Conductors in mixed characteristic

To Craig Huneke, on the occasion of his sixty-fifth birthday

Daniel Katz[1]

Department of Mathematics, University of Kansas, Lawrence, KS 66045

Abstract

In this paper we study conductors that occur in an integral extension of an unramified regular local ring S of mixed characteristic $p > 0$ obtained by adjoining a p^nth root ω of an element of S. We calculate the primary decomposition of the conductor of the integral closure of $S[\omega]$ and give some applications of this calculation. In particular, we show that under certain special circumstances, the integral closure of $S[\omega]$ admits a finitely generated, maximal Cohen-Macaulay module.

1. Introduction

Let S be an unramified regular local ring of mixed characteristic $p > 0$ and R the integral closure of S in a finite extension of the quotient field of S. Since the quotient field of S has characteristic zero, R is a finite S-module. Let ω be an integral primitive element for the extension of quotient fields and write J for the conductor of R into $S[\omega]$. The purpose of this note is to examine the structure of J when $w^{p^n} = f \in S$. By calculating the primary decomposition of J for such extensions with $n = 1$, in [6] the present author was able to construct a finitely generated birational maximal Cohen-Macaulay module over R. Note that R is not automatically Cohen-Macaulay for such an extension. The purpose of this note is to take the first step towards a more general result by calculating the primary decomposition for the conductor in the case $\omega^{p^n} = f$ when $n \geq 1$. This is done in section three. As in [6], to obtain our results, we rely on the fact that $R = J^{-1}$. While at present we are not able to construct a finitely generated maximal Cohen-Macaulay module for general R when $\omega^{p^n} = f$, we can give some sufficient conditions for the existence of such a module in some special cases. In particular, in section four, we show that R is a free S-module in each of the following cases: f is square-free, f is not a pth power modulo p, or the p-adic order of f is relatively prime to p. We also show that if the unique prime ideal P in $S[\omega]$ lying over pS is the P-primary component of J and $S[\omega]/P$ is integrally closed, then the main theorem in [6] extends for certain roots of higher order. In section five we illustrate some of our results with specific examples.

2. Preliminaries

In this section we will establish our notation and present a few preliminary observations. It turns out that many of our results do not require our base ring S to be an unramified regular local ring of mixed characteristic p, but rather that it have two crucial properties enjoyed by such a ring, namely, that for the prime $p > 0$, pS is a prime ideal and S/pS is integrally closed. *The following will remain in effect throughout this paper.* S will denote a Noetherian normal domain. Write L for the quotient field of S and assume $char(L) = 0$. Fix $p \in \mathbb{Z}$ a prime and assume either that p is a unit in S or pS is a (proper) prime ideal and S/pS is integrally closed. Let W be an indeterminate and take $f \in S$ not a pth power. Then

Email address: dlk53@ku.edu (Daniel Katz)

$F(W) := W^{p^n} - f \in S[W]$ is a monic irreducible polynomial. Let R denote the integral closure of S in $K := L(\omega)$, for ω a root of $F(W)$. Thus, R is the integral closure of $S[\omega]$. Note that if p is a unit in S and f is square-free, i.e., $f_Q = Q_Q$ in S_Q for all height-one primes Q containing f, then $R = S[\omega]$. We will use this fact (and minor variants of it) below.

Our basic strategy in this paper is to exploit the fact that R can be realized as J^{-1} for a suitable ideal $J \subseteq S[\omega]$. Recall that for an integral domain A with quotient field E, if $J \subseteq A$ is an ideal, then J^{-1} denotes the set of elements $\alpha \in E$ such that $J \cdot \alpha \subseteq A$. Since S is integrally closed, $S[\omega]$ is a free S-module and therefore satisfies Serre's condition S_2. It follows that C^{-1} satisfies S_2 as an $S[\omega]$-module, for any ideal $C \subseteq S[\omega]$. If C^{-1} happens to be a ring, then C^{-1} satisfies S_2 both as an $S[\omega]$-module and as a ring (see the proposition below). This means that in constructing a prospective candidate for R, if the candidate is J^{-1} for some J, then only Serre's condition R_1 must be checked.

The following proposition summarizes the conditions relating R to J^{-1} for suitable J that we will call upon in the next section. Part (i) of the proposition is well known to experts, but we have included it for lack of a suitable reference. We will see in the next section that part (iv) of the proposition plays a key role in calculating the primary components of J, since it turns out that the pre-images of these components in $S[W]$ are grade two perfect ideals.

Proposition 2.1. *Let A be a Noetherian domain satisfying S_2 and assume that A', the integral closure of A, is a finite A-module.*

(i) For an ideal $C \subseteq A$, C^{-1} satisfies S_2 as an A-module. If C^{-1} is a ring, then C^{-1} also satisfies S_2 as a ring.

(ii) Suppose $\{P_1, \dots, P_n\}$ are the height-one primes of A for which A_{P_i} is not a DVR. If for each $1 \leq i \leq n$, $J_i \subseteq A$ is P_i-primary and $(J_i^{-1})_{P_i} = A'_{P_i}$, then $A' = J^{-1}$ for $J := J_1 \cap \cdots \cap J_n$.

(iii) If $A \neq A'$, then $A' = J^{-1}$, for some height-one unmixed ideal $J \subseteq A$.

(iv) Suppose that $A = B/(F)$ for $F \in B$ a principal prime and $\tilde{J} \subseteq B$ is a grade-two ideal arising as the ideal of $n \times n$ minors of an $(n+1) \times n$ matrix ϕ. Assume further that $F \in \tilde{J}$ and set $J := \tilde{J}/(F)$. Let $\Delta_1, \dots, \Delta_{n+1}$ denote the signed minors of ϕ, write $F := b_1\Delta_1 + \cdots + b_{n+1}\Delta_{n+1}$ and let ϕ' denote the $(n+1) \times (n+1)$ matrix obtained by augmenting the column of b_i's to ϕ (so F is the determinant of ϕ'). Then J^{-1} can be generated as an A-module by $\{\psi_{1,1}/\delta_1, \dots, \psi_{n+1,n+1}/\delta_{n+1} = 1\}$, where $\psi_{i,i}$ denotes the image in A of the (i,i)th cofactor of ϕ' and δ_i denotes the image of Δ_i in A (which we assume to be non-zero). Moreover, $p.d._B(J) = p.d._B(J^{-1}) = 1$. Here $p.d._B(J)$ denotes the projective dimension of J as a B-module.

Proof. For part (i), we prove the case that C^{-1} is a ring. The first statement of part (i) follows in a similar fashion. If $C^{-1} = A$, there is nothing to prove, so we assume $C^{-1} \neq A$. Take $v \in C^{-1}$ and assume $P \subseteq C^{-1}$ belongs to $\mathrm{Ass}(C^{-1}/vC^{-1})$. Thus, C_P^{-1} has depth one and therefore P is an associated prime of any principal ideal contained in P. Since $P \cap A \neq 0$, we may assume $v \in A$. Let $Q = P \cap A$. Without loss of generality, we may assume that A is local at Q. Write $P = (vC^{-1} : u)$, for some $u \in C^{-1}$. Then $Qu \subseteq vC^{-1}$. Thus, $Q(uC) \subseteq vA$. Note that uC is an ideal of A. Moreover, $uC \not\subseteq vA$, otherwise, $C \cdot (u/v) \subseteq A$, in which case $u/c \in C^{-1}$ and thus $u \in vC^{-1}$, a contradiction. Therefore, Q consists of zerodivisors on A/vA, and hence $Q \in \mathrm{Ass}(A/vA)$. Since A satisfies S_2, $\mathrm{height}(Q) = 1$. On the other hand, C^{-1} is an integral extension of A (it is finite over A), so $\mathrm{height}(P) = 1$, which is what we want.

For parts (ii) and (iii), note that since A satisfies S_2, if A is not integrally closed, it fails to satisfy Serre's condition R_1. On the other hand, there are only finitely many height one primes $P \subseteq A$ such that $S[\omega]_P$ is not a DVR, since any such prime must contain the conductor of R into A. For proofs of (ii) and (iii), see Proposition 2.1 in [6]. For the first part of (iv), see [9], Proposition 3.14 or [8], Lemma 2.5. For the second statement in (iv), consult [8], Proposition 3.1. □

Returning to our basic set-up, we note that since S is a normal domain, $S[\omega]$ is free over S and thus satisfies S_2, and since $char(S) = 0$, R is a finite S-module and a finite $S[\omega]$-module. Thus, Proposition 2.1

applies with $A := S[\omega]$. In particular, there exists a height-one, unmixed ideal $J \subseteq S[\omega]$ for which $J^{-1} = R$. Note that J must be the conductor of R into $S[\omega]$. Indeed, J is clearly contained in the conductor, i.e., $J \subseteq (J^{-1})^{-1}$. On the other hand, let Q be a height-one prime containing J. Then $S[\omega]_Q$ is a one-dimensional Gorenstein local domain [1], so

$$J_Q = (J_Q^{-1})^{-1} = ((J^{-1})^{-1})_Q.$$

Since this holds for each Q, we see that $J = (J^{-1})^{-1}$, so that J is the conductor of R into $S[\omega]$. In the next section we will identify the primary components of the ideal $J \subseteq S[\omega]$.

Proposition 2.2. *In the notation above, suppose that p is not a unit in S. Then there is a unique height-one prime in $S[\omega]$ containing p.*

Proof. Suppose $p \mid f$. Then $P := (\omega, p)$ is clearly the unique height-one prime in $S[\omega]$ containing p. Moreover, in this case, $S[\omega]_P$ is a DVR if and only if $p^2 \nmid f$. Suppose $p \nmid f$. If f is not a pth power modulo pS, then f is not a pth power over the quotient field of S/pS (since S/pS is integrally closed) and it follows that $F(W)$ is irreducible mod pS (see [5], Theorem 51). Thus $(p, F(W))S[W]$ is the unique height -two prime in $S[W]$ containing $F(W)$ and p, so $pS[\omega]$ is the unique height-one prime in $S[\omega]$ containing p. Now suppose that $p \nmid f$ and f is a pth power modulo pS. Choose $h \in S$ such that $f \equiv h^{p^t} \pmod{pS}$, but f is not a p^{t+1}st power modulo pS if $t < n$. If f is a p^nth power module pS, we just take $t = n$, even if f is a p^rth power modulo pS, for $r > n$. Set $m := n - t$. Then $W^{p^m} - h$ is the unique irreducible factor of $F(W)$ modulo pS and it follows that $(p, w^{p^m} - h)S[\omega]$ is the unique height-one prime containing pS. Thus, in all cases, there exists a unique height-one prime in $S[\omega]$ lying over pS. ☐

For the remainder of the paper, we denote by P the unique prime in $S[\omega]$ lying over pS. We will also refer to the preimage of P in $S[W]$ as $\tilde{P}$.

Now, suppose $f = h^{p^t} + gp$ $(p \nmid h)$ so

$$P = (\omega^{p^m} - h, p)S[\omega] \text{ and } \tilde{P} = ((W^{p^m} - h, p)S[W].$$

Then

$$F(W) = (W^{p^m})^{p^t} - h^{p^t} - gp = ((W^{p^m})^{p^t - 1} + \cdots + h^{p^t - 1}) \cdot (W^{p^m} - h) - gp.$$

In $S[W]$, $(W^{p^m})^{p^t-1} + \cdots + h^{p^t-1} \equiv p^t h^{p^t-1}$ modulo $(W^{p^m} - h)$, so $(W^{p^m})^{p^t-1} + \cdots + h^{p^t-1}$ belongs to $\tilde{P}$. Thus, $F(W) \in \tilde{P}^2$ if and only if $p \mid g$. In other words, in all cases, P_P is not principal if and only if $f = h^{p^t} + p^2 g$, for some t and some $h, g \in S$. It follows from Proposition 2.1 that this happens if and only if J has a P-primary component.

In order to identify the P-primary component of J in the case that $p \nmid f$, we will need to take into consideration how f factors modulo higher powers of p as well. It so happens that this in turn is determined by the highest power of $\tilde{P}$ containing $F(W)$. To elaborate, suppose that, as above, $p \nmid f$ and $h \in S$ and $t, m \in \mathbb{Z}$ are such that $W^{p^m} - h$ is the unique irreducible factor of $F(W)$ modulo pS and that $f \equiv h^{p^t} \pmod{pS}$. Thus, we may write $F(W) = (W^{p^m})^{p^t} - h^{p^t} - pg$. Set $V := W^{p^m}$, so we have $\tilde{P} = (V - h, p)S[W]$. We wish to identify the largest power of $\tilde{P}$ containing $F(W)$. Set $\tilde{P}_0 := (V - h, p)S[V]$. Since like powers of $\tilde{P}$ contract to like powers of $\tilde{P}_0$, we may work in $S[V]$. [2]

We first note that $V^{p^t} - h^{p^t} \in \tilde{P}_0^{t+1} \backslash \tilde{P}_0^{t+2}$. This follows by an easy induction on t. Since the argument for the base case $t = 1$ and the inductive step are essentially the same, we assume the base case. For the inductive step,

$$V^{p^t} - h^{p^t} = (V^{p^{t-1}} - h^{p^{t-1}})((V^{p^{t-1}})^{p-1} + \cdots + (h^{p^{t-1}})^{p-1}).$$

[1] To see that $S[\omega]_Q$ is Gorenstein, set $q := Q \cap S$. Since height$(q) = 1$, S_q is a DVR. Thus $S_q[W]$ is a regular domain and hence $S[\omega]_Q = (S_q[W]/(F(W)))_Q$ is Gorenstein.

[2] The extension $S[V] \subseteq S[W]$ is a finite extension, so $\tilde{P}_0^n S[W] \cap S[V] = \tilde{P}^n \cap S[V]$ is contained in the integral closure of $\tilde{P}_0^n$. Since $\tilde{P}_0$ is a prime ideal generated by a regular sequence, its powers are integrally closed, thus $\tilde{P}^n \cap S[V] = \tilde{P}_0^n$, for all n.

By induction, the first term on the right hand side in the equation above belongs to $\tilde{P}_0^t \backslash \tilde{P}_0^{t+1}$, so it suffices to show that the second term belongs to $\tilde{P}_0 \backslash \tilde{P}_0^2$ (recall, $\tilde{P}_0$ is generated by a regular sequence). Upon setting $V = h$, the second term becomes $p \cdot h^{(p^{t-1}) \cdot (p-1)}$, which shows what we want (since $p \nmid h$). In other words, $V^{p^t} - h^{p^t} \in \tilde{P}_0^{t+1} \backslash \tilde{P}_0^{t+2}$.

We now note that $F(V) = V^{p^t} - h^{p^t} - pg \notin \tilde{P}_0^{t+2}$. If $F(V) \in \tilde{P}_0^{t+2}$, upon setting $V = h$, we get $pg \in p^{t+2}S$ which implies $V^{p^t} - h^{p^t} \in \tilde{P}_0^{t+2}$, a contradiction. Now we show $F(V) \in \tilde{P}_0^{i+1}$ if and only if $p^i \mid g$, for $i \leq t$. If $F(V) \in \tilde{P}_0^{i+1}$, then $pg \in \tilde{P}_0^{i+1}$, since $V^{p^t} - h^{p^t} \in \tilde{P}_0^{t+1}$. Thus, $pg \in p^{i+1}S$ (since S is normal), which gives what we want. The converse is similar. Thus, we have that for some $0 \leq k \leq t$, $F(W) \in \tilde{P}^{k+1} \backslash \tilde{P}^{k+2}$, in which case $f = h^{p^t} + p^{k+1}g$, for some $h, g \in S$. Morever, $p \nmid h$ and $p \nmid g$ if $k < t$.

Therefore, in the case that $p \nmid f$, *we will adopt the following conventions once and for all.*

Convention. In the notation above, assume p is not a unit in S and $p \nmid f$. We assume that t, m and h have been chosen so that $W^{p^m} - h$ is the unique irreducible factor of $F(W)$ modulo p and that $f \equiv h^{p^t}$ (mod pS), so $n = m + t$. We select $0 \leq k \leq t$ such that $F(W) \in \tilde{P}^{k+1} \backslash \tilde{P}^{k+2}$. This means that we can write $f = h^{p^t} + p^{k+1}g$, where $p \nmid g$ if $k < t$.

3. Primary components of the conductor

In this section we identify the primary components of J ($J^{-1} = R$) in each of the following cases: f can be written as a product of primes and $p \nmid f$ or f can be written as a product of primes and the p-adic order of f is relatively prime to p. As noted in the previous section, there is a unique height-one prime $P \subseteq S[\omega]$ lying over pS and J has a P-primary component if and only if f is a pth power modulo p^2S. When f can be written as a product of primes, and $q \neq p$ is one of the factors, then clearly $Q := (\omega, q)S[\omega]$ is the unique height-one prime in $S[\omega]$ containing q. Moreover, $S[\omega]_Q$ is not a DVR if and only if $q^2 \mid f$. It follows that J has a Q-primary component whenever $q^2 \mid f$. Thus we see that if $p \nmid f$, then J has at most one primary component corresponding to the prime pS and exactly one primary component for every principal prime in S whose square divides f. Similarly, one can see that if $p \mid f$, then J has exactly one primary component for every prime (including p) whose square divides f. We now proceed to describe the primary components of J. We start with an easy lemma.

Lemma 3.1. *Suppose $p > 2$ is not a unit in S. Take $h \in S \backslash pS$ and write $p = 2l + 1$. Set $V := W^{p^m}$ and $\tilde{P} := (V - h, p)S[W]$. For $s \geq 0$, define*

$$C(s) := \frac{1}{p \cdot (V^{p^s} - h^{p^s})} \cdot \sum_{j=1}^{l} (-1)^{j+1} \binom{p}{j} (V^{p^s} \cdot h^{p^s})^j [(V^{p^s})^{p-2j} - (h^{p^s})^{p-2j}].$$

Then $C(s) \notin \tilde{P}$.

Proof. Note that since p divides $\binom{p}{j}$ for all $1 \leq j \leq l$, and $V^{p^s} - h^{p^s}$ divides $(V^{p^s})^j - (h^{p^s})^j$, $C(s)$ is a well-defined element of $S[W]$. Now, $C(s) \notin \tilde{P}$ if and only if the residue class of $C(s)$ modulo $V - h$, as an element of S, does not belong to pS. This happens if and only if

$$\sum_{j=1}^{l} (-1)^{j+1} \binom{p}{j} \frac{(h^{p^s})^{2jp^s + p - 2j - 1}}{p} (p - 2j) = \sum_{j=1}^{l} (-1)^{j+1} \binom{p}{j} (h^{p^s})^{2jp^s + p - 2j - 1} (1 - \frac{2j}{p})$$

as an element of S, is not divisible by p. Since

$$\sum_{j=1}^{l} (-1)^{j+1} \binom{p}{j} (h^{p^s})^{2jp^s + p - 2j - 1}$$

is divisible by p and each $(h^{p^s})^{2jp^s+p-2j-1}$ is not divisible by p, it's enough to show that

$$\sum_{j=1}^{l}(-1)^{j+1}\binom{p}{j}\frac{2j}{p}$$

is not divisible by p, as an element of S. However,

$$\sum_{j=1}^{l}(-1)^{j+1}\binom{p}{j}\frac{2j}{p} = 2\cdot\sum_{j=1}^{l}(-1)^{j+1}\binom{p-1}{j-1} = (-1)^{l+1}\binom{2l}{l}.$$

Because p does not divide $\binom{2l}{l}$ in $\mathbb{Z}$, p does not divide $\binom{2l}{l}$ as an element of S (since $pS \neq S$). Thus $C(s) \notin \tilde{P}$, as claimed. $\square$

Lemma 3.2. *Let A be a Noetherian domain satisfying S_2, $Q \subseteq A$ a height-one prime and $I \subseteq Q$ a height-one ideal. Suppose that Q is the only height-one prime containing I for which A_Q is not a DVR. Suppose $\tau \in I^{-1}\backslash A$ satisfies $g(T) := T^2 - cT - q = 0$, where $c \in A\backslash Q$ and $q \in Q$. Then $A[\tau]$ has exactly two height-one primes lying over Q, namely $Q_1 := (Q,\tau)A[\tau]$ and $Q_2 := (Q, \tau - c)A[\tau]$.*

Proof. Let $H \subseteq A[T]$ denote the kernel of the canonical map from $A[T]$ to $A[\tau]$ taking T to τ. Clearly $\tilde{Q}_1 := (Q,T)A[T]$ and $\tilde{Q}_2 := (Q, T-c)A[T]$ are the unique height two primes in $A[T]$ containing Q and $g(T)$. If we show that $H \subseteq \tilde{Q}_1 \cap \tilde{Q}_2$, then Q_1 and Q_2 are the required primes. Clearly, $H \subseteq \tilde{Q}_1$ or $H \subseteq \tilde{Q}_2$. We now show that $H \subseteq \tilde{Q}_1$ if and only if $H \subseteq \tilde{Q}_2$, which will complete the proof. For this, we claim that whenever $aT + b \in H$, then $a \in Q$. Suppose the claim holds. If $H \subseteq \tilde{Q}_1$, to see that $H \subseteq \tilde{Q}_2$, it suffices to show that any linear polynomial in H belongs to $\tilde{Q}_2$ (since $g(T) \in \tilde{Q}_2$). Let $aT + b \in H$. By our claim, $a \in Q$, so $b \in \tilde{Q}_1 \cap S = Q$. Thus, $aT + b \in QS[T] \subseteq \tilde{Q}_2$. The converse is similar. For the claim, suppose $aT + b \in H$. Then $\tau = \frac{-b}{a}$, so $I \subseteq (aA : b)$. Since A satisfies S_2, any prime minimal over $(aA : b)$ has height one. By our assumption on I, Q is the only such prime. Hence $(aA : b) \subseteq Q$, so $a \in Q$, as required. $\square$

In the next proposition, and in several subsequent instances, we will use the following observation. Let

$$A = \begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 \\ b_1 & a_2 & \cdots & 0 & 0 \\ 0 & b_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{c-1} & 0 \\ 0 & 0 & \cdots & b_{c-1} & a_c \\ 0 & 0 & \cdots & 0 & b_c \end{pmatrix}$$

be a $(c+1)\times c$ matrix with entries in S. If δ_i denotes the determinant obtained by deleting the i^{th} row of A, then then $\delta_1 = b_1\cdots b_n$ and $\delta_i = a_1\cdots a_{i-1}b_i\cdots b_n$, for $i \geq 2$.

Proposition 3.3. *Assume that $p \nmid f$, $p > 2$ and $f = h^{p^t} + p^{k+1}g$, for $k \geq 1$ and t adhering to our conventions established above. Thus, $F(W) \in \tilde{P}^{k+1}\backslash\tilde{P}^{k+2}$, for some $1 \leq k \leq t$. Set $\nu := \omega^{p^m}$ and for each $1 \leq j \leq k$ set*

$$\tau_j := \frac{p^{k-j+1}g}{\nu^{p^{t-j}} - h^{p^{t-j}}} = \frac{(\nu^{p^{t-j}})^{p^j-1} + \cdots + (h^{p^{t-j}})^{p^j-1}}{p^j}$$

and

$$I_j := (\nu^{p^{t-1}} - h^{p^{t-1}}, p(\nu^{p^{t-2}} - h^{p^{t-2}}), \ldots, p^{j-1}(\nu^{p^{t-j}} - h^{p^{t-j}}), p^j)S[\omega].$$

Then

(i) I_j^{-1} is generated as an $S[\omega]$-module by $1, \tau_1, \ldots, \tau_j$.

(ii) $I_j^{-1} = S[\omega, \tau_1, \ldots, \tau_j]$.

(iii) $(I_k^{-1})_Q$ *is a DVR for all height-one primes* $Q \subseteq I_k^{-1}$ *containing* P.

(iv) I_k *is* P*-primary.*

Moreover, I_k *is the* P*-primary component of* J*, the conductor of of* R *into* $S[\omega]$*.*

Proof. We first note that the final statement follows from statements (iii) and (iv). To see this, by (iv), I_k is P-primary. Since $(I_k)^{-1}$ satisfies S_2 (by Proposition 2.1), $R_P = (I_k^{-1})_P$ by (iii). Thus, $(J^{-1})_P = (I_k^{-1})_P$, from which it follows that $J_P = (I_k)_P$ - since $J_P = (J^{-1})_P^{-1}$ and $(I_k)_P = (I_k^{-1})_P^{-1}$ - which gives what we want.

We now proceed to proofs of parts (i)-(iv). For (i), we set $L(i) := (\nu^{p^i})^{p-1} + \cdots + (h^{p^i})^{p-1}$ for any $0 \leq i \leq t$. An easy calculation gives that

$$\nu^{p^i} - h^{p^i} = L(i-1) \cdot L(i-2) \cdots L(i-s)(\nu^{p^{i-s}} - h^{p^{i-s}}),$$

for $1 \leq s \leq i$. It follows that (up to changes of sign) I_j is the ideal of $j \times j$ minors of the $(j+1) \times j$ matrix

$$\phi_j := \begin{pmatrix} -p & 0 & \cdots & 0 & 0 \\ L(t-2) & -p & \cdots & 0 & 0 \\ 0 & L(t-3) & \cdots & 0 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & \cdots & -p & 0 \\ 0 & 0 & \cdots & L(t-j) & -p \\ 0 & 0 & \cdots & 0 & \nu^{p^{t-j}} - h^{p^{t-j}} \end{pmatrix}.$$

Let ϕ_j' denote the $(j+1) \times (j+1)$ matrix obtained by augmenting the column that is the transpose of the row vector

$$(L(t-1)\ 0\ \cdots\ 0\ -p^{k+1-j}g),$$

after the last column of ϕ_j. If we apply Proposition 2.1 with $B := S[W]$, $A := S[\omega]$, $\tilde{\phi}_j$ the inverse image of ϕ_j and $\tilde{\phi}_j'$ the inverse image of ϕ_j', we get that I_j^{-1} is generated by the fractions $\frac{c_i}{d_i}$, where c_i is the (i,i)th cofactor of ϕ_j' and d_i is (up to a sign) the ith minor of ϕ_j. But $\frac{c_i}{d_i} = \tau_i$, for $1 \leq i \leq j$ and $\frac{c_{j+1}}{d_{j+1}} = 1$, which yields (i).

For (ii) we will show that $\tau_i \cdot \tau_j \in I_j^{-1}$, for all $1 \leq i \leq j \leq k$. However, we first note that for all s, $L(s) = (\nu^{p^s} - h^{p^s})^{p-1} + p \cdot c(s)$, where $c(s)$ denotes the image in $S[\omega]$ of the element $C(s)$ defined in Lemma 3.1. Indeed,

$$\begin{aligned} L(s) &= \frac{L(s) \cdot (\nu^{p^s} - h^{p^s})}{\nu^{p^s} - h^{p^s}} \\ &= \frac{\nu^{p^{s+1}} - h^{p^{s+1}}}{\nu^{p^s} - h^{p^s}} \\ &= \frac{(\nu^{p^s} - h^{p^s})^p + \sum_{j=1}^{p-1} (-1)^{j+1} \binom{p}{j} (\nu^{p^s})^{p-j} (h^{p^s})^j}{\nu^{p^s} - h^{p^s}} \\ &= (\nu^{p^s} - h^{p^s})^{p-1} + \frac{\sum_{j=1}^{l} (-1)^{j+1} \binom{p}{j} (\nu^{p^s} \cdot h^{p^s})^j [(\nu^{p^s})^{p-2j} - (h^{p^s})^{p-2j}]}{\nu^{p^s} - h^{p^s}} \\ &= (\nu^{p^s} - h^{p^s})^{p-1} + p \cdot c(s). \end{aligned}$$

We now proceed by induction on j. Suppose $j = 1$. On the one hand, we have

$$(\nu^{p^{t-1}} - h^{p^{t-1}}) \cdot \tau_1 = (p^{k-1}g) \cdot p.$$

On the other hand,

$$p \cdot \tau_1 = L(t-1) = (\nu^{p^{t-1}} - h^{p^{t-1}})^{p-2} \cdot (\nu^{p^{t-1}} - h^{p^{t-1}}) + c(t-1) \cdot p.$$

Thus, by the usual determinant argument, τ_1 satisfies a degree two polynomial with coefficents in $S[\omega]$. Therefore $I_1^{-1} = S[\omega, \tau_1]$, which is what we want. In fact, we have the following equations:

$$\tau_1(\tau_1 - c(t-1)) = p^{k-1} g(\nu^{p^{t-1}} - h^{p^{t-1}})^{p-2} \text{ and } p(\tau_1 - c(t-1)) = (\nu^{p^{t-1}} - h^{p^{t-1}})^{t-1}. \tag{*}$$

Now suppose $j > 1$. We will show that $\tau_i \cdot \tau_j \in I_J^{-1}$ for all $i \leq j$ by a second induction on i. In fact, taking $0 \leq i < j$ (and $\tau_0 := 1$), we have

$$\begin{aligned}
\tau_{i+1} \cdot \tau_j &= \frac{p^{k-i} g}{\nu^{p^{t-i-1}} - h^{p^{t-i-1}}} \cdot \frac{p^{k-j+1} g}{\nu^{p^{t-j}} - h^{p^{t-j}}} \\
&= p^{k-j-i} g \cdot \frac{p^{k+1} g}{(\nu^{p^{t-j}} - h^{p^{t-j}}) \cdot (\nu^{p^{t-i-1}} - h^{p^{t-i-1}})} \\
&= p^{k-j-i} g \cdot \frac{\nu^{p^t} - h^{p^t}}{(\nu^{p^{t-j}} - h^{p^{t-j}}) \cdot (\nu^{p^{t-i-1}} - h^{p^{t-i-1}})} \\
&= p^{k-j-i} g \cdot \frac{((\nu^{p^{t-i}})^{p^i - 1} + \cdots + (h^{p^{t-i}})^{p^i - 1}) \cdot (\nu^{p^{t-i}} - h^{p^{t-i}})}{(\nu^{p^{t-j}} - h^{p^{t-j}}) \cdot (\nu^{p^{t-i-1}} - h^{p^{t-i-1}})} \\
&= g p^{k-j} \cdot \tau_i \cdot \frac{\nu^{p^{t-i}} - h^{p^{t-i}}}{(\nu^{p^{t-j}} - h^{p^{t-j}}) \cdot (\nu^{p^{t-i-1}} - h^{p^{t-i-1}})} \\
&= g p^{k-j} \cdot \tau_i \cdot \frac{L(t-i-1)}{\nu^{p^{t-j}} - h^{p^{t-j}}} \\
&= g p^{k-j} \cdot \tau_i \cdot \frac{(\nu^{p^{t-i-1}} - h^{p^{t-i-1}})^{p-1} + p \cdot c(t-i-1)}{\nu^{p^{t-j}} - h^{p^{t-j}}} \\
&= g p^{k-j} \cdot \tau_i \cdot A(i+1, j) + \tau_i \cdot \tau_j \cdot c(t-i-1),
\end{aligned}$$

where for all $r \leq j$, $A(r, j) := \frac{(\nu^{p^{t-r}} - h^{p^{t-r}})^{p-1}}{\nu^{p^{t-j}} - h^{p^{t-j}}} \in P$. Thus

$$\tau_{i+1} \cdot \tau_j = g p^{k-j} \cdot \tau_i + \tau_i \cdot \tau_j \cdot c(t-i-1), \tag{**}$$

so induction yields $\tau_i \cdot \tau_j \in I_J^{-1}$ for all $i \leq j$, as required. Therefore, $I_j^{-1} = S[\omega, \tau_1, \ldots, \tau_j]$ and statement (ii) has been verified.

For (iii), we will show that, starting with $j = 0$, each I_j^{-1} has only one height-one prime, P_j, lying over P and satisfying $(I_j^{-1})_{P_j}$ is not a DVR and that I_{j+1}^{-1} has two height-one primes lying over P_j, one of which is P_{j+1} and the other, P'_{j+1}, has the property that $(I_{j+1}^{-1})'_{P_{j+1}}$ is a DVR. When $j = k$, $(I_k^{-1})_{P_k}$ is also a DVR. This will prove the third claim. When $j = 0$, we take $I_0 := S[\omega]$ and $P_0 := P$.

Now, if we combine Lemmas 3.1 and 3.2 with the first equation in (*), we get that $P_1 := (P, \tau_1 - c(t-1))$ and $P'_1 := (P, \tau_1)$ are the unique height-one primes in I_1^{-1} lying over P. The two equations in (*) show that $(P'_1)_{P'_1} = (\nu - h)_{P'_1}$, while the first equation in (*) gives $(P_1)_{P_1} = (\nu - h, p)_{P_1}$. Thus, $(I_1^{-1})_{P'_1}$ is a DVR and hence, in any integral extension of I_1^{-1}, if we localize at any prime lying over P'_1 we get a DVR.
For $j = 2$, we use (**) to get

$$\tau_2 = c(t-2)\tau_1 \cdot \tau_2 + A(2,2) \cdot g p^{k-2} \cdot \tau_1. \tag{$\star$}$$

By Lemmmas 3.1 and 3.2, the height-one primes in I_2^{-1} lying over $P_1 \subseteq I_1^{-1}$ are $P'_2 := (P_1, \tau_2)$ and $P_2 := (P_1, \tau_2 - \tau_1 \cdot c(t-2))$. Since $\tau_2 - \tau_1 \cdot c(t-2) \notin P'_2$, ($\star$) gives $\tau_2 \in (p, \nu - h)_{P'_2}$ (recalling $(P_1)_{P_1} = (p, \nu - h)_{P_1}$). Moreover,

$$p \cdot \tau_2 = L(t-2) \cdot \tau_1 = \{(\nu^{p^{t-2}} - h^{p^{t-2}})^{p-1} + p \cdot c(t-2)\} \cdot \tau_1,$$

so

$$p \cdot (\tau_2 - c(t-2) \cdot \tau_1) = (\nu^{p^{t-2}} - h^{p^{t-2}}) \cdot \tau_1.$$

Therefore, $p \in (\nu - h)_{P_2'}$, so $(P_2')_{P_2'} = (\nu - h)_{P_2'}$. That is, $(I_2^{-1})_{P_2'}$ is a DVR (and hence, $(I_2^{-1})_Q$ is a DVR for all height-one primes $Q \subseteq I_2^{-1}$ lying over P, save P_2.) Moreover, $(\star)$ shows that $(P_2)_{P_2} = (p, \nu - h)_{P_2}$ (since $\tau_2 \notin P_2$ and $(P_1)_{P_1} = (p, \nu - h)_{P_1}$.

If we continue inductively, we get that I_{k-1}^{-1} has one height-one prime

$$P_{k-1} := (p, \nu - h, \tau_1 - c(t-1), \tau_2 - c(t-2) \cdot \tau_1, \ldots, \tau_{k-1} - c(t-k+1) \cdot \tau_{k-2})$$

containing P and for which $(I_{k-1}^{-1})_{P_{k-1}}$ is not a DVR. Moreover, $(P_{k-1})_{P_{k-1}} = (\nu - h, p)_{P_{k-1}}$. From (**), we obtain

$$\tau_k \cdot (\tau_k - \tau_{k-1} c(t-k)) = \tau_{k-1} \cdot g(\nu - h)^{p-2}. \qquad (\star\star)$$

As before, $P_k' := (P_{k-1}, \tau_k)$ and $P_k := (P_{k-1}, \tau_k - \tau_{k-1} c(t-k))$ are the unique height-one primes in I_k^{-1} lying over P_{k-1}. Equation $(\star\star)$ gives $\tau_k \in (\nu - h)_{P_k'}$ and the equation

$$p \cdot \tau_k = \{(\nu - h)^{p-1} + p \cdot c(t-k)\} \cdot \tau_{k-1}$$

yields $p \cdot (\tau_k - c(t-k) \cdot \tau_{k-1}) = (\nu - h)^{p-1}$. Thus (as before), $(P_k')_{P_k'} = (\nu - h)_{P_k'}$, so $(I_k^{-1})_{P_k'}$ is a DVR. Finally, from (**) we get

$$\tau_k(\tau_k - c(t-k)\tau_{k-1}) = g\tau_{k-1} \cdot A(k,k),$$

so $\tau_k - c(t-k)\tau_{k-1} \in (\nu - h)_{P_k}$. Thus, by induction, $(P_k)_{P_k} = (p, \nu - h)_{P_k}$. However, $(\nu^{p^{t-k}} - h^{p^{t-k}}) \cdot \tau_k = p \cdot g$. If $k < t$, then $p \nmid g$, so $g \notin P_k$. Hence, $p \in (\nu - h)_{P_k}$, so $(P_k)_{P_k} = (\nu - h)_{P_k}$. If $k = t$, we have $(\nu - h) \cdot \tau_t = p \cdot g$ and since $\tau_t \notin P_t$, $\nu - h \in (p)_{P_t}$. Thus, in either case, P_k is principal, so $(I_k^{-1})_{P_k}$ is a DVR. Therefore, $(I_k^{-1})_Q$ is a DVR for every (height-one) $Q \subseteq I_k^{-1}$ lying over P. It follows that part (iii) has been verified.

For part (iv), to see that I_k is P-primary, we start by noting that, on the one hand, $\tilde{I}_k$, the preimage of I_k in $S[W]$, is a grade-two ideal, since $p^k, V^{p^{t-1}} - h^{p^{t-1}}$ is a maximal regular sequence in $\tilde{I}_k$, while on the other hand, $\tilde{I}_k$ is the ideal of $k \times k$ minors of a $(k+1) \times k$ matrix - this follows from the proof of statement (i). Thus, $\tilde{I}_k$ is a grade-two perfect ideal and is therefore grade unmixed. That is, $grade(\tilde{Q}) = 2$ for all associated primes $\tilde{Q}$ of $\tilde{I}_k$. If we show that any associated prime of $\tilde{I}_k$ has height two, then since $rad(\tilde{I}_k) = \tilde{P}$, it will follow that $\tilde{I}_k$ is $\tilde{P}$-primary and hence that I_k is P-primary. However, if $\tilde{Q}$ is an associated prime of $\tilde{I}_k$, then for $Q := \tilde{Q} \cap S$, $grade(Q) = 1$, since $\tilde{Q}$ contains a monic polynomial. Thus, $height(Q) = 1$ (since S satisfies S_2), so $height(\tilde{Q}) = 2$, as desired. This completes the proof of Proposition 3.3. □

Our next Proposition will allow us to identify the primary components of J that do not correspond to P.

Proposition 3.4. *For S as above, set $G(W) := W^d - \lambda a^e$, where $a \in S$ is a prime element and $\lambda \in S$ is a unit in S. Assume that $G(W)$ is irreducible over S and set $S[\omega] := S[W]/(G(W))$.*

(i) Assume d is a unit in S, $d > e$ and write $d = sd'$ and $e = se'$ with d' and e' relatively prime. Let u and v be positive integers such that $u \cdot d' + (-v) \cdot e' = 1$ and set $\tau := \frac{a^{e'}}{\omega^{d'}}$ and $\eta := \frac{a^u}{\omega^v}$. Then

$$R = S[\omega, \tau, \eta] = S[\tau, \eta] = J^{-1},$$

for

$$J := (\omega^{b_{e-1}}, \omega^{b_{e-2}} a, \ldots, \omega^{b_1} a^{e-2}, a^{e-1}) S[\omega],$$

with $b_1 < b_2 < \cdots < b_{e-1} < d$.

(ii) Assume $a = p$, $d = p^n > e$ and $p \nmid e$. For positive integers u and v such that $u \cdot p^n + (-v) \cdot e = 1$, set $\eta := \frac{a^u}{\omega^v}$. Then $R = S[\omega, \eta] = S[\eta] = J^{-1}$, for $J \subseteq S[\omega]$ having the same form as in (1).

(iii) If $e > d$ in (i) or (ii), then $R = J^{-1}$ for an ideal

$$J = (\omega^{d-1}, \omega^{d-2}a^{b_1}, \ldots, a^{b_{d-1}}),$$

with $b_1 < \cdots < b_{d-1} < e$.

Proof. For (i), we first observe that $g(T) := T^s - \lambda^{-1}$ is irreducible over S and $S[\tau]$ is integrally closed. For the first statement, if $g(T)$ were not irreducible over S, then $\lambda^{-1} = \gamma^s$, for some $\gamma \in S$. Thus, $(\omega^{d'})^s = (\gamma a^{e'})^s$, so that $\omega^{d'} = \epsilon a^{e'}$, for ϵ an s^{th} root of unity. Recalling that L denotes the quotient field of S, we have

$$L \subseteq L(\epsilon a^{e'}) = L(\epsilon) \subseteq L(\omega).$$

Since $[L(\epsilon) : L] < s$ and $[L(\omega) : L(\epsilon)] \leq d'$, it follows that $[L(\omega) : L] < d$, a contradiction. Thus, $g(T)$ is irreducible over S and $S[\tau] = S[T]/(g(T))$. To see that $S[\tau]$ is integrally closed, note that since s and λ are units in S, $g'(\tau)$ is a unit in $S[\tau]$, which gives what we want, since $g'(\tau)$ is in the conductor of the integral closure of $S[\tau]$ into $S[\tau]$. Therefore we have that τ is a unit in $S[\tau]$ and $S[\tau]$ is integrally closed.

Now adjoin ω to $S[\tau]$ and note $\omega^{d'} = \tau^{-1}a^{e'}$. We also have $\eta^{e'} = \tau^u\omega$ and $\eta^{d'} = \tau^v a$, which shows that $S[\omega, \tau, \eta] = S[\tau, \eta]$. But η satisfies $X^{d'} - \tau^v a$ over $S[\tau]$ (which is irreducible over $S[\tau]$ by degree considerations), so since d' is a unit in S, in order to see that $R = S[\tau, \eta]$, it suffices to see that a is square-free in $S[\tau]$. To see this, we use $S[\tau] = S[T]/(g(T))$. We may assume that S has been localized at aS. Let $Q \subseteq S[\tau]$ be a height-one prime containing a. Then $Q = (r(\tau), a)S[\tau]$, where $r(\tau)$ corresponds to a polynomial $r(T)$ which is an irreducible factor of $g(T)$ modulo aS. Since $g(T)$ and its derivative are relatively prime modulo aS (s is a unit in S), $g(T)$ has distinct irreducible factors modulo aS. Therefore, if $g(T) \equiv r(T) \cdot h(T)$ modulo aS, then $h(\tau) \notin Q$. Upon localizing, $Q_Q = (a)_Q$, i.e., a is square-free, as desired. Therefore, $R = S[\omega, \tau, \eta]$.

Now, $S[\tau]$ is generated as an S-module by the set $\{1, \frac{a^{e'}}{w^{d'}}, \ldots, (\frac{a^{e'}}{w^{d'}})^{s-1}\}$. Thus, this same set generates $S[\omega, \tau]$ as an $S[\omega]$-module. Moreover, R is generated over $S[\omega, \tau]$ by $1, \frac{a^u}{\omega^v}, \ldots, (\frac{a^u}{\omega^v})^{e'-1}$. We wish to replace these latter expressions by fractions of a similar type whose numerators are $a, a^2, \ldots, a^{e'-1}$. Since u and e' are relatively prime, the set $\{u, 2u, \ldots, (e'-1)u\}$, when reduced mod e', equals $\{1, 2, \ldots, e'-1\}$. Suppose $1 \leq i \leq e'-1$. Write $iu = le' + j$, with $j < e'$. Note there is a unique $1 \leq j \leq e'-1$ for each i. Since $1 = ud' + (-v)e'$,

$$i = iud' + (-v)ie' = (le' + j)d' + (-v)ie' = jd' + (-c_j)e'$$

for $c_j := iv - ld'$. It follows that c_j is less than d' and $c_j \equiv iv \bmod d'$. From these equations we get

$$\frac{a^j}{\omega^{c_j}} = \frac{a^j\omega^{ld'}}{\omega^{iv}} = \frac{a^j\tau^{-l}a^{e'l}}{\omega^{iv}} = \tau^{-l} \cdot \frac{a^{iu}}{\omega^{iv}} = \tau^{-l}\eta^i$$

Since τ is unit, $S[\omega, \tau, \eta]$ is generated over $S[\omega, \tau]$ by $1, \frac{a}{\omega^{c_1}}, \ldots, \frac{a^{e'-1}}{\omega^{c_{e-1}}}$. We now note that $c_1 < \cdots < c_{e'-1}$. If $i_1 = jd' + (-c_j)e'$ and $i_2 = (j+1)d' + (-c_{j+1})e'$, then $i_2 - i_1 = d' + (-c_{j+1} + c_j)e'$. Since $i_2 - i_1 < d'$ (the difference $i_2 - i_1$ can be negative), $c_{j+1} > c_j$.

It now follows that $R = S[\omega, \tau, \eta]$ is generated over $S[\omega]$ by the elements $\tau^i \cdot 1, \tau^i \cdot (\frac{a}{\omega^{c_1}}), \ldots, \tau^i \cdot (\frac{a^{e'-1}}{\omega^{c_{e'-1}}})$, $0 \leq i \leq s-1$, which can be written as $1, \frac{a}{\omega^{b_1}}, \ldots, \frac{a^{e-1}}{\omega^{b_{e-1}}}$, with $b_1 < \cdots < b_{e-1} < d$ (since $c_{e'-1} < d'$). In Proposition 2.1, take $A = S[\omega]$, $B = S[W]$, $F = F(W)$ and $\tilde{J}$, the ideal of $(e-1) \times (e-1)$ minors of the $e \times (e-1)$ matrix

$$\phi = \begin{pmatrix} -a & 0 & \cdots & 0 & 0 \\ W^{\alpha_{e-1}} & -a & \cdots & 0 & 0 \\ 0 & W^{\alpha_{e-2}} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & W^{\alpha_2} & -a \\ 0 & 0 & \cdots & 0 & W^{\alpha_1} \end{pmatrix}$$

with $\alpha_1 + \alpha_2 + \cdots + \alpha_i = b_i$, for $1 \leq i \leq e-1$. If we augment ϕ by adding the extra column which is the transpose of the row vector

$$(W^{m-b_{e-1}}\ 0\ \cdots\ 0\ -\lambda a),$$

it follows that for $J = (\omega^{b_{e-1}}, \omega^{b_{e-2}}a, \ldots, a^{e-1})$, J^{-1} is generated by $\{1, \frac{a}{\omega^{b_1}}, \ldots \frac{a}{\omega^{b_{e-1}}}\}$. Thus, $R = J^{-1}$, as desired.

The proofs of parts (ii) and (iii) are quite similar to the proof of part (i). Indeed, for part (ii), that $\eta^{p^n} = \lambda^{-u} \cdot \omega$ shows $S[\omega, \eta] = S[\eta]$. Moreover, $\eta^{p^n} = \lambda^{-v} \cdot p$, so from our discussion in section two, the only height one prime in $S[\eta]$ which might not yield a DVR upon localization is $P = (\eta, p)S[\eta]$. But clearly P_P is generated by η, so $S[\eta]$ is integrally closed. That $S[\omega, \eta] = R$ equals J^{-1} for J having the required form follows as in part (i) (via Proposition 2.1). The proof of part (iii) follows the proofs of parts (i) and (ii) by interchanging the roles of ω and a.

□

We are now ready to identify the primary components of J in the cases covered by Proposition 3.3 and Proposition 3.4.

Theorem 3.5. *Let $J \subseteq S[\omega]$ be the height-one unmixed ideal for which $J^{-1} = R$ and assume that f can be written as a product of primes.*
(i) Suppose $p \nmid f$, $p > 2$ and write $f = h^{p^t} + p^{k+1}g$ according to our conventions. Let $q_1, \ldots, q_m$ be the principal primes in S whose squares divide f, write e_i for the q_i-adic order of f and assume $e_i < p^n$. If $k > 0$, then

$$J = I_k \cap J_1 \cap \cdots \cap J_m,$$

where I_k is the P-primary ideal given in Proposition 3.3 and

$$J_i := (\omega^{b(i,e_{i-1})}, \omega^{b(i,e_{i-2})}q_i, \ldots, \omega^{b(i,1)}q_i^{e_i-2}, q_i^{e_i-1})$$

is the $Q_i := (\omega, q_i)$-primary ideal such that $(J_i^{-1})_{Q_i} = R_{Q_i}$, according to Lemma 3.4.(i). Here, the exponents $b(i,j)$ correspond to the exponents b_j appearing in Lemma 3.4. If f is not a pth power mod pS or $k = 0$, then

$$J = J_1 \cap \cdots \cap J_m.$$

When $e_i > p^n$, analogous statements hold (using part (iii) of Lemma 3.4).
(ii) Suppose $p \mid f$. Write e for the p-adic order of f and and assume that $p \nmid e$. Let

$$I_e := (\omega^{b_{e-1}}, \omega^{b_{e-2}}p, \ldots, p^{e-1})$$

be the ideal satisfying $(I_e^{-1})_P = R_P$, according to Lemma 3.4.(ii). As in (i), let $q_1, \ldots, q_m$ be the primes not equal to p whose squares divide f and write $J_1, \ldots, J_m$ for the corresponding ideals obtained from Lemma 3.4.(i). If $e \geq 2$, then

$$J = I_e \cap J_1 \cap \cdots \cap J_m.$$

If $e = 1$, then

$$J = J_1 \cap \cdots \cap J_m.$$

Proof. We first note that since $F'(\omega) \cdot R \subseteq S[\omega]$, if $Q \subseteq S[\omega]$ is a height-one prime for which $S[\omega]_Q$ is not a DVR, then $\omega F'(\omega) = p^n f \in Q$. Thus, if $k > 0$ in (i) or $e \geq 2$ in (ii), then P, $Q_1, \ldots, Q_m$ are exactly the height-one primes in $S[\omega]$ which upon localizing do not yield a DVR. If $k = 0$ in (i) or $e = 1$ in (ii), then we can exclude P. Therefore, Theorem 3.5 follows from Proposition 2.1, Proposition 3.3 and Proposition 3.4, once we note that each J_i is Q_i-primary. The proof of this is analogous to the proof in Proposition 3.3 that I_k is P-primary. Indeed, it follows from the proof of Proposition 3.4 that $\tilde{J}_i$, the pre-image of J_i in $S[W]$, is a grade-two perfect ideal - since it has grade two and is the ideal of $(e-1) \times (e-1)$ minors of an $e \times (e-1)$ matrix. Thus, $\tilde{J}_i$ is grade unmixed. On the other hand $\tilde{Q}_i$, the pre-image of Q_i in $S[W]$, is clearly the radical of $\tilde{J}_i$. Let P be an associated prime of $\tilde{J}_i$. Then P has grade two. Thus, $P \cap S$ has grade one, since P contains a monic polynomial. Since S satisfies S_2, $P \cap S$ has height one. Thus, P must have height two, and so $P = \tilde{Q}_i$. Therefore, $\tilde{J}_i$ is $\tilde{Q}_i$-primary, and hence, J_i is Q_i-primary, as required. □

4. Applications

In this section we will provide some applications of the results in section three. In particular, we give criteria for R to be a free S-module. We also prove that the main result in [6] carries over to our present situation if we assume that P is the P-primary component of J and $S[\omega]/P$ is integrally closed. These are precisely the conditions that hold on P in [6].

We begin with a lemma, interesting in its own right.

Lemma 4.1. *In $S[W]$ consider the ideals*

$$A := (W^{e_k}, W^{e_{k-1}}a_1, \ldots, W^{e_1}a_{k-1}, a_k) \quad \textit{and} \quad B := (W^{f_t}, W^{f_{t-1}}b_1, \ldots, W^{f_1}b_{t-1}, b_t),$$

where,

(a) $e_k > e_{k-1} > \cdots > e_1$ and $f_t > f_{t-1} > \cdots > f_1$.

(b) $a_1 \mid a_2 \mid \cdots \mid a_k$ and $b_1 \mid b_2 \mid \cdots \mid b_t$.

(c) Each a_i and b_j is a product of prime elements.

(d) For all i and j, a_i and b_j have no prime factor in common.

Then there exist integers $g_s > \cdots > g_1$ and products of primes $c_1 \mid c_2 \mid \cdots \mid c_s$ such that

$$A \cap B = (W^{g_s}, W^{g_{s-1}}c_1, \ldots, W^{g_1}c_{s-1}, c_s).$$

Moreover, A, B and $A \cap B$ are all grade-two perfect ideals. In particular, if S is Cohen-Macaulay, $S[W]/A \cap B$ is Cohen-Macaulay.

Proof. We follow a five step path. First, a matter of terminology. If $G(W) := s_nW^n + \cdots + s_0$ is a polynomial in W, then we call each term s_iW^i a "term" in $G(W)$.

(i) $G(W) \in A$ if and only if every term in $G(W)$ belongs to I. This follows since A is a homogenous ideal in $S[W]$ under the natural grading and the terms in $G(W)$ are just its homogenous components.

(ii) Any term in A is a multiple of one of the given generators. For this, suppose that $sW^e \in A$. Then we may express sW^e in terms of the given generators of A with degrees less than or equal to e. Say, $e_j \leq e$, $e_{j+1} > e$. Then we may write

$$sW^e = A_j \cdot (a_{k-j}W^{e_j}) + \cdots + A_0 \cdot a_k,$$

where each $A_i := \alpha_i W^{e-e_i}$, with $\alpha_i \in S$. For, $i < j$, $A_i(a_{k-i}W^{e_i}) = (\alpha_i a'_{k-i}W^{e-e_j}) \cdot (a_{k-j}W^{e_j})$, where $a_{k-i} = a'_{k-i} \cdot a_{k-j}$. Thus, sW^e is a multiple of $a_{k-j}W^{e-j}$.

(iii) The terms in the set $\{W^{max\{e_i,f_j\}}a_{k-i}b_{t-j}\}$ generate $A \cap B$. To see this, first note that the given set is contained in $A \cap B$. Second, we note that since statements (i) and (ii) apply equally well to B, $G(W) \in A \cap B$ if and only if each term in $G(W)$ is a multiple of one generator from A and one generator from B. So, suppose

$$sW^e = \alpha W^{e-e_i} \cdot a_{k-i}W^{e_i} = \beta W^{e-f_j} \cdot b_{t-j}W^{f_j}.$$

Then, $\alpha \cdot a_{k-i} = \beta \cdot b_{t-j}$, and since a_{k-i} and b_{t-j} have not common prime factors, we may write $\beta = \beta' \cdot a_{k-i}$. Thus

$$sW^e = (\beta' W^{e-max\{e_i,f_j\}}) \cdot (a_{k-i}b_{t-j}W^{max\{e_i,b_j\}}),$$

which is what we want.

(iv) The generating set in in the previous step can be refined as follows. Let $g_1 < \cdots < g_s$ be the distinct elements in the set $\{e_1, \ldots, e_k, f_1, \ldots, f_t\}$. Set $c_s := a_k \cdot b_t$ and for $1 \leq l \leq s-1$, define $c_{s-l} := a_{k-u}b_{t-v}$, where u is the largest index for which $e_u \leq g_l$ and v is the largest index for which $f_v \leq g_l$. We now show that $A \cap B = (W^{g_s}, c_1W^{g_{s-1}}, \ldots, c_{s-1}W^{g_1}, c_g)$. For this, by (iii), it suffices to show that each $c_{s-l}W^{g_l}$ is an element of the set in (iii) and that each element in the set in (iii) is a multiple of some $c_{s-l}W^{g_l}$. Suppose $c_{s-l}W^{g_l}$ is one of the proposed generators. Say $g_l = e_i$, some i. Then $c_{s-l} = a_{k-i}f_{t-v}$, for some (i.e., the largest) v for which $f_v \leq g_l = e_i$. Thus $g_l = e_i = max\{e_i, f_v\}$, so $c_{s-l}W^{g_l} = a_{k-i}f_{v-l}W^{max\{e_i,f_l\}}$ belongs to the set given in (iii). The argument is similar if $g_l = f_j$, some j. Conversely, consider the term $a_{k-i}b_{t-j}W^{max\{e_i,f_j\}}$. Suppose $max\{e_i, f_j\} = e_i = g_l$, say. Then certainly i is the largest index for which $e_i \leq g_l$. Moreover $f_j \leq g_l$, so that if v is the largest index for which $f_v \leq g_l$, then $f_j \leq f_v$. Therefore, $b_{t-v} \mid b_{t-j}$. Thus, $c_{s-l} := a_{k-i}b_{t-v}$ divides $a_{k-i}b_{k-j}$, so $a_{k-i}b_{t-j}W^{max\{e_i,f_j\}}$ is a multiple of $c_{s-l}W^{g_l}$.

(v) For $c_1, \ldots, c_s$ given in (iv), $c_1 \mid c_2 \mid \cdots \mid c_s$. Consequently, $A \cap B$ is a grade-two perfect ideal. For this, the first statement is basically clear from the definition of the c_r's. Indeed, if $c_{s-l} = a_{k-u}b_{t-v}$, then $g_l = e_u \geq f_v$ or $g_l = f_v \geq e_u$. We examine the case $g_l = e_u \geq f_v$, the case $g_l = f_v \geq e_u$ being similar. Since $g_{l-1} < g_l$, $g_{l-1} = e_{u-1}$ or $g_{l-1} = f_v$. In either case, $u-1$ is the largest index such $e_{u-1} \leq g_{l-1}$ and v is the largest index such that $f_v \leq g_{l-1}$, thus, $c_{s-l+1} = a_{k-u+1}f_v$, which shows $c_{s-l} \mid c_{s-l+1}$. Now, for all $i \geq 1$, write $c_{i+1} = c_i \cdot c'_{i+1}$. It now follows that $A \cap B$ is the ideal of $s \times s$ minors of the $(s+1) \times s$ matrix

$$\phi = \begin{pmatrix} -c_1 & 0 & \cdots & 0 \\ W^{g_s - g_{s-1}} & -c'_2 & \cdots & 0 \\ 0 & W^{g_{s-1}-g_{s-2}} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -c'_s \\ 0 & 0 & \cdots & W^{g_1} \end{pmatrix}.$$

Since the grade of $A \cap B$ is clearly two, it follows that $A \cap B$ is a grade-two perfect ideal. That A and B are also grade-two perfect ideals follows in similar fashion. The final statement follows by applying the Auslander-Buchsbaum formula locally in $S[W]/A \cap B$. □

Theorem 4.2. *R is a free S-module in each of the following cases :*

(i) $p \nmid f$ and f is square-free, i.e., $Q_Q = fS_Q$ for every height-one prime $Q \subseteq S$ containing f.

(ii) f can be written as a product of primes and one of the following conditions holds : (a) $p \nmid f$ and f is not a pth power modulo pS, (b) $p \nmid f$ and $f = h^{p^t} + pg$, with $p \nmid g$, (c) $p \mid f$ and the p-adic order of f is realtively prime to p or (d) p is a unit in S.

Proof. For (i), note that we are *not* assuming that primes minimal over f are principal. Thus P is the only possible height-one prime for which $S[\omega]_P$ is not a DVR. If f is not a pth power modulo pS, then as we saw in section two, $P = pS[\omega]$, so $R = S[\omega]$ is certainly a free S-module. If f is a pth power modulo pS, then write $f = h^{p^t} + p^{k+1}g$ according to our established conventions. If $k = 0$, then, as mentioned in section two, $P_P = (\omega)_P$, so again $R = S[\omega]$ is a free S-module. For $k > 0$, we have that $R = I_k^{-1}$, by Proposition 2.1 and Proposition 3.3 (or Theorem 3.5). Retaining the notation of Proposition 3.3, we have that I_k^{-1} is generated as an $S[\omega]$-module by $1, \tau_1, \ldots, \tau_k$. For each $1 \leq j \leq k$, let d_j denote the degree in ω of the numerator of τ_j, when τ_j is expressed as a fraction whose denominator is p^j (see the definition of τ_j in the second line of the proof of Proposition 3.3). Then $d_1 < \cdots < d_k$ and a moment's thought reveals that

$$1, \omega, \ldots, \omega^{d_1 - 1}, \tau_1, \omega\tau_1, \ldots, \omega^{d_2 - d_1 - 1}\tau_1, \tau_2, \ldots, \omega^{d_3 - d_2 - 1}\tau_2, \ldots, \tau_k, \ldots, \omega^{p^n - d_k - 1}\tau_k$$

generate R as an S-module. Since these elements are clearly linearly independent over S, R is a free S-module.

For part (ii), we first note that if conditions (a), (b) or (d) hold, then there is no P-primary component of J, and for condition (c), the P primary component of J has the form I_e taken in Propostion 3.4. By Proposition 3.4, all of these cases have the following in common : every primary component of J has the form $(\omega^{m_c}, q\omega^{m_{c-1}}, \ldots, q^{c-1}\omega^{m_1}, q^c)S[\omega]$ with q a principal prime (for which $c+1$ equals the q-adic order of f) and $m_c > m_{c-1} > \cdots > m_1$ positive integers less than p^n. If we lift each of these ideals to $S[W]$ and repeatedly apply Lemma 4.1, it follows that $J = (\omega^{e_d}, a_1\omega^{e_{d-1}}, \ldots, a_{d-1}\omega^{e_1}, a_d)$, where $1 < e_2 < \cdots < e_d < p^n$ and

$a_1 \mid a_2 \mid \cdots \mid a_d$ are products of primes whose squares divide f. Since $\tilde{J}$, the preimage of J in $S[W]$, is the ideal of $d \times d$ minors of a $(d+1) \times d$ matrix, we can find the generators of J^{-1} as an S-module using Proposition 2.1. Indeed, $\tilde{J}$ is given (up to changes in sign) by the $d \times d$ minors of the matrix

$$\phi = \begin{pmatrix} -a_1 & 0 & \cdots & 0 \\ W^{e_d - e_{d-1}} & -a_2' & \cdots & 0 \\ 0 & W^{e_{d-1}-e_{d-2}} & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -a_d' \\ 0 & 0 & \cdots & W^{e_1} \end{pmatrix},$$

where $a_i' := \frac{a_i}{a_{i-1}}$ for $2 \le i \le d$. If we express $F(W) = W^c \cdot W^{e_d} + u \cdot a_d$, then augmenting the appropriate column to ϕ allows us to calculate (up to a sign) the $S[\omega]$-module generators of J^{-1}. Via Proposition 2.1, the resulting generators are

$$1, \frac{a_2' \cdot a_3' \cdots a_d \cdot u}{\omega^{e_d}}, \frac{a_1 \cdot a_3' \cdots a_d' \cdot u}{a_1 \omega^{e_{d-1}}}, \ldots, \frac{a_1 \cdot a_2' \cdots a_{d-1}' \cdot u}{a_{d-1}\omega^{e_1}}.$$

We can rewrite these generators as :

$$1, \frac{\omega^{p^n - e_d}}{a_1}, \frac{\omega^{p^n - e_{d-1}}}{a_2}, \ldots, \frac{\omega^{p^n - e_1}}{a_d}.$$

As in the proof of part (i), we can multiply each of these generators by an appropriate power of ω to create a linearly independent set of generators of R as an S-module. This completes the proof of Theorem 4.2. $\square$

Our second theorem of this section generalizes part of the argument from [6] which shows the existence of a birational, finite Cohen-Macualy module in the case of radical extensions of prime order. As an application of this theorem, we show that in our present context, the argument applies when P is the primary component of J.

Theorem 4.3. *Let $(S, \mathfrak{n})$ be a regular local ring. Assume that $f(W) \in B := S[W]$ is a monic, irreducible polynomial such that $S[\omega] := B/f(W)B$ is local. Let R denote the integral closure of $S[\omega]$ and assume that R is a finite module over $S[\omega]$. Write $J \subseteq S[\omega]$ for the conductor of R into $S[\omega]$. Suppose $J = P \cap L$, where:*

(i) P is a height-one prime such that $S[\omega]_P$ is not a DVR and L is the intersection of the remaining primary components of J that are not P-primary.

(ii) $S[\omega]/P$ and $S[\omega]/L$ are Cohen Macaulay and $S[\omega]/P$ is integrally closed.

(iii) P is the only associated prime of J lying over $P \cap S$.

Then R admits a finite, birational maximal Cohen-Macaulay module.

Proof. For ideal $C \subseteq S[\omega]$, we will write $\tilde{C}$ to denote its preimage in B. Note that since $S[\omega]$ is local, there is a unique maximal ideal $\mathfrak{m}$ in B containing $f(W)$. Since B acts on $S[\omega]$ modules via the canonical map from B to $S[\omega]$, we may assume that B is local at $\mathfrak{m}$ when considering this action. Now, $L \cap S$ is a height-one, unmixed ideal of S, and therefore a principal ideal. Let $a \in L$ be a generator for $L \cap S$. Note that condition (iii) in the statement of the theorem guarantees that $a \notin P$. Set $K := aL^{-1}$, an ideal of $S[\omega]$. We first note that K is a height-one, unmixed ideal of $S[\omega]$ contained in L. For this, we recall the following fact. Suppose $C \subseteq S[\omega]$ is an ideal such that C^{-1} is a ring and $(C^{-1})^{-1} = C$. Then $C \cdot C^{-1} = C$. Indeed, $(C \cdot C^{-1})C^{-1} = C \cdot C^{-1}$, and thus, $C \cdot C^{-1} \subseteq (C^{-1})^{-1} = C$. It follows that $C \cdot C^{-1} = C$. Now, let Q be an associated prime of L, so that Q is an associated prime of J not equal to P. Then,

$$(LL^{-1})_Q = L_Q L_Q^{-1} = J_Q J_Q^{-1} = J_Q = L_Q.$$

Thus, $LL^{-1} \subseteq L$, and hence $LL^{-1} = L$. In particular, $K \subseteq L$. On the other hand, if Q is an associated prime of K, then $Q = (aL^{-1} : c)$, for some $c \notin aL^{-1}$. We also have $Qc \subseteq aL^{-1}$, and thus $QcL \subseteq aL^{-1}L = aL$. If $cL \subseteq aL$, then $\frac{c}{a} \in L^{-1}$, contrary to the choice of c. Thus, Q consists of zerodivisors modulo the ideal aL. It follows that Q is contained in Q' for Q' an associated prime of $aS[\omega]$ or L. Since these latter associated primes have height one, Q has height one. Thus, $K = aL^{-1}$ is a height-one, unmixed ideal contained in L. It follows that $\tilde{K} \subseteq B$ is an unmixed, grade-two ideal.

Now, since $S[\omega]/L = B/\tilde{L}$ is Cohen-Macaulay, $\tilde{L} \subseteq B$ is a grade-two perfect ideal, so $\tilde{L}$ is given by the $n \times n$ minors of an $(n+1) \times n$ matrix, by the Hilbert-Burch Theorem. Thus, $1 = \text{projdim}_B(L) = \text{projdim}_B(L^{-1})$, by Proposition 2.1. Thus, $\text{projdim}_B(aL^{-1}) = \text{projdim}_B(K) = 1$. Therefore,

$$\text{projdim}_B(S[\omega]/K) = \text{projdim}_B(B/\tilde{K}) = 2,$$

and $B/\tilde{K}$ is Cohen-Macaulay. Set $I := P \cap K$.

We will show that I^{-1} is the module we seek. To begin, we first show that I^{-1} is an R-module. Since $R = J^{-1}$, [6], Lemma 3.5 shows that I^{-1} is an R-module if and only if $I^{-1} = (I \cdot J^{-1})^{-1}$. Since $S[\omega]$ satisfies S_2, we only need to check equality at each height-one prime in $S[\omega]$. Let $Q \subseteq S[\omega]$ be a height-one prime. If $Q = P$, then $I_P = P_P = J_P$. Thus, since $J = J \cdot J^{-1}$, $I_P = (I \cdot J^{-1})_P$, so $I_P^{-1} = (I \cdot J^{-1})_P^{-1}$. Let $Q \in \text{Ass}(S[\omega]/L)$. Then, on the one hand, $J_Q = L_Q$. On the other hand $I_Q = K_Q = (aL^{-1})_Q = (aJ^{-1})_Q$. By [6], Lemma 3.5, I_Q^{-1} is a J_Q^{-1}-module, and hence $I_Q^{-1} = (I \cdot J^{-1})_Q^{-1}$. Finally, if Q is a height-one prime not containing J, $J_Q = S[\omega]_Q$, so the desired equality holds in $S[\omega]_Q$. Thus, $I_Q^{-1} = (I \cdot J^{-1})_Q^{-1}$, for every height-one prime Q, which implies $I^{-1} = (I \cdot J^{-1})^{-1}$, so I^{-1} is an J^{-1}-module, i.e., an R-module.

To see that $\text{depth}(I^{-1}) = \dim(R)$, it suffices to see that $\text{depth}_B(I^{-1}) = \dim(R) = \dim(B) - 1$. Arguing as in the first paragraph of the proof, it suffices to show that $\tilde{I}$ is a grade two perfect ideal in B. Consider the exact sequence,

$$0 \to B/\tilde{I} \to B/\tilde{P} \oplus B/\tilde{K} \to B/(\tilde{P} + \tilde{K}) \to 0.$$

Since $S[\omega]/P = B/\tilde{P}$ is Cohen-Macaulay, $\text{depth}(B/\tilde{P}) = \dim(B) - 2$. By what we have already shown, $\text{depth}(B/\tilde{K}) = \dim(B) - 2$. Thus, we will be done by the Depth Lemma if we show that $\text{depth}(B/\tilde{P} + \tilde{K}) = \dim(B) - 3$. For then $\text{depth}(B/\tilde{I}) = \dim(B) - 2$, which gives what we want.

We now claim that $\tilde{P} + \tilde{K} = (a, \tilde{P})B$. Since $a \notin \tilde{P}$, $\text{depth}(B/(a, \tilde{P})) = \text{depth}(B/\tilde{P}) - 1 = \dim(B) - 3$, this will complete the proof. By the definition of K, $a \in \tilde{K}$, and it follows that $(a, \tilde{P})B \subseteq \tilde{P} + \tilde{K}$. To finish, it suffices to show $\tilde{K} \subseteq (a, \tilde{P})B$. Let $c \in \tilde{K}$. Then its image c_0 in $S[\omega]$ belongs to $K = aL^{-1}$. Since $L^{-1} \subseteq J^{-1} = R$, $c_0 \in aR \cap S[\omega]$, i.e., c_0 is integral over the ideal $aS[\omega]$. But then the image of c_0 in $S[\omega]/P$ is integral over the (non-zero) image of a in $S[\omega]/P$. Since $S[\omega]/P$ is integrally closed, it follows that the image of c_0 in $S[\omega]/P$ belongs to the ideal $a \cdot (S[\omega]/P)$. Thus, in B, c belongs to $(a, \tilde{P})B$, which is what we want. This concludes the proof. □

Corollary 4.4. *Continuing our ongoing notation, with $\omega^{p^n} = f$, assume further that S is an unramified, regular local ring of mixed characteristic $p > 0$. Assume $p \nmid f$ and write $f = h^{p^t} + p^{k+1}g$ in accordance with our standard hypothesis. Assume:*

(i) $t = 1$.

(ii) $S[\omega]/P$ *is integrally closed.*

Then R admits a finite, birational maximal Cohen-Macaulay module.

Proof. We need to verify the conditions in Theorem 4.3. Note first, that our standing hypothesis that S/pS is integrally closed holds, since S/pS is a regular local ring. By Theorem 3.5, since $t = 1$, $k = 1$ and $P = (\omega^{p^m} - h, p)S[\omega]$ is the P-primary component of J. If we let L denote the intersection of primary components of J not corresponding to P, then by Theorem 3.5 and Lemma 4.1, $B/\tilde{L} = S[\omega]/L$ is Cohen-Macaulay. Thus, the conditions in Theorem 4.6 hold, so R admits a finite, birational, maximal Cohen-Macaulay module. □

Remarks. (i) Suppose S is an unramified regular local ring of mixed characteristic p and $w^p = f$, i.e., $n = 1$ in our standard set-up with $p \nmid f$. This is exactly the situation in [6], so $P = (\omega - h, p)S[\omega]$ and $S[\omega]/P = S/pS$ is integrally closed. Moreover, as shown in [6], P is the P-primary component of J. Thus, Corollary 4.7 is a generalization of the main result in [6].

(ii). Suppose, for example, that V is an unramified DVR of mixed characteristic p. Set $k(p) := V/pV$ and let $S = V[X_1, \ldots, X_n]$ be the polynomial ring with coefficients in V. Suppose $f \in S$ and $f = h^p + p^2 g$, in accordance with our standard convention (so $t = 1$). Thus, for ω satsifying $\omega^{p^n} = f$, $P = (\omega^{p^m} - h, p)S[\omega]$ is the P-primary component of J. Suppose that the partial derivatives of the image of h in $k(p)[X_1, \ldots, X_n]$ generate an ideal having height greater than one. It follows that $S[\omega]/P = k(p)[X_1, \ldots, X_n, W]/(W^{p^m} - h)$ is regular in codimension one and hence is integrally closed (and is the coordinate ring of a *Zariski hypersurface*). By Corollary 4.4, the integral closure of $S[\omega]$ admits a finite, birational maximal Cohen-Macaulay module.

(iii) Suppose $n = 1$ in Theorem 4.2. If f can be written as a product of primes, we can always assume that no prime dividing f appears more than $p - 1$ times. In particular, if $p \mid f$, we can always assume that the p-adic order of f is relatively prime to p. Thus, Theorem 4.2 recovers the freeness results in [7], where it was shown that for pth root extensions, R is a free S-module whenever $p \mid f$ or f is not a pth power modulo p (see [7] Proposition 2.2). Even when $n = 1$, Theorem 4.2 gives some additional cases for R to be a free S-module.

(iv) While the motivation for this paper comes from an attempt to use the structure of the conductor J to seek a finite, Cohen-Macaulay module over R, when R is the integral closure of the ring obtained from a regular local ring by adjoining the p^nth root of an element of S, for R the integral closure of $S[\omega]$ and ω a root of an *arbitrary* irreducible monic polynomial $f(W)$ over S, the structure of J seems to exert some influence over the property of S being a summand of R, even if S is just a normal domain. For example, if S is normal, whenever J contains an element of the form $g(\omega) \in J$ (with degree less than the degree of $f(W)$) so that some coefficient of $g(w)$ is a unit, an elementary argument [3] shows that $JR \cap S = J$, for all ideals $J \subseteq S$, i.e., S is *ideally integrally closed* in R. One can then use this in many cases (e.g., S is excellent) to prove that S is a summand of R, see [3]. Of course, when S is a regular local ring, the Direct Summand Conjecture is now a theorem (see [1]), so that S is always a summand of R, but the conductor argument does not, apriori, require that S be regular, though the Direct Summand conjecture does. Regarding the converse, I do not know if the condition that S is a summand of R implies that the conductor contains an element with a unit coefficient.

5. Examples

In this section we offer some examples illustrating our results and some of the phenomomena discussed in previous sections. Throughout this section, we continue to maintain our established notation and conventions. One of the key points about p^nth root extensions seems to be that R is a free S-module whenever J does not have a P-primary component. However, we will provide some examples where R is free, even when J has a P-primary component. Some of the examples will show that the nature of R is determined by the exponents appearing in the prime factorization of f while other examples will show that the nature of R sometimes depends upon the prime factorization of f modulo p (or powers of p).

We start with some "generic" examples.

Example 5.1. Suppose $S := \mathbb{Z}[X_1, \ldots, X_d]$. Take $f = X_1^{e_1} \cdots X_d^{e_d}$, or $f = p^e X_2^{e_2} \cdots X_d^{e_d}$, with $p \nmid e_i$, some i, in the first case, or $p \nmid e$ in the second. In the first case, f is not a pth power in S nor is f a pth power

[3]Suppose that the conductor of R to $S[\omega]$ contains an expression $g(\omega)$ in ω of degree less than n (the degree of $f(W)$) such that some coefficient of $g(\omega)$ is a unit in S. To see that $JR \cap S = J$, for all ideals $J \subseteq S$, suppose the i^{th} term of $g(\omega)$ is $\alpha \cdot \omega^i$, with $i < n$ and α a unit in S. Note that if $J \subseteq S$ is an ideal and $a \in JR \cap S$, we can write $a = j_1 r_1 + \cdots + j_s r_s$, with each $j_k \in I$ and $r_k \in R$. If we multiply both sides of this equation by $g(\omega)$, the right hand side belongs to $JS[\omega]$. Thus, $a \cdot g(\omega)$ can be written as an expression of degree less than n in ω with coefficients in J. Hence $a \cdot \alpha \in J$. Since α is a unit, $a \in J$, as required. Here we are using that $S[\omega]$ is a free S-module with basis, $1, \omega, \ldots, \omega^{n-1}$

modulo pS. Thus, R is a free S-module by Theorem 4.2. In the second case, R is also a free S-module, again by Theorem 4.2. In fact, combining Proposition 2.1 with the proofs of Lemma 3.4, Lemma 4.1 and Theorem 4.2, whenever we meet one of the hypotheses of Theorem 4.2, we have a *constructive* procedure for finding a basis of R as an S-module.

For example, suppose $p = 3$, $n = 2$ and $f = 3^8 X_2^7 X_3^6$, so $\omega^9 = 3^8 X_2^7 X_3^6$. Then $P = (\omega, 3)$, $Q_2 := (\omega, X_2)$ and $Q_3 := (\omega, X_3)$ are the height-one primes $Q \subseteq S[\omega]$ for which $S[\omega]_Q$ is not a DVR. If we apply Lemma 3.4 (and its proof) we obtain that R_P is generated over $S[\omega]_P$ by $\frac{p}{\omega}$, that R_{Q_2} is generated over $S[\omega]_{Q_2}$ by $\frac{X_2^4}{\omega^5}$ and that R_{Q_3} is generated over $S[\omega]_{Q_3}$ by $\frac{X_3}{\omega}$ and $\frac{X_3^2}{\omega^3}$. Moreover, for

$$I_1 := (\omega, p)^7,\ I_2 := (\omega^7, X_2\omega^6, X_2^2\omega^5, X_2^3\omega^3, X_2^4\omega^2, X_2^5\omega, X_2^6),\ I_3 := (\omega^7, X_3\omega^6, X_3^2\omega^4, X_3^3\omega^3, X_3^4\omega, X_3^5),$$

$R_P = (I_1^{-1})_P$, $R_{Q_2} = (I_2^{-1})_{Q_2}$, and $R_{Q_3} = (I_3^{-1})_{Q_3}$. Thus, $R = J^{-1}$, for $J = I_1 \cap I_2 \cap I_3$. Using Lemma 4.1 (by taking pre-images in $S[W]$), we have that

$$J = (\omega^7, 3X_2X_3\omega^6, 3^2X_2^2X_3^2\omega^5, 3^3X_2^3X_3^2\omega^4, 3^4X_2^3X_3^3\omega^3, 3^5X_2^4X_3^4\omega^2, 3^6X_2^5X_3^4\omega, 3^7X_2^6X_3^5).$$

Now J is easily seen to be generated (up to sign) by the 7×7 minors of the 8×7 matrix

$$\phi := \begin{pmatrix} -3X_2X_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ \omega & -3X_2X_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega & -3X_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega & -3X_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & -3X_2X_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega & -3X_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega & -3X_2X_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega \end{pmatrix}.$$

If we augment ϕ with the column whose transpose is $(\omega^2\ 0\ \cdots\ 0\ -3X_2X_3)$, we obtain an 8×8 matrix ϕ'. By Proposition 2.1, J^{-1} is generated as an $S[\omega]$-module by the fractions $\frac{\delta_i}{j_i}$, where for $1 \le i \le 8$, δ_i is the (i,i)th cofactor of ϕ' and j_i is the ith minor of ϕ. Thus, J^{-1} is generated over $S[\omega]$ by

$$1, \frac{\omega^2}{3X_2X_3}, \frac{\omega^3}{3^2X_2^2X_2^2}, \frac{\omega^4}{3^3X_2^3X_3^2}, \frac{\omega^5}{3^4X_2^3X_3^4}, \frac{\omega^6}{3^5X_2^4X_3^4}, \frac{\omega^7}{3^6X_2^5X_3^4}, \frac{\omega^8}{3^7X_2^6X_3^5}, 1.$$

It follows that the elements

$$1, \omega, \frac{\omega^2}{3X_2X_3}, \frac{\omega^3}{3^2X_2^2X_2^2}, \frac{\omega^4}{3^3X_2^3X_3^2}, \frac{\omega^5}{3^4X_2^3X_3^4}, \frac{\omega^6}{3^5X_2^4X_3^4}, \frac{\omega^7}{3^6X_2^5X_3^4}, \frac{\omega^8}{3^7X_2^6X_3^5}$$

form a basis for R as an S-module.

Example 5.2 In this example, we will show that even though the primary components of J depend upon the prime factors of f, the freeness of R as an S-module may depend not only on how f factors over S, but also on how f factors modulo powers of pS. In particular, for a certain factorization over S, we will give an example where R is not a free S-module (or Cohen-Maculay, since S will be regular) and an example where R is a free S-module, even though $p \nmid f$ and J has a P-primary component. Set $S := \mathbb{Z}[X,Y]_{(p,X,Y)}$ and take $p = 3$. We will write $f = a^8b^7 = h^9 + 27g$, with $a, b \in S$ prime elements. For different choices of a and b, we will get R free over S, i.e., R Cohen-Macaulay and R not free over S, i.e., R not Cohen-Macaulay.

(i) Take $a := X^7Y + 27$, $b := XY^4 + 27$ and $h := X^7Y^4$ (as in the previous example). We are going to show that R is not a free S-module by showing that R is not Cohen-Macaulay. Now, as in Example 5.2, $R = J^{-1}$, for $J = I_1 \cap I_2 \cap I_3$, with I_1, I_2 and I_3 as given in Example 5.2 (expressed in terms of ω, h, a, b.) Set $B := S[W]_{(3,X,Y,W)}$ and use "tilde" to denote preimages in B. By our comments in the proof of Proposition 2.1, $p.d._B(J) = 1$ if and only if $p.d._B(J^{-1}) = 1$, so $depth_B(R) = dim(B) - 1 = dim(R)$ if and only if $depth_B(\tilde{J}) = dim(B) - 1$ if and only if $depth_B(B/\tilde{J}) = dim(B) - 2$. Therefore, we will show that $depth_B(B/\tilde{J}) < dim(B) - 2$. For this, we set $\tilde{I} := \tilde{I}_2 \cap \tilde{I}_3 = (W^7, abW^6, a^2b^3W^5, a^3b^3W^4, a^4b^3W^3, a^5b^4W^2, a^6b^5W, a^7b^6)$ (by Lemma 4.1). From the exact sequence

$$B/\tilde{J} \to B/\tilde{I}_1 \oplus B/\tilde{I} \to B/(\tilde{I}_1 + \tilde{I}) \to 0,$$

and the Depth Lemma, it follows that we must prove that $depth_B(B/(\tilde{I}_1 + \tilde{I})) < dim(B) - 3 = 1$. Using the definitions of a, b, h, $\tilde{I}_1$ and $\tilde{I}$, it follows that

$$\tilde{I}_1 + \tilde{I} = (X^{50}Y^{29}, X^{52}Y^{28}, X^{42}Y^{24}W, X^{37}Y^{22}W^2, X^{39}Y^{21}W^2, W^3 - X^{21}Y^{12}, 3(W - X^7Y^4), 9).$$

Now, since $\tilde{I}_1 + \tilde{I}$ contains a monic in degree 3, $B/(\tilde{I}_1 + \tilde{I})$ is a finitely generated S-module. In fact, it is a quotient of S^3. It is not difficult to see that the depth of $B/(\tilde{I}_1 + \tilde{I})$ is the same, whether we regard it as a B-module or an S-module. We are now going to write $B/(\tilde{I}_1 + \tilde{I})$, viewed as an S-module, as S^3/M, for some $M \subseteq S^3$ and show that $p.d._S(S^3/M) = 3$. It will then follow that $0 = depth_S(S^3/M) = depth_B(B/(\tilde{I}_1 + \tilde{I}))$, which is what we want.

To proceed, we set $T := B/(W^3 - X^{21}Y^{12})B$ and $K := (\tilde{I}_1 + \tilde{I})T$. Now the T-ideal K is also a finitely generated S-module. To find a set of generators for K as an S-module, one simply multiplies the given B generators by 1, W, W^2. Upon doing so, we see that K is generated as a T-module by the images (in T) of the expressions :

$$X^{50}Y^{29}, X^{52}Y^{28}, X^{42}Y^{24}W, X^{37}Y^{22}, X^{39}Y^{21},$$

$$-3X^7Y^4 + 3W, -3X^7Y^4W + 3W^2, 3X^{21}Y^{12} - 3X^7Y^4W^2, 9, 9W, 9W^2.$$

However,

$$3X^{21}Y^{12} - 3X^7Y^4W^2 \equiv -X^{14}Y^8 \cdot (-3X^7Y^4 + 3W) - X^7Y^4 \cdot (-3X^7Y^4W + 3W^2),$$

$$9W \equiv 3 \cdot (-3X^7Y^4 + 3W) + X^7Y^{\cdot}9 \quad \text{and} \quad 9W^2 \equiv 3 \cdot (-3X^7Y^4W + 3W^2) + X^7Y^{\cdot}9W$$

in T. It follows that K is generated as an S-module by the images in T of :

$$X^{50}Y^{29}, X^{52}Y^{28}, X^{42}Y^{24}W, X^{37}Y^{22}, X^{39}Y^{21}, -3X^7Y^4 + 3W, -3X^7Y^4W + 3W^2, 9.$$

Therefore, as an S-module, $B/(\tilde{I}_1 + \tilde{I})$ is isomorphic to S^3/M, for M generated by the columns of the matrix

$$\hat{M} := \begin{pmatrix} X^{50}Y^{29} & X^{52}Y^{28} & 0 & 0 & 0 & -3X^7Y^4 & 0 & 9 \\ 0 & 0 & X^{42}Y^{24} & 0 & 0 & 3 & -3X^7Y^4 & 0 \\ 0 & 0 & 0 & X^{37}Y^{22} & X^{39}Y^{21} & 0 & 3 & 0 \end{pmatrix}.$$

We now note that S^3/M can be resolved over S as follows :

$$\mathcal{F}: \quad 0 \to S^2 \xrightarrow{\alpha} S^7 \xrightarrow{\psi} S^8 \xrightarrow{\hat{M}} S^3 \to S/M \to 0,$$

where

$$\alpha = \begin{pmatrix} X^2 & 0 \\ -Y & 0 \\ 0 & 0 \\ 0 & X^2 \\ 0 & -Y \\ 3 & 0 \\ 0 & 3 \end{pmatrix}$$

and

$$\psi = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & -X^2 & 0 \\ 0 & 3 & 0 & 0 & 0 & Y & 0 \\ -3XY & -3X^3 & -9 & 3X^2Y^2 & 3X^4Y & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & -X^2 \\ 0 & 0 & 0 & 0 & 3 & 0 & Y \\ X^{43}Y^{25} & X^{45}Y^{24} & 3X^{42}Y^{24} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -X^{37}Y^{22} & -X^{39}Y^{21} & 0 & 0 \\ 0 & 0 & X^{49}Y^{28} & 0 & 0 & 0 & 0 \end{pmatrix}.$$

A straight forward calculation shows that $\mathcal{F}$ is a complex. Moreover, we clearly have $grade(I_3(\hat{M})) = 2$ and $grade(I_2(\alpha)) = 3$. Using Macaulay2, one finds that $729, X^{132}Y^{175}$ is a regular sequence of length two contained in $I_5(\psi)$. Thus, $\mathcal{F}$ is an exact sequence, by the Buchsbaum-Eisenbud exactness criteria. Therefore, $p.d._S(S^3/M) = 3$, and this part of the example is complete.

(ii) Keeping S the same, we now take $a := XY^3 + 27$, $b := X^4Y^3 + 27$ and $h := X^4Y^5$, so

$$\omega^9 = f = a^8b^7 = h^9 + 27g.$$

We are going to show that R is Cohen-Macaulay (i.e., a free S-module), even though none of the hypotheses from Theorem 4.2 are in force. As before, $R = J^{-1}$, for $J = I_1 \cap I_2 \cap I_3$, for $I_1 = (\omega^3 - h^3, 3(\omega - h), 9)$, $I_2 := (\omega, a)^7$ and $I_3 = (\omega^7, b\omega^6, \dots, b^7)$ as above. Set $B := S[W]_{(p,X,Y,W)}$ and use "tilde" to denote preimages in B. Writing $\tilde{I} := \tilde{I}_2 \cap \tilde{I}_2$ and using the definitions of a, b, and h, we have

$$\tilde{I}_1 + \tilde{I} = (X^{28}Y^{36}, X^{24}Y^{30}W, X^{21}Y^{27}W^2, W^3 - X^{12}Y^{15}, 3(W - X^4Y^5), 9).$$

Following the line of thought used in part (i), to see that R is Cohen-Macaulay, it suffices to show that $B/(\tilde{I}_1 + \tilde{I})$ has depth equal to 1, either as a B-module or as an S-module. Arguing as before, one can show that $B/\tilde{I}_1 + \tilde{I}$ is isomorphic to S^3/M as an S-module, where M is the submodule of S^3 generated by the columns of the matrix

$$\hat{M} = \begin{pmatrix} X^{28}Y^{36} & 0 & 0 & -3X^4Y^5 & 0 & 9 \\ 0 & X^{24}Y^{30} & 0 & 3 & -3X^4Y^5 & 0 \\ 0 & 0 & X^{21}Y^{27} & 0 & 3 & 0 \end{pmatrix}.$$

To see that $depth_S(S^3/M) = 1$, we show $p.d._S(S^3/M) = 2$. In fact,

$$\mathcal{F} \quad : \quad 0 \to S^3 \xrightarrow{\psi} S^6 \xrightarrow{\hat{M}} S^3 \to S^3/M \to 0,$$

is easily seen to be a free resolution of S^3/M, where

$$\psi = \begin{pmatrix} 3 & 0 & 0 \\ -3Y & -9 & -3XY^2 \\ 0 & 0 & 3 \\ X^{24}Y^{31} & 3X^{24}Y^{30} & 0 \\ 0 & 0 & -X^{21}Y^{27} \\ 0 & X^{28}Y^{35} & 0 \end{pmatrix}$$

Therefore, $p.d._S(S^3/M) = 2$ and Example 5.3 is now complete

Example 5.3. We consider the example from [4]. Set $S := (\mathbb{Z}[U, V, X, T]/(T^2 - 4U - V^2X))_{(2,U,V,X,T)}$, $N := (2, U, V, X, T)S$, and use lower case to denote images in S. Then S is a (non-regular) local Cohen-Macauly UFD. Set $F(W) := W^2 - x \in S[W]$, so $\omega^2 = x$ in $S[\omega]$. In [4], it is shown that $S[\omega]$ has an integral extension (in fact R, the integral closure of $S[\omega]$) for which S is not a direct summand. It follows from part (iv) of the Remarks in section four, that the conductor J for this extension does not contain an expression of the form $a + b\omega$ with $a, b \in S$ and one of the elements a or b a unit in S. We wish to illustrate this explicitly in this example. We start by noting that since $\omega \cdot F'(\omega) = 2x$, the possible height-one primes $Q \subseteq S[\omega]$ for which $S[\omega]_Q$ is not a DVR are those containing either x or 2. In the first case, we have $\tilde{Q} = (W, x)S[W] = (W, F(W))S[W]$, so $Q = xS[\omega]$. Thus, $S[\omega]_Q$ is a DVR in this case. Suppose Q contains 2. Then $W^2 - x, 2 \in \tilde{Q}$. Since in $S[W]$,

$$t^2 - v^2W^2 = -v \cdot (W^2 - x) + (2u) \cdot 2,$$

$(2, t - vW, W^2 - x) \subseteq \tilde{Q}$. In $\mathbb{Z}[U, V, X, T]$, $T^2 - 4U - V^2X \in (2, T - VW, W^2 - X)$, a height-three prime, so we must have $\tilde{Q} = (2, t - vW, W^2 - x)$ in $S[W]$. The displayed equation shows that $F(W) \in \tilde{Q}^{(2)}$, so $S[\omega]_Q$ is not a DVR for $Q := (2, t - v\omega)S[\omega]$. Moreover, since $\tilde{Q}$ is the only height-two prime in B containing 2 and $W^2 - x$, Q is the only height-one prime in $S[\omega]$ for which $S[\omega]_Q$ is not a DVR. Thus, by Proposition 2.1, $J \subseteq Q$. Since $Q \subseteq NS[\omega]$, $J \subseteq NS[\omega]$, and hence the conductor J does not contain an expression of the form $a\omega + b$, with with either a or b a unit in S.

References

[1] Y. Andres, *La conjecture du facteur direct*, preprint.

[2] M. Hochster, *Contracted ideals from integral extensions of regular rings*, Nagoya Math. J. **51** (1973), 25-43.

[3] M. Hochster, *Cyclic purity versus purity in excellent Noetherian rings*, Trans. Amer. Math. Soc. **231** (1977), no. 2, 463-488.

[4] M. Hochster and J.E. McGaughlin, *Splitting theorems for quadratic ring extensions*, Illinois J. Math. **127**, no. 1 (1983), 94-103.

[5] I. Kaplansky, Fields and Rings, Second Edition, Chicago Lecture Series, The University of Chicago Press, 1972.

[6] D. Katz, *On the existence of maximal Cohen-Macaulay modules over pth root extensions*, Proc. Amer. Math. Soc. **127**, no. 9 (1999), 2601-2609.

[7] J. Koh, *Degree p extensions of an unramified regular local ring of characteristic p > 0*, J. of Algebra **99** (1986), 310-323.

[8] S. Kleiman and B. Ulrich, *Gorenstein algebras, symmetric matrices, self-linked ideals, and symbolic powers*, Trans. Amer. Math. Soc. **349** (1997), 4973-5000.

[9] D. Mond and R. Pellikaan, *Fitting ideals and multiple points of analytic mappings*, Springer Lecture Notes in Mathematics **1414** (1989), 107-161.