EXISTENCE OF DICRITICAL DIVISORS

BY SHREERAM S. ABHYANKAR AND WILLIAM J. HEINZER.

Abstract. We prove an existence theorem for dicritical divisors.
Key Words: Dicritical, DVR.

Section 1: Introduction. The analytical (topological) concept of dicritical divisors was developed by several authors such as Artal [Art], Eisenbud-Neumann [EiN], Fourrier [Fou], Le-Weber [LeW], and Mattei-Moussu [MaM]. It was then algebracized by Abhyankar in the paper [Ab5] entitled "Inversion and Invariance of Characteristic Terms Part I." We shall use the notation and terminology of [Ab5]. Especially Sections 1 and 5 of [Ab5], together with the preamble and Note (II**) of Section 4 of [Ab5], will be used mostly without explicit mention.

To introduce some more terminology, let R be a two dimensional regular local domain with quotient field L. For any z in L, the set of all dicritical divisors of z in R will be denoted by $\mathfrak{D}(R,z)$. Note that $D(R)^\Delta$ is the set of all prime divisors of R, and $\mathfrak{D}(R,z)$ is the finite set consisting of those V in $D(R)^\Delta$ relative to which z is residually transcendental over R; see Note (5.6) of Section 5 of [Ab5]. Conversely, for any finite subset U of $D(R)^\Delta$, by $\mathfrak{D}^*(R,U)$ we denote the set of all $z \in L$ such that $\mathfrak{D}(R,z) = U$.

To enhance the study of dicritical divisors started in [Ab5] we prove the following ET= Existence Theorem and ask the following EQ = Existence Question:

ET. Given any finite subset U of the set $D(R)^\Delta$ of all prime divisors of a two dimensional regular local domain R with quotient field L, there exists $z \in L^\times$ such that U coincides with the set of all dicritical divisors of z in R. Moreover, if the residue field $R/M(R)$ is infinite then z can be chosen so that for every V in U we have $z \in V$ with $H(V) = K'(H_V(z))$ where $H_V : V \to H(V) = V/M(V)$ is the residue class epimorphism and K' is the relative algebraic closure of $K = H_V(R)$ in $H(V)$.

EQ. Can you describe the set $\mathfrak{D}^*(R,U)$?

Our main tools will be Appendix 5 of volume II of Zariski's algebra book [Zar] and the Northcott-Rees paper [NoR]. We shall also refer to the 1956 paper [Ab1] which is a precursor of the present paper. The paper [Ab1] was expanded into the monograph [Ab2]. We shall use the language of models introduced in [Ab2] and expanded in the books [Ab3] and [Ab4]. In general we shall follow the notation and terminology of [Ab4] and we shall use results from it tacitly.

Section 2: Notation and ZQT. We introduce some more terminology.

If i is any nonnegative integer then the set of all i-dimensional members of $\mathfrak{V}(S)$, $\mathfrak{V}(S,J)$, $\mathfrak{W}(S,J)$, $\mathfrak{W}(S,J)^\Delta$, $\mathfrak{W}(k;x_1,\dots,x_p)$ is denoted by $\mathfrak{V}(S)_i$, $\mathfrak{V}(S,J)_i$, $\mathfrak{W}(S,J)_i$, $\mathfrak{W}(S,J)_i^\Delta$, $\mathfrak{W}(k;x_1,\dots,x_p)_i$ respectively, and the set of all height i members of spec(S) is denoted by spec$(S)_i$, where these objects are as defined in the preamble of Section 4 of [Ab5] and item (5.4) of Section 5 of [Ab5].

Let A be a domain with quotient field L. For any $V \in \overline{D}(L/A)$, by a V-ideal in A we mean an ideal J in A such that $J = I \cap A$ for some ideal I in V. Let $\overline{A}$ be the integral closure of A in L. By a **complete** ideal in A we mean an ideal J in A such that $J = \cap_{V \in \overline{D}(L/\overline{A})}(I(V) \cap \overline{A})$ where, for each $V \in \overline{D}(L/\overline{A})$, $I(V)$ is some ideal in V. By $\overline{C}(A)$ we **denote** the set of all nonzero complete ideals in A. Ideal J in A is **simple** means (1) $J \neq A$ and (2) J_1, J_2 ideals in A with $J = J_1J_2 \Rightarrow J_1 = A$ or $J_2 = A$. If A is quasilocal then we define $A^{\mathfrak{N}}$ to be the set of all members of $\mathfrak{V}(\overline{A})$ which dominate A and we call $A^{\mathfrak{N}}$ the **local normalization** of A. Likewise, for any set U of quasilocal domains we put $U^{\mathfrak{N}} = \cup_{B\in U} B^{\mathfrak{N}}$.

For any positive dimensional regular local domain S with quotient field L, let $o(S)$ denote the DVR with quotient field L such that $\text{ord}_{o(S)}x = \text{ord}_S x$ for all $x \in L$. In other words, $o(S)$ is the unique one dimensional first QDT of S. We call $o(S)$ the **natural** DVR of S.

Let R be a two dimensional regular local domain with quotient field L. Let $C(R)$ **denote** the set of all $M(R)$-primary simple complete ideals in R. Let $Q(R)$ **denote** the set of all two dimensional regular local domains whose quotient field is L and which dominate R. By Section 2 of [Ab1] we see that $S \mapsto o(S)$ gives a **bijection** $o_R : Q(R) \to D(R)^{\Delta}$. By Section 2 of [Ab1] we also see that, given any V in $D(R)^{\Delta}$, there exists a unique sequence $(R_j)_{0\le j\le\nu}$ with $\nu \in \mathbb{N}$ and $R_0 = R$ such that R_{j+1} is a two dimensional first QDT of R_j for $0 \le j < \nu$ and $o(R_\nu) = V$; we call this sequence the finite QDT **sequence** of R along V. Note the disjoint partition $Q(R) = \coprod_{j\in\mathbb{N}} Q_j(R)$ **where** $Q_j(R)$ is the set of all those members of $Q(R)$ which are j-th QDTs of R. Note that $o_R(R_\nu) = V$ and $o_R^{-1}(V) = R_\nu$.

Given any $S \in Q(R)$ and any nonzero ideal I in R we define the (R, S)-transform of I to be the unique ideal J in S which we shall **denote** by $(R, S)(I)$ and which is characterized by requiring that

$$IS = J \prod_{M(R)\subset M(W)} (S \cap M(W))^{\mathrm{ord}_W(IS)}$$

where the product is taken over the set $\overline{W}$ of all one dimensional members W of $\mathfrak{V}(S)$ with $M(R) \subset M(W)$. Note that $S = R \Leftrightarrow \overline{W} = \emptyset$. Moreover, if $S \ne R$ then either $\overline{W} = \{S_{xS}\}$ with $x \in M(S)\backslash M(S)^2$ or $\overline{W} = \{S_{xS}, S_{yS}\}$ with $(x, y)S = M(S)$.

The following ZQT = Zariski Quadratic Theorem is the main message of the Appendix 5 of volume II of Zariski's book [Zar].

ZQT. (I) Given any $V \in D(R)^{\Delta}$ there is at least one and at most a finite number of V-ideals in R which are members of $C(R)$. Labelling these members of $C(R)$ as

$$M(R) = J_0 \supsetneqq J_1 \supsetneqq \cdots \supsetneqq J_\nu$$

we get a bijection $\zeta_R : D(R)^{\Delta} \to C(R)$ by taking $\zeta_R(V) = J_\nu$. We call ζ_R the **Zariski map** of R. Also we call $(J_i)_{0\le i\le\nu}$ the **simple** V**-ideal sequence** of R.

(II) To describe the inverse map ζ_R^{-1} more explicitly we proceed thus. Given any $I \in C(R)$ let $(R_0, I_0) = (R, I)$. It can be shown that if $I_0 \ne M(R_0)$ then there is a unique $R_1 \in Q_1(R_0)$ such that upon letting $I_1 = (R_0, R_1)(I_0)$ we have $I_1 \ne R_1$. It can also be shown that $I_1 \in C(R_1)$. If $I_1 \ne M(R_1)$ then let (R_2, I_2) be the pair such that $R_2 \in Q_1(R_1)$ and $I_2 = (R_1, R_2)(I_1) \ne R_2$. And so on. It can be shown that this process is finite. Thus we get a unique sequence $(R_j, I_j)_{0\le j\le\nu}$ with $\nu\in\mathbb{N}$ such that $R_{j+1}\in Q_1(R_j)$ with $I_j\in C(R_j)\setminus\{M(R_j)\}$ and $I_{j+1}=(R_j,R_{j+1})(I_j)$ for $0\le j<\nu$, and $I_\nu=M(R_\nu)$. We call this sequence the **transform sequence** of (R,I). Let $V=o(R_\nu)$. Now clearly $(R_j)_{0\le j\le\nu}$ is the finite QDT sequence of R along V. It can be shown that the map $\eta_R: C(R)\to D(R)^\Delta$ given by $I\mapsto V$ is a bijection. Indeed $\eta_R=\zeta_R^{-1}$. Moreover, if the V here is the same as the V above then the two values of ν coincide and we have $J_i=R\cap I_{\nu-i}$ for $0\le i\le\nu$. We call η_R the **inverse Zariski map** of R. Note that $\zeta_R o_R: Q(R)\to C(R)$ is a bijection and its inverse is the bijection $o_R^{-1}\eta_R: C(R)\to Q(R)$. Moreover $(o_R^{-1}\eta_R)(I)=R_\nu$.

(III) The product of any finite number of members of $\overline{C}(R)$ is again a member of $\overline{C}(R)$. Every $I\in\overline{C}(R)$ has a unique factorization

$$I=\widehat{I}\prod_{J\in C(R)}J^{u(I,J)}\qquad\text{with nonzero principal ideal } \widehat{I} \text{ in } R$$

where $u(I,J)\in\mathbb{N}$ with $u(I,J)=0$ for all except finitely many J.

(IV) In the situation of (III), upon letting

$$\overline{\eta}_R(I)=\{\eta_R(J): J\in C(R) \text{ with } u(I,J)>0\}$$

we have that $\overline{\eta}_R(I)$ is a finite subset of $D(R)^\Delta$ and

$$\mathfrak{W}(R,I)_1^\Delta=\overline{\eta}_R(I).$$

Conversely, for any finite subset U of $D(R)^\Delta$, upon letting

$$\overline{\zeta}_R(U)=\prod_{V\in U}\zeta_R(V)$$

we have $\overline{\zeta}_R(U)\in\overline{C}(R)$ and

$$\mathfrak{W}(R,\overline{\zeta}_R(U))_1^\Delta=U.$$

Section 3: Sketch Proof of ET. In (3.1) we shall outline a sketch proof of ET. A complete proof of ET will be given in Section 9. In (3.2) we shall expand on ZQT. Let R be a two dimensional regular local domain with quotient field L and maximal ideal $M=M(R)$. Let U be a finite subset of prime divisors of R.

SKETCH PROOF OF ET (3.1). Let $I = \overline{\zeta}_R(U)$. Since R is noetherian, I has a finite set of generators $x_1, \ldots, x_p$. Take two generic linear combinations

$$x = a_1x_1 + \cdots + a_px_p \quad \text{and} \quad y = b_1x_1 + \cdots + b_px_p$$

where $a_1, \ldots, a_p, b_1, \ldots, b_p$ are elements of R whose images in $R/M(R)$ avoid the zeroset of a certain nonzero polynomial $P(A_1, \ldots, A_p, B_1, \ldots, B_p)$ with coefficients in $R/M(R)$. Then $z = x/y$ is a desired member of $L^\times$. In the more general case, generic linear combinations can be replaced by a two-generated reduction of I as in Northcott-Rees [NoR].

Another helpful idea is to make induction on the **depth** $d(R,U)$ of R in U which is defined to be the maximum of $d(R,V)$ with V varying over U, where the **depth** $d(R,V)$ of R in V is defined to be $\nu+1$ where $(R_j)_{0\le j\le \nu}$ is the QDT sequence of R along V; convention: $d(R,U) = 0 \Leftrightarrow U = \emptyset$. By (5.6)(†*) of Section 5 of [Ab5] we have

$$d(R,U) = 0 \Leftrightarrow \mathfrak{D}^*(R,U) = \{z \in L^\times : \text{either } z \in R \text{ or } 1/z \in R\}.$$

So let $d(R,U) > 0$ and assume for all smaller values of $d(R,U)$. And so on.

COMPLEMENT TO ZQT (3.2). Appendix 5 of volume II of Zariski's book [Zar] is not easy to read. So here is some help especially for deciphering ZQT(IV). Let us observe that ZQT(I) and ZQT(II) are proved in Subsection 5 on pages 388-393 of Appendix 5. Likewise ZQT(III) is proved in Theorems $2'$ and 3 on pages 385-386 of Appendix 5. Theorem $2'$ says that the set $\overline{C}(R)$ of all nonzero complete ideals in R is closed under multiplication. Theorem 3 proves that an M-primary complete ideal I has a unique factorization into members J of $C(R)$ = the set of all M-primary simple complete ideals in R.

Before turning to ZQT(IV), a word about QDTs. Let k be the residue field R/M, let κ be a coefficient set of R, let (t_1,t_2) be generators of M, and let (z_1,z_2) be their respective leading forms. For the graded ring of R we have $\mathrm{grad}(R,M)$ = the bivariate polynomial ring $k[z_1,z_2]$. The **leading form** $l(t)$ of any $t \in M^n \setminus M^{n+1}$ with $n \in \mathbb{N}$ is the image of t under the canonical epimorphism $M^n \to M^n/M^{n+1}$ followed by the canonical monomorphism $M^n/M^{n+1} \to k[z_1,z_2]$; if $t = 0$ then

$l(t) = 0$. Let $\overline{W}$ be the set consisting of z_1 together with all homogeneous irreducible members of $k[z_1, z_2]$ of the form

$$\overline{g} = \overline{g}(z_1, z_2) = z_2^{\omega} + \sum_{1 \le i \le \omega} \overline{a}_i z_1^i z_2^{\omega - i} \quad \text{with} \quad \overline{a}_i \in k.$$

For the above $\overline{g}$ let

$$g = (t_2/t_1)^{\omega} + \sum_{1 \le i \le \omega} a_i (t_2/t_1)^{\omega - i} \quad \text{where} \quad a_i \in \kappa \quad \text{with} \quad H_R(a_i) = \overline{a}_i.$$

If $\overline{g} = z_1$ then take $g = t_1/t_2$. This gives a subset W of L such that $g \mapsto \overline{g}$ gives a bijection $W \to \overline{W}$. In turn $g \mapsto S_g$ gives a bijection $W \to Q_1(R)$ where $M(S_g) = (g, t_2)S_g$ or $M(S_g) = (t_1, g)S_g$ according as $\overline{g} = z_1$ or $\overline{g} \neq z_1$. We let

$$\epsilon : \overline{W} \to Q_1(R) \quad \text{and} \quad \delta : Q_1(R) \to \overline{W}$$

be the bijections $\overline{g} \mapsto S_g$ and $S_g \mapsto \overline{g}$ respectively.

With this preparation in hand, let us complete the proof of ZQT(IV). In doing so we shall **tacitly use the implication** to be proved in Lemma (8.2) of Section 8 which says that for any complete ideal I in a two dimension regular local domain R we have $\mathfrak{W}(R, I)^{\mathfrak{N}} = \mathfrak{W}(R, I)$.

The "conversely" part of ZQT(IV) follows from the first part of ZQT(IV) and hence it suffices to show that, given any nonzero complete ideal I in R, upon letting $U = \{\eta_R(J) : J \in C(R) : u(I, J) > 0\}$, we have $\mathfrak{W}(R, I)_1^{\Delta} = U$.

Now contracted ideals of R are defined at the top of page 373 of Appendix 5, and on the same page Theorem 1 about their factorization is proved using characteristic form c defined on page 363 and using order r of an ideal or element of R defined on page 362; this order is our ord_R. Now look at our ZQT(III) = Theorem 3 of Appendix 5. In the first paragraph of page 379 which is the beginning of Subsection 4 of Appendix 5, Zariski proves the **important fact** that complete ideals are contracted ideals. Now $M \in C(R)$ and the argument in the proof of Theorem 3 shows that $c(M) = 1$ whereas for any $J \in C(R) \setminus \{M\}$ we have $c(J) = \overline{g}^{\lambda}$ for a unique $\overline{g} \in \overline{W}$ and $\lambda \in \mathbb{N}_+$. In ZQT(III) let us label the $J \neq M$ with $u(I, J) > 0$ as $(J_{ij})_{1 \le i \le m, 1 \le j \le n_i}$ with $m \in \mathbb{N}$ and $n_i \in \mathbb{N}_+$ so that $c(J_{ij})$ and $c(J_{i'j'})$ are powers of the same member of $\overline{W}$ iff $i = i'$; let $c(J_{ij}) = \overline{g}_i^{\lambda_{ij}}$. Since $\mathfrak{W}(R, I)$ is unchanged if we multiply I by a nonzero principal ideal, we may assume $\widehat{I} = R$. By the said argument we can match up with Theorem 1 by taking

$$\mathfrak{A} = I \quad \text{with} \quad u(I,M) = r - s$$

and

$$\mathfrak{B}_i = \prod_{1 \le j \le n_i} J_{ij} \quad \text{and} \quad \lambda_i = \sum_{1 \le j \le n_i} \lambda_{ij} \quad \text{for} \quad 1 \le i \le m.$$

with

$$\mathrm{ord}_R \mathfrak{A} = r \quad \text{and} \quad \mathrm{ord}_R \prod_{1 \le i \le m} \mathfrak{B}_i = s.$$

We claim that

(1) $$u(I,M) = 0 \Leftrightarrow o(R) \notin \mathfrak{W}(R,I)_1^{\Delta}.$$

To see this, take a finite set of generators $(x_1, \dots, x_p)$ of I. After suitable relabelling we may assume that (i) $\mathrm{ord}_R x_i = r$ or $\mathrm{ord}_R x_i > r$ according as $1 \le i \le q$ or $q < i \le p$ with $q \in \mathbb{N}_+$. Replacing $x_2, \dots, x_q$ by $x_2 - a_2 x_1, \dots, x_q - a_q x_1$ with suitable $a_2, \dots, a_q$ in R and then again relabelling we may assume that in addition (i) we have that (ii) $l(x_i)/l(x_1) \notin k$ for $2 \le i \le q$. Note that then (iii) for $2 \le i \le q$ we have $l(x_i)/l(x_1) \notin k$ and $l(x_1)/l(x_i) \notin k$. Clearly $u(I,M) = 0 \Leftrightarrow q = 1$. Upon letting $A = R[x_2/x_1, \dots, x_p/x_1]$ we have $A \subset o(R)\ \mathfrak{V}(A) \subset \mathfrak{W}(R,I)$. Moreover, upon letting S be the center of $o(R)$ on $\mathfrak{V}(A)$ we see that $q = 1$ or $q \ge 2$ according as $\dim(S) = 2$ or $\dim(S) = 1$. QED.

For $1 \le i \le m$, upon letting $S_i = \epsilon(\overline{g}_i)$ we see that S_i is the center of $\eta_R(J_{ij})$ on $\mathfrak{W}(R,M)$ for $1 \le j \le n_i$. Moreover, $S_1, \dots, S_m$ are exactly all those distinct members S of $Q_1(R)$ such that $(R,S)(I) \ne S$. In view of (6.6.6) and (6.6.8) on pages 182-183 of [Ab3], by ZQT(I) and ZQT(II) we get the following.

(2) $$\begin{cases} \text{Assuming } d(R,U) > 0, \text{ for } 1 \le i \le m, \\ \text{upon letting } I_i = (R,S_i)(I) \text{ we have} \\ I_i \in \overline{C}(S_i) \text{ and } \{\eta_R(J_{ij} : 1 \le j \le n_i\} = \overline{\eta}_{S_i}(I_i). \\ \text{Moreover we have } \mathfrak{W}(R,I)_1^{\Delta} \setminus \{o(R)\} = \bigcup_{1 \le i \le m} \mathfrak{W}(S_i,I_i)_1^{\Delta}. \end{cases}$$

Finally we observe the following.

(3) $$\begin{cases} \text{As noted in (3.1), } d(R,U) = 0 \Leftrightarrow U = \emptyset. \\ \text{Hence if } U = \emptyset \text{ then } I = R \text{ and } \mathfrak{W}(R,I)_1^{\Delta} = \emptyset. \end{cases}$$

In view of (1) to (3) we are done by induction on $d(R,U)$.

Section 4: Integral Dependence and Reductions of Ideals. Let $R \subset S$ be nonnull rings and let J be an ideal in R. An element x of S is **integral over** J means $f(x) = 0$ for a univariate polynomial $f(Z)$ of the form

$$(*) \qquad f(Z) = Z^n + y_1 Z^{n-1} + \cdots + y_n \text{ with } n \in \mathbb{N}_+ \text{ and } y_i \in J^i \text{ for } 1 \leq i \leq n.$$

A subset T of S is **integral over** J means every $x \in T$ is integral over J. We may write x/J (is) integral or T/J (is) integral to indicate that x is integral over J or T is integral over J respectively. By the **integral closure** of J in S we mean the set of all elements of S which are integral over J. Note that if $J = R$ then $J^i = J$ for all i and hence in that case these definitions of integral over and integral closure coincide with the usual definitions. For the above definitions see L4§10(E2) on pages 161-163 of [Ab4] and Definition 2 on page 349 of volume II of [Zar].

Let I be an ideal in R. We say that J is a **reduction** of I to mean that

$$(\dagger) \qquad J \subset I \quad \text{and} \quad JI^n = I^{n+1} \quad \text{for some} \quad n \in \mathbb{N}.$$

The above definition of reduction was first introduced by Northcott-Rees in [NoR]. We may write J/I (is a) reduction to indicate that J is a reduction of I. Clearly

$$(\ddagger) \qquad (\dagger) \Rightarrow J^p I^q = I^{p+q} \text{ for all integers } p > 0 \text{ and } q \geq n.$$

To see this, multiply both sides of $(\dagger)$ by I^{q-n} to get $JI^q = JI^{q+1}$, i.e., we get $(\ddagger)$ for $p = 1$. Now letting $p > 1$ and assuming $(\ddagger)$ for $p - 1$ we have $J^{p-1}I^q = I^{p+q-1}$. Multiplying both sides by J we get $J^p I^q = JI^{p+q-1} = I^{p+q}$. So we are done by induction on p.

We shall use various concepts concerning graded rings and homogeneous rings. For the basic material about these matters see L5§§2-3 on pages 206-216 of [Ab4].

By the **Rees ring** of I relative to R with variable Z we mean the ring $E_R(I)$ obtained by putting

$$E_R(I) = R[IZ].$$

Note that $R[Z]$ is the univariate polynomial ring as a naturally graded homogeneous ring with $R[Z]_n =$ the set of all homogeneous polynomials of degree n including the zero polynomial, and n varying over $\mathbb{N}$. Now $E_R(I)$ is a graded subring of $R[Z]$. We make the convention that the reference to R and Z may be omitted when it is clear from the context. Thus we write $E(I)$ instead of $E_R(I)$. Note that

$$\text{(4.1)}\qquad \begin{cases} \text{as a ring } E(I) \text{ is generated over its subring } R \\ \text{by the set } IZ = \{xZ : x \in I\}. \end{cases}$$

and

$$\text{(4.2)}\qquad \begin{cases} \text{for any } P(Z) = \sum P_n Z^n \in R[Z] \text{ with } P_n \in R \text{ we have:} \\ P(Z) \in E(I) \Leftrightarrow P_n \in I^n \text{ for all } n \in \mathbb{N}. \end{cases}$$

Also note that, writing $E(I)_n$ for the n-th homogeneous component of $E(I)$ we have

$$\text{(4.3)}\qquad E(I)_n = \{xZ^n : x \in I^n\}.$$

Finally note that, if $J \subset I$ then $E(J)$ is a graded subring of $E(I)$.

We claim that

$$\text{(4.4)}\qquad \begin{cases} \text{for any } x \in I \text{ we have:} \\ (xZ)/E(J) \text{ is integral} \\ \Leftrightarrow x/J \text{ is integral} \\ \Rightarrow x^n \in JI^{n-1} \text{ for some } n \in \mathbb{N}_+. \end{cases}$$

PROOF. First suppose that x/J is integral. Then for some $n \in \mathbb{N}_+$ we have

$$x^n + \sum_{1\le i\le n} y_i x^{n-i} = 0 \quad \text{with} \quad y_i \in J^i \ \text{ for } \ 1 \le i \le n.$$

Clearly $y_i x^{n-i} \in J^i I^{n-i} \subset JI^{n-1}$ for $1 \le i \le n$ and hence $x^n \in JI^{n-1}$. Multiplying both sides of the above equation by Z^n and invoking (4.3) we get

$$(xZ)^n + \sum_{1\le i\le n} (y_i Z^i)(xZ)^{n-i} = 0 \quad \text{with} \quad (y_i Z^i) \in E(J)_i \ \text{ for } \ 1 \le i \le n$$

and hence $(xZ)/E(J)$ is integral.

Next suppose that $(xZ)/E(J)$ is integral. Then for some $n \in \mathbb{N}_+$ we have

$$(xZ)^n + \sum_{1\le i\le n} z_i (xZ)^{n-i} = 0 \quad \text{with} \quad z_i \in E(J) \ \text{ for } \ 1 \le i \le n.$$

By (4.3) we can write

$$z_i = \sum_{m\in\mathbb{N}} y_{im} Z^m \quad \text{where} \quad y_{im} \in J^m \quad \text{with} \quad y_{im} = 0 \text{ for almost all } m.$$

Substituting the last display into the previous to last display and then equating the coefficients of Z^n we get

$$x^n + \sum_{1\le i\le n} y_{ii} x^{n-i} = 0 \quad \text{with} \quad y_{ii} \in J^i \ \text{ for } \ 1 \le i \le n$$

and hence x/J is integral.

We claim that

$$(4.5)\qquad \begin{cases} \text{assuming that } R \text{ is noetherien and } J \subset I, \text{ we have:} \\ E(I)/E(J) \text{ is integral } \Leftrightarrow I/J \text{ is integral } \Leftrightarrow J/I \text{ is a reduction} \\ \text{where for the first } \Leftrightarrow \text{ we do not need the noetherian hypothesis.} \end{cases}$$

PROOF. Without invoking the noetherian hypothesis, the first $\Leftrightarrow$ follows from (4.1) and (4.4). With the noetherian hypothesis, first assume that I/J is integral, and let $x_1, \ldots, x_p$ be a finite number of generators of I with $p \in \mathbb{N}_+$. For $1 \le i \le p$, by (4.4) we can find $n(i) \in \mathbb{N}_+$ such that $x_i^{m(i)} \in JI^{m(i)-1}$. Let $m = m(1) + \cdots + m(p)$. Now every $x \in I$ can be expressed as $x = a_1x_1 + \cdots + a_px_p$ with $a_1, \ldots, a_p$ in R, and by raising both sides of the equation to the m-th power we get $x^m \in JI^{m-1}$. In particular $x_i^m \in JI^{m-1}$ for $1 \le i \le p$. Let $n = mp$. Since every element of I^n is an R-linear combination of monomials in $x_1, \ldots, x_p$ of degree mp, we get $I^n \subset JI^{n-1}$ and hence $JI^{n-1} = I^n$. Therefore J/I is a reduction.

Now with the noetherian hypothesis, assume that J/I is a reduction. Then by (‡) we find $n \in \mathbb{N}_+$ such that for all $p \in \mathbb{N}_+$ we have $J^pI^n = I^{n+p}$, and multiplying this equation by Z^{p+n} we get $J^pI^nZ^{p+n} = I^{n+p}Z^{p+n}$. In view of (4.3), the last equation tell us that $E(I)$, as an $E(J)$-module, is generated by the submodule $\sum_{1 \le q \le n} E(I)_q$. The noetherian hypothesis tells us that the ideal I is finitely generated, and hence so is the said submodule. Therefore $E(I)$ is a finitely generated $E(J)$-module and hence the ring $E(I)$ is integral over the subring $E(J)$.

We observe that

$$(4.6)\qquad J/I \text{ is a reduction} \Rightarrow \mathrm{rad}_R J = \mathrm{rad}_R I.$$

PROOF. If J/I is a reduction then for some $n \in \mathbb{N}_+$ we have $I^n \subset JI^{n-1} \subset J$ and hence $\mathrm{rad}_R I = \mathrm{rad}_R I^n \subset \mathrm{rad}_R J$ and obviously $\mathrm{rad}_R J \subset \mathrm{rad}_R I$ and therefore $\mathrm{rad}_R J = \mathrm{rad}_R I$.

Recall from page 231 of [Ab4] that a **minimal prime** of R is a prime ideal in R which does not properly contain any other prime ideal in R. In the next two items (4.7) and (4.8) we shall gather some general properties of the nonnull rings $R \subset S$. In comparing the dimensions of two rings, say R and S, we use the convention that for any $n \in \mathbb{Z}$ we have $n + \infty = \infty$. First we claim that

$$(4.7) \qquad \begin{cases} \text{for any minimal prime } P \text{ of } R \\ \text{there is a minimal prime } Q \text{ of } S \text{ with } P = Q \cap R. \end{cases}$$

PROOF. By taking $(I, S, R) = (P, R \setminus P, S)$ in $(12^\bullet)$ on page 121 of [Ab4] we can find a prime ideal Q' in S with $Q' \cap (R \setminus P) = \emptyset$. Let $P' = Q' \cap R$. Then P' is a prime ideal in R with $P' \subset P$, and hence the minimality of P tells us that $P' = P$. By (T51) on page 265 of [Ab4] we can find a minimal prime of Q of S with $Q \subset Q'$. The minimality of P now tells us that $P = Q \cap R$.

Next we claim that

$$(4.8) \qquad \begin{cases} \text{if } R \text{ is a noetherian ring} \\ \text{and } S \text{ is a finitely generated ring extension of } R \\ \text{and } S \text{ is a subring of the polynomial ring } R[Z_1, \dots, Z_m] \\ \text{in indeterminates } Z_1, \dots, Z_m \text{ with } m \in \mathbb{N}_+ \\ \text{then: } \dim(S) \le m + \dim(R), \\ \text{and } \dim(S/MS) \le m - 1 + \dim(R) \text{ for every ideal } M \text{ in } R \\ \text{which is not contained in any minimal prime of } R, \\ \text{and } \dim(S) = \dim(R) \text{ in case } S \subset R[NZ_1, \dots, NZ_m] \\ \text{for some } N \subset \mathrm{rad}_R\{0\}. \end{cases}$$

PROOF. To prove the first assertion, by (T51) on page 265 of [Ab4], it suffices to show that for any minimal prime B of S we have $\dim(S/B) \le m + \dim(R)$. To prove this inequality, by (4.8) we can find a minimal prime C of $T = R[Z_1, \dots, Z_m]$ with $B = C \cap S$. Let $A = C \cap R$. By (T30) on pages 233-234 of [Ab4] and (T51) on page 265 of [Ab4], the minimality of C tells us that A is a minimal prime of R and $C = AT$. Let $\phi : T \to \overline{T} = T/C$ be the residue class epimorphism, and let $\overline{R} = \phi(R)$, $\overline{S} = \phi(S)$, and $\overline{Z}_i = \phi(Z_i)$ for $1 \le i \le m$. Then $\overline{R} \subset \overline{S} \subset \overline{T} = \overline{R}[\overline{Z}_1, \dots, \overline{Z}_m]$ are noetherian domains, $\overline{S}$ is a finitely generated ring extension of $\overline{R}$, and, in view of

(C12) on page 235 of [Ab4], the elements $\overline{Z}_1, \dots, \overline{Z}_m$ are algebraically independent over $\overline{R}$. Consequently by (T55) on page 269 of [Ab4] we get $\dim(\overline{S}) \le m + \dim(\overline{R})$. Also clearly $\dim(\overline{R}) \le \dim(R)$. Therefore $\dim(S/B) \le m + \dim(R)$.

To prove the second assertion, let there be given any ideal M in R which is not contained in any minimal prime of R. Suppose if possible that $MS \subset B$ for a minimal prime B of S. By (4.7) we can find a minimal prime C of $T = R[Z_1, \dots, Z_m]$ with $B = C \cap S$. Let $A = C \cap R$. By (T30) on pages 233-234 of [Ab4] and (T51) on page 265 of [Ab4], the minimality of C tells us that A is a minimal prime of R and $C = AT$. By (T30) on pages 233-234 of [Ab4] we know that $(MT) \cap R = M$ and hence $(MS) \cap R = M$. Now $MS \subset B$ with $(MS) \cap R = M$ and $B \cap R = A$ tells us that $M \subset A$ which is a contradiction because M is not contained in any minimal prime of R but A is a minimal prime of R. Hence MS is not contained in any minimal prime of S; consequently $\dim(S/MS) \le -1 + \dim(S)$ and by the first assertion we have $\dim(S) \le m + \dim(R)$; putting the two inequalities together we get $\dim(S/MS) \le m - 1 + \dim(S)$.

To prove the third assertion note that now $S = R[Q]$ with $Q \subset \mathrm{rad}_S\{0\}$, i.e., with Q being a set of nilpotent elements in S. Hence, letting $\psi_S : S \to \overline{S} = S/\mathrm{rad}_S\{0\}$ be the residue class epimorphism we get $\overline{S} = \psi_S(R)$. S being an overring of R, we also have $R \cap \mathrm{rad}_S\{0\} = \mathrm{rad}_R\{0\}$. Therefore $\overline{S}$ is isomorphic to $\overline{R} = \psi_R(R)$ where $\psi_R : R \to R/\mathrm{rad}_R\{0\}$ is the residue class epimorphism. Consequently we get $\dim(S) = \dim(\overline{S}) = \dim(\overline{R}) = \dim(R)$ because of the fact that for any ring S we have $\dim(S) = \dim(\overline{S})$. The said fact is an obvious consequence of (T51) on page 265 of [Ab4].

Finally we observe that

$$
(4.9) \qquad \begin{cases} \text{assuming that } R \text{ is noetherien and ideal } J' \subset J \subset I, \text{ we have:} \\ I/J' \text{ is integral } \Leftrightarrow I/J \text{ is integral and } J/J' \text{ is integral, and} \\ I/J' \text{ is a reduction } \Leftrightarrow I/J \text{ is a reduction and } J/J' \text{ is a reduction.} \end{cases}
$$

PROOF. Follows from (4.5).

Section 5: Jacobson Radicals and Irrelevant Ideals. Let there be given a nonnull ring R.

Recall that an R-homomorphism means a homomorphism of R-modules. Recall that if $\mu : R \to T$ is a ring epimorphism and L is a T-module then L becomes an R-module by putting $rl = \mu(r)l$ for all $r \in R$ and $l \in L$. Recall that the intersection of all maximal ideals in R is called its **jacobson radical** and is denoted by $\mathrm{jrad}(R)$. Recall the definition of **irrelevant ideals** in graded rings given in (C4) on page 212 of [Ab4].

Let M be an ideal in R such that $M \subset \mathrm{jrad}(R)$. Let I be an ideal in R such that $I = (x_1, \dots, x_p)R$ for some $x_1, \dots, x_p$ in I and $p \in \mathbb{N}_+$. Let F be a naturally graded homogeneous ring and let F_n be its homogeneous component of degree n. Assume there is a ring epimorphism $\mu_0 : R \to F_0$ with kernel M and for every $n \in \mathbb{N}_+$ there is an R-epimorphism $\mu_n : I^n \to F_n$ with kernel MI^n such that $\mu_{u+v}(yz) = \mu_u(y)\mu_v(z)$ for all $(u, v, y, z) \in \mathbb{N} \times \mathbb{N} \times I^u \times I^v$.

We claim that

$$(5.1) \qquad \begin{cases} \text{for any ideal } J \text{ in } R \text{ with } J \subset I \text{ we have:} \\ \text{the ideal } \mu_1(J)F \text{ is irrelevant iff } J/I \text{ is a reduction.} \end{cases}$$

PROOF. In view of the definition of irrelevant ideals, our assertion is equivalent to saying that

$$F_1F \subset \mathrm{rad}_F(\mu_1(J)F) \Leftrightarrow I^n = JI^{n-1} \text{ for some } n \in \mathbb{N}_+.$$

Now for any $n \in \mathbb{N}_+$ we have

$$\begin{cases} \mu_n(I^n) \subset \mu_n(JI^{n-1}) \\ \Leftrightarrow I^n \subset JI^{n-1} + MI^n \\ \Leftrightarrow I^n = JI^{n-1} + MI^n \\ \Leftrightarrow I^n = JI^{n-1} \end{cases}$$

where the first two $\Leftrightarrow$ are obvious while the last $\Leftrightarrow$ follows by taking $(U, V, J) = (JI^{n-1}, I^n, M)$ in the Nakayama Lemma (T3) on page 220 of [Ab4]. Thus it only remains to show that

$$F_1F \subset \mathrm{rad}_F(\mu_1(J)F) \Leftrightarrow \mu_n(I^n) \subset \mu_n(JI^{n-1}) \text{ for some } n \in \mathbb{N}_+.$$

Clearly

$$\begin{cases} F_1F \subset \mathrm{rad}_F(\mu_1(J)F) \\ \Rightarrow \{x_1^m, \ldots, x_p^m\} \subset \mu_1(J)F \text{ for some } m \in \mathbb{N}_+ \\ \Rightarrow F_n \subset \mu_1(J)F \text{ for some } n \in \mathbb{N}_+ \\ \Rightarrow \{x_1^m, \ldots, x_p^m\} \subset \mu_1(J)F \text{ for some } m \in \mathbb{N}_+ \\ \Rightarrow F_1F \subset \mathrm{rad}_F(\mu_1(J)F) \end{cases}$$

where the first $\Rightarrow$ is obvious, the second follows by taking $n = mp$, the third follows by taking $m = n$, and the fourth is obvious. Consequently it suffices to show that for any $n \in \mathbb{N}_+$ we have

$$F_n \subset \mu_1(J)F \Leftrightarrow \mu_n(I^n) \subset \mu_n(JI^{n-1}).$$

Obviously $F_n = \mu_n(I^n)$ and clearly

$$F_n \subset \mu_n(J)F \Leftrightarrow F_n \subset (\mu_1(J)F) \cap F_n.$$

Thus it suffices to show that

$$(\mu_1(J)F) \cap F_n = \mu_n(JI^{n-1}).$$

To prove the above equation, note that, by the rule $\mu_{u+v}(yz) = \mu_u(y)\mu_v(z)$, the RHS consists of all finite sums of the type

$$\sum_i \mu_1(y_i)\mu_{n-1}(z_i)$$

with $(y_i, z_i) \in J \times I^{n-1}$. Moreover the LHS consists of the n-th components of all finite sums of the type

$$\sum_i \left(\mu_1(y_i') \sum_{m \in \mathbb{N}} \mu_m(z_{i,m}') \right)$$

with $(y_i', z_{i,m}') \in J \times I^m$. Collecting terms of like degree we see that the LHS consists of all finite sums of the type

$$\sum_i \mu_1(y_i')\mu_{n-1}(z_{i,n-1}').$$

Therefore the LHS equals the RHS.

Using Noether Normalization (cf. pages 248 and 402 of [Ab4]) together with Veronese Embedding (cf. page 263 of [Ab3]) we shall now prove the following:

$$(5.2)\qquad \begin{cases} \text{Assume } R \text{ is a local ring with } I \subset M = M(R) \\ \text{and let } d = \dim(F) \text{ with } e = \dim(R). \\ \text{Then there exist elements } y_1, \dots, y_d \text{ in } I \text{ such that the ideal} \\ J = (y_1, \dots, y_d)R \text{ is a reduction of } I^c \text{ for some } c \in \mathbb{N}_+. \\ \text{If the field } R/M \text{ is infinite then this is true with } c = 1. \\ \text{If } I \text{ is } M\text{-primary then } d \geq e. \end{cases}$$

PROOF. If the field $K = R/M$ is infinite then by (T46) on page 248 of [Ab4] there exist R-linear combinations $y_1, \dots, y_d$ of $x_1, \dots, x_p$ such that $F/K[\mu_1(J)]$ is integral where $J = (y_1, \dots, y_d)R$, and then by (T104) on page 401 of [Ab4] we see that the ideal $\mu_1(J)F$ is irrelevant, and hence by (5.1) we conclude that J/I is a reduction.

In the general case, as on page 263 of [Ab3], for any $c \in \mathbb{N}_+$ we get a naturally graded homogeneous ring $F^{(c)} = K[\mu_c(I^c)]$ whose n-th homogeneous component is $F^{(c)} = F_{cn}$ for all $n \in \mathbb{N}$. Note that $F^{(c)}$ is a subring (but not necessarily a graded subring) of F. Moreover $\mu_{cn} : I^{cn} \to F_n^{(cn)}$ is an R-epimorphism with kernel MI^{cn} for all $n \in \mathbb{N}$. By (T105) on page 402 of [Ab4] there exist elements $y_1, \dots, y_d$ in I^c for some $c \in \mathbb{N}_+$ such that $F/K[\mu_c(J)]$ is integral where $J = (y_1, \dots, y_d)R$. It follows that $F^{(c)}/K[\mu_c(J)]$ is integral and therefore by (T104) on page 401 of [Ab4] we see that the ideal $\mu_c(J)F^{(c)}$ is irrelevant, and hence by (5.1) we conclude that J/I^c is a reduction.

Suppose I is M-primary and $e \neq 0$. Now $J = (y_1, \dots, y_d)R$ is a reduction of I^c and hence $\mathrm{rad}_R J = \mathrm{rad}_R I^c = \mathrm{rad}_R I = M$ where the first equality is by (4.6) and the second and third are obvious. Therefore J is M-primary and hence $d \geq e$.

Section 6: Form Rings. Let I be an ideal in a nonnull ring R and assume that

$$I \subset M = \text{a nonunit ideal in } R.$$

We define the **form ring** $F_{(R,M)}(I)$ of I relative to R with variable Z by putting

$$F_{(R,M)}(I) = E_R(I)/ME_R(I).$$

Again we make the convention that the reference to (R, M) and Z may be omitted when it is clear from the context. Thus we write $F(I)$ instead of $F_{(R,M)}(I)$. Now $ME(I)$ is a homogeneous ideal in $E(I)$ and hence $F(I)$ becomes a graded ring. Note that, upon letting $F_{(R,M)}(I)_n$ or $F(I)_n$ to be the n-th homogeneous component of $F(I)$ for all $n \in \mathbb{N}$ and upon letting

$$K = F(I)_0 \quad \text{we have} \quad F(I) = K[F(I)_1]$$

and, via the ring epimorphism $R \to K = R/M$, the K-module $F(I)$ becomes an R-module so that, for every $n \in \mathbb{N}$, the K-submodule $F(I)_n$ of $F(I)$ becomes an R-submodule of $F(I)$ and there is a canonical R-epimorphism $\mu_n : I^n \to F(I)_n$ with kernel MI^n such that

$$\mu_{u+v}(yz) = \mu_u(y)\mu_v(z) \quad \text{for all} \quad (u, v, y, z) \in \mathbb{N} \times \mathbb{N} \times I^u \times I^v.$$

Observe that $F(I)$ is isomorphic as a graded ring to the associated graded ring $\mathrm{grad}(R, I, M)$ of Definition (D3) on page 586 of [Ab4].

If J is an ideal in R with $J \subset I$ then $\mu_1(J)$ is a K-submodule of $F(I)_1$ and $K[\mu_1(J)]$ is a homogeneous subring of $F(I)$; we denote this subring by $F_{(R,M)}(I, J)$ and we note that for its n-th homogeneous component $F_{(R,M)}(I, J)_n = \mu_n(J^n)$ for all $n \in \mathbb{N}$. We call $F_{(R,M)}(I, J)$ the **form ring** of (I, J) relative to (R, M) with variable Z. Again we make the convention that the reference to (R, M) and Z may be omitted when it is clear from the context. Thus we write $F(I, J)$ and $F(I, J)_n$ instead of $F_{(R,M)}(I, J)$ and $F_{(R,M)}(I, J)_n$ respectively.

Note that, if R is noetherian and M is a maximal ideal in R then, for every $n \in \mathbb{N}$, $F(I)_n$ is a finite dimensional vector space over the field K, and $F(I)_1F(I)$ is the unique homogeneous maximal ideal in $F(I)$.

We claim that

$$(6.1) \qquad \begin{cases} \text{if } R \text{ is a local ring with ideal } J \subset I \subset M = M(R) \text{ then:} \\ F(I)/F(I, J) \text{ is integral} \Leftrightarrow I/J \text{ is integral} \Leftrightarrow J/I \text{ is a reduction.} \end{cases}$$

PROOF. By (T104) on page 401 of [Ab4] we know that $F(I)/F(I, J)$ is integral iff the ideal $\mu_1(J)F$ is irrelevant. Therefore we are done by (4.5) amd (5.1).

We also claim that

$$(6.2)\qquad \begin{cases} \text{if } R \text{ is a local ring with ideal } J \subset I \subset M = M(R) \\ \text{such that } J/I \text{ is a reduction} \\ \text{and } I \text{ is generated by a finite number of elements } (x_1, \dots, x_p) \\ \text{and } J \text{ is generated by a finite number of elements } (y_1, \dots, y_q) \\ \text{then } q \geq \dim(F(I,J)) = \dim(F(I)) \leq p, \\ \text{and furthermore if } \dim(F(I)) = p \text{ then } J = I, \\ \text{and moreover (without assuming } \dim(F(I)) = p\text{) if } q = \dim(F(I)) \\ \text{and ideal } J' \subset J \text{ is such that } J'/I \text{ is a reduction} \\ \text{then } J' = J. \end{cases}$$

PROOF. Now

$$F(I,J) = K[\mu_1(y_1), \dots, \mu_1(y_q)] \subset K[\mu_1(x_1), \dots, \mu_1(x_p)] = F(I)$$

and $F(I)/F(I,J)$ is integral by (6.1), and hence $q \geq \dim(F(I,J)) = \dim(F(I)) \leq p$, and if $\dim(F(I)) = p$ then $\mu_1(J) = \mu_1(I)$ and therefore $J = I$ by taking $(U,V,J) = (J,I,M)$ in the Nakayama Lemma (T3) on page 220 of [Ab4]. In view of (4.9), the "moreover" follows from the "furthermore."

Next we claim that

$$(6.3)\qquad \begin{cases} \text{if } R \text{ is a local ring with } I \subset M = M(R) \\ \text{then for all } c \in \mathbb{N}_+ \text{ we have } \dim(F(I^c)) = \dim(F(I)). \end{cases}$$

PROOF. The rings $F(I)$ and $F(I^c)$ are respectively isomorphic to the graded rings F and $F^{(c)}$ of the general case proof of (5.2). The ideal in F generated by $\mu_c(I^c)$ is clearly irrelevant, and hence $F/F^{(c)}$ is integral by (T104) on page 401 of [Ab4]. Therefore $\dim(F) = \dim(F^{(c)})$.

Finally we claim the following.

$$(6.4)\qquad \begin{cases} \text{Assuming } R \text{ is a local ring with } I \subset M = M(R) \\ \text{and letting } d = \dim(F(I)) \text{ with } e = \dim(R) \text{ we have } d \leq e \\ \text{and there exist elements } y_1, \dots, y_d \text{ in } I \text{ such that} \\ \text{the ideal } J = (y_1, \dots, y_d)R \text{ is a reduction of } I^c \text{ for some } c \in \mathbb{N}_+ \\ \text{where if } R/M \text{ is infinite then } c \text{ can be chosen to be } 1. \\ \text{Moreover, if } I \text{ is } M\text{-primary then } d = e. \end{cases}$$

PROOF. Taking $F = F(I)$ in (4.8) we get $d \le e$. The rest follows from (5.2).

Section 7: Proof of NRT. The following NRT = Northcott-Rees Theorem is the culmination of the Northcott-Rees paper [NoR]. Our proof will be completely independent of that paper. Indeed we have already done it in (6.1) to (6.4).

For an ideal I in a nonnull ring R, following page 289 of [Ab4], we define the **generating number** of I in R to be the smallest number of generators of I and denote it by $\mathrm{gnb}(I)$ (or $\mathrm{gnb}_R I$). In case $I \subset M =$ a nonunit ideal in R, following [NoR], we call $\dim(F_{(R,M)}(I))$ the **analytic spread** of I (relative to (R,M)) and denote it by $\sigma(I)$ (or $\sigma_R(I)$), and by a **minimal reduction** of I (relative to (R,M)) we mean an ideal J in R such that J is a reduction of I with $\mathrm{gnb}(J) = \sigma(I)$.

NRT. Let I be an ideal in a local ring R with $I \subset M = M(R)$. Then letting $e = \dim(R)$ and considering the form ring $F(I) = F_{(R,M)}(I)$ we have the following.

(I) $\sigma(I) \le e$. $\sigma(I^c) = \sigma(I)$ for all $c \in \mathbb{N}_+$. If I is M-primary then $\sigma(I) = e$.

(II) For some $c \in \mathbb{N}_+$, I^c has a minimal reduction.

(III) If $R/M(R)$ is an infinite field then I has a minimal reduction.

(IV) J/I is a reduction $\Rightarrow \mathrm{gnb}(J) \ge \sigma(I)$.

(V) $\mathrm{gnb}(I) = \sigma(I) \Rightarrow I$ is the only reduction of I.

(VI) Given any ideal J in R with $J \subset I$, for $F(I,J) = F_{(R,M)}(I,J)$ we have:

$$F(I)/F(I,J) \text{ is integral} \Leftrightarrow I/J \text{ is integral} \Leftrightarrow J/I \text{ is a reduction.}$$

Section 8: Modelic Proj. We shall now relate local normalization and ideal reduction. We shall also give supplements to ZQT. We shall do this by proving several Lemmas.

Note that an ideal I in a normal domain R is said to be **normal** if I^c is complete for all $c \in \mathbb{N}_+$. If $I = R$ then $I^c = I$ for all $c \in \mathbb{N}_+$ and hence in this case the definition of normality coincides with the usual definition. Also note that by the **completion** of an ideal J in a normal domain R with quotient field L we mean the complete ideal I in R obtained by putting

$$I = \bigcap_{V \in \overline{D}(L/R)} ((JV) \cap R).$$

We observe that, by Theorem 1 on page 350 of volume II of [Zar], I coincides with the **integral closure** of J in R by which we mean the set of all elements of R which are integral over J. Hence in particular I is an ideal in R such that I/J is integral, and hence if R is noetherian then J/I is a reduction by (4.5).

For the reader's convenience, here is a **brief review** of the theory of modelic proj developed in (Q34) on pages 534-552 of [Ab4] which itself is a transcription of §12 on pages 262-283 of [Ab3]. So let R be a noetherian domain with quotient field L and let $A = \sum_{n \in \mathbb{N}} A_n$ be a homogeneous domain with $A_0 = R$ and $A_1 \neq 0$. Now $\mathrm{proj}(A)$ is the set of all relevant homogeneous prime ideals in A; note that $\mathrm{proj}(A) \subset \mathrm{spec}(A)$ and for every $i \in \mathbb{N}$, upon letting $\mathrm{proj}(A)_i$ to be the set of all members of $\mathrm{proj}(A)$ of height i, we have $\mathrm{proj}(A)_i \subset \mathrm{spec}(A)_i$. Moreover

$$L \subset \mathfrak{K}(A) \subset \mathrm{QF}(A)$$

where the homogeneous quotient field $\mathfrak{K}(A)$ of A is defined by putting

$$\mathfrak{K}(A) = \bigcup_{n \in \mathbb{N}} \{y_n/z_n : y_n \in A_n \text{ and } z_n \in A_n^\times\}.$$

Likewise, the homogeneous localization $A_{[P]}$ of any P in $\mathrm{proj}(A)$ is defined by putting

$$A_{[P]} = \bigcup_{n \in \mathbb{N}} \{y_n/z_n : y_n \in A_n \text{ and } z_n \in A_n \setminus P\}.$$

The set of all homogeneous localizations $A_{[P]}$, with P varying over $\mathrm{proj}(A)$, is the modelic proj $\mathfrak{W}(A)$. Note that $\mathfrak{W}(A) = \mathfrak{W}(R, A_1)$ and for any finite set of generators $x_1, \ldots, x_p$ of the R-module A_1 we have $\mathfrak{W}(A) = \mathfrak{W}(R; x_1, \ldots, x_p)$. Also note that for every $i \in \mathbb{N}$, upon letting $\mathfrak{W}(A)_i$ to be the set of all i-dimensional members of $\mathfrak{W}(A)$, we have $\mathfrak{W}(A)_i = \mathfrak{W}(R, A_1)_i = \mathfrak{W}(R; x_1, \ldots, x_p)_i$. Recall that a homogeneous subdomain B of A is a homogeneous domain $B = \sum_{n \in \mathbb{N}} B_n$ such that B is a subring of A with $B_n = B \cap A_n$ for all $n \in \mathbb{N}$. Observe that if $\overline{B}$ is a subdomain of A then: $\overline{B}$ can be made into a homogeneous subdomain of $A \Leftrightarrow$ the homogeneous A-components of every element of $\overline{B}$ belong to $\overline{B}$, and $\overline{B} = \overline{B}_0[\overline{B}_1]$ where $\overline{B}_n = \overline{B} \cap A_n$ for all $n \in \mathbb{N}$; when this so then we may indicate it by saying that $\overline{B}$ is a homogeneous subdomain of A. Finally note that if B and $\overline{B}$ are homogeneous subdomains of A with $B \subset \overline{B}$ then automatically B is a homogeneous subdomain of $\overline{B}$.

LEMMA (8.1). Let R be a noetherian domain with quotient field L and let $A = \sum_{n\in\mathbb{N}} A_n$ be a homogeneous domain with $A_0 = R$ and $A_1 \neq 0$. Then we have the following.

(I) If A is normal then $\mathfrak{W}(A)^{\mathfrak{N}} = \mathfrak{W}(A)$.

(II) Given any element x in the integral closure of A in $\mathrm{QF}(A)$ we can find $0 \neq z \in A_e$ with $e \in \mathbb{N}$ such that $zx \in A$. Moreover, any $y \in A_1^\times$ is transcendental over $\mathfrak{K}(A)$ and we have $\mathrm{QF}(A) = \mathfrak{K}(A)(y)$.

(III) For any noetherian subdomain S of R and any homogeneous subdomain $B = \sum_{n\in\mathbb{N}} B_n$ of A with $B_0 = S$ and $\mathrm{QF}(B) = \mathrm{QF}(A)$, upon letting $\overline{S}$ and $\overline{B}$ be the integral closures of S and B in R and A respectively, we have that $\overline{B}$ is a graded subdomain of A with $\overline{B}_0 = \overline{S}$.

(IV) If B is a homogeneous subdomain of A with $B_0 = R$ and $\mathrm{QF}(B) = \mathrm{QF}(A)$ such that A/B is integral then $B_1 \neq 0$ with $\mathfrak{K}(B) = \mathfrak{K}(A)$ and $\mathfrak{W}(B)^{\mathfrak{N}} = \mathfrak{W}(A)^{\mathfrak{N}}$.

(V) If I is a nonzero ideal in R such that A is the Rees ring $E(I) = R[IZ]$ then $\mathfrak{W}(A) = \mathfrak{W}(R, I)$.

(VI) Assume R is normal and A is the Rees ring $E(I) = R[IZ]$ of a nonzero normal ideal I in R. Then A is normal. Moreover we have $\mathfrak{W}(R, I)^{\mathfrak{N}} = \mathfrak{W}(R, I)$. Furthermore, if J is any reduction of I then $E(I)/E(J)$ is integral and we have $\mathfrak{W}(R, J)^{\mathfrak{N}} = \mathfrak{W}(R, I)$.

PROOF OF (I). We only have to show that for any P in $\mathrm{proj}(A)$, the local ring $A_{[P]}$ is normal. So let x in $\mathfrak{K}(A)$ be integral over $A_{[P]}$. Writing $x = y/z$ with $y \in A_n$ and $0 \neq z \in A_n$ for some $n \in \mathbb{N}$, we get

$$\left(\frac{y}{z}\right)^m + \sum_{1\le i\le m} \alpha_i \left(\frac{y}{z}\right)^{m-i} = 0 \quad \text{with} \quad m \in \mathbb{N}_+ \quad \text{and} \quad \alpha_i \in A_{[P]}.$$

For $1 \le i \le m$ we have $\alpha_i = \beta_i/\gamma_i$ where $\beta \in A_{n(i)}$ and $\gamma_i \in A_{n(i)} \setminus P$ with $n(i) \in \mathbb{N}$. Let $t = \gamma_1 \dots \gamma_m$ with $d = n(1) + \cdots + n(m)$. Then $t \in A_d \setminus P$ with

$d \in \mathbb{N}$. Multiplying both sides of the above displayed equation by t^m we get

$$\left(\frac{ty}{z}\right)^m + \sum_{1\le i\le m} t_i \left(\frac{ty}{z}\right)^{m-i} = 0 \quad \text{with} \quad m \in \mathbb{N}_+ \text{ and } \quad t_i = t^i\alpha_i \in A_{id}$$

and hence $(ty/z) = s \in A$ by the normality of A. Multiplying both sides of the last equation by z we get $ty = zs$ and hence $s \in A_d$ by homogeneity. Therefore $x = y/z = s/t \in A_{[P]}$.

PROOF OF (II). Following pages 156-158 of volume II of Zariski's book [Zar] let us generalize the construction of $\mathfrak{K}(A)$ by introducing a subring C of $\mathrm{QF}(A)$ with $A \subset C$ such that C is a homogeneous ring $C = \sum_{q\in\mathbb{N}} C_q$ with $C_0 = \mathfrak{K}(A)$ where C_q is defined by putting

$$C_q = \bigcup_{n\in\mathbb{N}} \{y_n/z_n : y_n \in A_{q+n} \text{ and } z_n \in A_n^\times\}.$$

As on the cited pages of [Zar], taking $0 \ne y \in A_1$ we see that y is transcendental over C_0 with $\mathrm{QF}(A) = \mathfrak{K}(A)(y)$ and $C = C_0[y]$ with $C_q = \{ry^q : r \in C_0\}$ for all $q \in \mathbb{N}$. The domain C is normal because it is a polynomial ring over the normal domain R. Therefore every element x in the integral closure of A in $\mathrm{QF}(A)$ belongs to C, and hence for it we can find $0 \ne z \in A_e$ with $e \in \mathbb{N}$ such that $zx \in A$.

PROOF OF (III). It suffices to show that, given any $e \in \mathbb{N}$ and $x = u_0 + \cdots + u_e$ with $u_n \in A_n$ for $0 \le n \le e$ such that x/B is integral, we have that u_e/B is integral (and hence by induction u_n/B is integral for $0 \le n \le e$). Since x/B is integral, we get

$$x^m + \sum_{1\le i\le m} \alpha_i x^{m-i} = 0 \quad \text{with} \quad m \in \mathbb{N}_+ \text{ and } \quad \alpha_i \in B.$$

From the above equation it follows that for all $q \in \mathbb{N}$ we have

$$(1) \qquad x^q = \sum_{0\le i\le m} \alpha_{iq} x^i \quad \text{with} \quad \alpha_{iq} \in B$$

and by (II) we get

$$(2) \qquad zx \in B \quad \text{for some} \quad 0 \ne z \in B_e \quad \text{with} \quad e \in \mathbb{N}.$$

Upon letting $\zeta = z^m$, by (1) and (2) we see that

$$(3) \qquad 0 \ne \zeta \in B_{me} \quad \text{and} \quad \zeta x^q \in B \quad \text{for all} \quad q \in \mathbb{N}.$$

Taking the q-th power of the equation $x = u_0 + \cdots + u_e$ we see that for all $q \in \mathbb{N}$ we have

$$(4) \qquad x^q = u_e^q + \sum_{0 \le i < qe} v_{qi} \quad \text{with} \quad v_{qi} \in A_i.$$

Upon letting $w_{qi} = \zeta v_{qi}$, by (3) and (4) we get

$$(5) \qquad \zeta x^q = \zeta u_e^q + \sum_{0 \le i < qe} w_{qi} \quad \text{with} \quad w_{qi} \in A_{me+i}$$

where

$$(6) \qquad \zeta x^q \in B \quad \text{and} \quad \zeta u_e^q \in A_{me+qe}.$$

In view of (5) and (6), by homogeneity we conclude that for all $q \in \mathbb{N}$ we have $\zeta u_e^q \in B_{me+qe}$ and hence $\zeta u_e^q \in B$. Thus $B[u_e]$ is a subset of the finitely generated B-module $(1/\zeta)B$ and therefore, because B is noetherian, we see that u_e/B is integral.

PROOF OF (IV). By (II) we get $B_1 \neq 0$ with $\mathfrak{K}(B) = \mathfrak{K}(A)$. Now

$$\mathfrak{W}(A) = \bigcup_{0 \neq x \in A_1} \mathfrak{V}(R[A_1/x]) \quad \text{and} \quad \mathfrak{W}(B) = \bigcup_{0 \neq y \in B_1} \mathfrak{V}(R[B_1/y])$$

where

$$A_1/x = \{z/x : z \in A_1\} \ \text{ and } \ B_1/y = \{z/y : z \in B_1\}$$

and hence it suffices to show that, given any $0 \neq y \in B_1$, the ring $R[A_1/y]$ is integral over the ring $R[B_1/y]$. In turn it suffices to show that, for any $x \in A_1$, the element x/y is integral over the ring $R[B_1/y]$. Since A/B is integral, we get

$$x^m + \sum_{1 \le i \le m} \alpha_i x^{m-i} = 0 \quad \text{with} \quad m \in \mathbb{N}_+ \ \text{ and } \ \alpha_i \in B.$$

By homogeneity, upon replacing α_i by its i-th homogeneous component, without loss of generality we may suppose that $\alpha_i \in B_i$ for $1 \le i \le m$. Dividing the above equation by y^m we get

$$\left(\frac{x}{y}\right)^m + \sum_{1 \le i \le m} \left(\frac{\alpha_i}{y_i}\right)\left(\frac{x}{y}\right)^{m-i} = 0 \quad \text{with} \quad \left(\frac{\alpha_i}{y_i}\right) \in R[B_1/y]$$

showing that the element x/y in integral over $R[B_1/y]$.

PROOF OF (V). It suffices to note that

$$\mathfrak{W}(A) = \bigcup_{0\neq x\in A_1} \mathfrak{V}(R[A_1/x]) \quad \text{and} \quad \mathfrak{W}(R,I) = \bigcup_{0\neq x\in I} \mathfrak{V}(R[I/x])$$

where

$$A_1 = \{xZ : x \in I\} \text{ with } A_1/x = \{z/x : z \in A_1\} \text{ and } I/x = \{y/x : y \in I\}.$$

PROOF OF (VI). By taking $(B, A) = (E(I), R[Z])$ in (III), to prove the first assertion, it suffices to show that, given any $e \in \mathbb{N}$ and $x = rZ^e$ with $r \in R$ such that $x/E(I)$ is integral, we have that $r \in I^e$. Now we get

$$(rZ^e)^m + \sum_{1\le i\le m} \alpha_i (rZ^e)^{m-i} = 0 \quad \text{with} \quad m \in \mathbb{N}_+ \quad \text{and} \quad \alpha_i \in E(I).$$

For $1 \le i \le m$ we have $\alpha_i = \sum_{n\in\mathbb{N}} \alpha_{in} Z^n$ with $\alpha_{in} \in I^n$, and hence by equating the coefficients of Z^{em} on both sides of the above displayed equation we obtain

$$r^m + \sum_{1\le i\le m} \alpha_{ie} r^{m-i} = 0$$

and therefore by the normality of I we conclude that $r \in I^e$.

In view of (4.5), the rest now follows from (I), (IV) and (V).

LEMMA (8.2). Let I be any nonzero complete ideal in a two dimensional regular local domain R. Then I is a normal ideal in R and we have $\mathfrak{W}(R,I)^{\mathfrak{N}} = \mathfrak{W}(R,I)$. In view of (3.2) this completes the proof of ZQT(IV).

PROOF. I is normal by Theorem $2'$ on page 385 of volume II of [Zar], and hence we are done by (8.1)(VI).

LEMMA (8.3). Let R be a two dimensional regular local domain with maximal ideal $M = M(R)$ and quotient field L. Let J and I be nonzero ideals in R. Then we have the following.

(I) Assume that J/I is a reduction and let $\overline{J} = (R,S)(J)$ with $\overline{I} = (R,S)(I)$ where $S \in Q(R)$. Then $\overline{J}/\overline{I}$ is a reduction. Moreover, if $\overline{I} = M(S)$ then $J = M(S)$.

Furthermore, if $\overline{I} = M(S)$ and $J = (x, y)$ with $x \neq 0 \neq y$ in R then upon letting $z = x/y$ and $V = o(S)$ we have $z \in V$ and $H(V) = H_V(S)(H_V(z))$,

(II) Assume that $J = (x, y)R$ with $x \neq 0 \leq y$ in R, and let $z = x/y$. Then $\mathfrak{D}(R, z) = (\mathfrak{W}(R, J)_1^{\Delta})^{\mathfrak{N}}$. Moreover, $\mathfrak{D}(R, z) = \emptyset \Leftrightarrow J$ is principal $\Leftrightarrow$ either $z \in R$ or $1/z \in R$. Furthermore, if I is the integral closure of J in R, i.e., equivalently if I/J is integral and I is complete, then $\mathfrak{D}(R, z) = \mathfrak{W}(R, I)_1^{\Delta}$.

(III) Assume that $I = \overline{\zeta}_R(U)$ where U is a nonempty finite subset of $D(R)^{\Delta}$. Also assume that J/I^c is a reduction for some $c \in \mathbb{N}_+$ where $c = 1$ in case R/M is infinite. Finally assume that $J = (x, y)R$ with $x \neq 0 \neq y$ in R, and let $z = y/x$. Then $\mathfrak{D}(R, z) = U$. Moreover, if R/M is infinite then for every $V \in U$ we have $z \in V$ with $H(V) = K'(H_V(z))$ where $H_V : V \to H(V) = V/M(V)$ is the residue class epimorphism and K' is the relative algebraic closure of $H_V(R)$ in $H(V)$.

(IV) Assume that $J = (x, y)R$ with $x \neq 0 \neq y$ in R, and let $z = x/y$. Let I be the integral closure of J in R. Also let U be a nonempty finite subset of $D(R)^{\Delta}$, Then $z \in \mathfrak{D}^*(R, U) \Leftrightarrow \overline{\eta}(I) = U$.

PROOF OF (I). Upon letting $(R_j)_{0 \leq j \leq \nu}$ be the finite QDT sequence of R along $V = o(R)$ we have $R = R_0$ and $S = R_\nu$.

Note that for any overring S of R we have $JI^n = I^{n+1} \Rightarrow (JS)(IS)^n = (IS)^{n+1}$. Moreover if $S \in Q_1(R)$ then $JI^n = I^{n+1} \Rightarrow \mathrm{ord}_R J = \mathrm{ord}_R I = (\text{ say })e$ and dividing both sides of the equation $(JS)(IS)^n = (IS)^{n+1}$ by x^e where $x \in M \setminus M^2$, we get $(JS/x^e)(IS/x^e)^n = (IS)^{n+1}$, i.e., $\overline{J}\overline{I}^n = \overline{I}^{n+1}$. This shows that if $\nu = 1$ then $\overline{J}/\overline{I}$ is a reduction. Therefore by induction on ν we see that $\overline{J}/\overline{I}$ is a reduction in the general case.

The "Furthermore" follows from the "Moreover." Also the "Moreover" in the general case follows from the "Moreover" in the case of $\nu = 0$. Consequently it only remains to show that if J/M is a reduction then $J = M$. But this clearly follows from (6.1) + Nakayama by noting that if B is a subring of a finite variable polynomial ring $A = k[Z_1, \ldots, Z_r]$ over a field k such that A/B is integral and B is generated over k by homogeneous polynomials of degree one then we must have $B = A$.

PROOF OF (II). In view of (5.6)($\dagger^*$) of [Ab5], everything is straightforward except the "Furthermore" which follows from (8.1)(VI) and Theorem 1 on page 350 of volume II of [Zar].

PROOF OF (III). In view of ZQT(I) and ZQT(II), this follows from (8.3)(I) and (8.3)(II).

PROOF OF (IV). Follows from (8.3)(II).

REMARK (8.4). (8.3)(II) suggests an extension of the definition of dicritical divisors by taking any nonzero ideal J in any local domain R of dimension at least two and putting $\mathfrak{D}(R,J) = (\mathfrak{W}(R,J)_1^\Delta)^\mathfrak{N}$ and calling the members of this finite set the **dicritical divisors** of J in R.

Section 9: Proof of ET and Answer to EQ. In (9.1) we shall prove ET and in (9.2) we shall answer EQ.

PROOF OF ET (9.1). Now R is a two dimensional regular local domain with quotient field L and maximal ideal $M = M(R)$, and we are given a finite subset U of $D(R)^\Delta$. We want to find $z \in L^\times$ such that $\mathfrak{D}(R,z) = U$ and such that if R/M is infinite then for every $V \in U$ we have $z \in V$ with $H(V) = K'(H_V(z))$ where $H_V : V \to H(V) = V/M(V)$ is the residue class epimorphism and K' is the relative algebraic closure of $H_V(R)$ in $H(V)$. If $U = \emptyset$ then, in view of what is said at the end of (3.1), it suffices to take z to be any element of $L^\times$ such that either $z \in R$ or $1/z \in R$. If $U \neq \emptyset$ then, in view of NRT and the (8.3)(III) incarnation of ZQT, we are done by taking $I = \overline{\zeta}_R(U)$.

ANSWER TO EQ (9.2). If $U = \emptyset$ then, in view of what is said at the end of (3.1), $\mathfrak{D}^*(R,U)$ is the set of all $z \in L^\times$ such that either $z \in R$ or $1/z \in R$. If $U \neq \emptyset$ then, in view of (8.3)(IV), $\mathfrak{D}^*(R,U)$ may be described as the set of all $z = x/y$, where $x \neq 0 \neq y$ are elements in R such that for the integral closure I of the ideal $J = (x, y)R$ in R we have $\overline{\eta}_R(I) = U$.

References

[Ab1] S. S. Abhyankar, *On the valuations centered in a local domain,* American Journal of Mathematics, vol 78 (1956), pages 321-348.

[Ab2] S. S. Abhyankar, *Ramification Theoretic Methods in Algebraic Geometry,* Princeton University Press, 1959.

[Ab3] S. S. Abhyankar, *Resolution of Singularities of Embedded Algebraic Surfaces,* First Edition of 1966 Published by Academic Press, Second Enlarges Edition of 1998 Published by Springer-Verlag.

[Ab4] S. S. Abhyankar, *Lectures on Algebra I,* World Scientific, 2006.

[Ab5] S. S. Abhyankar, *Inversion and Invariance of Characteristic Terms Part I,* Developments in Mathematics, vol. xx (2010), pages xyz, Springer.

[Art] E. Artal-Bartolo, *Une démonstration géométrique du théorèm d'Abhyankar-Moh,* Crelle Journal, vol 464 (1995), pages 97-108.

[EiN] D. Eisenbud and W. D. Neumann, *Three-dimensional link theory and invariants of plane curve singularities,* Annals of Mathematics Studies, vol 101 (1985).

[Fou] L. Fourrier, *Topologie d'un polynome de deux variables complexes au voisinage de l'infini,* Annales de l'institut Fourier, vol 46 (1996), pages 645-687.

[LeW] D. T. Le and C. Weber *A geometrical approach to the jacobian conjecture for $n = 2$,* Kodai Journal of Mathematics, vol 17 (1994), pages 375-381.

[MaM] J. F. Mattei and R. Moussu, *Holonomie et intégrales premières,* Ann. Scient. Écoles Norm. Sup., vol 13 (1980), pages 469-523.

[Nag] M. Nagata, *Local Rings,* Wiley, 1962.

[NoR] D. G. Northcott and D. Rees, *Reductions of ideals in local rings,* Proc. Cambridge Philos. Soc., vol. 50 (1954), pages 145–158.

[Zar] O. Zariski and P. Samuel, *Commutative Algebra, Volumes I and II,* Springer-Verlag, 1975.

Mathematics Department, Purdue University, West Lafayette, IN 47907, USA
E-mail address: ram@cs.purdue.edu, heinzer@math.purdue.edu