1}, \end{array} \tag{29}$$

where $\gamma_1\in S'_1$ and $\delta_1\in S_1$ are units, $a_1,d_1>0$ and $c_1\geq 0$. We now compute the Jacobian determinant

$$J := \frac{\partial u_1}{\partial x_1}\frac{\partial v_1}{\partial y_1}-\frac{\partial u_1}{\partial y_1}\frac{\partial v_1}{\partial x_1}\in\hat{S}'_1\simeq k[[x_1,y_1]].$$

By standard arguments, the support of $\mathrm{div}(J)\hookrightarrow \mathrm{Spec}\hat{S}'_1$ is contained in $\mathrm{Spec}S_1$. Since $\hat{\nu}^*(K\backslash\{0\})=(0)\oplus\Gamma^*\subset\mathbf{Z}\oplus\Gamma^*$, we have $(x_1)\cap S_1=(0)$. Therefore x_1 does not divide J and this implies that $a_1=1$. Thus (29) reduces to

$$\begin{array}{rcl} u_1 &=& \gamma_1 x_1 y_1^{c_1}\\ v_1 &=& \delta_1 y_1^{d_1}. \end{array}$$

Let $c_1=q_1d_1+r_1$ be the Euclidian division. The inclusion

$$R'_2 := R'_1[u_2]_{(u_2,v_1)}\subset S'_2 := S'_1[x_2]_{(x_2,y_1)},$$

where $u_2 := \frac{u_1}{v_1^{q_1+1}}$, $x_2 := \frac{x_1}{y_1^{d_1-r_1}}$, is given by an expression

$$\begin{array}{rcl} u_2 &=& \gamma_2 x_2\\ v_1 &=& \delta_1 y_1^{d_1}, \end{array}$$

where $\gamma_2\in S'_2$ is a unit. R'_2 (resp. S'_2) corresponds to an iterated quadratic transform R' (resp. S') of R (resp. S). The pair (R',S') satisfies the conclusion of (2) in the theorem, with $v:=v_1$, $y:=y_1$, and any $u\in R'$ such that (u,v) is a r.s.p. by letting $x:=u\in S'$. This concludes the proof of (1) and (2).

Now assume that K^*/K is Galois. After possibly replacing R with an iterated quadratic transform along ν and S by an iterated quadratic transform along ν^*, it can be assumed that ν^* is the unique extension of ν which is centered in S.

Pick R', S' as in the conclusion of (1) of theorem 7.3. If A is a diagonal matrix, then $R'\subset S'$ is the localization of a finite map. Moreover $\hat{S}'\simeq k[[x,y]]$ is clearly a free $\hat{R}'$-module ($\hat{R}' \simeq k[[u,v]]$) with basis

$$B := \{x^i y^j,\ 0 \leq i \leq a-1,\ 0 \leq j \leq d-1\}.$$

Therefore $[QF(\hat{S}') : QF(\hat{R}')] = ad$. Assume now that A is not diagonal, say $a > 0$ and $b > 0$. Then assumption (1) or assumption (2) of proposition 7.2 is satisfied by the pair $R' \subset S'$. Then there exists $R_0 \subset S'$ as in the conclusion of proposition 7.2 such that

$$[\hat{S}' : \hat{R}_0] =\mid ad - bc \mid .$$

On the other hand, we have

$$\mid G^i(V^*/V) \mid= [K^* : K^i] = [\hat{S}' : \hat{R}_0] =\mid ad - bc \mid,$$

since ν^* is the unique extension of ν which is centered in S'.

By (1) of theorem 7.3, we have $\mid \Gamma^*/\Gamma \mid=\mid \det(A) \mid=\mid ad - bc \mid$. Comparing with (24) and (25), this proves that the defect of V^*/V is $p^{t_0} = 1$, and V^*/V is defectless as stated. Equation (26) implies that (3) remains true for K^*/K separable, but not necessarily Galois.

□

Remark 7.4. *Statement (3) of theorem 7.3 holds in a more general context. See* [18] *theorem 5 p.264 for valuations whose group is an integral direct sum. See also* [15] *theorem 3.1 for the case of valuations of maximal rational rank and ibid. theorem 1.1 for applications to local uniformization.*

7.3. **Prepared pairs and admissible coordinates.** In this section, we introduce notions which are needed in order to deal with the remaining case, that is, when the value group of ν (and ν^*) is a nondiscrete subgroup of $\mathbf{Q}$.

Let S (resp. R) be an algebraic regular local ring with quotient field K^* (resp. K) which is dominated by ν^* (resp. ν). We also assume that S dominates R. We restrict our attention to certain such pairs $R \subset S$ which are called prepared pairs.

Definition 7.5. *With notations as before,*

(1) *Given an index $i \geq 1$, R_i (resp. S_i) is said to be "free" if the reduced exceptional locus E_i (resp. F_i) of* $\mathrm{Spec}R_i \to \mathrm{Spec}R$ *(resp.* $\mathrm{Spec}S_i \to \mathrm{Spec}S$*) has precisely one irreducible component.*
(2) *Given a pair (r,s) of positive integers, the pair (R_r, S_s) is said to be prepared if the following properties hold:*
    (i) *S_s dominates R_r.*
    (ii) *Both of R_r and S_s are free.*
    (iii) *The critical locus of* $\mathrm{Spec}S_s \to \mathrm{Spec}R_r$ *is contained in F_s.*
    (iv) *We have $u = \gamma x^a$, where u (resp. x) is a regular parameter of R_r (resp. S_s) whose support is E_r (resp. F_s), and γ is a unit in S_s.*

Proposition 7.6. *Assume that the value group of ν (and ν^*) is a nondiscrete subgroup of* $\mathbf{Q}$.
The set of prepared pairs is cofinal in the set of all pairs (R_r, S_s). Given a prepared pair (R_r, S_s), any pair $(R_{r'}, S_{s'})$ with $r' \geq r$, $s' \geq s$, and such that both of $R_{r'}$ and $S_{s'}$ are free and $S_{s'}$ dominates $R_{r'}$ is also prepared.

Proof. Since the value group of V is a nondiscrete subgroup of $\mathbf{Q}$ it is true that the set of *free* R_r (resp. S_s) is cofinal in the set of all R_r (resp. S_s) ([1] theorem 4.7(A)).

Since L/K is separable, the critical locus of the map $\mathrm{Spec}S_s \to \mathrm{Spec}R_r$ is a (possibly empty) *curve* $C_{r,s}$ in $\mathrm{Spec}S_s$.

If C is a curve in SpecS_s, its total transform in Spec$S_{s'}$ is contained in $F_{s'}$ for all large enough s' ([1] *ibid.*). Applying this statement to E_r, and to $C_{r,s}$ for a given pair (R_r, S_s) satisfying (i) and (ii) of definition 7.5, one gets that (iii) and (iv) hold for all pairs $(R_{r'}, S_{s'})$ satisfying (i) and (ii) and with r' and s' large enough.

□

Lemma 7.7. *Assume that the value group of V (and V^*) is a nondiscrete subgroup of $\mathbf{Q}$.*
There exists $\alpha \in \Gamma$ such that $\nu(v) \leq \alpha$ for all regular parameters v of R.

Proof. Assume not. We fix a regular parameter u of R such that

$$\nu(u) = \min_{u' \in m_R}\{\nu(u')\}.$$

Notice that $\nu(v) = \nu(u)$ unless possibly if (u, v) is a r.s.p. of R. Let $f \in R$ be a nonunit and choose a regular parameter v of R such that $\nu(v) > \nu(f)$. By the Weierstrass preparation theorem, there is an expansion

$$f = \gamma_f \left(v^{d_f} - \sum_{i=1}^{d_f} a_i(u) v^{d_f - i} \right), \tag{30}$$

with $\gamma_f \in \hat{R} = k[[u, v]]$ a unit, and $a_i(u) \in k[[u]]$ a nonunit for $1 \leq i \leq d_f$. All terms in (30) have value larger than $\nu(v)$ except possibly $a_{d_f}(u)$. This implies that $\nu(f) = \nu(a_{d_f}(u)) = \nu(u)\mathrm{ord}_u a_{d_f}$. Since this holds for every $f \in R$, we get that $\Gamma = \mathbf{Z}\nu(u)$. This is a contradiction, since ν is not discrete. □

Since R is Noetherian, and ν has rank one, every subset of the *semigroup* $\Phi := \nu(R\backslash\{0\})$ which is bounded from above is finite ([22] top of p.332). By lemma 7.7, any prepared pair (R_r, S_s) has an admissible r.s.p. as defined below.

Definition 7.8. *(Choice of coordinates) Let (R_r, S_s) be prepared. A r.s.p. (u, v) of R_r is said to be admissible if the support of u is equal to E_r and if $\nu(v)$ is maximal among all such r.s.p. containing u.*

7.4. **The algorithm and the complexity.** From now on, it is assumed that the value group of V (and V^*) is a nondiscrete subgroup of $\mathbf{Q}$.

We fix a prepared pair $(R, S) =: (R_{r_0}, S_{s_0})$ such that $m_R S$ is *not* a principal ideal. By induction on $n \geq 0$, we associate with a given prepared pair (R_{r_n}, S_{s_n}) such that $m_{R_{r_n}} S_{s_n}$ is not a principal ideal, a new prepared pair $(R_{r_{n+1}}, S_{s_{n+1}})$, with $r_{n+1} > r_n$, $s_{n+1} > s_n$, and such that $m_{R_{r_{n+1}}} S_{s_{n+1}}$ is not a principal ideal.

Let (u_{r_n}, v_{r_n}) be an *admissible* r.s.p. of R_{r_n}. Let (x_{s_n}, y_{s_n}) be a r.s.p. of S_{s_n} such that the support of x_{s_n} is F_{s_n}. There are relations

$$\begin{array}{rcl} u_{r_n} & = & \gamma_n x_{s_n}^{a_n} \\ v_{r_n} & = & x_{s_n}^{b_n} f_n, \end{array}$$

where γ_n is a unit in S_{s_n}, and x_{s_n} does not divide f_n. Also f_n is *not* a unit, since $m_{R_{r_n}} S_{s_n}$ is not a principal ideal. Among all $s \geq s_n$, there is a least integer s_{n+1} such that $S_{s_{n+1}}$ is free and the strict transform of div(f_n) in $S_{s_{n+1}}$ is empty. We have $s_{n+1} > s_n$.

By construction, $m_{R_{r_n}} S_{s_{n+1}}$ is a principal ideal. The nonempty set of integers $r > r_n$ such that $S_{s_{n+1}}$ dominates R_{r_n} has a maximal element which is denoted by

r_{n+1}. This completes the definition of the pair $(R_{r_{n+1}}, S_{s_{n+1}})$. We postpone to section 7.6 the proof of the facts that $R_{r_{n+1}}$ is free (and hence that $(R_{r_{n+1}}, S_{s_{n+1}})$ is prepared by proposition 7.6) and that $R_{r_{n+1}}$ is independent of the choice of the admissible r.s.p. (u_{r_n}, v_{r_n}) of R_{r_n}.

Let now (R_r, S_s) be a prepared pair, such that R_r has a r.s.p. (u, v), S_s has a r.s.p. (x, y) with u and x satisfying property (2.iv) of definition 7.5. We assume that there is an expression

$$\begin{array}{rcl} u & = & \gamma x^a \\ v & = & x^b f, \end{array} \tag{31}$$

where $f \in S_s$ is a nonunit which is not divisible by x. Let v' be a regular parameter of R_r which is transversal to u. By the Weierstrass preparation theorem, there is an equation

$$\delta v' = v - P(u),$$

where δ is a unit and $P \in k[[u]]$. Let $\overline{\nu}_s$ be the natural valuation of the DVR $\frac{S_s}{(x)}$. Comparing with (31), we get that either

$$v' = \gamma' x^{b'},$$

where γ' is a unit and $b' \leq b$, or

$$v' = x^b f',$$

where $\overline{\nu}_s(f' \bmod x) = \overline{\nu}_s(f \bmod x)$. Hence the triple of integers $(a, b, \overline{\nu}_s(f) \bmod x)$ is independent of the choice of a r.s.p. of R_r such that f is *not* a unit in (31). Also notice that f is not a unit if $m_{R_r} S_s$ is not a principal ideal (this holds in particular if $(r, s) = (r_n, s_n)$ for some $n \geq 0$). Therefore the complexity introduced below is well defined.

Definition 7.9. *(The complexity) Let (R_r, S_s) be a prepared pair such that there exists an expression (31), where $f \in S_s$ is a nonunit which is not divisible by x. Let*

$$d (= d_{r,s}) := \overline{\nu}_s(f \bmod x) > 0,$$

where $\overline{\nu}_s$ denotes the natural valuation of the DVR $\frac{S_s}{(x)}$ as before. The complexity of the prepared pair (R_r, S_s) is defined to be $c_{r,s} := ad > 0$.
The complexity of the prepared pair (R_{r_n}, S_{s_n}) is denoted by $c_n (:= c_{r_n, s_n})$.

Remark 7.10. *The integer $i_{r,s}$ can be interpreted as a ramification index as follows: let ${\nu'}_s$ be the rank two valuation of K^* which is composed of the DVR of* ord_x *and of $\overline{\nu}_s$. Then $c_{r,s}$ is the ramification index of ${\nu'}_s$ relative to its restriction to K since,*

$${\nu'}_s(K^*) = \mathbf{Z}^2_{lex},$$

and

$${\nu'}_s(K) = \mathbf{Z}{\nu'}_s(u) \oplus \mathbf{Z}{\nu'}_s(v) = \mathbf{Z}(a, 0) \oplus \mathbf{Z}(b, d).$$

In particular, this shows that $c_{r,s}$ does not depend on r.

7.5. **The generating sequence of a valuation: an overview.** In this section, we collect and recall the necessary material about generating sequences of a valuation centered in a regular local ring of dimension two, as can be found in [19]. See also [9].

Let $R (= R_{r_0})$ be free. We fix a regular parameter $u \in R$, whose support is equal to E_{r_0}. By proposition 7.6, the set of *free* R_r is infinite. Therefore, the integers $(r'_{i+1}, \overline{r}_i)$ considered below are well defined.

Definition 7.11. *Let $r'_1 = \overline{r}_0 := r_0$. For all $i \geq 1$, let $(r'_{i+1}, \overline{r}_i)$ be the pair of integers with the following properties:*

(1) *$\overline{r}_i$ is the largest integer $r \geq r'_i$ such that $R_{r'}$ is free for all r' with $r'_i \leq r' \leq r$.*
(2) *r'_{i+1} is the smallest integer $r > \overline{r}_i$ such that R_r is free.*

Let $P_0 := u$ and let $P_1 = v$ be any regular parameter of S, transversal to u, and such that the strict transform of $\mathrm{div}(v)$ in $R_{\overline{r}_1}$ is not empty. For each $i \geq 1$, there exists $P_{i+1} \in R$ such that $\mathrm{div}(P_{i+1})$ is an analytically irreducible curve in $\mathrm{Spec}R$, and such that the strict transform of $\mathrm{div}(P_{i+1})$ in $\mathrm{Spec}R_{\overline{r}_{i+1}}$ is smooth and transversal to $E_{\overline{r}_{i+1}}$ (with notations as in [19] remark 7.5, P_{i+1} is the local equation of any curve $C_i \in \mathcal{C}_i$ (resp. $C_{i-1} \in \mathcal{C}_{i-1}$) if $\mathrm{div}(P_2)$ is singular (resp. nonsingular)). Such a sequence $(P_i)_{i \geq 0}$ is called a *generating sequence* of ν (see [19] definition 1.1 for explanations about this terminology).

Given $f \in R$, one defines

$$\deg f := \overline{\nu}_{r_0}(f \bmod u),$$

where $\overline{\nu}_{r_0}$ denotes the natural valuation of the DVR $\frac{R}{(u)}$. Let $m_0 := 1$, $m_1 := \deg(P_2)$, and $m_i := \frac{\deg(P_{i+1})}{\deg(P_i)}$. Then $m_i \in \mathbf{N}$ and $m_i \geq 2$ for all $i \geq 1$. Moreover, the m_i's do not depend on the choice of the P_i's with the properties listed above (this follows from (7.3) of [19]). By definition, we have

$$\deg P_{i+1} = \prod_{i'=0}^{i} m_{i'} \text{ for all } i \geq 0.$$

Let now R_r be an iterated quadratic transform of R along V and which is free (we assume that $R_r \neq R$). Let $u_r \in R_r$ be a regular parameter with support equal to E_r. There is an associated divisorial valuation of K, $\nu_r := \mathrm{ord}_{E_r}$. By definition, the following holds.

$$\text{Let } v_r := \frac{P_{g+1}}{u_r^{\nu_r(P_{g+1})}} \in R_r. \text{ Then } (u_r, v_r) \text{ is an } \textit{admissible} \text{ r.s.p. of } R_r. \tag{32}$$

Let $g \geq 0$ be the smallest integer $i \geq 0$ such that the strict transform of $\mathrm{div}(P_{i+1})$ in $\mathrm{Spec}R_r$ is nonempty. We thus have ${r'}_{g+1} \leq r \leq \overline{r}_{g+1}$. The values of the P_i's w.r.t. ν_r have the following classical properties.

Proposition 7.12. *The following holds.*

(1) $\nu_r(u) = \prod_{i=0}^{g} m_i$.

(2) *Let $\Gamma_i := < \{\nu_r(P_{i'})\}_{0 \leq i' \leq i} >$, for $0 \leq i \leq g$. Then*
$$\Gamma_i = \left(\prod_{i'=i+1}^{g} m_{i'} \right) \mathbf{Z}.$$

(3) *There are inequalities*
$$\nu_r(P_{i+1}) > m_i \nu_r(P_i) \text{ for } 1 \leq i < g.$$

Proof. By [19] proposition 7.7,

$$\nu_r(u) = \deg P_{i+1} = \prod_{i=0}^{g} m_i.$$

Statement (2) follows from remark 6.1 and the last statement in corollary 8.4 of [19] applied to the valuation ν_r. Statement (3) is (2) of remark 6.2 of [19]. □

We now introduce monomial expansions in terms of the P_i's. Similar considerations appear in [9] proposition 1.

Lemma 7.13. *Let $g \geq 0$ be an integer. Any integer $d \geq 0$ has a unique writing*

$$d = \sum_{i=0}^{g} d_{i+1} \left(\prod_{i'=0}^{i} m_{i'} \right),$$

with $d_{g+1} \geq 0$ and $0 \leq d_{i+1} < m_{i+1}$ for $0 \leq i < g$.

Proof. Consecutive Euclidian divisions. □

Definition 7.14. *Let $g \geq 0$ be a fixed integer. For each $d \geq 0$, we define*

$$M_d := \prod_{i=0}^{g} P_{i+1}^{d_{i+1}},$$

where the d_i's are those integers in Lemma 7.13.

Let $f \in R$. Assume that u does not divide f and that $d := \deg f > 0$. The set of monomials $(M_{d'})_{0 \leq d' < d}$ forms a basis of the free $k[[u]]$-module $\frac{\hat{R}}{(f)} = \frac{k[[u,v]]}{(f)}$. Consequently, there exists a unique writing

$$\delta f = M_d + \sum_{d'=0}^{d-1} \lambda_{d'}(u) M_{d'}, \tag{33}$$

where $\delta \in k[[u,v]]$ is a unit and $\lambda_{d'}(u) \in k[[u]]$ satisfies $\mathrm{ord}_u \lambda_{d'} > 0$ for all d'. The expansion (33) depends on a choice of $g \geq 0$ and of the P_i's, for $0 \leq i \leq g+1$. Let also $\lambda_d := 1$.

Proposition 7.15. *Let R_r and g be as above. The following holds:*

(1) *Let $f \in R$ be such that u does not divide f and $d := \deg f > 0$. There is a expansion of f as in (33). We have*

$$\nu_r(f) = \min_{d'} \{ \nu_r(\lambda_{d'}(u) M_{d'}) \},$$

and

$$\overline{\nu}_r \left(\frac{f}{u_r^{\nu_r(f)}} \right) = \min_{d'} \{ d'_{g+1} \ / \ \nu_r(\lambda_{d'}(u) M_{d'}) = \nu_r(f) \},$$

where $\overline{\nu}_r$ is the natural valuation of the DVR $\frac{R_r}{(u_r)}$. In particular, the strict transform of $\mathrm{div}(f)$ in $\mathrm{Spec} R_r$ is empty if and only if $\overline{\nu}_r \left(\frac{f}{u_r^{\nu_r(f)}} \right) = 0$, hence if and only if $\nu_r(f) = \nu_r(\lambda_{d'}(u) M_{d'})$ for some d' with $d' < \deg P_{g+1}$.

(2) *With notations as in (1), there is an inequality*

$$\left(\prod_{i=0}^{g} m_i \right) \overline{\nu}_r \left(\frac{f}{u_r^{\nu_r(f)}} \right) \leq d.$$

Equality holds if and only if $\nu_r(M_d) < \nu_r(\lambda_{d'}(u) M_{d'})$ for all d', $0 \leq d' \leq d-1$.

Proof. By definition of ν_r and $\overline{\nu}_r$, there are expansions

$$f = \gamma_d u_r^{\nu_r(M_d)} v_r^{d_{g+1}} + \sum_{d'=0}^{d-1} \gamma_{d'} u_r^{\nu_r(\lambda_{d'}(u)M_{d'})} v_r^{d'_{g+1}} \tag{34}$$

in R_r, where the $\gamma_{d'}$'s are units. Let $0 \leq d', d'' \leq d$, with $d' \neq d''$. By (2) of proposition 7.12 and the inequalities in Lemma 7.13, we have that

$$\nu_r(\lambda_{d'}(u)M_{d'}) = \nu_r(\lambda_{d''}(u)M_{d''}) \Longrightarrow d'_{g+1} \neq d''_{g+1}. \tag{35}$$

Let α be the minimal value w.r.t. ν_r of all monomials $\lambda_{d'}(u)M_{d'}$ appearing in the expansion (33) of f. Among all monomials in (33) satisfying the equality $\nu_r(\lambda_{d'}(u)M_{d'}) = \alpha$, there is a unique one with d'_{g+1} minimal by (35). Let $\delta \geq 0$ be this minimal value of d'_{g+1}. Then (34) can be rewritten as

$$f = \gamma u_r^{\alpha} \left(v_r^{\delta}(1 + v_r f_1(u_r, v_r)) + u_r f_2(u_r, v_r) \right),$$

where γ is a unit. This proves (1). Then (2) follows from the obvious inequality

$$\delta \left(\prod_{i=0}^{g} m_i \right) \leq d.$$

□

Proposition 7.15 is a useful tool in order to compute values w.r.t. the initial valution ν:

Proposition 7.16. *The following holds.*

(1) *Let $f \in R$. For any r such that R_r is free and the strict transform of* $\mathrm{div}(f)$ *in* $\mathrm{Spec}R_r$ *is empty, we have*

$$\nu_r(f) = \frac{\nu(f)}{\nu(u_r)}.$$

(2) *The value group of V is* $\Gamma = \bigcup_{g \geq 0} \frac{\mathbf{Z}}{\prod_{i=0}^{g} m_i} \nu(u).$

Proof. The assumption in (1) implies that $f = \gamma u_r^{\nu_r(f)}$, where $\gamma \in R_r$ is a unit. Hence

$$\nu(f) = \nu(u_r^{\nu_r(f)}) = \nu_r(f)\nu(u_r),$$

and this proves (1).

Let $f \in R$. We may choose r large enough so that the strict transform of $\mathrm{div}(f)$ in $\mathrm{Spec}(R_r)$ is empty. We may assume that R_r is free after possibly choosing some larger r. By (1), we have $\nu(f) \in \mathbf{Z}\nu(u_r)$. On the other hand, (1), together with (1) of proposition 7.12 imply that

$$\nu(u_r) = \frac{\nu(u)}{\prod_{i=0}^{g} m_i}$$

for some g. This proves (2). □

Given an *admissible* r.s.p. $(u, v) = (P_0, P_1)$ of R (see definition 7.8), one can choose equations for the P_i's in Weierstrass form as follows (this follows from the last statement in corollary 8.4 and theorem 8.6 of [19]):

$$P_2 := v^{m_1} - \lambda_1 u^{l_{1,0}} - \sum_{\mathbf{l}'_1} \lambda_{1,\mathbf{l}'_1} v^{l'_{1,1}} u^{l'_{1,0}}, \tag{E_1}$$

$$P_{i+1} = P_i^{m_i} - \lambda_i M_i - \sum_{\mathbf{l}'_i} \lambda_{i,\mathbf{l}'_i} M_{i,\mathbf{l}'_i}. \qquad (E_i)$$

Here, M_i is a monomial in $u, v, P_2, \ldots, P_{i-1}$, and each $M_{i,\mathbf{l}'_i}$ is a monomial in $u, v, P_2, \ldots, P_i$. They do satify conditions similar to those in lemma 7.13:

$$M_i := \prod_{i'=0}^{i-1} P_{i'}^{l_{i,i'}}, \text{ and } M_{i,\mathbf{l}'_i} := \prod_{i'=0}^{i} P_{i'}^{l'_{i,i'}}, \qquad (F_i)$$

with $0 \leq l_{i,i'}, l'_{i,i'} < m_{i'}$ for $1 \leq i' \leq i$, and $l_{i,0}, l'_{i,0} \geq 0$ arbitrary. Moreover, if $\Gamma_i :=< \{\nu(P_{i'})\}_{0 \leq i' \leq i} >$, then for $i \geq 1$,

$$\nu(M_i) \text{ has order precisely } m_i \text{ in } \frac{\Gamma_{i-1}}{m_i \Gamma_{i-1}} \simeq \frac{\mathbf{Z}}{m_i \mathbf{Z}}. \qquad (G_i)$$

The $\lambda_i, \lambda_{i,\mathbf{l}'_i}$ are constants, with $\lambda_i \neq 0$. We have

$$\nu(P_{i+1}) > \nu(P_i^{m_i}) = \nu(M_i) \qquad (H_i)$$

and

$$\nu(M_{i,\mathbf{l}'_i}) > \nu(P_i^{m_i}) \qquad (H'_i)$$

for $i \geq 1$ and for all $\mathbf{l}'_i$'s.

Remark 7.17. *Conversely, given a sequence of Weierstrass polynomials* $(P_{i+1})_{i \geq 1}$ *given by relations* (E_i), (F_i) *for all* $i \geq 1$, *let* $\overline{\beta}_0 := 1$, *and define by induction on* $i \geq 1$

$$\overline{\beta}_i := \frac{1}{m_i} \sum_{i'=0}^{i-1} l_{i,i'} \overline{\beta}_{i'}.$$

Let $\Gamma_i :=< \{\overline{\beta}_{i'}\}_{0 \leq i' \leq i} >$. *Then* $(P_i)_{i \geq 0}$ *is a generating sequence of a (uniquely determined) valuation ring* V *of* $\hat{R} = k[[u, v]]$ *whose value group is a nondiscrete subgroup of* $\mathbf{Q}$ *if the* $\overline{\beta}_i$*'s satisfy the following three properties:*

$$\sum_{i'=0}^{i-1} l_{i,i'} \overline{\beta}_{i'} \text{ has order precisely } m_i \text{ in } \frac{\Gamma_{i-1}}{m_i \Gamma_{i-1}} \text{ for all } i \geq 1,$$

$$\overline{\beta}_{i+1} > m_i \overline{\beta}_i \text{ for all } i \geq 1,$$

and

$$\sum_{i'=0}^{i} l'_{i,i'} \overline{\beta}_{i'} > m_i \overline{\beta}_i \text{ for all } i \geq 1 \text{ and for all } \mathbf{l}'_i.$$

This is a rephrasing of the irreducibility criterion ([9] 7.2). This fact is extremely useful to build up explicit examples and will be used in section 7.11.

7.6. **Consistency of the definition of the algorithm.** In this section, we prove that the algorithm in section 7.4 is well defined. This fact is a consequene of some of the considerations introduced in section 7.5.

Proposition 7.18. *The pair* (r_{n+1}, s_{n+1}) *in the definition of the algorithm does not depend on the choice of an admissible r.s.p.* (u_{r_n}, v_{r_n}) *of* R_{r_n}. *Moreover* $R_{r_{n+1}}$ *is free, and* $(R_{r_{n+1}}, S_{s_{n+1}})$ *is prepared.*

Proof. We may clearly assume that $n=0$. Since r_1 is determined by s_1, it is sufficient to prove that s_1 does not depend on the choice of an admissible r.s.p. (u_{r_n}, v_{r_n}) of R_{r_n} in order to prove the first statement. Fix a choice of an admissible r.s.p. (u,v) of R_{r_0}. The algorithm produces a value of s_1 associated with (u,v). Let v' be another regular parameter such that $\nu(v')=\nu(v)$.

By the Weierstrass preparation theorem, we have

$$\delta v' = v - P(u),$$

where δ is a unit, $P \in k[[u]]$ has order $n \geq 1$, and $n\nu(u) > \nu(v)$. We have an expression

$$\begin{array}{rcl} u & = & \gamma x^a \\ v & = & x^b f, \end{array}$$

where γ is a unit in S_{s_0}, and x does not divide f. We now apply (1) of proposition 7.16, with R replaced with S_{s_0}, V replaced with V^*, and R_r replaced with S_{s_1}. We get $\nu^*(v) = \nu_{s_1}(v)\nu^*(x_{s_1})$, since the strict transform of $\mathrm{div}(f)$ in $\mathrm{Spec} S_{s_1}$ is empty. Similarly,

$$n\nu^*(u) = n\nu_{s_1}(u)\nu^*(x_{s_1}).$$

It follows that $n\nu_{s_1}(u) > \nu_{s_1}(v)$, and

$$\nu_{s_1}(v) = \nu_{s_1}(v'). \tag{36}$$

Consequently, $\delta v' = \gamma' x_{s_1}^{\nu_{s_1}(v)}$, where $\gamma' \in S_{s_1}$ is a unit. This proves that the strict transform of v' in $\mathrm{Spec} S_{s_1}$ is empty and by symmetry, the first statement in the proposition is proved.

In order to prove that R_{r_1} is free, recall from definition 7.11 the integers $(r'_{i+1}, \overline{r}_i)$. There is a uniquely determined integer $i \geq 1$ such that

$$r'_i \leq r_1 < r'_{i+1}.$$

By definition, R_{r_1} is free if $r'_i \leq r_1 \leq \overline{r}_i$. Assume that $\overline{r}_i < r_1 < r'_{i+1}$. Recall that $R_{r'_i}$ has a r.s.p. obtained as in (32). There is an expression

$$\begin{array}{rcl} u_{r'_i} & = & \gamma' x_{s_1}^{a'} \\ v_{r'_i} & = & x_{s_1}^{b'} f', \end{array} \tag{37}$$

where x_{s_1} does not divide f' in S_{s_1}. We now claim that f' is a unit in S_{s_1}. Actually, a r.s.p. of $R_{\overline{r}_i}$ is given by

$$\begin{array}{rcl} u_{\overline{r}_i} & = & u_{r'_i} \\ v_{\overline{r}_i} & = & v_{r'_i}/u_{r'_i}^{\overline{r}_i - r'_i}. \end{array}$$

We have $\nu(v_{\overline{r}_i}) < \nu(u_{\overline{r}_i})$ because $R_{\overline{r}_i+1}$ is not free. This proves that

$$\begin{array}{rcl} u_{\overline{r}_i} & = & \gamma' x_{s_1}^{a'} \\ v_{\overline{r}_i} & = & {\gamma'}^{r'_i - \overline{r}_i} x_{s_1}^{\overline{b}} f', \end{array}$$

with $0 < \overline{b} < a$. Since it is assumed that $\overline{r}_i < r_1$, $m_{R_{\overline{r}_i}} S_{s_1}$ is invertible, and consequently f' is a unit and the claim is proved.

Now, R_{r_1} has a r.s.p. $u_{r_1} = u_{r'_i}^{\alpha_0} v_{r'_i}^{\alpha_1}$, $v_{r_1} = u_{r'_i}^{\beta_0} v_{r'_i}^{\beta_1}$, with $\alpha_0\beta_1 - \alpha_1\beta_0 = 1$. By (37), this implies that $(u_{r_1}, v_{r_1})S_{s_1}$ is a principal ideal. This contradicts the definition of r_1 and thus proves the second statement in the proposition. Finally, the fact that R_{r_1} is free implies that $(R_{r_{n+1}}, S_{s_{n+1}})$ is prepared follows from proposition 7.6. $\square$

7.7. **Behaviour of the complexity under blowing up.** In this section, it is proved that whenever there is a diagram

$$\begin{array}{ccccc} S_{s_n} & \to & S_{s'} & \to & S_{s_{n+1}} \\ \uparrow & & \uparrow & & \uparrow \\ R_{r_n} & = & R_{r_n} & \to & R_{r_{n+1}}, \end{array}$$

such that $(R_{r_n}, S_{s'})$ is prepared, the complexity of $(R_{r_n}, S_{s'})$ is not greater than that of (R_{r_n}, S_{s_n}).

Proposition 7.19. *Let $n \geq 0$ and let s' be an integer satisfying the inequality $s_n \leq s' < s_{n+1}$. Assume that $S_{s'}$ is free.*
Let $c' := c_{r_n,s'}$ be the complexity of the pair $(R_{r_n}, S_{s'})$. Then $0 < c' \leq c_n$.

Proof. Let (u_{r_n}, v_{r_n}) be an admissible r.s.p. of R_{r_n}, and (x, y) be a r.s.p. of $S_{s'}$ satisfying property (2.iv) of definition 7.5. There are expressions

$$\begin{array}{rcl} u_{r_n} & = & \gamma_n x_{s_n}^{a_n} \\ v_{r_n} & = & x_{s_n}^{b_n} f_n, \end{array} \tag{38}$$

and

$$\begin{array}{rcl} u_{r_n} & = & \gamma' x^{a'} \\ v_{r_n} & = & x^{b'} f'. \end{array}$$

By definition of r_{n+1}, f' is not a unit. With notations as in definition 7.9, let $d_n = \overline{\nu}_{s_n}(f_n \bmod x_{s_n})$ and $d' = \overline{\nu}_{s'}(f' \bmod x_{s'})$, so that $c_n = a_n d_n$ and $c' = a'd'$.

We now apply the results of section 7.5 with R replaced with S_{s_n}, V replaced with V^*, and R_r replaced with $S_{s'}$. The corresponding integer g is denoted by h, and the m_i's are called n_j's to avoid confusions. Then (1) of proposition 7.12 reads

$$a' = a_n \left(\prod_{j=0}^{h} n_j \right), \tag{39}$$

and (2) of proposition 7.15 reads

$$d' \left(\prod_{j=0}^{h} n_j \right) \leq d_n, \tag{40}$$

and the conclusion follows. □

7.8. **Behaviour of the complexity under factoring down.** In this section, we prove that the complexity function $n \mapsto c_n$ is non-increasing and study cases of equality.

Recall from (38) that the inclusion $R_{r_n} \subset S_{s_n}$ is given by an expression

$$\begin{array}{rcl} u_{r_n} & = & \gamma_n x_{s_n}^{a_n} \\ v_{r_n} & = & x_{s_n}^{b_n} f_n, \end{array}$$

and that $d_n = \overline{\nu}_{s_n}(f_n \bmod x_{s_n}) > 0$ as before. The complexity of the prepared pair (R_{r_n}, S_{s_n}) is denoted by c_n. Proposition 7.12 will be used repeatedly in this section, with R replaced with R_{r_n}, and R_r replaced with $R_{r_{n+1}}$. The corresponding integer g in proposition 7.12 is denoted by g_n. We have $g_n \geq 1$. By definition 7.11, there is a sequence of integers

$$r_n = r'_1 < r'_2 < \cdots < r'_{g_n+1} \leq r_{n+1}.$$

Given a positive integer N, the prime to p part of N is denoted by $N_{(p)}$, that is, $N_{(p)}$ is the largest prime to p integer dividing N.

Theorem 7.20. *Let $n \geq 0$. The following holds.*

(1) $0 < c_{n+1} \leq c_n$.
(2) *if equality holds in (1), then $(d_{n+1})_{(p)}$ divides $(d_n)_{(p)}$, and*

$$\prod_{i=0}^{g_n-1} m_i = p^t$$

for some $t \geq 0$.

(3) *if equality holds in (1) and if $R_{r_{n+1}} \subset S_{s_{n+1}}$ is not the localization of a finite map then*

$$\prod_{i=0}^{g_n} m_i = p^t$$

for some $t \geq 1$.

Proof. We break it up in several steps.

Step 1. Assume that there is a diagram

$$\begin{array}{ccccc} S_{s_n} & \to & S_{s'} & \to & S_{s_{n+1}} \\ \uparrow & & \uparrow & & \uparrow \\ R_{r_n} & = & R_{r_n} & \to & R_{r_{n+1}}, \end{array}$$

for some s', $s_n \leq s' < s_{n+1}$ such that $S_{s'}$ is free as in section 7.7. The complexity c' of $(R_{r_n}, S_{s'})$ is not greater than c_n by proposition 7.19. Also, equality holds in (40) if $c' = c_n$, and thus d' divides d_n.

Let now s' be chosen so that $S_{s''}$ is not free for all s'' with $s' < s'' < s_{n+1}$. By what preceeds, it is sufficient to prove that $c_{n+1} \leq c'$, that $(d_{n+1})_{(p)}$ divides $(d')_{(p)}$ if $c_{n+1} = c'$, and to prove both statements on the m_i's.

Let (x, y) be a r.s.p. of $S_{s'}$ satisfying property (2.iv) of definition 7.5. Notice that $\mu := \nu_{s_{n+1}}$ is then a *monomial* valuation in x, y (i.e. the value w.r.t. μ of a series in x, y is the minimal of the values of its monomials in x, y). We consider two cases:

Case 1: $s_{n+1} = s' + 1$. We have $\mu(x) = \mu(y) = 1$, and $S_{s_{n+1}}$ has a regular parameter $y_{s_{n+1}} := \frac{y}{x}$ transversal to $x_{s_{n+1}}$.

Case 2: $s_{n+1} > s' + 1$. We have $\mu(x) =: n_1 > 1$, $\mu(y) =: q_1 \geq 1$, with g.c.d.$(n_1, q_1) = 1$. $S_{s_{n+1}}$ has a regular parameter $y_{s_{n+1}} := \frac{y^{n_1} - \theta x^{q_1}}{x^{q_1}}$ transversal to $x_{s_{n+1}}$, where $\theta \in k$, $\theta \neq 0$.

Step 2. Newton polygons: the leftmost vertex.

From now on till the end of the proof of theorem 7.20, we further simplify notations by writing the equations defining the inclusion $R_{r_n} \subset S_{s'}$ in the form

$$\begin{array}{rcl} u & = & \gamma x^a \\ v & = & x^b f, \end{array} \tag{41}$$

with γ a unit. Also write $d := \overline{\nu}_{s_n}(f \bmod x) > 0$ and $g := g_n \geq 1$ for short.

Definition 7.21. *Let $F \in R_{r_n}$. The leading form of F is the unique polynomial $l(F) \in k[x, y]$, homogeneous for the monomial valuation μ of weight $\mu(F)$ such that $\mu(F - l(F)) > \mu(F)$.*

Notice that by (36), $l(v)$ is independent of the choice of an admissible r.s.p. (u, v) of R_{r_n}. Apply (1) of proposition 7.15 with R replaced with $S_{s'}$ and R_r replaced with

$S_{s_{n+1}}$. Then $\deg_y l(v) \le d$, and $\deg_y l(v) = d$ only if $l'(v) := \frac{l(v)}{x^b}$ is *unitary* in y of degree d.

Recall now the definition of the P_i's, $0 \le i \le g+1$ (beginning of section 7.5), and that they can be chosen in Weierstrass form (equation (E_i) of section 7.5).

Definition 7.22. *Let i, $0 \le i \le g+1$. P_i is said to be bad if its leading form $l(P_i)$ w.r.t. μ is of the form $l(P_i) = \theta_i x^{L_i}$ for some $\theta_i \in k$, $\theta_i \neq 0$. Otherwise, P_i is said to be good.*

Remark 7.23. *By definition of g, P_{g+1} is good . This follows from the last statement in (1) of proposition 7.15. Clearly, $P_0 = u$ is bad.*

Let i, $0 \le i \le g+1$. We write

$$P_i = x^{b_i} f_i \in S_{s'},$$

where x does not divide f_i. Let

$$\Delta_i :=< \{\mu(P_{i'})\}_{0 \le i' \le i} > \text{ and } \Gamma_i :=< \mu(x), \{\mu(f_{i'})\}_{0 \le i' \le i} > .$$

Each of Δ_i, Γ_i is a subgroup of the value group $\Gamma_\mu \simeq \mathbf{Z}$ of μ. There is an obvious inclusion $\Delta_i \subseteq \Gamma_i$. Let

$$e_i := [\Gamma_i : \Delta_i].$$

Write $\Gamma_i = \mathbf{Z}\xi_i$, with $\xi_i \in \mathbf{N}$. Let

$$\tau_i := \frac{\mu(x)}{\xi_i} \in \mathbf{N}.$$

Lemma 7.24. *Let i, $1 \le i \le g$. Assume that $P_{i'}$ is bad (definition 7.22) for $0 \le i' \le i-1$. The following properties hold:*

(1) *Replace μ with ν in the definition of Δ_i and Γ_i, and let e_i^ν, τ_i^ν be the resulting values of e_i, τ_i. Then $e_i^\nu = e_i, \tau_i^\nu = \tau_i$.*
Moreover, $\tau_i = \frac{\mu(x)}{\text{g.c.d.}(\mu(f_i), \mu(x))}$.
(2) *$e_0 = a$ and $e_i \mid e_{i-1}$.*
(3) *$m_i = \tau_i \frac{e_{i-1}}{e_i} \ge 2$.*
(4) *Let $u_{r'_{i+1}} \in R_{r'_{i+1}}$ be a regular parameter with support $E_{r'_{i+1}}$ (definition 7.11). We have*

$$u_{r'_{i+1}} = \gamma_{r'_{i+1}} x_{s_{n+1}}^{e_i \frac{\mu(x)}{\tau_i}} \in S_{s_{n+1}},$$

where $\gamma_{r'_{i+1}}$ is a unit.
(5) *Assume furthermore that P_i is bad. Then*

$$\frac{L_1}{b} > 1, \tag{42}$$

and, if $i \ge 2$,

$$\frac{L_i}{L_{i-1}} > m_{i-1}. \tag{43}$$

Proof. Let F be any of the $P_{i'}, f_{i'}$'s for some i', $0 \le i' \le i$. By definition of g, the strict transform of F in $\mathrm{Spec} S_{s_{n+1}}$ is empty. By (1) of proposition 7.16, $\nu(F) = \mu(F)\nu(x_{s_{n+1}})$. This proves the first statement in (1). The second statement in (1) is obvious, since $\mu(f_{i'}) \in \mathbf{Z}\mu(x)$ for $0 \le i' \le i-1$ by assumption.

By definition, $e_0 = [\mathbf{Z}\mu(x) : \mathbf{Z}\mu(u)] = a$. Since $P_{i'}$ is bad for $0 \le i' \le i-1$, we have $\Gamma_{i-1} = \mathbf{Z}\mu(x)$. Hence, $e_{i-1}\mu(f_i) = e_{i-1}\mu(P_i) - b_i e_{i-1}\mu(x) \in \Delta_i$. Since $\Gamma_i = \Gamma_{i-1} + \mathbf{Z}\mu(f_i)$, we have $e_{i-1}\Gamma_i \subseteq \Delta_i$. This proves (2).

There is a diagram

$$\begin{array}{ccc} \Gamma_{i-1} = \mathbf{Z}\mu(x) & \xrightarrow{\tau_i} & \Gamma_i \\ {\scriptstyle e_{i-1}}\uparrow & & \uparrow{\scriptstyle e_i} \\ \Delta_{i-1} & \xrightarrow{m_i} & \Delta_i. \end{array}$$

All maps are inclusions of subgroups of Γ_μ whose index is as indicated. This proves (3).

By (1) of proposition 7.12, with R_r replaced with $R_{r'_{i+1}}$, we have $u = \delta_{r'_{i+1}} u_{r'_{i+1}}^{\prod_{i'=0}^{i} m_{i'}}$, where $\delta_{r'_{i+1}}$ is a unit in $R_{r'_{i+1}}$. By definition, $x = \epsilon x_{s_{n+1}}^{\mu(x)}$, where ϵ is a unit. Since $u = \gamma x^a$, we get

$$u_{r'_{i+1}} = \gamma_{r'_{i+1}} x_{s_{n+1}}^{\frac{a\mu(x)}{\prod_{i=0}^{i} m_{i'}}}, \tag{44}$$

where $\gamma_{r'_{i+1}} \in S_{s_{n+1}}$ is a unit. We have $\tau_{i'} = 1$ for $0 \leq i' \leq i-1$, since $P_{i'}$ is bad. Hence

$$\prod_{i'=0}^{i} m_{i'} = a\frac{\tau_i}{e_i}$$

by (3). Comparing with (44), we get the formula in (4).

Statement (42) in (5) is trivial. Assume $i \geq 2$. By (3) of proposition 7.12, we have

$$\frac{\mu(P_i)}{\mu(P_{i-1})} > m_{i-1}.$$

Since both of P_{i-1}, P_i are bad, we have

$$\frac{\mu(P_i)}{\mu(P_{i-1})} = \frac{\mu(x^{L_i})}{\mu(x^{L_{i-1}})} = \frac{L_i}{L_{i-1}}.$$

This proves (43).

□

Let i, $0 \leq i \leq g+1$. The Newton polygon of P_i in the coordinates (x, y) is denoted by $NP(P_i)$.

Lemma 7.25. *Let i, $0 \leq i \leq g$. Assume that $P_{i'}$ is bad (definition 7.22) for $0 \leq i' \leq i$. Let $V_0 := (b, d)$. The leftmost vertex of $NP(P_{i+1})$ is*

$$\left(\prod_{i'=0}^{i} m_{i'}\right) V_0 := \left(b\prod_{i'=0}^{i} m_{i'}, d\prod_{i'=0}^{i} m_{i'}\right).$$

Proof. Induction on i. It follows from the definitions that the leftmost vertex of $NP(v)$ is $V_0 = (b, d)$. Let $i \geq 1$ and recall expression (E_i) of P_{i+1}. The induction step implies that

$$\mathrm{ord}_x M_i = bl_{i,i-1}\prod_{j=0}^{i-2} m_j + \sum_{i'=1}^{i-2} bl_{i,i'}\prod_{j=0}^{i'-1} m_j + l_{i,0}a. \tag{45}$$

Since $P_{i'}$ is bad for $0 \leq i' \leq i$, we have $\mu(P_{i'}) = L_{i'}\mu(x)$. Hence by $(H_{i'})$, we get the equality

$$m_iL_i = \sum_{i'=1}^{i-1} l_{i,i'}L_{i'} + l_{i,0}a. \tag{46}$$

Substituting in (45) the value of $l_{i,i-1}$ obtained from (46), we get

$$\mathrm{ord}_x M_i = b\left(m_i\frac{L_i}{L_{i-1}}\right)\prod_{j=0}^{i-2} m_j + \sum_{i'=1}^{i-2} bl_{i,i'}\left(1-\frac{L_{i'}}{L_{i-1}}\prod_{j=i'}^{i-2} m_j\right)\prod_{j=0}^{i'-1} m_j + al_{i,0}\left(1-\frac{b}{L_{i-1}}\prod_{j=0}^{i-2} m_j\right).$$

Applying inequalities (42) and (43), we get

$$\mathrm{ord}_x M_i > b\prod_{i'=0}^{i} m_{i'} + 0 + 0 = \mathrm{ord}_x P_i^{m_i}. \tag{47}$$

Similarly, using $(H'_{i'})$ instead of $(H_{i'})$, we get

$$\mathrm{ord}_x M_{i,\mathbf{l}'_i} > \mathrm{ord}_x P_i^{m_i} \tag{48}$$

for all indices $\mathbf{l}'_i$ appearing in (E_i).

By (47) and (48), we get from expression (E_i) that $NP(P_{i+1})$ and $NP(P_i^{m_i})$ have the same leftmost vertex. □

Step 3. The good case.

Lemma 7.26. *Let i, $1 \le i \le g$. Assume that P_i is good. Then $i = g$. With notations as in (H_i), we have*

$$l(P_{i+1}) = l(P_i)^{m_i} - \lambda_i l(M_i). \tag{49}$$

Moreover, $r_{n+1} = r'_{g+1}$ (definition 7.11) and $R_{r_{n+1}} \subset S_{s_{n+1}}$ is the localization of a finite map.

Proof. By induction on i, it can be assumed that $P_{i'}$ is bad for $0 \le i' \le i-1$. Recall expression (E_i). By definition of g, the strict transform of $\mathrm{div}(P_{i'})$, $0 \le i' \le g$, in $\mathrm{Spec}S_{s_{n+1}}$ is empty. Then (1) of proposition 7.16 implies that

$$\mu(P_i) = \frac{\nu(P_i)}{\nu(x_{s_{n+1}})}.$$

Equality (H_i) and inequality (H'_i) therefore imply that

$$l(P_{i+1}) = l(P_i)^{m_i} - \lambda_i l(M_i)$$

provided the right hand side is not zero. Since P_i is good and $P_{i'}$ is bad for $0 \le i' \le i-1$, this holds and (49) is proved. In particular

$$\mu(P_{i+1}) = m_i\mu(P_i). \tag{50}$$

By (H_i) and (H'_i), we have $\nu(P_{i+1}) > m_i\nu(P_i)$. By (1) of proposition 7.16, this is not compatible with (50) unless the strict transform of (at least one of) $\mathrm{div}(P_i)$, $\mathrm{div}(P_{i+1})$ in $\mathrm{Spec}(S_{s_{n+1}})$ is nonempty. By definition of g, this forces $i = g$.

By (4) of lemma 7.24, the inclusion $R_{r_{n+1}} < S_{s_{n+1}}$ has a local expression

$$
\begin{aligned}
u_{r'_{g+1}} &= \gamma_{r'_{g+1}} x_{s_{n+1}}^{e_g \frac{\mu(x)}{\tau_g}} \\
v_{r'_{g+1}} &= F_{r'_{g+1}},
\end{aligned}
$$

where $\gamma_{r'_{g+1}}$ is a unit, and

$$\mu(F_{r'_{g+1}}) = \mu(\frac{P_{g+1}}{P_g^{m_g}}) = 0$$

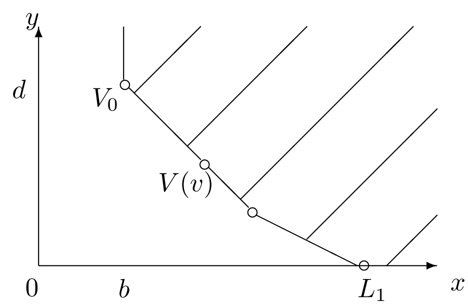
by (50).

Therefore $x_{s_{n+1}}$ does not divide $F_{r'_{g+1}}$ in $S_{s_{n+1}}$. Consequently, $R_{r_{n+1}} \subset S_{s_{n+1}}$ is the localization of a finite map and $r_{n+1} = r'_{g+1}$. □

Step 4. The bad case.

In case v is bad, it is convenient to introduce another vertex of $NP(v)$ as illustrated in the following picture (see below for a formal definition). We extend the notion to all P_i's, for $1 \leq i \leq g$.

$NP(v)$



Let $F \in R_{r_n}$ have an expansion

$$F = \sum_{\alpha,\beta} \theta_{\alpha,\beta} x^\alpha y^\beta \in k[[x,y]],$$

where $\theta_{\alpha,\beta} \in k$. Let $V_0(F)$ be the leftmost vertex of $NP(F)$.

Definition 7.27. *Let $F \in R_{r_n}$ be such that $NP(F)$ is not a translate of $\mathbf{R}^2_+$. Let $V(F)$ be the vertex of $NP(F)$ defined as follows: among all (α,β), distinct from $V_0(F)$, lying in a compact face of $NP(F)$ and such that $\theta_{\alpha,\beta} \neq 0$, $V(F)$ has α minimal.*

Let φ be a linear form on $\mathbf{R}^2$ which is nonnegative on $\mathbf{R}^2_+$. Then φ has a minimal value $\varphi(F)$ on $NP(F)$. Clearly, $\varphi(F_1F_2) = \varphi(F_1) + \varphi(F_2)$.

Let i, $1 \leq i \leq g$. From now on till the end of this step, it is assumed that P_i is bad. By lemma 7.26, this implies that $P_{i'}$ is bad for $1 \leq i' \leq i$. Notice that, since P_i is bad, $NP(P_i)$ is not a translate of $\mathbf{R}^2_+$.

In what follows, we choose $\varphi \neq 0$ which is constant on the first edge of $NP(P_i)$. That is, by lemma 7.25, φ satisfies

$$\left(\prod_{i'=0}^{i-1} m_{i'}\right) \varphi(V_0) = \varphi\left(V(P_i)\right)$$

Lemma 7.28. *Let i, $1 \leq i \leq g$. Assume that P_i is bad. The following holds:*

(1) *Assume that either m_i is not a power of p or that $V(P_i) \neq (L_i, 0)$. Then the first edge of $NP(P_{i+1})$ and that of $NP(P_i^{m_i})$ have the same slope. Moreover, the first edge of $NP(P_{i+1})$ does not intersect the x-axis.*

(2) *Assume that m_i is a power of p and that $V(P_i) = (L_i, 0)$. Then $NP(P_{i+1}) \subset NP(P_i^{m_i})$ and $\left(\prod_{i'=0}^{i} m_{i'}\right) V_0$ is the unique point of $NP(P_{i+1})$ lying in the unique compact face of $NP(P_i^{m_i})$.*

Proof. Induction on i. Let i_0 be the largest integer i', $0 \leq i' \leq i-1$, such that $V(P_{i'}) = (L_{i'}, 0)$.

All indices i' with $i_0 + 1 \leq i' \leq i-1$ satisfy by definition assumption (1) of the lemma. The induction step thus implies that

$$\varphi(P_{i'}) = \frac{\varphi(P_i)}{\prod_{j=i'}^{i-1} m_j} \text{ for } i_0 + 1 \leq i' \leq i-1. \tag{51}$$

By statement (1) of the induction step applied consecutively to all indices i' with $1 \leq i' \leq i_0 - 1$, we get that all indices i' with $1 \leq i' \leq i_0 - 1$ satisfy assumption (2) of the lemma. The index i_0 may satisfy either assumption (1) or (2). In any case, we get

$$\varphi(P_{i'}) = \varphi(x^{L_{i'}}) \text{ for } 1 \leq i' \leq i_0. \tag{52}$$

Recall expression (E_i). By (51) and (52), we get

$$\varphi(M_i) = \left(\sum_{i'=1}^{i_0} l_{i,i'} L_{i'} + l_{i,0} a\right) \varphi(x) + \sum_{i'=i_0+1}^{i-1} l_{i,i'} \frac{\varphi(P_i)}{\prod_{j=i'}^{i-1} m_j}.$$

By definition of φ, we have $\varphi(P_i) \leq \varphi(x^{L_i})$. Hence

$$\varphi(M_i) \geq \left(\sum_{i'=1}^{i_0} l_{i,i'} \frac{L_{i'}}{L_i} + l_{i,0} \frac{a}{L_i} + \sum_{i'=i_0+1}^{i-1} \frac{l_{i,i'}}{\prod_{j=i'}^{i-1} m_j}\right) \varphi(P_i) \tag{53}$$

Since $P_{i'}$ is bad for $0 \leq i' \leq i$, we have $\mu(P_{i'}) = L_{i'} \mu(x)$. Hence by (H_i), we get the equality

$$m_i L_i = \sum_{i'=1}^{i-1} l_{i,i'} L_{i'} + l_{i,0} a.$$

Substituting in (53), we get

$$\varphi(M_i) \geq m_i \varphi(P_i) + \varphi(P_i) \sum_{i'=i_0+1}^{i-1} l_{i,i'} \left(\frac{1}{\prod_{j=i'}^{i-1} m_j} - \frac{L_{i'}}{L_i}\right). \tag{54}$$

By (42) and (43), this implies that $\varphi(M_i) \geq m_i \varphi(P_i)$. Similarly, using (H'_i) instead of (H_i), we get

$$\varphi(M_{i,\mathbf{l}'_i}) > m_i \varphi(P_i)$$

for all indices $\mathbf{l}'_i$.

Given $F \in R_{r_n}$, let $\mathrm{in}_\varphi F \in k[x,y]$ denote the unique φ-homogeneous polynomial such that $\varphi(F - \mathrm{in}_\varphi F) > \varphi(F)$. Comparing with expression (E_i), we get from the previous considerations that

$$\mathrm{in}_\varphi P_{i+1} = (\mathrm{in}_\varphi P_i)^{m_i} \tag{55}$$

if inequality is strict in (54), and

$$\mathrm{in}_\varphi P_{i+1} = (\mathrm{in}_\varphi P_i)^{m_i} - \lambda_i \mathrm{in}_\varphi M_i \tag{56}$$

if equality holds in (54).

First assume that $\varphi(P_i) < L_i\varphi(x)$. This assumption precisely means that $NP(P_i)$ has more than one compact edge. Therefore assumption (1) of the lemma holds and this shows that inequality is strict in (54). The conclusion then follows from (55).

Assume now that $\varphi(P_i) = L_i\varphi(x)$. This assumption means that $NP(P_i)$ has precisely one compact edge. The induction step applied consecutively to all indices i' with $1 \leq i' \leq i-1$ implies that $m_{i'}$ is a power of p and that $V(P_{i'}) = (L_{i'}, 0)$. In particular, $i_0 = i-1$ and equality holds in (54). Statement (2) of the induction step applied consecutively to all indices i' with $1 \leq i' \leq i-1$ now shows that

$$\mathrm{in}_\varphi M_i = \eta x^{\sum_{i'=1}^{i-1} l_{i,i'} L_{i'} + l_{i,0} a},$$

with $\eta \in k$, $\eta \neq 0$. Under assumption (1), $\mathrm{in}_\varphi P_{i+1}$ contains at least two monomials, and none lying on the x-axis by (56), and the conclusion follows. Under assumption (2), we have

$$\mathrm{in}_\varphi P_{i+1} = \eta'(x^b y^d)^{\prod_{i'=0}^{i} m_{i'}},$$

with $\eta' \in k$, $\eta' \neq 0$, and the conclusion follows. This concludes the proof. □

Step 5. The proof of theorem 7.20.

We first prove statement (1). Recall cases 1 and 2 considered in step 1.

Case 1 By (1) of proposition 7.15 and (4) of lemma 7.24, we have

$$0 < c_{n+1} = \mathrm{ord}_y l(P_{g+1}) e_g \leq \deg_y l(P_{g+1}) e_g. \tag{57}$$

By lemma 7.25 if P_g is bad, or by (49) if P_g is good, we have

$$\deg_y l(P_{g+1}) \leq d \prod_{i=0}^{g} m_i. \tag{58}$$

Thus

$$0 < c_{n+1} \leq d e_g \prod_{i=0}^{g} m_i = d e_g \frac{a}{e_g} = c'$$

by (3) of lemma 7.24.

Case 2 Similarly, we have

$$0 < c_{n+1} = \mathrm{ord}_{y^{n_1} - \theta x^{q_1}} l(P_{g+1}) e_g \frac{n_1}{\tau_g} \leq \left[\frac{\deg_y l(P_{g+1})}{n_1}\right] e_g \frac{n_1}{\tau_g} \leq e_g \frac{n_1}{\tau_g} \frac{d}{n_1} \prod_{i=0}^{g} m_i = c'.$$

We now prove (2) of theorem 7.20 by analysing under which conditions equality holds in both of (57) and (58). The following lemma gives a refined version of statement (2) of theorem 7.20.

Lemma 7.29. *With notations as above, assume that $c_{n+1} = c'$. The following holds.*

1. *If P_g is bad, then $(\prod_{i=0}^{g} m_i)_{(p)} = 1$. We have $(d_{n+1})_{(p)} = d_{(p)}$ in case 1 and $d_{(p)} = (n_1)_{(p)}(d_{n+1})_{(p)}$ in case 2.*
2. *If P_g is good, then $(\prod_{i=0}^{g-1} m_i)_{(p)} = 1$.*
   In case 1, $(m_g)_{(p)} = 1$ and $(d_{n+1})_{(p)} = d_{(p)}$.
   In case 2, either $(m_g)_{(p)} = 1$ and $d_{(p)} = (n_1)_{(p)}(d_{n+1})_{(p)}$, or $(d_{n+1})_{(p)} = 1$ and $d_{(p)}(m_g)_{(p)} = (n_1)_{(p)}$.

Proof. First assume that P_g is bad.

Case 1 Equality holds in both of (57) and (58) if and only if

$$l(P_{g+1}) = \eta(x^b y^d)^{\prod_{i=0}^{g} m_i}, \tag{59}$$

with $\eta \in k$, $\eta \neq 0$. Since P_g is bad, we have

$$\mu(x^{L_g}) < \mu(x^b y^d)\prod_{i=0}^{g-1} m_i = \mu(V_0(P_g)). \tag{60}$$

If assumption (1) of lemma 7.28 holds, (60) implies that

$$m_g \mu(x^{L_g}) < \mu(V(P_{g+1})) < \mu(x^b y^d)\prod_{i=0}^{g} m_i = \mu(V_0(P_{g+1})),$$

so that inequality is strict in (58). Hence $c_{n+1} = c'$ implies that assumption (2) of lemma 7.28 holds, so that

$$\prod_{i=0}^{g} m_i = p^t$$

for some $t \geq 1$. Moreover, we have $d_{n+1} = dp^t$ by (59).

Case 2 Similarly, (59) is replaced with

$$l(P_{g+1}) = \eta x^{b\prod_{i=0}^{g} m_i}(y^{n_1} - \theta x^{q_1})^{\frac{d}{n_1}\prod_{i=0}^{g} m_i}, \tag{61}$$

and one gets that $d_{(p)} = (n_1)_{(p)}(d_{n+1})_{(p)}$ if $c_{n+1} = c'$.

Now assume that P_g is good and that $c_{n+1} = c'$. A similar argument shows that P_{g-1} satisfies assumption (2) of lemma 7.28, hence

$$\prod_{i=0}^{g-1} m_i = p^t$$

for some $t \geq 0$. In case 1, comparison of formulae (49) and (59) shows that m_g is a power of p and that

$$l(P_g) = \eta x^{bp^t}(y - \eta' x)^{dp^t},$$

with $\eta, \eta' \in k$ and $\eta, \eta' \neq 0$.

In case 2, comparison of formulae (49) and (61) shows that either m_g is a power of p and

$$l(P_g) = \eta x^{bp^t}\left((y^{n_1} - \theta x^{q_1})^{\frac{dp^t}{n_1}} + \eta' x^{\frac{dp^t q_1}{n_1}}\right),$$

with $\eta, \eta' \in k$ and $\eta, \eta' \neq 0$, or d_{n+1} is a power of p and

$$l(P_g) = \eta x^{bp^t} y^{dp^t},$$

with $dp^t < n_1$ and

$$dp^t m_g = n_1 d_{n+1}. \tag{62}$$

This proves the lemma, and therefore completes the proof of (2) of theorem 7.20. □

There remains to prove (3) of theorem 7.20. Assume that $R_{r_{n+1}} \subset S_{s_{n+1}}$ is not the localization of a finite map. By lemma 7.26, this implies that P_g is bad. If $c_{n+1} = c'$, we get

$$\prod_{i=0}^{g} m_i = p^t$$

for some $t \geq 1$ by (1) of lemma 7.29. □

Theorem 7.20 has the following immediate corollary.

Corollary 7.30. *There exist positive integers $\overline{a}, \overline{d}$ prime to p such that for all $n >> 0$, the inclusion $R_{r_n} \subset S_{s_n}$ is given by*

$$\begin{array}{rcl} u_{r_n} & = & \gamma_n x_{s_n}^{\overline{a}p^{\alpha_n}} \\ v_{r_n} & = & x_{s_n}^{b_n} f_n, \end{array} \tag{63}$$

where $\gamma_n \in S_{s_n}$ is a unit, $d_n := \overline{\nu}_{s_n}(f_n \mod x_{s_n}) = \overline{d}p^{\beta_n}$, with $b_n, \alpha_n, \beta_n \geq 0$, and $\alpha_n + \beta_n$ does not depend on n.

Remark 7.31. *It is interesting to compare both statements in proposition 7.2 and in corollary 7.30. That the complexity $c_n = a_n d_n$ is eventually constant along the algorithm is an easy consequence of proposition 7.2. But the argument in proposition 7.2 does not prove that the integers $(a_n)_{(p)}$ and $(d_n)_{(p)}$ are eventually constant.*

7.9. **Stable form of the equations.** It has been proved in corollary 7.30 that the equation (63) defining the inclusion $R_{r_n} \subset S_{s_n}$ gets a stable form. In this section, we refine corollary 7.30 and prove that the invariants of the extension of valuation rings V^*/V (see section 7.1) can be recovered from this stable form.

Recall that, given a prime number p, an abelian group Γ is said to be p-divisible if $p\Gamma = \Gamma$.

By (2) of proposition 7.16, the value group Γ of V can be computed from the m_i's through the formula

$$\Gamma = \bigcup_{g \geq 0} \frac{\mathbf{Z}}{\prod_{i=0}^{g} m_i} \nu(u).$$

The following lemma is elementary and the proof is left to the reader.

Lemma 7.32. *The following holds.*

1. *Γ is p-divisible if and only if p divides infinitely many of the m_i's.*
2. *Γ is isomorphic to $\bigcup_{g \geq 0} \frac{\mathbf{Z}}{p^g}$ if and only if $\forall i >> 0$, m_i is a power of p. Γ is then said to be "simply p-divisible".*
3. *Let Γ' be a torsion free group containing Γ and such that Γ has finite index in Γ'. Then Γ is (simply) p-divisible if and only if Γ' is (simply) p-divisible.*

Recall from section 7.1 the basic definitions of the ramification theory of V^* over V.

Theorem 7.33. *(Stable form of the equations) Let the inclusion $R_{r_n} \subset S_{s_n}$ be given for $n >> 0$ by formula (63) of corollary 7.30. The following holds.*

1. *$\overline{d} = 1$ (that is, $d_n = p^{\beta_n}$).*

(2) *Assume that Γ is not p-divisible. Then $R_{r_n} \subset S_{s_n}$ is the localization of a finite map (that is, $b_n = 0$), and (α_n, β_n, g_n) takes a constant value $(\alpha, \beta, 1)$ for $n >> 0$, so that (63) reduces to*

$$\begin{array}{lcl} u_{r_n} & = & \gamma_n x_{s_n}^{\overline{a}p^{\alpha}} \\ v_{r_n} & = & f_n \end{array},$$

where $\gamma_n \in S_{s_n}$ is a unit, $d_n = \overline{\nu}_{s_n}(f_n \bmod x_{s_n}) = p^{\beta}$, $\alpha, \beta \geq 0$ and $\overline{a} \geq 1$, p does not divide $\overline{a}$.
Moreover,

$$\Gamma^* / \ \Gamma \simeq \mathbf{Z}/\overline{a}p^{\alpha}\mathbf{Z},$$

and the defect of V^* over V is equal to p^{β}.

(3) *Assume that Γ is p-divisible. Then,*

$$\Gamma^* / \ \Gamma \simeq \mathbf{Z}/\overline{a}\mathbf{Z},$$

and the defect of V^* over V is equal to $p^{\alpha_n + \beta_n}$.
If Γ is not simply p-divisible, $R_{r_n} \subset S_{s_n}$ is the localization of a finite map (that is, $b_n = 0$) for infinitely many values of n.

Proof. Recall the definition of the integer $g_n \geq 0$ associated with the inclusion $R_{r_n} \subset R_{r_{n+1}}$ (beginning of section 7.8). By lemma 7.26, $R_{r_{n+1}} \subset S_{s_{n+1}}$ is the localization of a finite map if P_{g_n} is good. By (1) of lemma 7.29, P_{g_n} is good except possibly if

$$\mathrm{ord}_{u_{r_{n+1}}} u_{r_n} = \prod_{i=g_0+\cdots+g_{n-1}+1}^{g_0+\cdots+g_n} m_i = p^{t_n} \tag{64}$$

for some $t_n \geq 1$.

By lemma 7.32, the left hand side of (64) is not a power of p for infinitely many (resp. all large enough) values of n if Γ is not simply p-divisible (resp. not p-divisible). We then get from (2) of lemma 7.29 that $\overline{d} = 1$ if Γ is not simply p-divisible.

We now prove (2). Since Γ is not p-divisible, (2) of lemma 7.29 implies that $g_n = 1$ for $n >> 0$. Let h_n be the value of the integer h in proposition 7.19 (formulae (39) and (40)) associated with the pair (R_{r_n}, S_{s_n}). Since $c_{n+1} = c_n$, equality holds in (40), and therefore

$$(\prod_{j=0}^{h_n} n_j)_{(p)} = 1,$$

since $(d_n)_{(p)} = 1$. On the other hand, (1) and (3) of lemma 7.32 imply that p does not divide n_j for $j >> 0$. Consequently $h_n = 0$ for $n >> 0$.

Now replace (R, S) with (R_{r_n}, S_{s_n}) and renumber the r_i's of the algorithm accordingly. Equation (62) now reads

$$p^{\beta_0} m_1 = n_1 p^{\beta_1}. \tag{65}$$

Since both of m_1 and n_1 are prime to p, this proves that $m_1 = n_1$ and $\beta_0 = \beta_1$. Similarly, we get $m_i = n_i$ and $\beta_i = \beta_{i+1}$ for all $i \geq 1$.

There remains to prove the last two statements in (2). From what preceeds,

$$\Gamma = \bigcup_{g \geq 0} \frac{\mathbf{Z}}{\prod_{i=0}^{g} m_i} \nu(u) \subset \Gamma^* = \bigcup_{g \geq 0} \frac{\mathbf{Z}}{\prod_{i=0}^{g} m_i} \nu^*(x). \tag{66}$$

Since $\nu^*(u) = \overline{a}p^{\alpha}\nu^*(x)$, and all m_i's in (66) are prime to p, we have

$$\mathrm{ord}_p \mid \Gamma^*/\ \Gamma \mid = \alpha. \tag{67}$$

Assume that K^*/K is Galois. Let K^i be the inertia field of V^* over V. Let $\overline{R}_{r_n} := S_{s_n} \cap K^i$. With notations as in section 5, K^i is the inertia field of S_{s_n} over R_{r_n} for $n >> 0$. Moreover, $m_{R_{r_n}} = m_{\overline{R}_{r_n}}$. Therefore the local expression of the inclusion $\overline{R}_{r_n} \subseteq S_{s_n}$ is still given by

$$\begin{array}{rcl} u_{r_n} & = & \overline{\gamma}_n x_{s_n}^{\overline{a}p^\alpha} \\ v_{r_n} & = & \overline{f}_n \end{array}, \tag{68}$$

where $\overline{\gamma}_n \in S_{s_n}$ is a unit, $\overline{\nu}_{s_n}(\overline{f}_n \bmod x_{s_n}) = p^\beta$. By (68), $\hat{S}_{s_n}$ is a free $\hat{R}_{r_n}$-module of rank $\overline{a}p^{\alpha+\beta}$. Hence

$$[K^* : K^i] = \mathrm{rk}(\hat{S}_{s_n}/\hat{R}_{r_n}) = \overline{a}p^{\alpha+\beta}. \tag{69}$$

Equation (24) then reads

$$[K^* : K^i]_{(p)} = \mid \Gamma^*/\ \Gamma \mid_{(p)} = \overline{a}.$$

Equation (25) then reads

$$\mathrm{ord}_p[K^* : K^i] = \alpha + \delta_0 = \alpha + \beta.$$

This proves (2) in the Galois case.

One reduces to the Galois case as follows; let K'/K be a Galois closure of K^*/K. We fix an extension ν' of ν^* to K' with valuation ring V' and group Γ'. By (3) of lemma 7.32, Γ' is not p-divisible.

With obvious notations, we get as in (66) that

$$\Gamma' = \bigcup_{g \geq 0} \frac{\mathbf{Z}}{\prod_{i=0}^{g} m_i} \nu'(x'),$$

where $\nu'(x) = \overline{a}' p^{\alpha'} \nu'(x')$. Also the integer $\overline{a}(V'/V)$ associated with the extension V'/V is the product $\overline{a}\overline{a}'$ (by e.g. remark 7.10). From the Galois case, we have the following exact diagram:

$$\begin{array}{ccccccccc} 0 & \to & \frac{\Gamma^*}{\Gamma} & \longrightarrow & \frac{\Gamma'}{\Gamma} & \to & \frac{\Gamma'}{\Gamma^*} & \to & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \to & \frac{\mathbf{Z}}{\overline{a}p^\alpha \mathbf{Z}} & \xrightarrow{\times\, \overline{a}'} & \frac{\mathbf{Z}}{\overline{a}\overline{a}' p^{\alpha+\alpha'} \mathbf{Z}} & \to & \frac{\mathbf{Z}}{\overline{a}' p^{\alpha'} \mathbf{Z}} & \to & 0, \end{array}$$

where the center and right vertical arrows are isomorphisms. Therefore

$$\frac{\Gamma^*}{\Gamma} \simeq \frac{\mathbf{Z}}{\overline{a}p^\alpha \mathbf{Z}}.$$

Similarly, we have

$$\beta(V'/V) = \beta(V^*/V) + \beta(V'/V^*)$$

by applying multiplicativity of degree and ramification index in field extensions to (69). Comparing with (26), this completes the proof of (2).

We now sketch the argument for (3). By (3) of lemma 7.32, both Γ^* and Γ are p-divisible. Since the calculations of the non p-divisible case hold up to powers of p, formula (66) remains true. Therefore (67) is replaced with

$$\mathrm{ord}_p \mid \Gamma^*/\ \Gamma \mid = 0.$$

The argument for the non p-divisible case extends when Γ is not simply p-divisible by writing (68) for those values of n only such that $b_n = 0$. Equation (24) reads

$$[K^* : K^i]_{(p)} = \mid \Gamma^* / \Gamma \mid_{(p)} = \overline{a}.$$

as in the proof of (2). Equation (25) now reads

$$\mathrm{ord}_p[K^* : K^i] = \alpha_n + \beta_n = \delta_0.$$

Finally, let Γ be simply p-divisible. We have $(m_i)_{(p)} = 1$ for $i >> 0$ and $(n_j)_{(p)} = 1$ for $j >> 0$ by (2) of lemma 7.32. Obviously

$$\frac{\Gamma^*}{\Gamma} = \bigcup_{g \geq 0} \frac{\mathbf{Z}}{p^g} \Big/ \bigcup_{g \geq 0} \frac{\mathbf{Z}}{\overline{a}p^g} \simeq \frac{\mathbf{Z}}{\overline{a}\mathbf{Z}}.$$

There remains to prove that $\overline{d} = 1$. In the Galois case, proposition 7.2 applied to the pair $R_{r_n} \subset S_{s_n}$ for $n >> 0$ implies that

$$[K^* : K^i] = c_n = \overline{d}\overline{a}p^{\alpha_n + \beta_n}.$$

Equation (24) reads

$$[K^* : K^i]_{(p)} = \mid \Gamma^* / \Gamma \mid_{(p)} = \overline{a}.$$

Hence $\overline{d} = 1$. Equation (25) reads

$$\mathrm{ord}_p[K^* : K^i] = \delta_0 = \alpha_n + \beta_n.$$

One reduces to the Galois case as before. □

Remark 7.34. *We do not know if* $(\alpha_n, \beta_n, b_n, g_n)$ *also takes a constant value* $(\alpha, \beta, 0, 1)$ *for* $n >> 0$ *when* Γ *is p-divisible.*

7.10. **Ramification in defectless extensions.** In this section, We assume that V^*/V is defectless. Under this assumption, theorem 7.33 can be restated as:

Theorem 7.35. *[Strong monomialization] Let* V^*/V *be defectless. The inclusion* $R_{r_n} \subset S_{s_n}$ *is given for* $n >> 0$ *by*

$$\begin{array}{rcl} u_{r_n} & = & \gamma_n x_{s_n}^{\overline{a}p^{\alpha}} \\ v_{r_n} & = & y_{s_n} \end{array},$$

where $\gamma_n \in S_{s_n}$ *is a unit,* $\alpha \geq 0$ *and* (x_{s_n}, y_{s_n}) *is an admissible r.s.p. of* S_{s_n}*. We have* $\alpha = 0$ *if* Γ *is p-divisible. Moreover,*

$$\frac{\Gamma^*}{\Gamma} \simeq \frac{\mathbf{Z}}{\overline{a}p^{\alpha}\mathbf{Z}}.$$

Proof. Theorem 7.33 clearly implies that $\beta_n = 0$, and that $\alpha_n = 0$ for $n >> 0$ if Γ is p-divisible when V^*/V is defectless. In particular, this proves that $l(v_{r_n})$ is good, and therefore that $g_n = 0$, $b_n = 0$ for $n >> 0$ by lemma 7.26. Finally, (x_{s_n}, y_{s_n}) is an admissible r.s.p. of S_{s_n} since $\overline{\nu}_{s_{n+1}}(f_{n+1} \bmod x_{s_{n+1}}) = m_1 > 1$ in case 1. □

Remark 7.36. *The first statement in theorem 7.35 is the exact analogue of theorem 4.8 in dimension two and positive characteristic. In characteristic zero, all extensions* V^*/V *of valuation rings as considered in sections 3 to 6 are defectless by theorem 24 of* [22].
See next section for an example with nontrivial defect which does not satisfy the conclusion of theorem 7.35.

7.11. **Extensions with non trivial defect.** In this section, we give examples of valuations with nontrivial defect.

The following example is apparently due to Ostrowski ([18] (t)-adic version of example 2 p.246) and was communicated to us by F.V. Kuhlmann.

Let k_0 be a perfect field of characteristic $p > 0$, t be an indeterminate, and

$$K := \cup_{n \geq 0} k_0((t^{\frac{1}{p^n}})).$$

Then

$$V := \cup_{n \geq 0} k_0[[t^{\frac{1}{p^n}}]]$$

is the valuation ring of the k_0-valuation $\nu := \mathrm{ord}_t$ of K. The value group of ν is $\bigcup_{n \geq 0} \frac{\mathbf{Z}}{p^n}$. Let x be a root of the polynomial

$$F(X) := X^p - X - \frac{1}{t}.$$

See [18], example 2 p.246 for the ingredients of the proof of the following proposition.

Proposition 7.37. *There exists a unique extension ν^* of ν to the degree p Galois extension $K(x)/K$. Let d, e, f be respectively the defect, ramification index and residue degree of ν^* over ν. Then*

$$d = p, \; e = 1 \text{ and } f = 1.$$

The remaining part of this section is devoted to constructing an extension V^*/V with nontrivial defect in a two dimensional function field, and analyzing the corresponding algorithm of section 7.4. The main result is

Theorem 7.38. *There exists an inclusion $R \subset S$ of algebraic regular local rings of dimension two over k such that $K^*/K := QF(S)/QF(R)$ is a tower of two Galois extensions of degree p, and a k-valuation ν^* of K^* with valuation ring V^* with the following properties.*

1. *The value group Γ^* of ν^* is simply p-divisible. The extension of valuation rings $V^*/V := V^*/V^* \cap K$ has defect $d = p^2$, ramification index $e = 1$ and residue degree $f = 1$. V^* is the unique extension of V to K^*.*
2. *For all $n \geq 0$, the equation (63) of the inclusion $R_{r_n} \subset S_{s_n}$ of the algorithm is given by*

$$\begin{array}{rcl} u_{r_n} & = & \gamma_n x_{s_n}^p \\ v_{r_n} & = & f_n \end{array},$$

   where $\gamma_n \in S_{s_n}$ is a unit and $d_n = \overline{\nu}_{s_n}(f_n \bmod x_{s_n}) = p$. Hence $\alpha_n = \beta_n = 1$ with notations as in theorem 7.33.
3. *Let R_r be an iterated quadratic transform of R and S_s be an iterated quadratic transform of S such that $R_r \subset S_s$. Assume that $R_r \subset S_s$ is the localization of a finite map.*
   Then, either $(r, s) = (r_n, s_n)$ for some $n \geq 0$, or R_r has a r.s.p. (u_r, v_r) and S_s has a r.s.p. (x_s, y_s) such that there is an expression

$$\begin{array}{rcl} u_r & = & \gamma_{r,s} x_s^p \\ v_r & = & \delta_{r,s} y_s^p \end{array},$$

   where $\gamma_{r,s}, \delta_{r,s} \in S_s$ are units. In particuler, strong monomialization in the sense of theorem 4.8 does not hold for the pair $R \subset S$ w.r.t. the extension of valuation rings V^*/V.

Let $c \geq 1$, $K^* := k(x,y)$ and $K := k(u,v)$, where

$$\begin{array}{lll} u & := & x^p \ / \ (1 - x^{p-1}) \\ v & := & y^p - x^c y \end{array} \quad . \tag{70}$$

Proposition 7.39. *With notations as above, K^*/K is a finite, separable extension of degree p^2. K^*/K is a tower of two Artin-Schreier extensions of degree p if $p-1 \mid c$.*

Proof. Let $K_1 := k(x,v) = K(x)$. Then K_1/K is an Artin-Schreier extension of degree p. The minimal polynomial of $\frac{1}{x}$ is

$$F(X) := X^p - X - \frac{1}{u}.$$

The generator g of $\mathrm{Gal}(K(x)/K) = \mathbf{Z}/p\mathbf{Z}$ is determined by the relation

$$g(x) := \frac{x}{1+x}.$$

Similarly, $K^*/K_1 = K_1(y)/K_1$ is a separable extension of degree p. The minimal polynomial of y is

$$G(Y) := Y^p - x^c Y - v.$$

If $p-1 \mid c$, K^*/K_1 is also an Artin-Schreier extension. The generator g_1 of $\mathrm{Gal}(K^*/K_1) = \mathbf{Z}/p\mathbf{Z}$ is determined by the relation

$$g_1(y) := y + x^{\frac{c}{p-1}}.$$

□

Let now $R := k[u,v]_{(u,v)}$ and $S := k[x,y]_{(x,y)}$. We now define a k-valuation ν^* of K^* by using remark 7.17. Let:

$$\begin{array}{lll} Q_0 & := & x \\ Q_1 & := & y \\ Q_2 & := & y^{p^2} - x \\ Q_{j+1} & := & Q_j^{p^2} - x^{p^{2j-2}} Q_{j-1} \quad \text{for } j \geq 2. \end{array} \tag{71}$$

Proposition 7.40. *The sequence $(Q_j)_{j \geq 0}$ is the generating sequence of a unique k-valuation ν^* of K^*. Explicitly, the valuation ring V^* of ν^* is*

$$V^* := \bigcup_{j \geq 1} S_{s'_j},$$

where each $S_{s'_j}$ is an algebraic regular local ring of dimension two with r.s.p. $(x_{s'_j}, y_{s'_j})$. The $S_{s'_j}$'s are defined inductively by $S_{s'_1} := S$, and

$$S_{s'_{j+1}} := S_{s'_j}[y_{s'_{j+1}}]_{(x_{s'_{j+1}}, y_{s'_{j+1}})}$$

for $j \geq 1$. The $(x_{s'_j}, y_{s'_j})$'s are defined inductively by $x_{s'_2} := y, y_{s'_2} := \frac{Q_2}{x}$, and

$$y_{s'_{j+1}} := \frac{Q_{j+1}}{x^{p^{2j-2}} Q_{j-1}}, \ x_{s'_{j+1}} := y_{s'_j}$$

for $j \geq 2$.
The value group $\Gamma^* =$ of ν^* is isomorphic to $\bigcup_{n \geq 0} \frac{\mathbf{Z}}{p^n}$.

Proof. With the notation of remark 7.17, we get $n_j = p^2$ for all $j \geq 1$ from (71). Let $\overline{\beta}_0 := 1$, $\overline{\beta}_1 := \frac{1}{p^2}$, and

$$\overline{\beta}_j := \frac{1}{p^2}(p^{2j-2} + \overline{\beta}_{j-1})$$

for $j \geq 2$. By induction on j, we have

$$\overline{\beta}_{j+1} = p^{2j-2} \sum_{j'=0}^{j} \frac{1}{p^{4j'}} \tag{72}$$

for $j \geq 0$.

To prove that $(Q_j)_{j \geq 0}$ is the generating sequence of a unique k-valuation ν^*, it must be checked that

$$p^{2j-2} + \overline{\beta}_{j-1} \text{ has order precisely } p^2 \text{ in } \frac{\Gamma_{j-1}}{p^2 \Gamma_{j-1}}$$

for $j \geq 2$, where $\Gamma_j :=< \{\overline{\beta}_{j'}\}_{0 \leq j' \leq j} >$, and that

$$\overline{\beta}_{j+1} > p^2 \overline{\beta}_j$$

for $j \geq 1$ (see remark 7.17). By (72), we have

$$\Gamma_{j-1} = \frac{\mathbf{Z}}{p^{2j-2}}$$

for $j \geq 2$, so that by (72), $p^{2j-2} + \overline{\beta}_{j-1}$ has order precisely p^2 in $\Gamma_{j-1}/p^2\Gamma_{j-1}$ as asserted. Moreover,

$$\overline{\beta}_{j+1} - p^2 \overline{\beta}_j = \frac{1}{p^{2j+2}} > 0 \tag{73}$$

for $j \geq 1$. This proves the first statement in the proposition.

By (2) of proposition 7.16,

$$\Gamma^* = \bigcup_{j \geq 0} \frac{\mathbf{Z}}{p^{2j}} \nu^*(x) \simeq \bigcup_{n \geq 0} \frac{\mathbf{Z}}{p^n}.$$

Finally, one computes explicitly the quadratic sequence $S_{s'_j} \subset S_{s'_{j+1}}$ from the minimal resolution of $\mathrm{div}(Q_{j+1})$ in the following way.

Let $X_j \to \mathrm{Spec} S$ be the *minimal embedded* resolution of $\mathrm{div}(Q_j)$ (of $\mathrm{div}(xQ_2)$ if $j = 2$). Let $\eta_j \in X_j$ be the unique point on the strict transform of $\mathrm{div}(Q_j)$. By definition, $S_{s'_j} := \mathcal{O}_{X_j, \eta_j}$. Clearly,

$$S_{s'_2} = S \left[\frac{Q_2}{x} \right]_{(y, \frac{Q_2}{x})}.$$

Let now $j \geq 2$ and let $(\overline{x}_j, \overline{y}_j)$ be an admissible r.s.p. of $S_{s'_j}$. Any equation of the strict transform of $\mathrm{div}(Q_{j+1})$ in $\mathrm{Spec} S_{s'_{j+1}}$ is a possible choice for $\overline{y}_{j+1}$, so that we may choose

$$\overline{y}_{j+1} := \frac{Q_{j+1}}{x^{p^{2j-2}} Q_{j-1}}.$$

By (71), there is a relation

$$Q_{j+1} = \gamma \overline{x}_j^{p^2 \mathrm{ord}_{\overline{x}_j}(Q_j)} \overline{y}_j^{p^2} + \gamma' \overline{x}_j^{p^{2j-2} \mathrm{ord}_{\overline{x}_j}(x) + \mathrm{ord}_{\overline{x}_j}(Q_{j-1})}, \tag{74}$$

where $\gamma, \gamma' \in S_{s'_j}$ are units.

By (1) of proposition 7.12, we have $\mathrm{ord}_{\overline{x}_j}(x) = p^{2j-2}$. By proposition 7.15,

$$\mathrm{ord}_{\overline{x}_j}(Q_2) = \mathrm{ord}_{\overline{x}_2}(x),\ \mathrm{ord}_{\overline{x}_j}(Q_{j-1}) = \overline{\beta}_{j-1}\mathrm{ord}_{\overline{x}_j}(x),$$

and, for $j \geq 3$,

$$\mathrm{ord}_{\overline{x}_j}(Q_j) = \mathrm{ord}_{\overline{x}_j}(x^{p^{2j-4}}Q_{j-2}) = p^{2j-4}\mathrm{ord}_{\overline{x}_j}(x) + \overline{\beta}_{j-2}\mathrm{ord}_{\overline{x}_j}(x).$$

By (73), $p^{2j-2}(\overline{\beta}_{j-1} - p^2\overline{\beta}_{j-2}) = 1$ for $j \geq 3$. Hence, (74) can be rewritten for $j \geq 2$ as

$$Q_{j+1} = \gamma \overline{x}_j^{p^2\mathrm{ord}_{\overline{x}_j}(Q_j)}(\overline{y}_j^{p^2} + \delta\overline{x}_j), \tag{75}$$

where $\gamma, \delta \in S_{s'_j}$ are units. Thus

$$S_{s'_{j+1}} = S_{s'_j}[\overline{y}_{j+1}]_{(\overline{y}_j, \overline{y}_{j+1})}.$$

A particular choice of $\overline{x}_{j+1}$ is therefore obtained by letting $\overline{x}_{j+1} := \overline{y}_j$. This concludes the proof.

□

We now compute the valuation ring $V^* \cap K$. Let

$$\begin{array}{lcll} P_0 & := & u & \\ P_1 & := & v & \\ P_2 & := & v^{p^2} - u & \\ P_{i+1} & := & P_i^{p^2} - u^{p^{2i-2}}P_{i-1} & \text{for } i \geq 2. \end{array} \tag{76}$$

Since the equations defining the P_i's in terms of u, v are *the same as* those defining the Q_j's in terms of x, y, we have

Corollary 7.41. *The sequence $(P_i)_{i\geq 0}$ is the generating sequence of a unique k-valuation ν of K. The valuation ring V of ν is*

$$V := \bigcup_{i\geq 1} R_{r'_i},$$

where the $R_{r'_i}$ are defined in terms of u, v by the same equations as in proposition 7.40.
The value group Γ of ν is isomorphic to $\bigcup_{n\geq 0}\frac{\mathbf{Z}}{p^n}$.

We now prove that $V^* \cap K = V$.

Lemma 7.42. *Let $j \geq 1$. There exists a relation*

$$P_{j+1} = Q_{j+1}^p + x^{p^{2j-1}\sum_{j'=0}^{k}\frac{1}{p^{4j'}}} f_{j+1}(x, y), \tag{77}$$

where $k := \frac{j-1}{2}$ (resp. $k := \frac{j}{2} - 1$) if j is odd (resp. if j is even), $f_{j+1}(x, y) \in k[[x]][y]$ with

$$\deg_y f_{j+1} < p^{2j+1} = \deg_y Q_{j+1}^p \text{ and } x \mid f_{j+1}.$$

Proof. Induction on j. By (70), (71) and (76),We have

$$P_2 = (y^p - x^c y)^{p^2} - \frac{x^p}{1 - x^{p-1}} = Q_2^p - x^{cp^2}y^{p^2} - \frac{x^{2p-1}}{1 - x^{p-1}}.$$

Since $\min\{cp^2, 2p - 1\} \geq p + 1$, (77) holds for $j = 1$.

Let now $j \geq 2$. Similarly,

$$P_{j+1} = Q_j^{p^3} + x^{p^{2j-1}\sum_{j'=0}^{k'}\frac{1}{p^{4j'}}} f_j(x,y)^{p^2} - \left(\frac{x^p}{1-x^{p-1}}\right)^{p^{2j-2}} (Q_{j-1}^p + g_{j-1}(x,y)),$$

where k' is the integer k associated with $j-1$, $g_1(x,y) := -x^c y$, and

$$g_{j-1}(x,y) := x^{p^{2j-5}\sum_{j'=0}^{k-1}\frac{1}{p^{4j'}}} f_{j-1}(x,y)$$

for $j \geq 3$. We have $4k = 2j-2$, $4k' = 2j-6$ if j is odd, and $4k = 4k' = 2j-4$ if j is even. In both cases, we get

$$P_{j+1} = \left(Q_j^{p^2} - x^{p^{2j-2}} Q_{j-1}\right)^p + x^{p^{2j-1}\sum_{j'=0}^{k}\frac{1}{p^{4j'}}} f_{j+1}(x,y)$$

as required, using the inequalities

$$p^{2j-1} + (p-1)p^{2j-2} > p^{2j-1}(1 + \frac{2}{p^4}) + 1 > p^{2j-1}\sum_{j'=0}^{k}\frac{1}{p^{4j'}} + 1,$$

and

$$\mathrm{ord}_x(f_j(x,y)^{p^2}) \geq p^2 \geq p^{2j-1-(2j-2)} + 1 = p+1.$$

□

Proposition 7.43. *We have $V = V^* \cap K$.*

Proof. With the notation of corollary 7.41, it is sufficient to prove that $R_{r'_i} \subset V^*$ for all $i \geq 1$. Clearly, $R \subset S \subset V^*$. Let $i \geq 1$. We have

$$R_{r'_{i+1}} := R_{r'_i}[v_{r'_{i+1}}]_{(u_{r'_{i+1}}, v_{r'_{i+1}})},$$

where the $(u_{r'_i}, v_{r'_i})$'s are defined inductively by $u_{r'_2} := v, v_{r'_2} := \frac{P_2}{u}$, and

$$v_{r'_{i+1}} := \frac{P_{i+1}}{u^{p^{2i-2}}P_{i-1}},\ u_{r'_{i+1}} := v_{r'_i}$$

for $i \geq 2$. There remains to prove that $\nu^*(v_{r'_i}) > 0$ for all $i \geq 2$. By (72), we have

$$\nu^*(Q_{j+1}^p) = p\overline{\beta}_{j+1} < 1 + p^{2j-1}\sum_{j'=0}^{k}\frac{1}{p^{4j'}}$$

for $j \geq 1$, where k is defined as in lemma 7.42. Therefore

$$\nu^*(Q_{j+1}^p) = p\overline{\beta}_{j+1}\nu^*(x) < \nu^*\left(x^{p^{2j-1}\sum_{j'=0}^{k}\frac{1}{p^{4j'}}} f_{j+1}(x,y)\right) \tag{78}$$

in (77). Consequently,

$$\nu^*(P_{j+1}) = \nu^*(Q_{j+1}^p), \tag{79}$$

for $j \geq 1$. We get

$$\nu^*(v_{r'_2}) = \nu^*\left(\frac{P_2}{u}\right) = p\nu^*\left(\frac{Q_2}{x}\right) = p\nu^*(y_{s'_2}) > 0,$$

and

$$\nu^*(v_{r'_{i+1}}) = \nu^*\left(\frac{P_{i+1}}{u^{p^{2i-2}}P_{i-1}}\right) = p\nu^*\left(\frac{Q_{i+1}}{x^{p^{2i-2}}Q_{i-1}}\right) = p\nu^*(y_{s'_{i+1}}) > 0.$$

□

Proof of theorem 7.38. Choose c to be a multiple of $p-1$ so that K^*/K is a tower of two Galois extensions of degree p by proposition 7.39.

We first prove (2). We have

$$\frac{\partial u}{\partial x}\frac{\partial v}{\partial y}-\frac{\partial u}{\partial y}\frac{\partial v}{\partial x}=\frac{x^{c+2p-2}}{(1-x^{p-1})^2},$$

so that $\mathrm{Spec}S \to \mathrm{Spec}R$ is ramified precisely above $\mathrm{div}(u)$. Therefore, if $R \subset R_r$ and $S \subset S_s$ are any quadratic sequences along ν^* such that $R_r \subset S_s$, the pair (R_r, S_s) is prepared if and only if both R_r and S_s are free by proposition 7.6.

The strict transform of $\mathrm{div}(Q_{j+1})$ in $\mathrm{Spec}S_{s'_j}$ is tangent to $\mathrm{div}(\overline{x}_j)$ by (71) if $j=1$ or by (75) if $j \geq 1$. Therefore, $S_{s'_j+1}$ is *not* free. This implies that $\{S_{s'_j}\}$ is the list of all free iterated quadratic transforms of S along V^*. Similarly, $\{R_{r'_i}\}$ is the list of all free iterated quadratic transforms of R along V. In particular, the notation r'_i is compatible with that of definition 7.11, and similarly for the analogous integers s'_j associated with S. With notations as in definition 7.11, we also have $\overline{r}_{i+1}=r'_{i+1}$ for all $i \geq 1$ (and similarly $\overline{s}_{j+1}=s'_{j+1}$ with obvious notations).

Let $(x_{s'_{j+1}}, y_{s'_{j+1}})$ be as in proposition 7.40. We have

$$\mathrm{ord}_{x_{s'_{j+1}}}(Q_{j+1}^p)=p^3\mathrm{ord}_{x_{s'_{j+1}}}(Q_j)<p\overline{\beta}_{j+1}\mathrm{ord}_{x_{s'_{j+1}}}(x).$$

Comparing with (78), we get

$$\mathrm{ord}_{x_{s'_{j+1}}}(Q_{j+1}^p)<\mathrm{ord}_{x_{s'_{j+1}}}\left(x^{p^{2j-1}\sum_{j'=0}^{k}\frac{1}{p^{4j'}}}f_{j+1}(x,y)\right), \tag{80}$$

and therefore

$$\mathrm{ord}_{x_{s'_{j+1}}}(P_{j+1})=\mathrm{ord}_{x_{s'_{j+1}}}(Q_{j+1}^p)$$

and

$$\mathrm{ord}_{x_{s'_{j+1}}}(P_{j'})=\mathrm{ord}_{x_{s'_{j+1}}}(Q_{j'}^p)$$

for $0 \leq j' \leq j$ by (77). Hence

$$\begin{array}{rcl} u_{r'_j} & = & \gamma_j x_{s'_j}^p \\ v_{r'_j} & = & \gamma'_j(y_{s'_j}^p + x_{s'_j}f_j(x_{s'_j}, y_{s'_j})) \end{array}, \tag{81}$$

for all $j \geq 1$, where $\gamma_j, \gamma'_j \in S_{s'_j}$ are units, and $f_j(x_{s'_j}, y_{s'_j}) \in S_{s'_j}$. This proves that $r_j = r'_{j+1}$, $s_j = s'_{j+1}$ for all $j \geq 1$ and therefore completes the proof of (2).

We now prove (1). That Γ^* is simply p-divisible has been proved in proposition 7.40. We have $f=1$, since $k=V/m_V$ is algebraically closed. We have $e \mid [K^*:K]=p^2$. But Γ^* is simply p-divisible, so that p does not divide e. Therefore $e=1$. By (2) of theorem 7.38, $\alpha=\beta=1$. Thus (3) of theorem 7.33 implies that $d=p^2$. Then

$$def=[K^*:K]=p^2,$$

so V^* is the unique extension of V to K^*.

Finally, let $R_r \subset S_s$ as in (3). Let $j \geq 0$ be the unique integer such that $r_j \leq r < r_{j+1}$. Then

$$R_{r_j} \subset S_{s_j} \subseteq S_s \tag{82}$$

since S_{s_j} lies above R_{r_j}.

First assume that $r = r_j$. Then $s = s_j$ since $R_r \subset S_s$ is the localization of a finite map.

Assume now that $r_j < r < r_{j+1}$. Similarly, (82) implies that $s > s_j$. By definition of s_{j+1}, we have $R_{r+1} \subset S_{s_{j+1}}$, and this proves that $s < s_{j+1}$, since $R_r \subset S_s$ is the localization of a finite map. Then S_s has a r.s.p. (x_s, y_s) given by

$$\begin{array}{rcl} x_{s_j} & =: & x_s y_s^{s-s_j} \\ y_{s_j} & =: & y_s \end{array},$$

and R_r has a r.s.p. given by

$$\begin{array}{rcl} u_{r_j} & =: & u_r v_r^{r-r_j} \\ v_{r_j} & =: & v_r \end{array}.$$

Since $p-1 \mid c$, we have $\mathrm{ord}_{(x,y)}(x^c y) \geq p$. Similarly, refining inequality (80), one gets for $j \geq 1$ that

$$\mathrm{ord}_{x_{s'_{j+1}}} \left(x^{p^{2j-1} \sum_{j'=0}^{k} \frac{1}{p^{4j'}}} f_{j+1}(x,y) \right) - \mathrm{ord}_{x_{s'_{j+1}}} (Q_{j+1}^p) \geq p.$$

Consequently, since $R_r \subset S_s$ is the localization of a finite map, we have $s - s_j = r - r_j$ and

$$\begin{array}{rcl} u_r & = & \gamma_{r,s} x_s^p \\ v_r & = & \delta_{r,s} y_s^p \end{array},$$

where $\gamma_{r,s}, \delta_{r,s} \in S_s$ are units, as required.

Remark 7.44. *Theorem 7.38 has an interesting formulation in the language of* [20]. *Let ν_j^* (resp. ν_j) be the $m_{S_{s_j}}$-adic order (resp. $m_{R_{r_j}}$-adic order) on K^* (resp. K) for $j \geq 1$. Then ν_j^* and ν_j are valuations and ν_j^* is an extension of ν_j to K^*.*

Thus for all $g \geq 1$, there is an inclusion of graded algebras associated with the corresponding filtrations

$$\mathrm{gr}_{\nu_g}(R) \subset \mathrm{gr}_{\nu_g^*}(S). \tag{83}$$

These algebras are toric. Explicitly ([19] *theorem 8.6 and remark 6.2), there is a presentation*

$$\mathrm{gr}_{\nu_g}(R) \simeq \frac{k[U_0, U_1, \ldots, U_g]}{(U_1^{p^2} - U_0, \{U_j^{p^2} - U_0^{p^{2j-2}} U_{j-1}\}_{2 \leq j \leq g})},$$

where $U_j := \mathrm{in}_{\nu_j}(P_j)$. Similarly,

$$\mathrm{gr}_{\nu_g^*}(S) \simeq \frac{k[X_0, X_1, \ldots, X_g]}{(X_1^{p^2} - X_0, \{X_j^{p^2} - X_0^{p^{2j-2}} X_{j-1}\}_{2 \leq j \leq g})},$$

where $X_j := \mathrm{in}_{\nu_j^*}(Q_j)$. It follows from (70) and (79) that (83) is obtained from the p^{th}-power map $U_j \mapsto X_j^p$. Notice that the defect $d = p^2$ of V^*/V also appears in (83) through the fact that the inclusion

$$QF(\mathrm{gr}_{\nu_g}(R)) \subset QF(\mathrm{gr}_{\nu_g^*}(S))$$

is purely inseparable of degree p^2.

References

[1] Abhyankar, S., Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$, Annals of Math, 63 (1956), 491-526.
[2] Abhyankar, S., On the valuations centered in a domain, Amer. J. Math. 78 (1956), 321-348.
[3] Abhyankar, S., Simultaneous resolution for algebraic surfaces, Amer. J. Math 78 (1956), 761-790.
[4] Abhyankar, S., Ramification theoretic methods in algebraic geometry, Annals of Math. Studies 43, Princeton University Press, 1959.
[5] Abhyankar, S., Resolution of singularities of embedded algebraic surfaces, second edition, Springer, 1998.
[6] Abhyankar, S., Resolution of singularities and modular Galois theory, Bulletin of the AMS, 38, 131-171.
[7] Abhyankar, S., Tame Coverings and fundamental groups of algebraic varieties, Amer. J. Math. 81. 1959, 46-94.
[8] Campillo, A., Algebroid curves in positive characteristic, LNM 813, Springer Verlag.
[9] Cossart, V. and Moreno-Socias, G., Racines approchees, suites génératrices, suffisance des jets, to appear in Fields. Inst. Comm 32 (2002).
[10] Cutkosky, S.D., Local Factorization and Monomialization of Morphisms, Asterisque, 1999.
[11] Cutkosky, S.D., Simultaneous resolution of singularities, Proc. American Math. Soc. 128, (2000), 1905-1910.
[12] Cutkosky, S.D. Generically finite morphisms and simultaneous resolution of singularities, to appear in Contemporary Math., AG/0109003.
[13] Cutkosky, S.D. and Piltant, O., Monomial resolutions of morphisms of algebraic surfaces, Communications in Algebra 28(12), (2000), 5935-5959.
[14] Hironaka, H., Resolution of singularities of an algebraic variety over a field of characteristic zero, Annals of Math, 79 (1964), 109-326.
[15] Knaf, H. and Kuhlmann, F.V., Abhyankar places admit local uniformization in any characteristic, preprint Valuation Theory homepage http://math.usask.ca (2001).
[16] Krull, W., Galoissche Theorie bewerteter Körper, Sitzungsberichte der Bayerischen Akademie der Wissenschaften, München (1930), 225-238.
[17] Lipman, J., Rational singularities, with applications to algebraic surfaces and unique factorization, Publ. Math. IHES 36 (1969), 195-279.
[18] Ribenboim, P., Théorie des valuations, 9 (1964), Presse Univ. Montréal.
[19] Spivakovsky, M., Valuations in function fields of surfaces, Amer. J. Math., 112, 1990, 107-156.
[20] Teissier, B., Valuations, Deformations and Toric Geometry, preprint.
[21] Zariski, O., Local uniformization of algebraic varieties, Annals of Math., 41, (1940), 852-896.
[22] Zariski, O. and Samuel, P., Commutative Algebra II, Van Nostrand, Princeton (1960).

Steven Dale Cutkosky, Department of Mathematics, University of Missouri
Columbia, MO 65211, USA
dale@cutkosky.math.missouri.edu

Olivier Piltant, LAMA-UMR 8100 du CNRS, Université de Versailles
45, avenue des Etats-Unis, Bâtiment Fermat
78035 Versailles, FRANCE
piltant@math.uvsq.fr