THE COHEN-MACAULAY PROPERTY OF INVARIANT RINGS

AYAN NATH

Contents

1 Introduction

In this expository report, we discuss a short proof of the Hochster-Roberts theorem (see Theorem 1.6) given in Knop's unpublished note [3] written in German. Section 1 introduces and defines some algebraic notions just enough to understand the statement of Theorem 1.6, and Section 2 provides a rapid review of the background needed for the proof. The reader may skip to Section 3 for the main proof.

1.1. *Notation.* The letters A, B, C, R, and S always denote commutative unital rings and k denotes a field. For maximal ideals, we always use $\mathfrak{m}$ or $\mathfrak{n}$. All rings are Noetherian.

Before stating the main theorem, we need to introduce some notions. Noetherian local rings $(R,\mathfrak{m})$ always have finite Krull dimension– $\dim R \leqslant \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ follows by a simple application of Nakayama and Krull's height theorem.

1.2. Definition (Regular sequence). A sequence of elements $f_1, f_2, \ldots, f_r \in \mathfrak{m}$ in a Noetherian local ring $(R,\mathfrak{m})$ is called *regular* if f_1 is a nonzerodivisor and f_i is a nonzerodivisor on $R/(f_1,\ldots,f_{i-1})$ for each $i = 2,\ldots,r$.

This notion a priori depends on the order of the sequence. Intuitively, a regular sequence "cuts down" the maximal ideal as much as possible at each step. If $f \in R$ is any non-unit and nonzerodivisor, we have $\dim R/(f) \leqslant \dim R - 1$[1]. It follows that a regular sequence can have at most $\dim R$ terms.

Date: 25th November, 2022
Affiliation: BSc 2nd year, Chennai Mathematical Institute
[1] This is because minimal primes only have zerodivisors. If $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ is a chain in $R/(f)$ then we can find $\mathfrak{p}_0 \in \operatorname{Spec} R$ such that $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 + (f)$ as $\mathfrak{p}_1 + (f)$ cannot be a minimal prime, f being a nonzerodivisor. In fact, this is an equality, see Atiyah-Macdonald [1, Corollary 11.18].

1.3. Definition (Depth). The length of a maximal regular sequence in a Noetherian local ring R is called the *depth* of R. It is denoted $\operatorname{depth} R$. For a general Noetherain ring R and prime ideal $\mathfrak{p}$, we write $\operatorname{depth} \mathfrak{p}$ for $\operatorname{depth} R_{\mathfrak{p}}$.

Just like (co)dimension, depth can be thought of as a measure of how big a local ring or an ideal is. Since $\operatorname{depth} R \leqslant \dim R$ holds for all Noetherian local rings R, it is natural to investigate the equality case.

1.4. Definition (Cohen-Macaulay rings). A Noetherian local ring R is called *Cohen-Macaulay* if $\operatorname{depth} R = \dim R$. In general, a ring A is called Cohen-Macaulay if $A_{\mathfrak{p}}$ is a Cohen-Macaulay local ring for each $\mathfrak{p} \in \operatorname{Spec} A$.

For a finite-dimensional k-vectorspace V, we denote the free algebra $k[\phi_1, \phi_2, \ldots, \phi_n]$ as $k[V]$, where $(\phi_1, \ldots, \phi_n)$ is a fixed dual basis for the dual space of V. It is clear that $k[V]$ doesn't depend on the choice of basis upto isomorphism. Let G be a group. A finite-dimensional G-representation V naturally induces an action of G on $k[V]$ by identifying the unit degree graded piece of $k[V]$ with V.

1.5. Definition (Linearly reductive group). A group G is called *linearly reductive*[2] if every finite-dimensional G-representation V can be decomposed into irreducible subrepresentations.

We can now finally state the main theorem–

1.6. Theorem (Hochster-Roberts). — *Let G be a linearly reductive group and V a finite-dimensional G-representation, both defined over a field k of characteristic zero. Then $k[V]^G$ is a Cohen-Macaulay ring.*

The linearly reductive hypothesis on G is solely to ensure that $Ik[V] \cap k[V]^G = I$ holds for all $k[V]^G$-ideals I (see Proposition 2.10). Any graded k-subalgebra S of $k[V]$ such that $Ik[V] \cap S = I$ holds for all S-ideals I is also Cohen-Macaulay.

2 Background

2.1. Cohen-Macaulayness, generic freeness, graded Noether normalization. Checking Cohen-Macaulayness in the graded case is much easier due to the following result–

2.2. Lemma (Cohen-Macaulayness criterion for graded rings). — *Let R be a postively graded Noetherian ring and $\mathfrak{m} = R_+$ be the irrelevant ideal. Then R is Cohen-Macaulay if and only if $R_{\mathfrak{m}}$ is Cohen-Macaulay.*

Proof. See Bruns-Herzog [2, Exercise 2.1.27 (c), Theorem 1.5.8 (b), Theorem 1.5.9]. □

2.3. Theorem (Generic freeness). — *Let A be a Noetherian domain and B be a finitely generated A-algebra. Then there exists a nonzero $f \in A$ such that B_f is a free A_f-module.*

Proof. See Matsumura [4, 22.A]. Also see https://en.wikipedia.org/wiki/Noether_normalization_lemma#Illustrative_application:_generic_freeness. □

The following lemma is true without the infiniteness constraint on k, but since our base field is of characteristic 0, we assume k is infinite to simplify the proof.

[2] G is an algebraic group in the original paper, but we avoid this as the Hochster-Roberts theorem has nothing to do with the scheme structure of G in characteristic zero.

2.4. Lemma (Graded Noether normalization). — *Let R be a finitely-generated positively-graded k-algebra, where k is an infinite field. Assume that the degree zero graded piece of R is just k. There exist homogeneous elements $x_1, x_2, \dots, x_n \in R$ such that*

(i) *R is a finite extension of $k[x_1, x_2, \dots, x_n]$.*
(ii) *$n = \dim R$.*
(iii) *$x_1, x_2, \dots, x_n$ are algebraically independent over k.*

Proof. We give a brief sketch. There exists $d > 0$ such that $R^{(d)} \overset{\text{def}}{=} R_0 \oplus R_d \oplus R_{2d} \oplus \cdots$ is generated by R_d over k. See Stacks [5, Tag: 0EGH]. As R is finite over $R^{(d)}$ we replace R with $R^{(d)}$. Take some homogeneous generators $y_1, y_2, \dots, y_m$ of R_d as a k-vectorspace. If y_i are algebraically independent, there is nothing to do. So suppose there is some nontrivial polynomial $f \in k[X_1, \dots, X_m]$ with $f(y_1, \dots, y_m) = 0$. We can pick f to be homogeneous as y_i are homogeneous. Due to infiniteness of k, there exist $a_i \in k$ such that $f(a_1, \dots, a_{m-1}, 1) \neq 0$. Then $f(a_1, \dots, a_{m-1}, 1)^{-1} f(a_1 y_m + z_1, a_2 y_m + z_2, \dots, a_{m-1} y_m + z_{m-1}, y_m)$, where $z_i = y_i - a_i y_m$, is monic in y_m. Note that z_i are homogeneous. Thus, $R^{(d)}$ is finite over $k[z_1, z_2, \dots, z_{m-1}]$ and we can induct on the k-vectorspace dimension of the degree 1 graded piece. The fact that the size of such a sequence of elements is $\dim R$ is a consequence of going-up theorem for integral extensions. □

2.5. Lemma. — *Let $B \hookrightarrow C$ be a finite type inclusion of domains. Then $\operatorname{Spec} C \to \operatorname{Spec} B$ maps closed points to closed points.*

Proof. By induction, we may assume C is singly generated over B. Write $C = B[X]/\mathfrak{p}$. Then $\operatorname{Spec} C \to \operatorname{Spec} B$ factors through $\operatorname{Spec} B[X]$. Obviously, $\operatorname{Spec} C \to \operatorname{Spec} B[X]$ maps closed points to closed points. So we must show that $\operatorname{Spec} B[X] \to \operatorname{Spec} B$ maps closed points to closed points. Indeed, suppose if $\mathfrak{m} \in \operatorname{MaxSpec} B[X]$ and $\mathfrak{m} \cap B = \mathfrak{n}$. Then $\mathfrak{n}[X] + (X)$ is a proper ideal and it contains $\mathfrak{m}$. As $\mathfrak{m}$ is maximal, this means that $\mathfrak{n}[X] + (X) = \mathfrak{m}$. Hence, $B[X]/\mathfrak{m} = B[X]/(\mathfrak{n}[X] + (X)) \cong B/\mathfrak{n}$. Thus, $\mathfrak{n}$ is maximal in B. □

2.6. Finite-generation of the invariant ring. We give a brief outline of the proof of finite-generation of the invariant ring.

2.7. Definition (Reynolds operator). — Let $S \subseteq R$ be rings. An S-module map $\rho \colon R \to S$ is called a *Reynolds operator corresponding to* $S \subseteq R$ if it fixes S pointwise.

2.8. Lemma. — *Let G be a linearly reductive group acting linearly on a finite-dimensional k-vectorspace V. Then there is a linear map $V \to V^G$ which fixes V^G pointwise.*

Proof. This is clear because the linearly reductive hypothesis means that we can decompose V into irreducible subrepresentations. One of the components would be the trivial subrepresentation V^G. So, we can decompose V as $V^G \oplus U$ where U is invariant under G. Now, the required map $V \to V^G$ is just the natural projection from V to V^G. □

2.9. Lemma. — *Let G be a linearly reductive group acting linearly on a free k-algebra $A = k[X_1, \dots, X_n]$. Then there is a Reynolds operator corresponding to $A^G \subseteq A$.*

Proof. We provide a brief sketch. Decompose A into the graded pieces as $A = k \oplus A_1 \oplus A_2 \oplus \cdots$. Then G acts linearly on each of the graded pieces. So, corresponding to each A_i, there is a Reynolds operator $\rho_i \colon A_i \to A_i^G$ by Lemma 2.8. Now the required Reynolds operator is just $\mathrm{id}_k \oplus \rho_1 \oplus \rho_2 \oplus \cdots$. □

2.10. Proposition. — *If there is a Reynolds operator for $S \subseteq R$. Then*

(i) $IR \cap S = I$ *for each* S*-ideal* I.
(ii) *if* R *is Noetherian, then so is* S.

Proof. All of these are pretty straightforward to show. Omitted. [2, Proposition 6.4.4] $\square$.

It can be shown by a routine induction on the degree that positively graded Noetherian k-algebras are generated by the (finitely many) generators of the irrelevant ideal. Concluding, R^G is a finitely generated k-algebra by Lemma 2.9 and Proposition 2.10 (ii).

3 The proof

3.1. Setup. Set $R = k[V] = k[X_1, \dots, X_n]$, and $S = R^G$. We know that S is a finitely generated (graded) k-subalgebra of R. By graded Noether normalization (see Lemma 2.4), we can find homogeneous $f_1, \dots, f_s \in S$ such that S is a finite B-module, where $B = k[f_1, \dots, f_s]$ and $s = \dim S$. By Lemma 2.2, it suffices to show that $f_1, \dots, f_s$ is a regular sequence in the localization of S at the irrelevant ideal, which is equivalent to the following for each $r = 1, 2, \dots, s-1$:

$$\text{If } g_i \in S,\ 1 \leqslant i \leqslant r+1, \text{ and } g_{r+1} f_{r+1} \in g_1 f_1 + g_2 f_2 + \cdots + g_r f_r \text{ then } g_{r+1} \in (f_1, \dots, f_r)S.$$

In fact, we may assume that all the g_i's are homogeneous because the ideal $(f_1, \dots, f_r)S$ is homogeneous. By Proposition 2.10 (i), it suffices to show that $g_{r+1} \in (f_1, \dots, f_r)R$. Let us assume the contrary that $g_{r+1} \notin (f_1, \dots, f_r)R$. This is same as saying there doesn't exist $a_1, a_2, \dots, a_r \in R$ with $g_{r+1} = a_1 f_1 + a_2 f_2 + \cdots + a_r f_r$. Because of homogeneity, we may assume that either $\deg a_i = \deg g_{r+1} - \deg f_i$ or $a_i = 0$ for each $i = 1, 2, \dots, r$. The nonexistence of $a_i \in R$ with $g_{r+1} = a_1 f_1 + a_2 f_2 + \cdots + a_r f_r$ is equivalent to unsolvability of a (finite) system of inhomogeneous linear equations, call it S, with coefficients in k obtained by comparing coefficients in R.

3.2. Finite generation trick. Let $r_1, \dots, r_m \in S$ generate S as a B-module. Suppose A is a finitely generated (as a $\mathbb{Z}$-algebra) subring of k containing

(a) all coefficients of g_i as a polynomial in $X_1, \dots, X_n$, $1 \leqslant i \leqslant r+1$,
(b) all the coefficients of $c_{ij} \in B$, as polynomials in $f_1, \dots, f_s$, for some arbitrary representation

$$g_i = c_{i1} r_1 + c_{i2} r_2 + \cdots + c_{im} r_m, \quad 1 \leqslant i \leqslant r+1.$$

(c) all the coefficients of $d_{ijk} \in B$, as polynomials in $f_1, \dots, f_s$, for some representation

$$r_i r_j = d_{ij1} r_1 + d_{ij2} r_2 + \cdots + d_{ijm} r_m, \quad 1 \leqslant i, j \leqslant m.$$

The upshot of the above construction is that we can now replace k by the ring A which has the property that $A/\mathfrak{m}$ is a finite field for each $\mathfrak{m} \in \operatorname{MaxSpec} A$. Indeed, applying Noether normalization with respect to the prime subfield of $A/\mathfrak{m}$ we see that it is a finite field. To be precise, define $R_0 = A[X_1, \dots, X_n]$, $B_0 = A[f_1, \dots, f_s]$, and $S_0 = B_0[r_1, \dots, r_m]$, then we have

(a) $S_0 \subseteq R_0$,
(b) $S_0 = B_0 r_1 + \cdots + B_0 r_m$,
(c) $g_{r+1} \in S_0$,
(d) $g_{r+1} f_{r+1} \in S_0 f_1 + \cdots + S_0 f_r$.

So we can safely replace k with A in the theorem statement. Because of our assumption that S is unsolvable, it is also unsolvable in $\operatorname{Frac} A$ for any such $A \subseteq k$. Write the system of equations as $Mx = b$, where $M \in \operatorname{Mat}_{p \times q}(A)$, $b \in A^{\oplus p} \setminus \{0\}$. Let $N = [M \mid b]$ be the augmented matrix of the system. Consider the following claim:

3.3. Claim. — *The system of equations $Mx = b$ has no solutions in $x \in (\operatorname{Frac} A)^{\oplus q}$ if and only if the A-span of rows of N has a vector of the form $(0,0,\dots,0,b_0)$ for some nonzero $b_0 \in A$.*

Proof. Suppose the A-span of rows of N has no vector of form $(0,0,\dots,0,b_0)$ for any nonzero $b_0 \in A$. We must show that $Mx = b$ has a solution. If a set of rows of M are linearly dependent[3] then we have redundant equations. So we can delete all the redundant equations and assume that all rows of M are linearly independent. Therefore, the linear map $(\operatorname{Frac} A)^{\oplus q} \to (\operatorname{Frac} A)^{\oplus p}$ determined by M is surjective, and hence, a solution must exist. □

Thus, unsolvability of a system of inhomogeneous linear equations $Mx = b$ occurs due to the A-span of rows of the augmented matrix having a vector of the form $(0,0,\dots,0,b_0)$ for some nonzero $b_0 \in A$.

We can now replace A by $A[1/b_0]$ to assume that S is not solvable modulo any $\mathfrak{m} \in \operatorname{MaxSpec} A$.

3.4. Modding out by maximal ideals. We now want to mod out everything by a maximal ideal to reduce the problem to the case of finite fields. Let $\mathfrak{m}$ be a maximal ideal of A to be chosen later.

Define $\overline{A} = A/\mathfrak{m}$, $\overline{R} = R/\mathfrak{m}R$, $\overline{B} = B/\mathfrak{m}B$, and $\overline{S} = S/\mathfrak{m}S$. Let $\overline{X_i} \in \overline{R}$, $\overline{f_i} \in \overline{B}$, and $\overline{g_i} \in \overline{S}$ denote the images of X_i, f_i, and g_i, respectively. Note that $\overline{R} = \overline{A}[\overline{X_1},\dots,\overline{X_n}]$ is a free algebra and $\overline{B} = \overline{A}[\overline{f_1},\dots,\overline{f_s}]$. Let the characteristic of $\overline{A}$ be $p > 0$. We still have $\overline{g_{r+1}} \notin (\overline{f_1},\dots,\overline{f_r})\overline{R}$. But there is something more we want– we would hope that $f_1,\dots,f_r \pmod{\mathfrak{m}R}$ are algebraically independent over $A/\mathfrak{m}$. This can be ensured by having $\overline{B} \subseteq \overline{R}$, i.e., the induced map $B/\mathfrak{m}B \to R/\mathfrak{m}R$ to be an injection[4,5]. By generic freeness (Theorem 2.3), there exists a nonzero $f \in B$ such that R_f is a free B_f-module. The Jacobson radical of a free algebra over a domain is 0. So, we can find a maximal ideal $\mathfrak{n} \in \operatorname{MaxSpec} B$ not containing f so that $\mathfrak{m} = \mathfrak{n} \cap A$ is a maximal ideal of A (see Lemma 2.5). We claim that $B/\mathfrak{m}B \to R/\mathfrak{m}R$ is an injection. This follows from the following commutative diagram:

$$\begin{array}{ccc} B/\mathfrak{m}B & \xhookrightarrow{\text{localization}} & B_f/\mathfrak{m}B_f \\ \downarrow & & \downarrow \\ R/\mathfrak{m}R & \hookrightarrow & R_f/\mathfrak{m}R_f \end{array}$$

Obviously, the horizontal localization maps are inclusions. The vertical map on the right hand side is also an injection because R_f is a free B_f-module. Hence, $B/\mathfrak{m}B \to R/\mathfrak{m}R$ is also an inclusion.

3.5. Characteristic p: exploiting the Frobenious endomorphism. We mod out by the $\mathfrak{m}$ obtained in the previous subsection and write k for $A/\mathfrak{m}$. Because $B/\mathfrak{m}B \hookrightarrow R/\mathfrak{m}R$, we can think of $\overline{f_i}$ as elements of $R/\mathfrak{m}R$. For brevity, we also drop the bars. So, for e.g., we just write f_i for $\overline{f_i}$, B for $\overline{B}$, etc.

The B-module S has a maximum-rank[6] free submodule, say F. Then S/F is a torsion B-module. So there exists a nonzero $c \in B$ so that $cS \subseteq F$ as S/F is finitely generated. We have

$$g_{r+1}f_{r+1} = g_1f_1 + g_2f_2 + \cdots + g_rf_r.$$

---

[3] Linear (in)dependence is independent of whether we choose A or $\operatorname{Frac} A$ as our base ring because we can always clear denominators.

[4] In general, this is *not* an injection. Take, for example, $\mathbb{Z}[2X]/2\mathbb{Z}[2X] \to \mathbb{Z}[X]/2\mathbb{Z}[X]$.

[5] For if $P \in A[T_1,\dots,T_s]$ is a polynomial, not all coefficients in $\mathfrak{m}$, such that $P(f_1,\dots,f_s) \in \mathfrak{m}R$ (this is same as saying $f_i \pmod{\mathfrak{m}R}$ are algebraicaly dependent over $A/\mathfrak{m}$) then $P(f_1,\dots,f_s) \in \mathfrak{m}R \cap B = \mathfrak{m}B$, from the injectivity of $B/\mathfrak{m}B \to R/\mathfrak{m}R$. Therefore, the image of $P(f_1,\dots,f_s)$ in $B/\mathfrak{m}B$ is 0, which forces all coefficients of P to be in $\mathfrak{m}$ as $B/\mathfrak{m}B$ is a free $A/\mathfrak{m}$-algebra generated by $\overline{f_1},\dots,\overline{f_s}$. Thus, $f_i \pmod{\mathfrak{m}R}$ are indeed algebraically independent over $A/\mathfrak{m}$.

[6] The rank is defined as the cardinality of a maximal set of elements of S which are linearly independent over B. Here, maximum-rank means that $\operatorname{rank}_B F = \operatorname{rank}_B S$. It can be shown that $\operatorname{rank}_B S = \dim_{\operatorname{Frac} B} F \otimes_B \operatorname{Frac} B$.

Set $q = p^N$. Exponentiating by q and multiplying by c, we get

$$\underbrace{(cg_{r+1}^q)}_{\in F} f_{r+1}^q = \underbrace{(cg_1^q)}_{\in F} f_1^q + \underbrace{(cg_2^q)}_{\in F} f_2^q + \cdots + \underbrace{(cg_r^q)}_{\in F} f_r^q.$$

If f_{r+1}^q is a zerodivisor on $F/(f_1^q, f_2^q, \ldots, f_r^q)F$ then it is also a zerodivisor on $F/(f_1, \ldots, f_r)F$ because $(f_1^q, \ldots, f_r^q) \subseteq (f_1, \ldots, f_r)$, which is clearly false because

$$F/(f_1, \ldots, f_r)F \cong (B/(f_1, \ldots, f_r)B)^{\oplus \ell} \cong^{7} k[f_{r+1}, f_{r+2}, \ldots, f_s]^{\oplus \ell},$$

where $\ell = \operatorname{rank}_B F$. In particular, cg_{r+1}^q must be zero modulo $(f_1^q, \ldots, f_r^q)F$. So, there exists $h_i \in F$, $i = 1, \ldots, r$, dependent on q, such that

$$cg_{r+1}^q = h_1 f_1^q + h_2 f_2^q + \cdots + h_r f_r^q.$$

Since the Frobenious endomorphism is an automorphism in the case of finite fields, every element of k is a qth power. Denote $\mathscr{M} = \{X_1^{e_1} \cdots X_n^{e_n} : 0 \leqslant e_i < q \text{ for each } i = 1, \ldots, n\}$. Therefore, every element h of R can be written as $h = \sum_{m \in \mathscr{M}} h_m^q m$ in a unique way. In other words, $k[X_1, \ldots, X_n]$ is a free $k[X_1^q, \ldots, X_n^q]$-module. Let $h_i = \sum_{m \in \mathscr{M}} h_{im}^q m$ for each i. Thus,

$$cg_{r+1}^q = \sum_{i=1}^r h_i f_i^q = \sum_{i=1}^r \sum_{m \in \mathscr{M}} h_{im}^q f_i^q m = \sum_{m \in \mathscr{M}} \left(\sum_{i=1}^r h_{im} f_i \right)^q m = \sum_{m \in \mathscr{M}} k_m^q m,$$

where $k_m = \sum_{i=1}^r h_{im} f_i \in (f_1, \ldots, f_r)R$. It is now crucial that c doesn't depend on q. We choose q so large that $c = \sum_{m \in \mathscr{M}} c_m^q m$ for $c_m \in k$. Here we are using the fact that all elements of k are qth powers. Then

$$\sum_{m \in \mathscr{M}} (c_m g_{r+1})^q m = \sum_{m \in \mathscr{M}} k_m^q m.$$

As $c \neq 0$, there exists $m \in \mathscr{M}$ with $c_m \neq 0$ so that

$$c_m g_{r+1} = k_m \implies g_{r+1} = c_m^{-1} k_m \in (f_1, \ldots, f_r)R.$$

Contradiction! □

References

[1] M. Atiyah and I. Macdonald, *Introduction to Commutative Algebra*, Addision-Wesley (1969).
[2] W. Bruns and J. H. Herzog, *Cohen-Macaulay Rings*, Cambridge Studies in Advanced Mathematics (1998).
[3] F. Knop, Die Cohen-Macaulay-Eigenschaft von Invariantenringen, https://www.researchgate.net/publication/238698485, *Unpublished* (1990).
[4] H. Matsumura, *Commutative Algebra*, 2nd ed., W.A. Benjamin, New York (1970).
[5] The Stacks authors, The Stacks project, https://stacks.math.columbia.edu (2022).

[7] Here, we are using that $f_i \pmod{\mathfrak{m}R}$ are algebraically independent over $A/\mathfrak{m}$.