PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 9, Pages 2601–2609
S 0002-9939(99)04880-7
Article electronically published on April 15, 1999

ON THE EXISTENCE OF MAXIMAL COHEN-MACAULAY MODULES OVER pth ROOT EXTENSIONS

DANIEL KATZ

(Communicated by Wolmer V. Vasconcelos)

Abstract. Let S be an unramified regular local ring having mixed characteristic $p > 0$ and R the integral closure of S in a pth root extension of its quotient field. We show that R admits a finite, birational module M such that $depth(M) = dim(R)$. In other words, R admits a maximal Cohen-Macaulay module.

1. Introduction

Let R be a Noetherian local ring. In considering the local homological conjectures over R, one may reduce to the situation where R is a finite extension of an unramified regular local ring S. Therefore, it is a natural point of departure to assume that R is the integral closure of S in a "well-behaved" algebraic extension of its quotient field. Certainly, when S has mixed characteristic $p > 0$, one ought to consider the case that R is the integral closure of S in an extension of its quotient field obtained by adjoining the pth root of an element of S. This was done in [Ko] where it was shown that S is a direct summand of R, i.e., the Direct Summand Conjecture holds for the extension $S \subseteq R$. In this note we show that a number of the other local homological conjectures hold for such R by showing that R admits a finite, birational module M satisfying $depth(M) = dim(R)$ (see [H]). In other words, R admits a maximal Cohen-Macaulay module. Such a module is necessarily free over S. Aside from regularity, one of the crucial points in the mixed characteristic case seems to be that S/pS is integrally closed. By contrast, using an example from [HM], Roberts has noted that even if S is a Cohen-Macaulay UFD and R is the integral closure of S in a quadratic extension of quotient fields, R needn't admit a finite, S-free module at all (see [R]). For the example in question, S has mixed characteristic 2, yet $S/2S$ is not integrally closed.

2. Preliminaries

In this section we will establish our notation and present a few preliminary observations. Throughout, S will be a Noetherian normal domain with quotient field L. We assume $char(L) = 0$. Fix $p \in \mathbb{Z}$ to be a prime integer and suppose that either p is a unit in S or that pS is a (proper) prime ideal and S/pS is integrally closed. Let $f \in S$ be an element that is not a pth power and select W an indeterminate. Write $F(W) := W^p - f \in S[W]$, a monic irreducible polynomial

Received by the editors August 26, 1997 and, in revised form, November 26, 1997.
1991 *Mathematics Subject Classification.* Primary 13B21, 13B22, 13H05, 13H15.

and 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 $S[\omega]$.

Our strategy in this paper is to exploit the fact that R can be realized as J^{-1} for a suitable ideal $J \subseteq S[\omega]$. The study of birational algebras of the form J^{-1} seems to have captured the attention of a number of researchers during the last few years, albeit in notably different contexts (see [EU], [Ka], [KU], [MP] and [V]). Since J^{-1} inherits S_2 from $S[\omega]$, this means that in attempting to "construct" R, if the candidate is J^{-1} for some J, then only the condition R_1 must be checked.

The following proposition summarizes some of the conditions relating R to J^{-1} for suitable J that we will call upon in the next section. Parts (i) and (ii) of the proposition were inspired by the main results in [V] and Proposition 3.1 in [KU]. Special cases of part (iii) of the proposition have apparently been known to algebraic geometers for a long while. For some historical comments and fascinating variations, the interested reader should consult [KU].

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) *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 $1 \le i \le n$, $rad(J_i) = P_i$ and $(J_i^{-1})_{P_i} = A'_{P_i}$, then $A' = J^{-1}$, for $J := J_1 \cap \cdots \cap J_n$.*
- (ii) *If $A \neq A'$, then $A' = J^{-1}$, for some height one unmixed ideal $J \subseteq A$. Moreover, if A is Gorenstein in codimension one, then $A' = J^{-1}$ for a unique height one unmixed ideal J satisfying $J \cdot J^{-1} = J = (J^{-1})^{-1}$.*
- (iii) *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, $p.d._B(J) = p.d._B(J^{-1}) = 1$.*

Proof. To prove (i), note that $J_Q^{-1} = A'_Q$ for all height one primes $Q \subseteq A$. Since J^{-1} and A' are birational and satisfy S_2, we obtain $J^{-1} = A'$. For the first statement in (ii), we may, by part (i), consider the case where A is a one-dimensional local ring which is not a DVR. Let Q denote the maximal ideal of A. Then $QQ^{-1} \subseteq Q$. Since it always holds that $Q \subseteq QQ^{-1}$, we have $Q = QQ^{-1}$. Therefore Q^{-1} is a finite ring extension properly containing A (since for any ideal J, $(JJ^{-1})^{-1}$ is a ring). If $Q^{-1} = A'$, we're done. If not, then since Q^{-1} inherits S_2 from A, Q^{-1} contains a height one prime P for which $(Q^{-1})_P$ is not a DVR. Thus P^{-1} is a finite ring extension properly containing Q^{-1}. An easy calculation shows that P^{-1}, considered over Q^{-1}, equals $(QP)^{-1}$, considered over A. Iterating this process shows we eventually obtain $A' = J^{-1}$, for some $J \subseteq A$. Now suppose that A is Gorenstein in codimension one. Then $I_Q = ((I^{-1})^{-1})_Q$, for all ideals $I \subseteq A$ and all height one primes $Q \subseteq A$. Therefore, $I = (I^{-1})^{-1}$, for all height one, unmixed ideals $I \subseteq A$. In particular, this holds for J. Moreover, if $J^{-1} = A' = K^{-1}$, for K height one and unmixed, then $J = K$. Finally, since J^{-1} is a ring, $(J \cdot J^{-1}) \cdot J^{-1} = J \cdot J^{-1}$, so $J \cdot J^{-1} \subseteq (J^{-1})^{-1} = J$. Thus, $J \cdot J^{-1} = J$, as desired. For (iii), the description of the generators for J^{-1} follows either from [MP], Proposition 3.14 or [KU], Lemma 2.5. For the second part of (iii), see [KU], Proposition 3.1. □

Returning to our basic set-up, we note that since S is a normal domain, $S[\omega]$ satisfies Serre's condition S_2. Moreover, since $char(S) = 0$, R is a finite S-module. Thus Proposition 2.1 applies. In Section 3 we will identify the ideal $J \subseteq S[\omega]$ for which $J^{-1} = R$. In the meantime, we observe that if p is not a unit in S, then there is a unique height one prime in $S[\omega]$ containing p. Suppose $p \mid f$. Then $P := (\omega, p)$ is clearly the unique height one prime in $S[\omega]$ containing p. Moreover, $S[\omega]_P$ 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. Thus $(p, F(W))$ 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. If $f \equiv h^p \bmod pS$, then $F(W) \equiv (W-h)^p \bmod pS$ and it follows that $(\omega - h, p)S[\omega]$ is the unique height one prime in $S[\omega]$ containing p. Thus, in all cases, there exists a unique height one prime in $S[\omega]$ lying over pS. *For the remainder of the paper, we call this prime P.* Suppose $f = h^p + gp$, so $P = (\omega - h, p)S[\omega]$. Write $\tilde{P} := (W - h, p)S[W]$ for the preimage of P in $S[W]$. Then

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

In $S[W]$, $W^{p-1} + \cdots + h^{p-1} \equiv ph^{p-1}$ modulo $(W - h)$, so $W^{p-1} + \cdots + h^{p-1} \in \tilde{P}$. 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 $f = h^p + p^2 g$, for some $h, g \in S$.

3. The main result

In this section we will present our main result, Theorem 3.8. Lemmas 3.2 and 3.3 will enable us to describe the ideal $J \subseteq S[\omega]$ for which $R = J^{-1}$. We will then see in the proof of Theorem 3.8 that the module we seek has the form I^{-1}, for some ideal $I \subseteq J$.

Lemma 3.1. *Suppose p is not a unit in S, $h \in S\backslash pS$ and $p = 2k + 1$. Set*

$$C := \sum_{j=1}^{k} (-1)^{j+1} \binom{p}{j} (W \cdot h)^j [W^{p-2j} - h^{p-2j}],$$

$C' := C \cdot (p(W - h))^{-1}$ and $\tilde{P} := (p, W - h) \cdot S[W]$. Then $C' \notin \tilde{P}$.

Proof. Note that since p divides $\binom{p}{j}$ for all $1 \le j \le k$, C' is a well-defined element of $S[W]$. Now, $C' \notin \tilde{P}$ if and only if the residue class of C' modulo $W - h$, as an element of S, does not belong to pS if and only if $\sum_{j=1}^{k} (-1)^{j+1} \binom{p}{j} \frac{h^{p-1}}{p} (p - 2j)$, as an element of S, is not divisible by p. Since

$$\sum_{j=1}^{k} (-1)^{j+1} \binom{p}{j} h^{p-1}$$

is divisible by p and h^{p-1} is not divisible by p, it is enough to show that

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

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

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

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

For the next lemma, we borrow the following terminology from [Kap]. We shall say that $f \in S$ is "square-free" if $qS_q = fS_q$ for all height one prime ideals $q \subseteq S$ containing f. Since $F'(\omega)\cdot R \subseteq S[\omega]$ and $\omega\cdot F'(\omega) = p\cdot f$, it follows from the discussion in Section 2 that if f is square-free, then either $R = S[\omega]$ or P is the only height one prime for which $S[\omega]_P$ is not a DVR.

Lemma 3.2. *Suppose $f \in S$ is square-free and $S[\omega] \neq R$ (thus p is not a unit in S). Then $R = P^{-1}$. Moreover, R is a free S-module.*

Proof. We first consider the case $p > 2$. Since $S[\omega]$ is not integrally closed, we have $f = h^p + p^2 g$, for some h not divisible by p and $g \neq 0$ in S. Thus, $P = (\omega - h, p)S[\omega]$. It follows from the proof and statement of Proposition 2.1 that P^{-1} is a ring and that P^{-1} is generated as an $S[\omega]$-module by $\{1, \tau\}$, for

$$\tau = \frac{1}{p}\cdot\sum_{j=1}^{p}\omega^{p-j}h^{j-1} = \frac{g\cdot p}{\omega - h}.$$

Therefore $P^{-1} = S[\omega,\tau]$. If we show that $S[\omega,\tau]$ satisfies R_1, then $S[\omega,\tau] = R$, since P^{-1} satisfies S_2 (as an $S[\omega]$-module and as a ring). Since f is square-free, it suffices to show that P^{-1}_Q is a DVR for each height one $Q \subseteq P^{-1}$ containing p. To do this, we find an equation satisfied by τ over $S[\omega]$. On the one hand,

$$(\omega - h)\cdot\tau = 0\cdot(w - h) + g\cdot p.$$

On the other hand,

$$p\cdot\tau = (\omega - h)^{p-2}\cdot(\omega - h) + c'\cdot p,$$

where c' denotes the image in $S[\omega]$ of the element $C' \in S[W]$ defined in Lemma 3.1. Therefore, by the standard determinant argument, τ satisfies

$$l(T) := T^2 - c'T - g(\omega - h)^{p-2}$$

over $S[\omega]$. Now, let $\pi : S[W,T] \to S[\omega,\tau]$ denote the canonical map and set $H := ker(\pi)$ and let $Q \subseteq S[\omega,\tau]$ be any height one prime containing p. Then Q corresponds to a height three prime $Q' \subseteq S[W,T]$ containing p and H. Since $P \subseteq Q$ and $H \subseteq Q'$, $W - h$ and $T^2 - C'T - g(W-h)^{p-2}$ belong to Q'. Therefore, $Q' = (p, W-h, T)$ or $Q' = (p, W-h, T-C')$. Suppose $Q' = (p, W-h, T)$. Then $Q = (p, \omega - h, \tau)S[\omega,\tau]$. We have

$$\tau^2 - c'\tau - g(\omega - h)^{p-2} = 0 \quad\text{and}\quad p(\tau - c') = (\omega - h)^{p-1}.$$

By Lemma 3.1, $c' \notin Q$, so $\tau - c' \notin Q$, and it follows that $Q_Q = (\omega - h)_Q$. Now suppose $Q' = (p, W-h, T-C')$. Then $Q = (p, \omega - h, \tau - c')S[\omega,\tau]$. Since

$$\tau^2 - c'\tau - g(\omega - h)^{p-2} = 0 \quad\text{and}\quad (\omega - h)\cdot\tau = g\cdot p,$$

it follows that $Q_Q = (p)_Q$ (since $\tau \notin Q$, by Lemma 3.1). Thus, in either case, Q_Q is principal, so $R = S[\omega,\tau] = P^{-1}$.

The proof is similar if $p = 2$ and $f = h^2 + 4g$, with $2 \nmid h$. One notes that $P^{-1} = S[\omega, \tau] = S[\tau]$, for $\tau := \frac{h+\omega}{2}$ and that τ satisfies $l(T) := T^2 - hT - g$. To show $R = S[\tau]$, one uses the fact that $l(T)$ and $l'(T)$ are relatively prime over the quotient field of $S/2S$.

To see that R is a free S-module, we first note that R is clearly generated as an S-module by the set $\{1, \omega, \dots, \omega^{p-1}, \tau, \tau\omega, \dots, \tau\omega^{p-1}\}$. However, $\tau\omega = pg \cdot 1 + h \cdot \tau$. This implies that $\tau\omega^i$ belongs to the S-module generated by $\{1, \omega, \dots, \omega^{p-1}, \tau\}$, for all $1 \le i \le p-1$. Moreover, since

$$\omega^{p-1} = -h^{p-1} \cdot 1 - h^{p-2} \cdot \omega - \cdots - h \cdot \omega^{p-2} + p \cdot \tau,$$

we may dispose of ω^{p-1} as well. Thus, R is generated as an S-module by the set $\{1, \omega, \dots, \omega^{p-2}, \tau\}$. Since these elements are clearly linearly independent over S, R is a free S-module. □

Lemma 3.3. *Suppose $f = \lambda a^e$, with $a \in S$ a prime element, λ a unit in S and $2 \le e < p$. If p is not a unit in S, assume $a = p$. Then there exist integers $1 \le s_1 < s_2 < \cdots < s_{e-1} < p$ satisfying*

(i) $s_{e-i} \le p - s_i$, $1 \le i \le e-1$.
(ii) $R = J^{-1}$ *for* $J := (\omega^{s_{e-1}}, \omega^{s_{e-2}}a, \dots, \omega^{s_1}a^{e-2}, a^{e-1})S[\omega]$.

Proof. We begin by noting that either condition in the hypothesis implies that $Q := (\omega, a)S[\omega]$ is the only height one prime for which $S[\omega]_Q$ is not a DVR. Now, since p and e are relatively prime, we can find positive integers u and v such that $1 = u \cdot p + (-v) \cdot e$. If we set $\tau := \frac{a^u}{\omega^v}$, then $\tau^e = \lambda^{-u}\omega$ and $\tau^p = \lambda^{-v}a$. It follows that $S[\omega, \tau] = S[\tau] = R$, since either p is a unit and a is square-free or p is not a unit and $(\tau, p)S[\tau] = \tau S[\tau]$. Thus, $\{1, \tau, \dots, \tau^{e-1}\}$ generate R as an $S[\omega]$-module. Since u and e are relatively prime, the set $\{uj\}_{1 \le j \le e-1}$, when reduced mod e, equals the set $\{i\}_{1 \le i \le e-1}$. This will enable us to replace the generators $\{1, \tau, \dots, \tau^{e-1}\}$ by $\{1, \frac{\lambda a}{\omega^{s_1}}, \dots, \frac{\lambda a^{e-1}}{\omega^{s_{e-1}}}\}$. To elaborate, given $1 \le i \le e-1$, there is a unique $1 \le j_i \le e-1$ such that $uj_i \equiv i \pmod{e}$. Write $uj_i = t_i e + i$, $t_i \ge 0$. Then

$$(1 + ve)j_i = puj_i = t_i ep + ip,$$

so $(vj_i)e + j_i = (t_i p)e + ip$. If we write $ip = s_i e + r$, with $0 \le r < e$, then uniqueness of the euclidean algorithm gives $vj_i = t_i p + s_i$ and $r = j_i$. Thus, $\tau^{j_i} = \frac{a^{uj_i}}{\omega^{vj_i}} = \frac{a^i}{\lambda^{t_i}\omega^{s_i}}$ and $ip = s_i e + j_i$. For $i = e-1$, this yields $s_{e-1} < p$. Moreover, $p = (s_{i+1} - s_i)e + (j_{i+1} - j_i)$, so $s_{i+1} - s_i > 0$. Similarly, $ep = (s_{e-i} + s_i)e + (j_{e-i} + j_i)$, so $s_{e-i} + s_i \le p$. Thus, $s_1, \dots, s_{e-1}$ have the required numerical properties.

We now have $\{1, \tau, \dots, \tau^{e-1}\} = \{1, \frac{a}{\lambda^{t_1}\omega^{s_1}}, \dots, \frac{a^{e-1}}{\lambda^{t_{e-1}}\omega^{s_{e-1}}}\}$. Multiplying by appropriate powers of λ allows us to use $\{1, \frac{\lambda a}{\omega^{s_1}}, \dots, \frac{\lambda a^{e-1}}{\omega^{s_{e-1}}}\}$ as a generating set for R over $S[\omega]$. In Proposition 2.1 take $A := S[\omega]$, $B := S[W]$, $F := F(W)$ and $\tilde{J}$ the ideal of $(e-1) \times (e-1)$ signed 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 $\alpha_1 + \alpha_2 + \cdots + \alpha_i = s_i$, for $1 \le i \le e-1$. To obtain ϕ', we augment ϕ by the column whose transpose is $(W^{p-c}, 0, \ldots, 0, (-1)^e \lambda a)$ (so $det(\phi') = F(W)$). Then J^{-1} is generated as an $S[\omega]$-module by $\{1, \frac{\lambda a}{\omega^{s_1}}, \ldots, \frac{\lambda a^{e-1}}{\omega^{s_{e-1}}}\}$. Thus, $R = S[\omega, \tau] = J^{-1}$ for $J = (\omega^{s_{e-1}}, \omega^{s_{e-2}} a, \ldots, a^{e-1})$, as desired. □

For a proof of the next lemma, see [Ka], Lemma 4.1.

Lemma 3.4. *In $S[W]$ consider the ideals $H := (W^{e_k}, W^{e_{k-1}} a_1, \ldots, W^{e_1} a_{k-1}, a_k)$ and $K := (W^{f_t}, W^{f_{t-1}} b_1, \ldots, W^{f_1} b_{t-1}, b_t)$, where*

(i) *$e_k > e_{k-1} > \cdots > e_1$ and $f_t > f_{t-1} > \cdots > f_1$.*
(ii) *$a_1 \mid a_2 \mid \cdots \mid a_k$ and $b_1 \mid b_2 \mid \cdots \mid b_t$.*
(iii) *Each a_i and b_j is a product of prime elements.*
(iv) *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 $H \cap K = (W^{g_s}, W^{g_{s-1}} c_1, \ldots, W^{g_1} c_{s-1}, c_s)$. Moreover, H, K and $H \cap K$ are all grade two perfect ideals.

Lemma 3.5. *Let A be a domain and $I \subseteq J$ ideals such that J^{-1} is a ring. Then I^{-1} is a J^{-1}-module if and only if $I^{-1} = (I \cdot J^{-1})^{-1}$. In particular, if $x \in J$ and $x \cdot J^{-1} \subseteq J$, then $(x \cdot J^{-1})^{-1}$ is a J^{-1}-module.*

Proof. We first observe $(I \cdot J^{-1})^{-1}$ is always a J^{-1}-module. Indeed, $y \in (I \cdot J^{-1})^{-1}$ implies $I \cdot J^{-1} y \subseteq R$. Thus $J^{-1} J^{-1} y = J^{-1} y \subseteq I^{-1}$, so $(I \cdot J^{-1})(J^{-1} y) \subseteq R$ and $J^{-1} y \subseteq (I \cdot J^{-1})^{-1}$. Therefore, $(I \cdot J^{-1})^{-1}$ is a J^{-1}-module and the first statement follows easily from this. For the second statement, we note that if $x \cdot J^{-1} \subseteq J$, then for $I := x \cdot J^{-1}$, $I \cdot J^{-1} = x \cdot J^{-1} J^{-1} = x \cdot J^{-1} = I$. Thus, $I^{-1} = (I \cdot J^{-1})^{-1}$, so I^{-1} is a J^{-1}-module by the first statement. □

Remark 3.6. Proposition 2.2 in [Ko] states that R is a free S-module, if S is an unramified regular local ring and $p \mid f$. The proof shows that R is a free S-module just under the assumption that f can be written as a product of primes and S/pS is a domain. In [Ko], Proposition 1.5, it is shown that if S is a UFD, then there exists a free S-module $F \subseteq R$ such that pR is contained in F. Thus, if p is a unit in S, then R is also a free S-module. Finally, if f is square-free, R is a free S-module by Lemma 3.2. We record these facts in a common setting in the following proposition. For a version of the proposition for p^nth root extensions, see [Ka], Theorem 4.2.

Proposition 3.7. *In addition to our standing hypotheses, assume that S is a UFD. Then R is a free S-module in each of the following cases:*

(i) *p is a unit in S.*
(ii) *p is not a unit and either $p \mid f$ or f is square-free.*

We are now ready for our theorem.

Theorem 3.8. *Assume that S is a regular local ring. Then there exists a finite, birational R-module M satisfying $depth_S(M) = dim(R)$. In other words, M is a maximal Cohen-Macaulay module for R.*

Proof. By Proposition 3.7, R is a free S-module, and therefore Cohen-Macaulay, unless we assume that p is not a unit in S, $p \nmid f$ and f is not square-free. In particular, we may assume that f is not a unit in S. Factor f as a unit λ times prime elements a_i, say $f = \lambda a_1^{e_1} \cdots a_r^{e_r}$. We may assume that for $1 \le t \le r$, $1 < e_i < p$, if $1 \le i \le t$ and $e_i = 1$, if $t < i \le r$. Set $Q_i := (\omega, a_i) S[\omega]$ for $1 \le i \le t$. For each $1 \leq i \leq t$ choose $s(i,1) < \cdots < s(i,e_i-1)$ satisfying the conclusion of Lemma 3.3 over $S[\omega]_{Q_i}$ and set $J_i := (\omega^{s(i,e_i-1)}, \omega^{s(i,e_i-2)}a_i, \ldots, \omega^{s(i,1)}a_i^{e_i-2}, a_i^{e_i-1})S[\omega]$. Thus, $R_{Q_i} = (J_i^{-1})_{Q_i}$ for all i. We now have two cases to consider. Suppose first that f is not a pth power modulo p^2S. We will show that R is Cohen-Macaulay. By our discussion in section two, $Q_1, \ldots, Q_t$ are exactly the height one primes $Q \subseteq S[\omega]$ for which $S[\omega]_Q$ is not a DVR, so by Proposition 2.1 and Lemma 3.3, $R = J^{-1}$ for $J := J_1 \cap \cdots \cap J_t$. Set $B := S[W]_{(W,N)}$ (for N, the maximal ideal of S) and use "tilde" to denote pre-images in B. By Lemma 3.4, $\tilde{J} \subseteq B$ is a grade two perfect ideal. Therefore, $p.d._B(J) = p.d._B(J^{-1}) = 1$, by Proposition 2.1(iii). Thus, $depth_B(J^{-1}) = dim(B) - 1$, so $depth_S(R) = dim(R)$, which is what we want.

Suppose that f is a pth power modulo p^2S. Write $f = h^p + p^2g$, for $h, g \in S$, $p \nmid h$. Then $P = (\omega - h, p)$. Moreover, P and $Q_1, \ldots, Q_t$ are the height one primes $Q \subseteq S[\omega]$ for which $S[\omega]_Q$ is not a DVR. By Proposition 2.1 and Lemma 3.2, $R = J^{-1}$, for $J := J_1 \cap \cdots \cap J_t \cap P$. Now, as in the proof of Lemma 3.3, J_i^{-1} is generated as an $S[\omega]$-module by the set $\{1, \frac{\lambda_i a_i}{\omega^{s(i,1)}}, \ldots, \frac{\lambda_i a_i^{e_i-1}}{\omega^{s(i,e_i-1)}}\}$, where, for each i, $\lambda_i := \prod_{i \neq j=1}^{r} \lambda a_j^{e_j}$. Thus $K_i = (\omega^{p-s(i,1)}, \omega^{p-s(i,2)}a_i, \ldots, a_i^{e_i-1})S[\omega]$, for $K_i := a_i^{e_i-1} \cdot J_i^{-1}$ and $1 \leq i \leq t$. By Lemma 3.3, $K_i \subseteq J_i$, so upon setting $I := K_1 \cap \cdots \cap K_t \cap P$, it follows from Lemma 3.5 that I^{-1} is a J^{-1}-module (since this holds locally for every height one prime in $S[\omega]$). Taking $M := I^{-1}$, we will show that M is the required module. For this, we claim that $\tilde{I} \subseteq B$ is a grade two perfect ideal. If the claim holds, $1 = p.d._B(I) = p.d._B(I^{-1}) = p.d._B(M)$. Thus $depth_B(M) = dim(B) - 1$, so $depth_S(M) = dim(R)$, which is what we want.

To prove the claim, we set $\tilde{K} := \tilde{K}_1 \cap \cdots \cap \tilde{K}_t$ and consider the short exact sequence

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

Since $\tilde{K}$ is a grade two perfect ideal (by Lemma 3.4), the Depth Lemma and the Auslander-Buchsbaum formula imply that $\tilde{I}$ is a grade two perfect ideal, once we show $depth(B/(\tilde{K}+\tilde{P})) = dim(B) - 3$. Set $a := a_1^{e_1-1} \cdots a_t^{e_t-1}$. We now argue that $\tilde{K} + \tilde{P} = (a, p, W - h)$. If we can show this, clearly $depth(B/(\tilde{K}+\tilde{P})) = dim(B) - 3$ and we will have verified the claim. Take $\tilde{k} \in \tilde{K}$ and consider its image k in $K \subseteq S[\omega]$. Select $Q \subseteq S[\omega]$, a height one prime. If $Q = Q_i$, for some $1 \leq i \leq t$, then $k \in (a_i^{e_i-1}J_i^{-1})_{Q_i} = aR_{Q_i}$. If $Q \neq Q_i$ for any $1 \leq i \leq t$, then clearly $k \in aR_Q = R_Q$. It follows that $k \in aR \cap S[\omega]$. In other words, k is integral over the principal ideal $aS[\omega]$. Therefore, the image of k in $S[\omega]/(\omega - h, p) = S/pS$ is integral over the principal ideal generated by the image of a. Since S/pS is integrally closed, the image of k in S/pS is a multiple of the image of a. Therefore, $\tilde{k} \in (a, p, W - h)$ in $S[W]$. It follows that $\tilde{K} \subseteq (a, p, W - h)$. Since $a \in \tilde{K}$, we obtain $\tilde{K} + \tilde{P} = (a, p, W - h)$, which is what we want. This completes the proof of Theorem 3.8. □

Remark 3.9. Of course if S is an unramified regular local ring, S fulfills our standing hypotheses, so Theorem 3.8 applies. However, the theorem also applies to certain ramified regular local rings. For instance, take T to be the ring $\mathbb{Z}[X_1, \ldots, X_d]$ localized at $(p, X_1, \ldots, X_d)$ and let $H \in \mathbb{Z}[X_1, \ldots, X_d]$ be any polynomial in $(X_1, \ldots, X_d)^2$ for which $\mathbb{Z}_p[X_1, \ldots, X_d]/(\overline{H})$ is an integrally closed domain. If we set $S := T/(p - H)$, then S is a ramified regular local ring and S/pS is an integrally closed domain.

We close with an example where R is not a free S-module, yet R admits a finite, birational module which is a free S-module. The example is an unramified variation of Koh's Example (2.4).

Example 3.10. Let S be an unramified regular local ring having mixed characteristic 3 and take $x, y \in S$ such that $3, x, y$ form part of a regular system of parameters. Set $a := xy^4 + 9$, $b := x^4y + 9$ and $f := ab^2$, so $\omega^3 = f = ab^2 = h^3 + 9g$, for $h = x^3y^2$. From Lemmas 3.2 and 3.3 it follows that $R = (Q \cap P)^{-1}$ for $Q := (\omega, b)$ and $P := (\omega - h, 3)$. Set $J := Q \cap P$. We first show that $R = J^{-1}$ is not a free S-module. Suppose to the contrary that J^{-1} is free over S. As in the proof of Theorem 3.8, set $B := S[W]_{(N,W)}$ and use "tilde" to denote pre-images in B. Since J^{-1} is free over S, we have $p.d._B(J^{-1}) = 1$, so J^{-1} is a grade one perfect B-module. By [KU, Proposition 3.6], J is a grade one perfect B-module, so $\tilde{J}$ is a grade two perfect ideal. On the other hand, $depth_B(B/\tilde{J}) = 1 + depth_B(B/(\tilde{Q} + \tilde{P}))$. But, $\tilde{Q} + \tilde{P} = (W, x^4y, x^3y^2, 3)B$, so $B/(\tilde{Q} + \tilde{P}) = S/(3, x^4y, x^3y^2)S$, which is easily seen to have depth equal to $depth(S) - 3 = depth(B) - 4$. This is a contradiction, so it must hold that R is not a free S-module.

Now, Q^{-1} is generated as an $S[\omega]$-module by $\{1, \frac{ab}{\omega}\}$. If we set $K := b \cdot Q^{-1}$, then $K = (\omega^2, b)S[\omega]$. The proof of Theorem 3.8 shows that $M := (K \cap P)^{-1}$ is a finite, birational R-module satisfying $depth_S(M) = dim(R)$. In other words, M is an R-module which is free over S. To calculate a basis for M, one must calculate $K \cap P$ and then use Proposition 2.1. We leave it to the reader to check that $K \cap P = (\omega^2 - h^2 - 9x^2y^3, b(\omega - h), 3b)$. Therefore, $K \cap P = I_2(\phi)$ for

$$\phi = \begin{pmatrix} -b & 0 \\ \omega + h & -3 \\ -3x^2y^3 & \omega - h \end{pmatrix}.$$

The augmented matrix that determines $(K \cap P)^{-1} = M$ is the 3×3 matrix

$$\begin{pmatrix} -b & 0 & \omega \\ \omega + h & -3 & x^2y^3 \\ -3x^2y^3 & \omega - h & t \end{pmatrix},$$

where t is defined by the equation $x^5y^5 = ab + 3t$. By Proposition 2.1, M is generated as an $S[\omega]$-module by the set $\{1, \gamma, \delta\}$, for

$$\gamma := \frac{-3t - x^2y^3(\omega - h)}{\omega^2 - h^2 - 9x^2y^3} = \frac{\omega}{b}, \qquad \delta := \frac{-bt + 3x^2y^3\omega}{b(\omega - h)} = \frac{\omega^2 + \omega h + h^2 + 9x^2y^3}{3b}.$$

If we show that $\{1, \gamma, \delta\}$ also generate M as an S-module, then since they are clearly linearly independent over S, they form a basis for M as an S-module. To see that $\{1, \gamma, \delta\}$ generate M as an S-module, it suffices to show that $\omega, \omega \cdot \gamma$ and $\omega \cdot \delta$ can be expressed as S-linear combinations of $\{1, \gamma, \delta\}$. This clearly holds for ω. Using $9x^2y^3 = bx^2y^3 - x^6y^4$, we obtain

$$\omega \cdot \gamma = \frac{\omega^2}{b} = -x^2y^3 \cdot 1 - h \cdot \gamma + 3 \cdot \delta.$$

Since $\omega^3 = h^3 + 9g$ and $g = x^5y^5 + bxy^4 + b^2$, we get

$$\omega \cdot \delta = (3xy^4 + 3b) \cdot 1 + 3x^2y^3 \cdot \gamma + h \cdot \delta,$$

and the example is complete.

Acknowledgements

I would like to thank both the referee and Craig Huneke for their helpful comments on how to improve the readability of this paper.

References

[EU] D. Eisenbud and B. Ulrich, *Modules that are finite birational algebras*, Illinois Jl. Math **141 No. 1** (1997), 10-15. CMP 97:08

[H] M. Hochster, *Topics in the homological theory of modules over commutative rings*, C.B.M.S. Reg. Conf. Ser. in Math., vol. 24, A.M.S., Providence, RI, 1975. MR **51:**8096

[HM] M. Hochster and J.E. McLaughlin, *Splitting theorems for quadratic ring extensions*, Illinois Jl. Math. **127 No. 1** (1983), 94-103. MR **85c:**13015

[Kap] I. Kaplansky, *Commutative Rings II*, University of Chicago, Lecture Notes.

[Ka] D. Katz, *P^nth root extensions in mixed characteristic p*, preprint (1997).

[KU] S. Kleiman and B. Ulrich, *Gorenstein algebras, symmetric matrices, self-linked ideals, and symbolic powers*, Trans. AMS **349** (1997), 4973–5000. MR **98c:**13019

[Ko] J. Koh, *Degree p extensions of an unramified regular local ring of mixed characteristic* $p > 0$, J. of Algebra **99** (1986), 310-323. MR **87j:**13027

[MP] D. Mond and R. Pellikaan, *Fitting ideals and multiple points of analytic mappings*, Springer Lecture Notes in Mathematics **1414** (1989), 107-161. MR **91e:**32035

[R] P. Roberts, *Abelian extensions of regular local rings*, Proc AMS **78, No 3** (1980), 307-319. MR **81a:**13017

[V] W. Vasconcelos, *Computing the integral closure of an affine domain*, Proc. AMS **113** (1991), 633-638. MR **92b:**13013

Department of Mathematics, University of Kansas, Lawrence, Kansas 66045
E-mail address: dlk@math.ukans.edu