ELSEVIER
Available online at www.sciencedirect.com
SciVerse ScienceDirect
Advances in Mathematics 229 (2012) 1847–1861
ADVANCES IN Mathematics
www.elsevier.com/locate/aim

Galois extensions, plus closure, and maps on local cohomology

Akiyoshi Sannai [a,1], Anurag K. Singh [b,*,2]

[a] *Graduate School of Mathematical Sciences, The University of Tokyo, 3-8-1 Komaba, Meguro, Tokyo 153-8914, Japan*
[b] *Department of Mathematics, University of Utah, 155 S. 1400 E., Salt Lake City, UT 84112, USA*

Received 1 April 2011; accepted 20 December 2011

Available online 23 December 2011

Communicated by Karen Smith

Abstract

Given a local domain $(R, \mathfrak{m})$ of prime characteristic that is a homomorphic image of a Gorenstein ring, Huneke and Lyubeznik proved that there exists a module-finite extension domain S such that the induced map on local cohomology modules $H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(S)$ is zero for each $i < \dim R$. We prove that the extension S may be chosen to be generically Galois, and analyze the Galois groups that arise.

MSC: primary 13D45; secondary 13A35, 14B15, 14F17

Keywords: Characteristic p methods; Local cohomology; Big Cohen–Macaulay algebras; Integral ring extensions; Galois extensions

1. Introduction

Let R be a commutative Noetherian integral domain. We use R^+ to denote the integral closure of R in an algebraic closure of its fraction field. Hochster and Huneke proved the following:

* Corresponding author.
E-mail addresses: sannai@ms.u-tokyo.ac.jp (A. Sannai), singh@math.utah.edu (A.K. Singh).

[1] The author was supported by the Excellent Young Researcher Overseas Visit Program of the Japan Society for Promotion of Science (JSPS).

[2] The author was supported by NSF grant DMS 0856044.

0001-8708/$ – see front matter
doi:10.1016/j.aim.2011.12.021

Theorem 1.1. *(See [8, Theorem 1.1].) If R is an excellent local domain of prime characteristic, then each system of parameters for R is a regular sequence on R^+, i.e., R^+ is a balanced big Cohen–Macaulay algebra for R.*

It follows that for a ring R as above, and $i < \dim R$, the local cohomology module $H^i_{\mathfrak{m}}(R^+)$ is zero. Hence, given an element $[\eta]$ of $H^i_{\mathfrak{m}}(R)$, there exists a module-finite extension domain S such that $[\eta]$ maps to 0 under the induced map $H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(S)$. This was strengthened by Huneke and Lyubeznik, albeit under mildly different hypotheses:

Theorem 1.2. *(See [10, Theorem 2.1].) Let $(R, \mathfrak{m})$ be a local domain of prime characteristic that is a homomorphic image of a Gorenstein ring. Then there exists a module-finite extension domain S such that the induced map*

$$H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(S)$$

is zero for each $i < \dim R$.

By a *generically Galois extension* of a domain R, we mean an extension domain S that is integral over R, such that the extension of fraction fields is Galois; $\mathrm{Gal}(S/R)$ will denote the Galois group of the corresponding extension of fraction fields. We prove the following:

Theorem 1.3. *Let R be a domain of prime characteristic.*

(1) *Let $\mathfrak{a}$ be an ideal of R and $[\eta]$ an element of $H^i_{\mathfrak{a}}(R)_{\mathrm{nil}}$ (see Section 2.3). Then there exists a module-finite generically Galois extension S, with $\mathrm{Gal}(S/R)$ a solvable group, such that $[\eta]$ maps to 0 under the induced map $H^i_{\mathfrak{a}}(R) \longrightarrow H^i_{\mathfrak{a}}(S)$.*
(2) *Suppose $(R, \mathfrak{m})$ is a homomorphic image of a Gorenstein ring. Then there exists a module-finite generically Galois extension S such that the induced map $H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(S)$ is zero for each $i < \dim R$.*

Set $R^{+\mathrm{sep}}$ to be the R-algebra generated by the elements of R^+ that are separable over $\mathrm{frac}(R)$. Under the hypotheses of Theorem 1.3(2), $R^{+\mathrm{sep}}$ is a separable balanced big Cohen–Macaulay R-algebra; see Corollary 3.3. In contrast, the algebra R^∞, i.e., the purely inseparable part of R^+, is not a Cohen–Macaulay R-algebra in general: take R to be an F-pure domain that is not Cohen–Macaulay; see [8, p. 77].

For an $\mathbb{N}$-graded domain R of prime characteristic, Hochster and Huneke proved the existence of a $\mathbb{Q}$-graded Cohen–Macaulay R-algebra $R^{+\mathrm{GR}}$, see Theorem 5.1. In view of this and the preceding paragraph, it is natural to ask whether there exists a $\mathbb{Q}$-graded separable Cohen–Macaulay R-algebra; in Example 5.2 we show that the answer is negative.

In Example 5.3 we construct an $\mathbb{N}$-graded domain of prime characteristic for which no module-finite $\mathbb{Q}$-graded extension domain is Cohen–Macaulay.

We also prove the following results for closure operations; the relevant definitions may be found in Section 2.1.

Theorem 1.4. *Let R be an integral domain of prime characteristic, and let $\mathfrak{a}$ be an ideal of R.*

(1) *Given an element $z \in \mathfrak{a}^F$, there exists a module-finite generically Galois extension S, with $\mathrm{Gal}(S/R)$ a solvable group, such that $z \in \mathfrak{a}S$.*

(2) *Given an element $z \in \mathfrak{a}^+$, there exists a module-finite generically Galois extension S such that $z \in \mathfrak{a}S$.*

In Example 4.1 we present a domain R of prime characteristic where $z \in \mathfrak{a}^+$ for an element z and ideal $\mathfrak{a}$, and conjecture that $z \notin \mathfrak{a}S$ for each module-finite generically Galois extension S with $\mathrm{Gal}(S/R)$ a solvable group. Similarly, in Example 4.3 we present a 3-dimensional ring R where we conjecture that $H^2_{\mathfrak{m}}(R) \longrightarrow H^2_{\mathfrak{m}}(S)$ is nonzero for each module-finite generically Galois extension S with $\mathrm{Gal}(S/R)$ a solvable group.

Remark 1.5. The assertion of Theorem 1.2 does not hold for rings of characteristic zero: Let $(R, \mathfrak{m})$ be a normal domain of characteristic zero, and S a module-finite extension domain. Then the field trace map $\mathrm{tr} : \mathrm{frac}(S) \longrightarrow \mathrm{frac}(R)$ provides an R-linear splitting of $R \subseteq S$, namely

$$\frac{1}{[\mathrm{frac}(S) : \mathrm{frac}(R)]}\mathrm{tr} : S \longrightarrow R.$$

It follows that the induced maps on local cohomology $H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(S)$ are R-split. A variation is explored in [15], where the authors investigate whether the image of $H^i_{\mathfrak{m}}(R)$ in $H^i_{\mathfrak{m}}(R^+)$ is killed by elements of R^+ having arbitrarily small positive valuation. This is motivated by Heitmann's proof of the direct summand conjecture for rings $(R, \mathfrak{m})$ of dimension 3 and mixed characteristic $p > 0$ [5], which involves showing that the image of

$$H^2_{\mathfrak{m}}(R) \longrightarrow H^2_{\mathfrak{m}}\big(R^+\big)$$

is killed by $p^{1/n}$ for each positive integer n.

Throughout this paper, a *local ring* refers to a commutative Noetherian ring with a unique maximal ideal. Standard notions from commutative algebra that are used here may be found in [2]; for more on local cohomology, consult [11]. For the original proof of the existence of big Cohen–Macaulay modules for equicharacteristic local rings, see [6].

2. Preliminary remarks

2.1. Closure operations

Let R be an integral domain. The *plus closure* of an ideal $\mathfrak{a}$ is the ideal $\mathfrak{a}^+ = \mathfrak{a}R^+ \cap R$.

When R is a domain of prime characteristic $p > 0$, we set

$$R^\infty = \bigcup_{e \geqslant 0} R^{1/p^e},$$

which is a subring of R^+. The *Frobenius closure* of an ideal $\mathfrak{a}$ is the ideal $\mathfrak{a}^F = \mathfrak{a}R^\infty \cap R$. Alternatively, set

$$\mathfrak{a}^{[p^e]} = \big(a^{p^e} \bigm| a \in \mathfrak{a}\big).$$

Then $\mathfrak{a}^F = (r \in R \mid r^{p^e} \in \mathfrak{a}^{[p^e]} \text{ for some } e \in \mathbb{N})$.

2.2. Solvable extensions

A finite separable field extension L/K is *solvable* if $\mathrm{Gal}(M/K)$ is a solvable group for some Galois extension M of K containing L. Solvable extensions form a *distinguished class*, i.e.,

(1) for finite extensions $K \subseteq L \subseteq M$, the extension M/K is solvable if and only if each of M/L and L/K is solvable;
(2) for finite extensions L/K and M/K contained in a common field, if L/K is solvable, then so is the extension LM/M.

A finite separable extension L/K of fields of characteristic $p > 0$ is solvable precisely if it is obtained by successively adjoining

(1) roots of unity;
(2) roots of polynomials $T^n - a$ for n coprime to p;
(3) roots of *Artin–Schreier polynomials*, $T^p - T - a$;

see, for example, [12, Theorem VI.7.2].

2.3. Frobenius-nilpotent submodules

Let R be a ring of prime characteristic p. A *Frobenius action* on an R-module M is an additive map $F : M \longrightarrow M$ with $F(rm) = r^p F(m)$ for each $r \in R$ and $m \in M$. In this case, $\ker F$ is a submodule of M, and we have an ascending sequence

$$\ker F \subseteq \ker F^2 \subseteq \ker F^3 \subseteq \cdots.$$

The union of these is the *F-nilpotent* submodule of M, denoted M_{nil}. If R is local and M is Artinian, then there exists a positive integer e such that $F^e(M_{\mathrm{nil}}) = 0$; see [13, Proposition 4.4] or [4, Theorem 1.12].

3. Proofs

We record two elementary results that will be used later:

Lemma 3.1. *Let K be a field of characteristic $p > 0$. Let a and b be elements of K where a is nonzero. Then the Galois group of the polynomial*

$$T^p + aT - b$$

is a solvable group.

Proof. Form an extension of K by adjoining a primitive $p - 1$ root of unity and an element c that is a root of $T^{p-1} - a$. The polynomial $T^p + aT - b$ has the same roots as

$$\left(\frac{T}{c}\right)^p - \left(\frac{T}{c}\right) - \frac{b}{c^p},$$

which is an Artin–Schreier polynomial in T/c. □

Lemma 3.2. *Let R be a domain, and $\mathfrak{p}$ a prime ideal. Given a domain S that is a module-finite extension of $R_\mathfrak{p}$, there exists a domain T, module-finite over R, with $T_\mathfrak{p} = S$.*

Proof. Given $s_i \in S$, there exists $r_i \in R \smallsetminus \mathfrak{p}$ such that $r_i s_i$ is integral over R. If $s_1, \ldots, s_n$ are generators for S as an R-module, set $T = R[r_1 s_1, \ldots, r_n s_n]$. $\square$

Proof of Theorem 1.3. Since solvable extensions form a distinguished class, (1) reduces by induction to the case where $F([\eta]) = 0$. Compute $H^i_\mathfrak{a}(R)$ using a Čech complex $C^\bullet(\boldsymbol{x}; R)$, where $\boldsymbol{x} = x_0, \ldots, x_n$ are nonzero elements generating the ideal $\mathfrak{a}$; recall that $C^\bullet(\boldsymbol{x}; R)$ is the complex

$$0 \longrightarrow R \longrightarrow \bigoplus_{i=0}^{n} R_{x_i} \longrightarrow \bigoplus_{i<j} R_{x_i x_j} \longrightarrow \cdots \longrightarrow R_{x_0 \cdots x_n} \longrightarrow 0.$$

Consider a cycle η in $C^i(\boldsymbol{x}; R)$ that maps to $[\eta]$ in $H^i_\mathfrak{a}(R)$. Since $F([\eta]) = 0$, the cycle $F(\eta)$ is a boundary, i.e., $F(\eta) = \partial(\alpha)$ for some $\alpha \in C^{i-1}(\boldsymbol{x}; R)$.

Let $\mu_1, \ldots, \mu_m$ be the square-free monomials of degree $i - 2$ in the elements $x_1, \ldots, x_n$, and regard $C^{i-1}(\boldsymbol{x}; R) = C^{i-1}(x_0, \ldots, x_n; R)$ as

$$R_{x_0\mu_1} \oplus \cdots \oplus R_{x_0\mu_m} \oplus C^{i-1}(x_1, \ldots, x_n; R).$$

There exist a power q of the characteristic p of R, and elements $b_1, \ldots, b_m$ in R, such that α can be written in the above direct sum as

$$\alpha = \left(\frac{b_1}{(x_0\mu_1)^q}, \ldots, \frac{b_m}{(x_0\mu_m)^q}, *, \ldots, *\right).$$

Consider the polynomials

$$T^p + x_0^q T - b_i \quad \text{for } i = 1, \ldots, m,$$

and let L be a finite extension field where these have roots $t_1, \ldots, t_m$ respectively. By Lemma 3.1, we may assume L is Galois over $\operatorname{frac}(R)$ with the Galois group being solvable. Let S be a module-finite extension of R that contains $t_1, \ldots, t_m$, and has L as its fraction field; if R is excellent, we may take S to be the integral closure of R in L.

In the module $C^{i-1}(\boldsymbol{x}; S)$ one then has

$$\alpha = \left(\frac{t_1^p + x_0^q t_1}{(x_0\mu_1)^q}, \ldots, \frac{t_m^p + x_0^q t_m}{(x_0\mu_m)^q}, *, \ldots, *\right) = F(\beta) + \gamma,$$

where

$$\beta = \left(\frac{t_1}{(x_0\mu_1)^{q/p}}, \ldots, \frac{t_m}{(x_0\mu_m)^{q/p}}, 0, \ldots, 0\right)$$

and

$$\gamma = \left(\frac{t_1}{\mu_1^q}, \ldots, \frac{t_m}{\mu_m^q}, *, \ldots, *\right)$$

are elements of

$$C^{i-1}(\boldsymbol{x};S) = S_{x_0\mu_1} \oplus \cdots \oplus S_{x_0\mu_m} \oplus C^{i-1}(x_1,\dots,x_n;S).$$

Since $F(\eta) = \partial(F(\beta)+\gamma)$, we have

$$F\bigl(\eta - \partial(\beta)\bigr) = \partial(\gamma).$$

But $[\eta] = [\eta - \partial(\beta)]$ in $H^i_{\mathfrak{a}}(S)$, so after replacing η we may assume that

$$F(\eta) = \partial(\gamma).$$

Next, note that γ is an element of $C^{i-1}(1,x_1,\dots,x_n;S)$, viewed as a submodule of $C^{i-1}(\boldsymbol{x};S)$. There exits ζ in $C^{i-2}(1,x_1,\dots,x_n;S)$ such that

$$\partial(\zeta) = \left(\frac{t_1}{\mu_1^q},\dots,\frac{t_m}{\mu_m^q},*,\dots,*\right).$$

Since

$$F(\eta) = \partial\bigl(\gamma - \partial(\zeta)\bigr),$$

after replacing γ we may assume that the first m coordinate entries of γ are 0, i.e., that

$$\gamma = \left(0,\dots,0,\frac{c_1}{\lambda_1^Q},\dots,\frac{c_l}{\lambda_l^Q}\right),$$

where Q is a power of p, the c_i belong to S, and $\lambda_1,\dots,\lambda_l$ are the square-free monomials of degree $i-1$ in $x_1,\dots,x_n$.

The coordinate entries of $\partial(\gamma)$ include each c_i/λ_i^Q. Since $\partial(\gamma) = F(\eta)$, each c_i/λ_i^Q is a p-th power in $\operatorname{frac}(S)$; it follows that each c_i has a p-th root in $\operatorname{frac}(S)$. After enlarging S by adjoining each $c_i^{1/p}$, we see that $\gamma = F(\xi)$ for an element ξ of $C^{i-1}(\boldsymbol{x};S)$. But then

$$F(\eta) = \partial\bigl(F(\xi)\bigr) = F\bigl(\partial(\xi)\bigr).$$

Since the Frobenius action on $C^i(\boldsymbol{x};S)$ is injective, we have $\eta = \partial(\xi)$, which proves (1).

For (2), it suffices to construct a module-finite generically separable extension S such that $H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(S)$ is zero for $i < \dim R$; to obtain a generically Galois extension, enlarge S to a module-finite extension whose fraction field is the Galois closure of $\operatorname{frac}(S)$ over $\operatorname{frac}(R)$.

We use induction on $d = \dim R$, as in [10]. If $d = 0$, there is nothing to be proved; if $d = 1$, the inductive hypothesis is again trivially satisfied since $H^0_{\mathfrak{m}}(R) = 0$. Fix $i < \dim R$. Let $(A,\mathfrak{M})$ be a Gorenstein local ring that has R as a homomorphic image, and set

$$M = \operatorname{Ext}_A^{\dim A - i}(R,A).$$

Let $\mathfrak{p}_1,\dots,\mathfrak{p}_s$ be the elements of the set $\operatorname{Ass}_A M \smallsetminus \{\mathfrak{M}\}$.

Let $\mathfrak{q}$ be a prime ideal of R that is not maximal. Since R is catenary, one has

$$\dim R = \dim R_{\mathfrak{q}} + \dim R/\mathfrak{q}.$$

Thus, the condition $i < \dim R$ may be rewritten as

$$i - \dim R/\mathfrak{q} < \dim R_{\mathfrak{q}}.$$

Using the inductive hypothesis and Lemma 3.2, there exists a module-finite extension R' of R such that $\operatorname{frac}(R')$ is a separable field extension of $\operatorname{frac}(R_{\mathfrak{q}}) = \operatorname{frac}(R)$, and the induced map

$$H^{i-\dim R/\mathfrak{q}}_{\mathfrak{q}R_{\mathfrak{q}}}(R_{\mathfrak{q}}) \longrightarrow H^{i-\dim R/\mathfrak{q}}_{\mathfrak{q}R_{\mathfrak{q}}}\big(R'_{\mathfrak{q}}\big) \tag{3.2.1}$$

is zero. Taking the compositum of finitely many such separable extensions inside a fixed algebraic closure of $\operatorname{frac}(R)$, there exists a module-finite generically separable extension R' of R such that the map (3.2.1) is zero when $\mathfrak{q}$ is any of the primes $\mathfrak{p}_1 R, \dots, \mathfrak{p}_s R$. We claim that the image of the induced map $H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(R')$ has finite length.

Using local duality over A, it suffices to show that

$$M' = \operatorname{Ext}^{\dim A - i}_A\big(R', A\big) \longrightarrow \operatorname{Ext}^{\dim A - i}_A(R, A) = M$$

has finite length. This, in turn, would follow if

$$M'_{\mathfrak{p}} = \operatorname{Ext}^{\dim A - i}_{A_{\mathfrak{p}}}\big(R'_{\mathfrak{p}}, A_{\mathfrak{p}}\big) \longrightarrow \operatorname{Ext}^{\dim A - i}_{A_{\mathfrak{p}}}(R_{\mathfrak{p}}, A_{\mathfrak{p}}) = M_{\mathfrak{p}}$$

is zero for each prime ideal $\mathfrak{p}$ in $\operatorname{Ass}_A M \smallsetminus \{\mathfrak{M}\}$. Using local duality over $A_{\mathfrak{p}}$, it suffices to verify the vanishing of

$$H^{\dim A_{\mathfrak{p}} - \dim A + i}_{\mathfrak{p}R_{\mathfrak{p}}}(R_{\mathfrak{p}}) \longrightarrow H^{\dim A_{\mathfrak{p}} - \dim A + i}_{\mathfrak{p}R_{\mathfrak{p}}}\big(R'_{\mathfrak{p}}\big)$$

for each $\mathfrak{p}$ in $\operatorname{Ass}_A M \smallsetminus \{\mathfrak{M}\}$. This, however, follows from our choice of R' since

$$\dim A_{\mathfrak{p}} - \dim A + i = i - \dim A/\mathfrak{p} = i - \dim R/\mathfrak{p}R.$$

What we have arrived at thus far is a module-finite generically separable extension R' of R such that the image of $H^i_{\mathfrak{m}}(R) \longrightarrow H^i_{\mathfrak{m}}(R')$ has finite length; in particular, this image is finitely generated. Working with one generator at a time and taking the compositum of extensions, given $[\eta]$ in $H^i_{\mathfrak{m}}(R')$, it suffices to construct a module-finite generically separable extension S of R' such that $[\eta]$ maps to 0 under $H^i_{\mathfrak{m}}(R') \longrightarrow H^i_{\mathfrak{m}}(S)$.

By Theorem 1.2, there exists a module-finite extension R_1 of R' such that $[\eta]$ maps to 0 under the map $H^i_{\mathfrak{m}}(R') \longrightarrow H^i_{\mathfrak{m}}(R_1)$. Setting R_2 to be the separable closure of R' in R_1, the image of $[\eta]$ in $H^i_{\mathfrak{m}}(R_2)$ lies in $H^i_{\mathfrak{m}}(R_2)_{\text{nil}}$. The result now follows by (1). □

Corollary 3.3. *Let $(R, \mathfrak{m})$ be a local domain of prime characteristic that is a homomorphic image of a Gorenstein ring. Then $H^i_{\mathfrak{m}}(R^{+\text{sep}}) = 0$ for each $i < \dim R$.*

Moreover, each system of parameters for R is a regular sequence on $R^{+\text{sep}}$, i.e., $R^{+\text{sep}}$ is a separable balanced big Cohen–Macaulay algebra for R.

Proof. Theorem 1.3(2) implies that $H^i_{\mathfrak{m}}(R^{+\mathrm{sep}}) = 0$ for each $i < \dim R$. The proof that this implies the second statement is similar to the proof of [10, Corollary 2.3]. □

Proof of Theorem 1.4. Let p be the characteristic of R. If $z \in \mathfrak{a}^F$, then there exists a prime power $q = p^e$ with $z^q \in \mathfrak{a}^{[q]}$. In this case, $z^{q/p}$ belongs to the Frobenius closure of $\mathfrak{a}^{[q/p]}$, and

$$\left(z^{q/p}\right)^p \in \left(\mathfrak{a}^{[q/p]}\right)^{[p]}.$$

Since solvable extensions form a distinguished class, we reduce to the case $e = 1$, i.e., $q = p$.

There exist nonzero elements, $a_0, \ldots, a_m \in \mathfrak{a}$ and $b_0, \ldots, b_m \in R$ with

$$z^p = \sum_{i=0}^{m} b_i a_i^p.$$

Consider the polynomials

$$T^p + a_0^p T - b_i \quad \text{for } i = 1, \ldots, m,$$

and let L be a finite extension field where these have roots $t_1, \ldots, t_m$ respectively. By Lemma 3.1, we may assume L is Galois over $\operatorname{frac}(R)$ with the Galois group being solvable. Set

$$t_0 = \frac{1}{a_0}\left(z - \sum_{i=1}^{m} t_i a_i\right). \tag{3.3.1}$$

Taking p-th powers, we have

$$t_0^p = \frac{1}{a_0^p}\left(\sum_{i=0}^{m} b_i a_i^p - \sum_{i=1}^{m} t_i^p a_i^p\right) = b_0 + \frac{1}{a_0^p}\sum_{i=1}^{m}\left(b_i - t_i^p\right)a_i^p = b_0 + \sum_{i=1}^{m} t_i a_i^p.$$

Thus, t_0 belongs to the integral closure of $R[t_1, \ldots, t_m]$ in its field of fractions. Let S be a module-finite extension of R that contains $t_0, \ldots, t_m$, and has L as its fraction field; if R is excellent, we may take S to be the integral closure of R in L. Since (3.3.1) may be rewritten as

$$z = \sum_{i=0}^{m} t_i a_i,$$

it follows that $z \in \mathfrak{a}S$, completing the proof of (1).

Assertion (2) follows from [17, Corollary 3.4], though we include a proof using (1). There exists a module-finite extension domain T such that $z \in \mathfrak{a}T$. Decompose the field extension $\operatorname{frac}(R) \subseteq \operatorname{frac}(T)$ as a separable extension $\operatorname{frac}(R) \subseteq \operatorname{frac}(T)$ followed by a purely inseparable extension $\operatorname{frac}(T) \subseteq \operatorname{frac}(T)$. Let T_0 be the integral closure of R in $\operatorname{frac}(T)$.

Since T is a purely inseparable extension of T_0, and $z \in \mathfrak{a}T$, it follows that z belongs to the Frobenius closure of the ideal $\mathfrak{a}T_0$. By (2) there exists a generically separable extension S_0 of T_0 with $z \in \mathfrak{a}S_0$. Enlarge S_0 to a generically Galois extension S of R. This concludes the argument in the case R is excellent; in the event that S is not module-finite over R, one may replace it by a subring satisfying $z \in \mathfrak{a}S$ and having the same fraction field. □

The equational construction used in the proof of Theorem 1.4(1) arose from the study of symplectic invariants in [16].

4. Some Galois groups that are not solvable

Let R be a domain of prime characteristic, and let $\mathfrak{a}$ be an ideal of R. If z is an element of $\mathfrak{a}^F$, Theorem 1.4(1) states that there exists a solvable module-finite extension S with $z \in \mathfrak{a}S$. In the following example one has $z \in \mathfrak{a}^+$, and we conjecture $z \notin \mathfrak{a}S$ for any module-finite generically Galois extension S with $\operatorname{Gal}(S/R)$ solvable.

Example 4.1. Let a, b, c_1, c_2 be algebraically independent over $\mathbb{F}_p$, and set R be the hypersurface

$$\frac{\mathbb{F}_p(a, b, c_1, c_2)[x, y, z]}{(z^{p^2} + c_1(xy)^{p^2-p}z^p + c_2(xy)^{p^2-1}z + ax^{p^2} + by^{p^2})}.$$

We claim $z \in (x, y)^+$. Let u, v be elements of R^+ that are, respectively, roots of the polynomials

$$T^{p^2} + c_1y^{p^2-p}T^p + c_2y^{p^2-1}T + a, \tag{4.1.1}$$

and

$$T^{p^2} + c_1x^{p^2-p}T^p + c_2x^{p^2-1}T + b.$$

Set S to be the integral closure of R in the Galois closure of $\operatorname{frac}(R)(u, v)$ over $\operatorname{frac}(R)$. Then $(z - ux - vy)/xy$ is an element of S, since it is a root of the monic polynomial

$$T^{p^2} + c_1T^p + c_2T.$$

It follows that $z \in (x, y)S$.

We next show that $\operatorname{Gal}(S/R)$ is not solvable for the extension S constructed above. Since u is a root of (4.1.1), u/y is a root of

$$T^{p^2} + c_1T^p + c_2T + \frac{a}{y^{p^2}}. \tag{4.1.2}$$

The polynomial (4.1.2) is irreducible over $\mathbb{F}_q(c_1, c_2, a/y^{p^2})$, and hence over the purely transcendental extension $\mathbb{F}_q(c_1, c_2, a, x, y, z) = \operatorname{frac}(R)$. Since $\operatorname{frac}(S)$ is a Galois extension of $\operatorname{frac}(R)$ containing a root of (4.1.2), it contains all roots of (4.1.2). As (4.1.2) is separable, its roots are distinct; taking differences of roots, it follows that $\operatorname{frac}(S)$ contains the p^2 distinct roots of

$$T^{p^2} + c_1T^p + c_2T. \tag{4.1.3}$$

We next verify that the Galois group of (4.1.3) over $\operatorname{frac}(R)$ is $\mathrm{GL}_2(\mathbb{F}_q)$.

Quite generally, let L be a field of characteristic p. Consider the standard linear action of $\mathrm{GL}_2(\mathbb{F}_p)$ on the polynomial ring $L[x_1, x_2]$. The ring of invariants for this action is generated over L by the *Dickson invariants* c_1, c_2, which occur as the coefficients in the polynomial

$$\prod_{\alpha,\beta\in\mathbb{F}_p}(T-\alpha x_1-\beta x_2)=T^{p^2}+c_1T^p+c_2T,$$

see [3] or [1, Chapter 8]. Hence the extension $L(x_1,x_2)/L(c_1,c_2)$ has Galois group $\mathrm{GL}_2(\mathbb{F}_p)$.

It follows from the above that if c_1, c_2 are algebraically independent elements over a field L of characteristic p, then the polynomial

$$T^{p^2}+c_1T^p+c_2T\in L(c_1,c_2)[T]$$

has Galois group $\mathrm{GL}_2(\mathbb{F}_p)$.

The group $\mathrm{PSL}_2(\mathbb{F}_p)$ is a subquotient of $\mathrm{GL}_2(\mathbb{F}_p)$, and, we conjecture, a subquotient of $\mathrm{Gal}(S/R)$ for *any* module-finite generically Galois extension S of R with $z\in\mathfrak{a}S$. For $p\geqslant 5$, the group $\mathrm{PSL}_2(\mathbb{F}_p)$ is a nonabelian simple group; thus, conjecturally, $\mathrm{Gal}(S/R)$ is not solvable for any module-finite generically Galois extension S with $z\in\mathfrak{a}S$.

Example 4.2. Extending the previous example, let $a, b, c_1, \dots, c_n$ be algebraically independent elements over $\mathbb{F}_q$, and set R to be the polynomial ring $\mathbb{F}_q(a,b,c_1,\dots,c_n)[x,y,z]$ modulo the principal ideal generated by

$$z^{q^n}+c_1(xy)^{q^n-q^{n-1}}z^{q^{n-1}}+c_2(xy)^{q^n-q^{n-2}}z^{q^{n-2}}+\cdots+c_n(xy)^{q^n-1}z+ax^{q^n}+by^{q^n}.$$

Then $z\in(x,y)^+$; imitate the previous example with u, v being roots of

$$T^{q^n}+c_1y^{q^n-q^{n-1}}T^{q^{n-1}}+c_2y^{q^n-q^{n-2}}T^{q^{n-2}}+\cdots+c_ny^{q^n-1}T+a,$$

and

$$T^{q^n}+c_1x^{q^n-q^{n-1}}T^{q^{n-1}}+c_2x^{q^n-q^{n-2}}T^{q^{n-2}}+\cdots+c_nx^{q^n-1}T+b.$$

If S is any module-finite generically Galois extension of R with $z\in\mathfrak{a}S$, we conjecture that $\mathrm{frac}(S)$ contains the splitting field of

$$T^{q^n}+c_1T^{q^{n-1}}+c_2T^{q^{n-2}}+\cdots+c_nT. \tag{4.2.1}$$

Using a similar argument with Dickson invariants, the Galois group of (4.2.1) over $\mathrm{frac}(R)$ is $\mathrm{GL}_n(\mathbb{F}_q)$. Its subquotient $\mathrm{PSL}_n(\mathbb{F}_q)$ is a nonabelian simple group for $n\geqslant 3$, and for $n=2$, $q\geqslant 4$.

Likewise, we record conjectural examples R where $H^i_{\mathfrak{m}}(R)\longrightarrow H^i_{\mathfrak{m}}(S)$ is nonzero for each module-finite generically Galois extension S with $\mathrm{Gal}(S/R)$ solvable:

Example 4.3. Let a, b, c_1, c_2 be algebraically independent over $\mathbb{F}_p$, and consider the hypersurface

$$A=\frac{\mathbb{F}_p(a,b,c_1,c_2)[x,y,z]}{(z^{2p^2}+c_1(xy)^{p^2-p}z^{2p}+c_2(xy)^{p^2-1}z^2+ax^{p^2}+by^{p^2})}.$$

Let $(R, \mathfrak{m})$ be the Rees ring $A[xt, yt, zt]$ localized at the maximal ideal x, y, z, xt, yt, zt. The elements $x, yt, y+xt$ form a system of parameters for R, and the relation

$$z^2t \cdot (y+xt) = z^2t^2 \cdot x + z^2 \cdot yt$$

defines an element $[\eta]$ of $H^2_{\mathfrak{m}}(R)$. We conjecture that if S is any module-finite generically Galois extension such that $[\eta]$ maps to 0 under the induced map $H^2_{\mathfrak{m}}(R) \longrightarrow H^2_{\mathfrak{m}}(S)$, then $\operatorname{frac}(S)$ contains the splitting field of

$$T^{p^2} + c_1T^p + c_2T,$$

and hence that $\operatorname{Gal}(S/R)$ is not solvable if $p \geqslant 5$.

5. Graded rings and extensions

Let R be an $\mathbb{N}$-graded domain that is finitely generated over a field R_0. Set $R^{+\mathrm{GR}}$ to be the $\mathbb{Q}_{\geqslant 0}$-graded ring generated by elements of R^+ that can be assigned a degree such that they then satisfy a homogeneous equation of integral dependence over R. Note that $[R^{+\mathrm{GR}}]_0$ is the algebraic closure of the field R_0. One has the following:

Theorem 5.1. *(See [8, Theorem 6.1].) Let R be an $\mathbb{N}$-graded domain that is finitely generated over a field R_0 of prime characteristic. Then each homogeneous system of parameters for R is a regular sequence on $R^{+\mathrm{GR}}$.*

Let R be as in the above theorem. Since $R^{+\mathrm{GR}}$ and $R^{+\mathrm{sep}}$ are Cohen–Macaulay R-algebras, it is natural to ask whether there exists a $\mathbb{Q}$-graded separable Cohen–Macaulay R-algebra. The answer to this is negative:

Example 5.2. Let R be the Rees ring

$$\frac{\overline{\mathbb{F}}_2[x, y, z]}{(x^3+y^3+z^3)}[xt, yt, zt]$$

with the $\mathbb{N}$-grading where the generators x, y, z, xt, yt, zt have degree 1. Set B to be the R-algebra generated by the homogeneous elements of $R^{+\mathrm{GR}}$ that are separable over $\operatorname{frac}(R)$. We prove that B is not a balanced Cohen–Macaulay R-module.

The elements $x, yt, y+xt$ constitute a homogeneous system of parameters for R since the radical of the ideal that they generate is the homogeneous maximal ideal of R, and $\dim R = 3$. Suppose, to the contrary, that they form a regular sequence on B. Since

$$z^2t \cdot (y+xt) = z^2t^2 \cdot x + z^2 \cdot yt,$$

it follows that $z^2t \in (x, yt)B$. Thus, there exist elements $u, v \in B_1$ with

$$z^2t = u \cdot x + v \cdot yt. \tag{5.2.1}$$

Since $z^3 = x^3 + y^3$, we also have $z^2 = x\sqrt{xz} + y\sqrt{yz}$ in $R^{+\mathrm{GR}}$, and hence

$$z^2 t = t\sqrt{xz} \cdot x + \sqrt{yz} \cdot yt. \tag{5.2.2}$$

Comparing (5.2.1) and (5.2.2), we see that

$$(u + t\sqrt{xz}) \cdot x = (v + \sqrt{yz}) \cdot yt$$

in $R^{+\mathrm{GR}}$. But x, yt is a regular sequence on $R^{+\mathrm{GR}}$, so there exists an element c in $[R^{+\mathrm{GR}}]_0$ with $u + t\sqrt{xz} = cyt$ and $v + \sqrt{yz} = cx$. Since $[R^{+\mathrm{GR}}]_0 = \bar{\mathbb{F}}_2$, it follows that $c \in R$, and hence that $\sqrt{yz} \in B$. This contradicts the hypothesis that elements of B are separable over $\operatorname{frac}(R)$.

The above argument shows that any graded Cohen–Macaulay R-algebra must contain the elements $\sqrt{yz}$ and $t\sqrt{xz}$.

We next show that no module-finite $\mathbb{Q}$-graded extension domain of the ring R in Example 5.2 is Cohen–Macaulay.

Example 5.3. Let R be the Rees ring from Example 5.2, and let S be a graded Cohen–Macaulay ring with $R \subseteq S \subseteq R^{+\mathrm{GR}}$. We prove that S is not finitely generated over R.

By the previous example, S contains $\sqrt{yz}$ and $t\sqrt{xz}$. Using the symmetry between x, y, z, it follows that $\sqrt{xy}$, $\sqrt{xz}$, $t\sqrt{xy}$, $t\sqrt{yz}$ are all elements of S. We prove inductively that S contains

$$\begin{array}{lll} x^{1-2/q}(yz)^{1/q}, & y^{1-2/q}(xz)^{1/q}, & z^{1-2/q}(xy)^{1/q}, \\ tx^{1-2/q}(yz)^{1/q}, & ty^{1-2/q}(xz)^{1/q}, & tz^{1-2/q}(xy)^{1/q}, \end{array} \tag{5.3.1}$$

for each $q = 2^e$ with $e \geqslant 1$. The case $e = 1$ has been settled.

Suppose S contains the elements (5.3.1) for some $q = 2^e$. Then, one has

$$\begin{aligned} & x^{1-2/q}(yz)^{1/q} \cdot ty^{1-2/q}(xz)^{1/q} \cdot (y + xt) \\ & \quad = tx^{1-2/q}(yz)^{1/q} \cdot ty^{1-2/q}(xz)^{1/q} \cdot x + x^{1-2/q}(yz)^{1/q} \cdot y^{1-2/q}(xz)^{1/q} \cdot yt. \end{aligned}$$

Using as before that x, yt, $y + xt$ is a regular sequence on S, we conclude

$$x^{1-2/q}(yz)^{1/q} \cdot ty^{1-2/q}(xz)^{1/q} = u \cdot x + v \cdot yt$$

for some $u, v \in S_1$. Simplifying the left-hand side, the above reads

$$t(xy)^{1-1/q} z^{2/q} = u \cdot x + v \cdot yt. \tag{5.3.2}$$

Taking q-th roots in

$$z^2 = x\sqrt{xz} + y\sqrt{yz}$$

and multiplying by $t(xy)^{1-1/q}$ yields

$$t(xy)^{1-1/q} z^{2/q} = ty^{1-1/q}(xz)^{1/2q} \cdot x + x^{1-1/q}(yz)^{1/2q} \cdot yt. \tag{5.3.3}$$

Comparing (5.3.2) and (5.3.3), we see that

$$\big(u + ty^{1-1/q}(xz)^{1/2q}\big) \cdot x = \big(v + x^{1-1/q}(yz)^{1/2q}\big) \cdot yt,$$

so there exists c in $[R^{+\mathrm{GR}}]_0 = \overline{\mathbb{F}}_2$ with

$$u + ty^{1-1/q}(xz)^{1/2q} = cyt \quad \text{and} \quad v + x^{1-1/q}(yz)^{1/2q} = cx.$$

It follows that $ty^{1-1/q}(xz)^{1/2q}$ and $x^{1-1/q}(yz)^{1/2q}$ are elements of S. In view of the symmetry between x, y, z, this completes the inductive step. Setting

$$\theta = \frac{xy}{z^2},$$

we have proved that

$$\theta^{1/q} \in \operatorname{frac}(S) \quad \text{for each } q = 2^e.$$

We claim $\theta^{1/2}$ does not belong to $\operatorname{frac}(R)$. Indeed if it does, then $(xy)^{1/2}$ belongs to $\operatorname{frac}(R)$, and hence to R, as R is normal; this is readily seen to be false. The extension

$$\operatorname{frac}(R) \subseteq \operatorname{frac}(R)\big(\theta^{1/q}\big)$$

is purely inseparable, so the minimal polynomial of $\theta^{1/q}$ over $\operatorname{frac}(R)$ has the form $T^Q - \theta^{Q/q}$ for some $Q = 2^E$. Since $\theta^{1/2} \notin \operatorname{frac}(R)$, we conclude that the minimal polynomial is $T^q - \theta$. Hence

$$\big[\operatorname{frac}(R)\big(\theta^{1/q}\big) : \operatorname{frac}(R)\big] = q \quad \text{for each } q = 2^e.$$

It follows that $[\operatorname{frac}(S) : \operatorname{frac}(R)]$ is not finite.

Theorems 1.2 and 1.3(2) discuss the vanishing of the image of $H^i_{\mathfrak{m}}(R)$ for $i < \dim R$. In the case of graded rings, one also has the following result for $H^d_{\mathfrak{m}}(R)$.

Proposition 5.4. *Let R be an $\mathbb{N}$-graded domain that is finitely generated over a field R_0 of prime characteristic. Set $d = \dim R$. Then $[H^d_{\mathfrak{m}}(R)]_{\geqslant 0}$ maps to zero under the induced map*

$$H^d_{\mathfrak{m}}(R) \longrightarrow H^d_{\mathfrak{m}}\big(R^{+\mathrm{GR}}\big).$$

Hence, there exists a module-finite $\mathbb{Q}$-graded extension domain S of R such that the induced map $[H^d_{\mathfrak{m}}(R)]_{\geqslant 0} \longrightarrow H^d_{\mathfrak{m}}(S)$ is zero.

Proof. Let $F^e : H^d_{\mathfrak{m}}(R) \longrightarrow H^d_{\mathfrak{m}}(R)$ denote the e-th iteration of the Frobenius map. Suppose $[\eta] \in [H^d_{\mathfrak{m}}(R)]_n$ for some $n \geqslant 0$. Then $F^e([\eta])$ belongs to $[H^d_{\mathfrak{m}}(R)]_{np^e}$ for each e. As $[H^d_{\mathfrak{m}}(R)]_{\geqslant 0}$ has finite length, there exists $e \geqslant 1$ and homogeneous elements $r_1, \ldots, r_e \in R$ such that

$$F^e\big([\eta]\big) + r_1 F^{e-1}\big([\eta]\big) + \cdots + r_e[\eta] = 0. \tag{5.4.1}$$

We imitate the equational construction from [10]: Consider a homogeneous system of parameters $\boldsymbol{x} = x_1, \ldots, x_d$, and compute $H^i_{\mathfrak{m}}(R)$ as the cohomology of the Čech complex $C^\bullet(\boldsymbol{x}; R)$ below:

$$0 \longrightarrow R \longrightarrow \bigoplus_{i=1}^{d} R_{x_i} \longrightarrow \bigoplus_{i<j} R_{x_i x_j} \longrightarrow \cdots \longrightarrow R_{x_1 \cdots x_d} \longrightarrow 0.$$

This complex is $\mathbb{Z}$-graded; let η be a homogeneous element of $C^d(\boldsymbol{x}; R)$ that maps to $[\eta]$ in $H^d_{\mathfrak{m}}(R)$. Eq. (5.4.1) implies that

$$F^e(\eta) + r_1 F^{e-1}(\eta) + \cdots + r_e \eta$$

is a boundary in $C^d(\boldsymbol{x}; R)$, say it equals $\partial(\alpha)$ for a homogeneous element α of $C^{d-1}(\boldsymbol{x}; R)$. Solving integral equations in each coordinate of $C^{d-1}(\boldsymbol{x}; R)$, there exists a module-finite extension domain S and β in $C^{d-1}(\boldsymbol{x}; S)$ with

$$F^e(\beta) + r_1 F^{e-1}(\beta) + \cdots + r_e \beta = \alpha.$$

Moreover, we may assume S is a normal ring. Since $\eta - \partial(\beta)$ is an element on $\operatorname{frac}(S)$ satisfying

$$T^{p^e} + r_1 T^{p^{e-1}} + \cdots + r_e T = 0,$$

it belongs to S. But then $\eta - \partial(\beta)$ maps to zero in $H^d_{\mathfrak{m}}(S)$. Thus, each homogeneous element of the module $[H^d_{\mathfrak{m}}(R)]_{\geqslant 0}$ maps to 0 in $H^d_{\mathfrak{m}}(R^{+\mathrm{GR}})$.

For the final statement, note that $[H^d_{\mathfrak{m}}(R)]_{\geqslant 0}$ has finite length. □

The next example illustrates why Proposition 5.4 is limited to $[H^d_{\mathfrak{m}}(R)]_{\geqslant 0}$.

Example 5.5. Let K be a field of prime characteristic, and take R to be the semigroup ring

$$R = K\left[x_1 \cdots x_d, x_1^d, \ldots, x_d^d\right].$$

It is easily seen that R is normal, and that $[H^d_{\mathfrak{m}}(R)]_n$ is nonzero for each integer $n < 0$. We claim that the induced map

$$H^d_{\mathfrak{m}}(R) \longrightarrow H^d_{\mathfrak{m}}(S)$$

is injective for each module-finite extension ring S. For this, it suffices to check that R is a *splinter* ring, i.e., that R is a direct summand of each module-finite extension ring; the splitting of $R \subseteq S$ then induces an R-splitting of $H^d_{\mathfrak{m}}(R) \longrightarrow H^d_{\mathfrak{m}}(S)$.

To check that R is splinter, note that normal affine semigroup rings are weakly F-regular by [7, Proposition 4.12], and that weakly F-regular rings are splinter by [9, Theorem 5.25]. For more on splinters, we point the reader towards [14,9,18].

Acknowledgment

We thank Kazuhiko Kurano for pointing out an error in an earlier version of this manuscript.

References

[1] D.J. Benson, Polynomial Invariants of Finite Groups, London Math. Soc. Lecture Note Ser., vol. 190, Cambridge University Press, Cambridge, 1993.
[2] W. Bruns, J. Herzog, Cohen–Macaulay Rings, revised edition, Cambridge Stud. Adv. Math., vol. 39, Cambridge University Press, Cambridge, 1998.
[3] L.E. Dickson, A fundamental system of invariants of the general modular linear group with a solution to the form problem, Trans. Amer. Math. Soc. 12 (1911) 75–98.
[4] R. Hartshorne, R. Speiser, Local cohomological dimension in characteristic p, Ann. of Math. (2) 105 (1977) 45–79.
[5] R.C. Heitmann, The direct summand conjecture in dimension three, Ann. of Math. (2) 156 (2002) 695–712.
[6] M. Hochster, Topics in the Homological Theory of Modules Over Commutative Rings, CBMS Reg. Conf. Ser. Math., vol. 24, Amer. Math. Soc., Providence, RI, 1975.
[7] M. Hochster, C. Huneke, Tight closure, invariant theory, and the Briançon–Skoda theorem, J. Amer. Math. Soc. 3 (1990) 31–116.
[8] M. Hochster, C. Huneke, Infinite integral extensions and big Cohen–Macaulay algebras, Ann. of Math. (2) 135 (1992) 53–89.
[9] M. Hochster, C. Huneke, Tight closure of parameter ideals and splitting in module-finite extensions, J. Algebraic Geom. 3 (1994) 599–670.
[10] C. Huneke, G. Lyubeznik, Absolute integral closure in positive characteristic, Adv. Math. 210 (2007) 498–504.
[11] S.B. Iyengar, G.J. Leuschke, A. Leykin, C. Miller, E. Miller, A.K. Singh, U. Walther, Twenty-Four Hours of Local Cohomology, Grad. Stud. Math., vol. 87, Amer. Math. Soc., Providence, RI, 2007.
[12] S. Lang, Algebra, revised third edition, Grad. Texts in Math., vol. 211, Springer-Verlag, New York, 2002.
[13] G. Lyubeznik, F-modules: Applications to local cohomology and D-modules in characteristic $p > 0$, J. Reine Angew. Math. 491 (1997) 65–130.
[14] F. Ma, Splitting in integral extensions, Cohen–Macaulay modules and algebras, J. Algebra 116 (1988) 176–195.
[15] P. Roberts, A.K. Singh, V. Srinivas, Annihilators of local cohomology in characteristic zero, Illinois J. Math. 51 (2007) 237–254.
[16] A.K. Singh, Failure of F-purity and F-regularity in certain rings of invariants, Illinois J. Math. 42 (1998) 441–448.
[17] A.K. Singh, Separable integral extensions and plus closure, Manuscripta Math. 98 (1999) 497–506.
[18] A.K. Singh, $\mathbb{Q}$-Gorenstein splinter rings of characteristic p are F-regular, Math. Proc. Cambridge Philos. Soc. 127 (1999) 201–205.