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

Communicated by Karen Smith

Abstract

Given a local domain \((R, m)\) 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 \(H^i_m(R) \to H^i_m(S)\) 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.

© 2011 Elsevier Inc. All rights reserved.

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 © 2011 Elsevier Inc. All rights reserved.

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 $H^i_m(R^+)$ is zero. Hence, given an element $[\eta]$ of $H^i_m(R)$, there exists a module-finite extension domain $S$ such that $[\eta]$ maps to 0 under the induced map $H^i_m(R) \to H^i_m(S)$. 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

$$H^i_m(R) \to H^i_m(S)$$

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; $\text{Gal}(S/R)$ 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 $H^i_{\mathfrak{a}}(R)_{\text{nil}}$ (see Section 2.3). Then there exists a module-finite generically Galois extension $S$, with $\text{Gal}(S/R)$ a solvable group, such that $[\eta]$ maps to 0 under the induced map $H^i_{\mathfrak{a}}(R) \to H^i_{\mathfrak{a}}(S)$.

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 $H^i_m(R) \to H^i_m(S)$ is zero for each $i < \dim R$.

Set $R^{+\text{sep}}$ to be the $R$-algebra generated by the elements of $R^+$ that are separable over $\text{frac}(R)$. Under the hypotheses of Theorem 1.3(2), $R^{+\text{sep}}$ is a separable balanced big Cohen–Macaulay $R$-algebra; see Corollary 3.3. In contrast, the algebra $R^{\infty}$, 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 $R^{+\text{GR}}$, 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 $\text{Gal}(S/R)$ 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 $z \not\in \mathfrak{a}S$ for each module-finite generically Galois extension $S$ with $\text{Gal}(S/R)$ a solvable group. Similarly, in Example 4.3 we present a 3-dimensional ring $R$ where we conjecture that $H^2_m(R) \rightarrow H^2_m(S)$ is nonzero for each module-finite generically Galois extension $S$ with $\text{Gal}(S/R)$ 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 $\text{tr} : \frac{S}{\mathfrak{m}} \rightarrow \frac{R}{\mathfrak{m}}$ provides an $R$-linear splitting of $R \subseteq S$, namely

$$\frac{1}{[\frac{S}{\mathfrak{m}} : \frac{R}{\mathfrak{m}}]} \text{tr} : S \rightarrow R.$$ 

It follows that the induced maps on local cohomology $H^i_m(R) \rightarrow H^i_m(S)$ are $R$-split. A variation is explored in [15], where the authors investigate whether the image of $H^i_m(R)$ in $H^i_m(R^+)$ 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 $H^2_m(R) \rightarrow H^2_m(R^+)$ 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

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

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

$$\mathfrak{a}^{\{p^e\}} = (a^{p^e} \mid a \in \mathfrak{a}).$$

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 $\text{Gal}(M/K)$ 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 $F : M \rightarrow M$ 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 $M_{\text{nil}}$. If $R$ is local and $M$ is Artinian, then there exists a positive integer $e$ such that $F^e(M_{\text{nil}}) = 0$; 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 $T/c$. $\square$
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 $r_i \in R \setminus \mathfrak{p}$ such that $r_is_i$ is integral over $R$. If $s_1, \ldots, s_n$ are generators for $S$ as an $R$-module, set $T = R[r_1s_1, \ldots, r_ns_n]$.

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

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

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

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 $C^{i-1}(x; R) = C^{i-1}(x_0, \ldots, x_n; R)$ 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 $\alpha$ 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 $\text{frac}(R)$ 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 $C^{i-1}(x; S)$ 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
\[ C^{i-1}(x; S) = S_{x_0\mu_1} \oplus \cdots \oplus S_{x_0\mu_m} \oplus C^{i-1}(x_1, \ldots, x_n; S). \]
Since \( F(\eta) = \partial(F(\beta) + \gamma) \), we have
\[ F(\eta - \partial(\beta)) = \partial(\gamma). \]
But \([\eta] = [\eta - \partial(\beta)]\) in \( H_0^i(S) \), so after replacing \( \eta \) we may assume that
\[ F(\eta) = \partial(\gamma). \]
Next, note that \( \gamma \) is an element of \( C^{i-1}(1, x_1, \ldots, x_n; S) \), viewed as a submodule of \( C^{i-1}(x; S) \).
There exists \( \zeta \) in \( C^{-2}(1, x_1, \ldots, x_n; S) \) such that
\[ \partial(\zeta) = \left( \frac{t_1}{\mu_1}, \ldots, \frac{t_m}{\mu_m}, *, \ldots, * \right). \]
Since
\[ F(\eta) = \partial(\gamma - \partial(\zeta)), \]
after replacing \( \gamma \) we may assume that the first \( m \) coordinate entries of \( \gamma \) are 0, i.e., that
\[ \gamma = \left( 0, \ldots, 0, \frac{c_1}{\lambda_1^Q}, \ldots, \frac{c_l}{\lambda_l^Q} \right), \]
where \( Q \) is a power of \( p \), the \( c_i \) belong to \( S \), and \( \lambda_1, \ldots, \lambda_l \) are the square-free monomials of degree \( i - 1 \) in \( x_1, \ldots, x_n \).
The coordinate entries of \( \partial(\gamma) \) include each \( c_i/\lambda_i^Q \). Since \( \partial(\gamma) = F(\eta) \), each \( c_i/\lambda_i^Q \) is a \( p \)-th power in frac\((S)\); it follows that each \( c_i \) has a \( p \)-th root in frac\((S)\). After enlarging \( S \) by adjoining each \( c_i^{1/p} \), we see that \( \gamma = F(\xi) \) for an element \( \xi \) of \( C^{i-1}(x; S) \). But then
\[ F(\eta) = \partial(F(\xi)) = F(\partial(\xi)). \]
Since the Frobenius action on \( C^i(x; S) \) 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 \( H_0^i(R) \to H_0^i(S) \) 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 frac\((S)\) over 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 \( H_0^0(R) = 0 \). Fix \( i < \dim R \). Let \((A, M)\) be a Gorenstein local ring that has \( R \) as a homomorphic image, and set
\[ M = \text{Ext}^1_A R^{-i}(R, A). \]
Let \( p_1, \ldots, p_s \) be the elements of the set \( \text{Ass}_A M \setminus \{M\} \).
Let \( q \) be a prime ideal of \( R \) that is not maximal. Since \( R \) is catenary, one has
\[
\dim R = \dim R_q + \dim R/q.
\]
Thus, the condition \( i < \dim R \) may be rewritten as
\[
i - \dim R/q < \dim R_q.
\]
Using the inductive hypothesis and Lemma 3.2, there exists a module-finite extension \( R' \) of \( R \) such that \( \text{frac}(R') \) is a separable field extension of \( \text{frac}(R_q) = \text{frac}(R) \), and the induced map
\[
H_{qR_q}^{i-\dim R/q}(R_q) \longrightarrow H_{qR_q}^{i-\dim R/q}(R'_q)
\] (3.2.1)
is zero. Taking the compositum of finitely many such separable extensions inside a fixed algebraic closure of \( \text{frac}(R) \), there exists a module-finite generically separable extension \( R' \) of \( R \) such that the map (3.2.1) is zero when \( q \) is any of the primes \( p_1 R, \ldots, p_s R \). We claim that the image of the induced map
\[
H_i^m(R) \longrightarrow H_i^m(R')
\] has finite length.

Using local duality over \( A \), it suffices to show that
\[
M' = \text{Ext}_A^{\dim A - i}(R', A) \longrightarrow \text{Ext}_A^{\dim A - i}(R, A) = M
\]
has finite length. This, in turn, would follow if
\[
M'_p = \text{Ext}_A^{\dim A - i}(R'_p, A_p) \longrightarrow \text{Ext}_A^{\dim A - i}(R_p, A_p) = M_p
\]
is zero for each prime ideal \( p \) in \( \text{Ass}_A M \setminus \{ M \} \). Using local duality over \( A_p \), it suffices to verify the vanishing of
\[
H_{pR_p}^{\dim A_p - \dim A + i}(R_p) \longrightarrow H_{pR_p}^{\dim A_p - \dim A + i}(R'_p)
\]
for each \( p \) in \( \text{Ass}_A M \setminus \{ M \} \). This, however, follows from our choice of \( R' \) since
\[
\dim A_p - \dim A + i = i - \dim A/p = i - \dim R/p R.
\]

What we have arrived at thus far is a module-finite generically separable extension \( R' \) of \( R \) such that the image of \( H_i^m(R) \longrightarrow H_i^m(R') \) 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 \( H_i^m(R') \), it suffices to construct a module-finite generically separable extension \( S \) of \( R' \) such that \( \eta \) maps to 0 under \( H_i^m(R') \longrightarrow H_i^m(S) \).

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

**Corollary 3.3.** Let \( (R, m) \) be a local domain of prime characteristic that is a homomorphic image of a Gorenstein ring. Then \( H_i^m(R^{+\text{sep}}) = 0 \) 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 $H^i_m(R^{+\text{sep}}) = 0$ 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 $z \in a^F$, then there exists a prime power $q = p^e$ with $z^q \in a^{[q]}$. In this case, $z^q/p$ belongs to the Frobenius closure of $a^{[q/p]}$, and

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

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

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

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

Consider the polynomials

$$T^p + a_0^p T - b_i$$

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 $\text{frac}(R)$ with the Galois group being solvable. Set

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

(3.3.1)

Taking $p$-th powers, we have

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

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 $z \in aS$, 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 $z \in aT$. Decompose the field extension $\text{frac}(R) \subseteq \text{frac}(T)$ as a separable extension $\text{frac}(R) \subseteq \text{frac}(T)$ followed by a purely inseparable extension $\text{frac}(T) \subseteq \text{frac}(T)$. Let $T_0$ be the integral closure of $R$ in $\text{frac}(T)$.

Since $T$ is a purely inseparable extension of $T_0$, and $z \in aT$, it follows that $z$ belongs to the Frobenius closure of the ideal $aT_0$. By (2) there exists a generically separable extension $S_0$ of $T_0$ with $z \in aS_0$. 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 $z \in aS$ 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 $a$ be an ideal of $R$. If $z$ is an element of $a^F$, Theorem 1.4(1) states that there exists a solvable module-finite extension $S$ with $z \in aS$. In the following example one has $z \in a^+$, and we conjecture $z \notin aS$ for any module-finite generically Galois extension $S$ with $\text{Gal}(S/R)$ solvable.

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

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

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

$$T^{p^2} + c_1 y^{p^2} - p T^p + c_2 y^{p^2-1} T + a,$$  \hspace{1cm} (4.1.1)

and

$$T^{p^2} + c_1 x^{p^2} - p T^p + c_2 x^{p^2-1} T + b.$$  \hspace{1cm} (4.1.2)

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

$$T^{p^2} + c_1 T^p + c_2 T.$$  \hspace{1cm} (4.1.3)

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

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

$$T^{p^2} + c_1 T^p + c_2 T + \frac{a}{y^{p^2}}.$$  \hspace{1cm} (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 $\mathbb{F}_q(c_1, c_2, a, x, y, z) = \text{frac}(R)$. Since $\text{frac}(S)$ is a Galois extension of $\text{frac}(R)$ 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 $\text{frac}(S)$ contains the $p^2$ distinct roots of

$$T^{p^2} + c_1 T^p + c_2 T.$$  \hspace{1cm} (4.1.3)

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

Quite generally, let $L$ be a field of characteristic $p$. Consider the standard linear action of $\text{GL}_2(\mathbb{F}_p)$ 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
\( \prod_{\alpha, \beta \in \mathbb{F}_p} (T - \alpha x_1 - \beta x_2) = T^{p^2} + c_1 T^p + c_2 T, \)

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

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
\[
T^{p^2} + c_1 T^p + c_2 T \in L(c_1, c_2)[T]
\]
has Galois group \( \text{GL}_2(\mathbb{F}_p) \).

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

**Example 4.2.** Extending the previous example, let \( a, b, c_1, \ldots, c_n \) be algebraically independent elements over \( \mathbb{F}_q \), and set \( R \) to be the polynomial ring \( \mathbb{F}_q(a, b, c_1, \ldots, c_n)[x, y, z] \) modulo the principal ideal generated by
\[
z^{q^n} + c_1 (xy)^{q^n-1} z^{q^{n-1}} + c_2 (xy)^{q^n-2} z^{q^{n-2}} + \cdots + c_n (xy)^{q^n-1} z + ax y^{q^n} + by y^{q^n}.
\]

Then \( z \in (x, y)^+ \); imitate the previous example with \( u, v \) being roots of
\[
T^{q^n} + c_1 y^{q^n-1} T^{q^{n-1}} + c_2 y^{q^n-2} T^{q^{n-2}} + \cdots + c_n y^{q^n-1} T + a,
\]
and
\[
T^{q^n} + c_1 x^{q^n-1} T^{q^{n-1}} + c_2 x^{q^n-2} T^{q^{n-2}} + \cdots + c_n x^{q^n-1} T + b.
\]

If \( S \) is any module-finite generically Galois extension of \( R \) with \( z \in aS \), we conjecture that \( \text{frac}(S) \) contains the splitting field of
\[
T^{q^n} + c_1 T^{q^{n-1}} + c_2 T^{q^{n-2}} + \cdots + c_n T. \quad (4.2.1)
\]

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

Likewise, we record conjectural examples \( R \) where \( H^i_m(R) \to H^i_m(S) \) is nonzero for each module-finite generically Galois extension \( S \) with \( \text{Gal}(S/R) \) solvable:

**Example 4.3.** Let \( a, b, c_1, c_2 \) be algebraically independent over \( \mathbb{F}_p \), and consider the hypersurface
\[
A = \frac{\mathbb{F}_p(a, b, c_1, c_2)[x, y, z]}{(z^2 p^2 + c_1 (xy) p^2 + c_2 (xy) p^2 - z^2 + ax p^2 + by p^2)}.
\]
Let \((R, m)\) 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 \(H^2_m(R)\). We conjecture that if \(S\) is any module-finite generically Galois extension such that \([\eta]\) maps to 0 under the induced map \(H^2_m(R) \longrightarrow H^2_m(S)\), then \(\text{frac}(S)\) contains the splitting field of
\[
T^{p^2} + c_1 T^{p} + c_2 T,
\]
and hence that \(\text{Gal}(S/R)\) is not solvable if \(p \geq 5\).

5. Graded rings and extensions

Let \(R\) be an \(\mathbb{N}\)-graded domain that is finitely generated over a field \(R_0\). Set \(R^{+\text{GR}}\) to be the \(\mathbb{Q}_{\geq 0}\)-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 \([R^{+\text{GR}}]_0\) 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 \(R^{+\text{GR}}\).

Let \(R\) be as in the above theorem. Since \(R^{+\text{GR}}\) and \(R^{+\text{sep}}\) 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
\[
\mathbb{F}_2[x, y, z]_{[xt, yt, zt]} / (x^3 + y^3 + z^3)[xt, yt, zt]
\]
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 \(R^{+\text{GR}}\) that are separable over \(\text{frac}(R)\). 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 $R^{+GR}$, and hence
\[ z^2 t = t \sqrt{xz} \cdot x + \sqrt{yz} \cdot yt. \] (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 $R^{+GR}$. But $x$, $yt$ is a regular sequence on $R^{+GR}$, so there exists an element $c$ in $[R^{+GR}]_0$ with $u + t\sqrt{xz} = cyt$ and $v + \sqrt{yz} = cx$. Since $[R^{+GR}]_0 = \mathbb{F}_2$, it follows that $c \in R$, and hence that $\sqrt{yz} \in B$. This contradicts the hypothesis that elements of $B$ are separable over $\text{frac}(R)$.

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 $R \subseteq S \subseteq R^{+GR}$. 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 $\sqrt{xy}$, $\sqrt{yz}$, $t\sqrt{xy}$, $t\sqrt{yz}$ are all elements of $S$. We prove inductively that $S$ contains
\[ x^{1-2/q} (yz)^{1/q}, \quad y^{1-2/q} (xz)^{1/q}, \quad z^{1-2/q} (xy)^{1/q}, \]
\[ tx^{1-2/q} (yz)^{1/q}, \quad ty^{1-2/q} (xz)^{1/q}, \quad tz^{1-2/q} (xy)^{1/q}, \]
for each $q = 2^e$ with $e \geq 1$. The case $e = 1$ has been settled.

Suppose $S$ contains the elements (5.3.1) for some $q = 2^e$. Then, one has
\[
x^{1-2/q} (yz)^{1/q} \cdot ty^{1-2/q} (xz)^{1/q} \cdot (y + xt)
= tx^{1-2/q} (yz)^{1/q} \cdot ty^{1-2/q} (xz)^{1/q} \cdot x + x^{1-2/q} (yz)^{1/q} \cdot y^{1-2/q} (xz)^{1/q} \cdot yt.
\]

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
\[ t(xy)^{1-1/q} z^{2/q} = u \cdot x + v \cdot yt. \] (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
\[ t(xy)^{1-1/q} z^{2/q} = ty^{1-1/q} (xz)^{1/2q} \cdot x + x^{1-1/q} (yz)^{1/2q} \cdot yt. \] (5.3.3)
Comparing (5.3.2) and (5.3.3), we see that
\[
(u + ty^{1-1/q}(xz)^{1/2q}) \cdot x = (v + x^{1-1/q}(yz)^{1/2q}) \cdot yt,
\]
so there exists \( c \in [R^{+GR}]_0 \) with
\[
u + x^{1-1/q}(yz)^{1/2q} = cx.
\]
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
\[
\theta^{1/q} \in \text{frac}(S) \quad \text{for each } q = 2^e.
\]
We claim \( \theta^{1/2} \) does not belong to \( \text{frac}(R) \). Indeed if it does, then \( (xy)^{1/2} \) belongs to \( \text{frac}(R) \), and hence to \( R \), as \( R \) is normal; this is readily seen to be false. The extension
\[
\text{frac}(R) \subseteq \text{frac}(R)(\theta^{1/q})
\]
is purely inseparable, so the minimal polynomial of \( \theta^{1/q} \) over \( \text{frac}(R) \) has the form \( T^Q - \theta^{Q/q} \) for some \( Q = 2^E \). Since \( \theta^{1/2} \notin \text{frac}(R) \), we conclude that the minimal polynomial is \( T^q - \theta \). Hence
\[
[\text{frac}(R)(\theta^{1/q}) : \text{frac}(R)] = q \quad \text{for each } q = 2^e.
\]
It follows that \( [\text{frac}(S) : \text{frac}(R)] \) is not finite.

Theorems 1.2 and 1.3(2) discuss the vanishing of the image of \( H_i^m(R) \) for \( i < \dim R \). In the case of graded rings, one also has the following result for \( H_d^m(R) \).

**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 \( [H_d^m(R)]_{\geq 0} \) maps to zero under the induced map
\[
H_d^m(R) \to H_d^m(R^{+GR}).
\]

Hence, there exists a module-finite \( \mathbb{Q} \)-graded extension domain \( S \) of \( R \) such that the induced map \([H_d^m(R)]_{\geq 0} \to H_d^m(S)\) is zero.

**Proof.** Let \( F^e : H_d^m(R) \to H_d^m(R) \) denote the \( e \)-th iteration of the Frobenius map. Suppose [\( \eta \) \( \in [H_d^m(R)]_n \)] for some \( n \geq 0 \). Then \( F^e([\eta]) \) belongs to \([H_d^m(R)]_{np^e} \) for each \( e \). As \([H_d^m(R)]_{\geq 0} \) has finite length, there exists \( e \geq 1 \) and homogeneous elements \( r_1, \ldots, r_e \in R \) such that
\[
F^e([\eta]) + r_1 F^{e-1}([\eta]) + \cdots + r_e[\eta] = 0.
\]
(5.4.1)
We imitate the equational construction from [10]: Consider a homogeneous system of parameters \( x = x_1, \ldots, x_d \), and compute \( H^i_m(R) \) as the cohomology of the Čech complex \( C^*(x; R) \) below:

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

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

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

is a boundary in \( C^d(x; R) \), say it equals \( \partial(\alpha) \) for a homogeneous element \( \alpha \) of \( C^{d-1}(x; R) \). Solving integral equations in each coordinate of \( C^{d-1}(x; R) \), there exists a module-finite extension domain \( S \) and \( \beta \) in \( C^{d-1}(x; S) \) 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 \( \text{frac}(S) \) 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 \( H^d_m(S) \). Thus, each homogeneous element of the module \( \{H^d_m(R)\}_{\geq 0} \) maps to 0 in \( H^d_m(R+GR) \).

For the final statement, note that \( \{H^d_m(R)\}_{\geq 0} \) has finite length. \( \square \)

The next example illustrates why Proposition 5.4 is limited to \( \{H^d_m(R)\}_{\geq 0} \).

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

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

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

\[
H^d_m(R) \rightarrow H^d_m(S)
\]

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 \( H^d_m(R) \rightarrow H^d_m(S) \).

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


