JOURNAL OF ALGEBRA **202,** 1–9 (1998)
ARTICLE NO. JA977333

The Content of Gaussian Polynomials

Sarah Glaz

Department of Mathematics, University of Connecticut, Storrs, Connecticut 06269
E-mail: glaz@uconnvm.uconn.edu

Wolmer V. Vasconcelos*

Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903
E-mail: vasconce@rings.rutgers.edu

Communicated by Mel Hochster

Received August 24, 1995

DEDICATED TO IRVING KAPLANSKY

1. INTRODUCTION

Let R be a commutative ring and let $f(t)$ be a polynomial with coefficients in R,

$$f = f(t) = a_d t^d + \cdots + a_0.$$

The *content ideal* of $f(t)$, or simply the *content* of f, is the ideal $(a_d, \ldots, a_0)R$. We denote it by $c(f)$. One of its properties is that $c(\cdot)$ is semi-multiplicative, that is

$$c(f \cdot g) \subset c(f) \cdot c(g).$$

We examine the case in which for a fixed f this relation is an equality for all polynomials g; f is then said to be a *multiplicative* or a *Gaussian* polynomial. From what one can tell this property may not be independent of the generators of $c(f)$; it may even depend on the sequence of its

* Partially supported by the NSF.

0021-8693/98 $25.00

coefficients. Also, it may not behave well under change of rings more general than epimorphisms. On the other hand the set of these polynomials is a monoid.

Examples of Gaussian polynomials are those with a content $c(f)$ which is a principal ideal at each localization, or, if $(R, \mathfrak{m})$ is a local Artinian ring with $\mathfrak{m}^2 = 0$ then any polynomial of $R[t]$ is Gaussian.

Our guiding question is the following broad converse of the classical lemma of Gauss.

Conjecture 1.1. Let R be an integral domain. If $f(t) \in R[t]$ is a Gaussian polynomial then $c(f)$ is an invertible ideal.

Questions on the behavior of the content of polynomials have been raised by several workers [1, 2, 4, 9]. One of the authors heard the question above from Irving Kaplansky in the early 1960's. It also appeared in the thesis of H. T. Tsang [9] (but not in her paper [10]).

In this note we settle this question in the affirmative for all Noetherian normal domains (Theorem 4.4). Actually, if the ring has finite characteristic, then being integrally closed will suffice (Theorem 3.1). Several other special cases are dealt with as well.

2. HILBERT FUNCTIONS

We may assume throughout that $(R, \mathfrak{m})$ is a local ring, and $f(t)$ is a Gaussian polynomial. We use the notation $\nu(M)$ for the minimum number of generators of an R-module M.

The path to our analysis is a close examination of the numerical function

$$n \mapsto \nu(c(f^n)). \tag{1}$$

One gives a combinatorial setting for this function as follows. Set $I = c(f)$ and let

$$R[IT] = R + IT + I^2T^2 + \cdots \subset R[T]$$

be the Rees algebra of the ideal I. The function (1) is then the Hilbert function of the special fiber $F(I)$ of the ring $R[IT]$, that is of the graded ring

$$F(I) = R[IT] \otimes R/\mathfrak{m} = \bigoplus_{n \geq 0} I^n/\mathfrak{m} I^n,$$

where $\mathfrak{m}$ is the maximal ideal of R.

PROPOSITION 2.1. *If $f(t)$ is a Gaussian polynomial then the Hilbert polynomial of $F(I)$ has degree at most* 1.

Proof. Denote $d = \deg(f)$. For any integer n, by definition we have that $c(f^n) = c(f)^n$. This implies that

$$\dim F(I)_n = \nu\big(c(f)^n\big) \leq dn + 1, \tag{2}$$

since f^n has at most $dn + 1$ coefficients.

As $\dim F(I)_n$ is bounded by a polynomial of degree 1, the Hilbert polynomial of $F(I)$ must be a form $e_0 n + e_1$, of degree at most 1, that is

$$\dim F(I)_n = e_0 n + e_1, \qquad n \gg 0,$$

as asserted. ∎

By abuse of terminology we say that $e_0 n + e_1$ is the Hilbert polynomial of $f(t)$.

At this point we have not used the Noetherianess of R, just that of $F(I)$ which is finitely generated over the residue field $\mathfrak{k} = R/\mathfrak{m}$. If $\mathfrak{k}$ is infinite, $F(I)$ admits a Noether normalization

$$\mathfrak{k}[\mathbf{z}] \hookrightarrow F(I),$$

where $\mathbf{z}$ is a set of 1 or 2 algebraically independent elements according to whether the Krull dimension $\dim F(I)$ is 1 or 2, which is reflected in its Hilbert polynomial by the conditions $e_0 = 0$ or $e_0 \neq 0$, respectively. Furthermore, the elements of $\mathbf{z}$ can be chosen in degree 1, $\mathbf{z} \subset F(I)_1$. When lifted to I this gives rise to an equality

$$I^n = (a, b) I^{n-1} \tag{3}$$

valid for all $n \gg 0$. The ideal $J = (a, b) \subset I$ (or just $J = (a)$ if $e_0 = 0$) is a reduction of I (see [8] for these basic facts).

If $\mathfrak{k}$ is finite, we make a field extension such as $\mathfrak{k} \to K = \mathfrak{k}(x)$ (or, at the local ring level, the faithfully flat extension $R \to R(x) = R[x]_{\mathfrak{m} R[x]}$) that leaves the Hilbert function unchanged and obtain the equality

$$I^n R(x) = (a, b) I^{n-1} R(x), \tag{4}$$

where $(a, b) \subset IR(x)$. Note that we are not asserting that the polynomial $f(t)$ remains Gaussian after the base ring change, only that its Hilbert polynomial is unchanged.

Our means to test Conjecture 1.1 are the following two elementary criteria.

PROPOSITION 2.2. *Let R be an integrally closed local domain and let $f(t)$ be a Gaussian polynomial. Then $c(f)$ is principal if and only if $e_0 = 0$.*

Proof. By the faithfully flat change of rings indicated above (which preserves normality and the Hilbert polynomial of $f(t)$), we may assume that the residue field is infinite.

If $e_0 = 0$, we have $I^n = (a)I^{n-1}$ for some $n \geq 0$, which means that the elements of the fractional ideal Ia^{-1} are integral over R, and thus $I \subset (a)$. The converse is clear. ∎

PROPOSITION 2.3. *Let R be a local domain. If $f(t)$ is a Gaussian polynomial where $c(f)$ is generated by at most 2 elements then $c(f)$ is principal.*

Proof. If $c(f)$ is not principal, suppose the generators a, b of $c(f)$ occur in degrees m and n (achievable through Nakayama lemma). We write

$$f(t) = ag(t) + bh(t),$$

where $g(t)$ has a coefficient of 1 in degree m and 0 in degree n, and $h(t)$ has in those degrees the reverse coefficients.

Consider the polynomial $r(t) = ag(t) - bh(t)$, $c(r) = (a, b)$. By hypothesis

$$c(f \cdot r) = (a, b)^2,$$

while

$$c(f \cdot r) \subset (a^2, b^2).$$

Thus a^2 and b^2 form a generating set for $(a, b)^2$.

Now consider the polynomial $q(t) = bg(t) + ah(t)$. Note that $c(q) = (a, b)$. By hypothesis,

$$c(f \cdot q) = (a, b)^2,$$

while obviously

$$c(f \cdot q) \subset (ab, a^2 + b^2).$$

This means that

$$(a, b)^2 = (ab, a^2 + b^2).$$

If (a, b) is not principal, this equation says that $(a, b)^2$ is minimally generated by ab and $a^2 + b^2$. It follows that

$$ab = \alpha a^2 + \beta b^2,$$

where either α or β is a unit.

Consider now the polynomial $p(t) = \beta b g(t) + \alpha a h(t)$. Then $c(p) = (\beta b, \alpha a)$, and from

$$f(t) \cdot p(t) = \beta a b g^2 + \left(\alpha a^2 + \beta b^2\right) g h + \alpha a b h^2,$$

we get

$$(a, b)(\beta b, \alpha a) = c(f) c(p) = c(f \cdot p) \subset (ab),$$

but since α or β is a unit $ab \in (a, b)(\beta b, \alpha a)$. Therefore $(ab) = (a, b)(\beta b, \alpha a)$ and $c(f) = (a, b)$ is invertible. ∎

3. PRIME CHARACTERISTIC

We establish the conjecture for these algebras. In this section, it will be seen that "finite" will refer to the characteristic of the residue fields of local rings.

THEOREM 3.1. *Let $(R, \mathfrak{m})$ be a local integral domain (not necessarily Noetherian) with residue field of characteristic $p > 0$. If $f(t)$ is a Gaussian polynomial over R then $e_0 = 0$. In particular if R is also integrally closed, then $c(f)$ is principal.*

Proof. The proof is similar to that of Proposition 2.1, except that we take n to be of the form p^m, with $p = \operatorname{char} R/\mathfrak{m}$. We claim that

$$\nu\left(c(f)^n\right) = \nu(c(f^n)) \leq d + 1,$$

which will permit us to obtain $e_0 = 0$, since the Hilbert function of $F(I)$ is bounded. For this, it suffices to note that for $m = p^n$, the coefficients of f^m are combinations of mth powers of the generators of $c(f)$ and power products of "degree" m in those elements:

$$\sum \binom{m}{\alpha_0, \ldots, \alpha_d} a_0^{\alpha_0} \cdots a_d^{\alpha_d}, \qquad \sum \alpha_i = m.$$

Since all the multinomial coefficients, except those with a single power a_i^m, are divisible by p, by Nakayama lemma all those mixed powers can be thrown away in the generation of $c(f)^m$.

The last assertion now follows from Proposition 2.2. ∎

4. CHARACTERISTIC ZERO

We discuss the conjecture in rings of characteristic zero but only settle it for Noetherian rings.

Let R be a local ring containing the rational numbers and assume $f(t)$ is a Gaussian polynomial. We can now be much more precise regarding the function $\nu(I^n)$, where $I = c(f)$.

PROPOSITION 4.1. *If R is a local ring containing the rational numbers $\mathbb{Q}$ and $f(t)$ is a Gaussian polynomial with Hilbert polynomial $e_0 n + e_1$ then $e_0 \leq 1$.*

Proof. By assumption the ideal I admits a reduction (a, b), that is there exists an integer s such that $I^{s+1} = (a, b)I^s$, with $(a, b) \subset I$, guaranteed by the fact that the residue field of R is infinite.

Consider the polynomials

$$g(t) = \sum_{i+j=rn} a^i b^j t^i,$$

where r, n are arbitrary positive integers. Suppose now that $n > s$ and r is still arbitrary. We have

$$c\big(f(t)^n \cdot g(t)\big) = c(f^n) \cdot c(g) = I^n (a, b)^{rn} = I^{rn+n},$$

since $f(t)^n$ is also Gaussian. Thus

$$\nu(I^{rn+n}) = e_0(rn + n) + e_1 \leq dn + rn + 1,$$

since $c(f)^n \cdot g(t)$ has degree $dn + rn$ and therefore its content can be generated by at most $dn + rn + 1$ coefficients. This implies that

$$e_0 \leq \frac{d}{r+1} + \frac{r}{r+1} + \frac{1-e_1}{(r+1)n} = 1 + \left(\frac{d-1}{r+1} + \frac{1-e_1}{(r+1)n} \right).$$

Given that n and r can be made arbitrarily large and e_0 is an integer while d and e_1 are fixed, we must have $e_0 \leq 1$, as asserted. ∎

THEOREM 4.2. *Let $(R, \mathfrak{m})$ be an integrally closed Noetherian local domain containing the rationals and let $f(t)$ be a Gaussian polynomial. Then $c(f)$ is principal.*

Proof. Let $J = (a, b)$ be a reduction of the ideal $I = c(f)$. We first show that $I = J$. If $I \neq J$, let $\mathfrak{p}$ be a minimal prime ideal of the annihilator of the module I/J. Localizing at $\mathfrak{p}$, preserves all the hypotheses: $R_\mathfrak{p}$ is integrally closed, contains $\mathbb{Q}$, and $f(t)$ is still Gaussian. Changing notation we will still denote this localization R and its maximal ideal by $\mathfrak{m}$ and may assume that $I/J \neq 0$ is a module of finite length and $\dim R \geq 2$.

Let $R[JT]$ be the Rees algebra of J; the embedding $R[JT] \hookrightarrow R[IT]$ makes $R[IT]$ a finitely generated module over $R[JT]$. By Proposition 4.1, we may assume that the Hilbert polynomial of $f(t)$ is a form $n + e_1$. This means that the ring $F(I) = R[IT] \otimes R/\mathfrak{m}$ is a module of rank 1 over the ring of polynomials $F(J) = R[JT] \otimes R/\mathfrak{m}$ (which is its Noether normalization).

The ideal J being generated by two elements of a normal Noetherian domain, it is of linear type according to [6, Proposition 1.5]. This means that the Rees algebra $R[JT]$ coincides with the symmetric algebra of J (see [12, Chapter 2] for a full discussion of these conditions). In particular if L denotes the module of relations of the ideal (a, b),

$$0 \to L \to R \oplus R \to (a, b) \to 0,$$

the algebra $R[JT]$ has a presentation

$$0 \to L \otimes_R R[x, y] \to R[x, y] \to R[JT] \to 0, \qquad x \mapsto aT, \qquad y \mapsto bT.$$

LEMMA 4.3. *Let $\mathfrak{M} = (\mathfrak{m}, aT, bT)$ be the irrelevant maximal ideal of the graded algebra $R[JT]$. Then the grade of the ideal $\mathfrak{M}$ is at least* 3.

Proof. This grade can also be determined as the $P = (\mathfrak{m}, x, y)$-depth of $R[JT]$ as a module over $R[x, y]$. Since R is integrally closed of dimension at least 2, the grade of $\mathfrak{m}$ is at least 2 and therefore the grade of P is at least 4. By the same token, the module L, being a syzygy module of an ideal, has $\mathfrak{m}$-depth at least 2 so that the $R[x, y]$-module $L \otimes_R R[x, y]$ will have P-depth at least 4. We now may use the depth-lemma on the exact sequence (see [3, Proposition 1.2.9]), to get the assertion. ∎

We are now ready to assemble all parts of the proof of the theorem. Consider the embedding of Rees algebras

$$0 \to R[JT] \to R[IT] \to C \to 0, \tag{5}$$

viewed as a sequence of $R[JT]$-modules. By assumption, I and J coincide in every proper localization of R, and therefore C is annihilated by some power of $\mathfrak{m}$. Using precisely the same argument in the proof of [11, Proposition 2.2], we are going to show that the module C is either zero (and $I = J$ as desired) or has Krull dimension 2 and $\mathfrak{m}R[JT]$ is its unique associated prime ideal.

Suppose $C \neq 0$ and let P be a prime ideal of $R[JT]$ which is associated to C; since C is a graded module, P is a homogeneous ideal. We claim that $P = \mathfrak{m}R[JT]$. Note that otherwise, as $\mathfrak{m}$ must be contained in P and $\dim R[JT]/P \leq 1$, $\mathfrak{M}$ is minimal over (P, h) for any (homogeneous) element in $\mathfrak{M} \setminus P$. This implies that grade $P \geq 2$, since under these conditions the grade of $\mathfrak{M}$ can go up by at most 1 from grade P.

Applying the functor $\mathrm{Hom}_{R[JT]}(R[JT]/P, \cdot)$ to the sequence (5), we get the exact sequence

$$0 \to \mathrm{Hom}_{R[JT]}(R[JT]/P, R[JT]) \to \mathrm{Hom}_{R[JT]}(R[JT]/P, R[IT])$$
$$\to \mathrm{Hom}_{R[JT]}(R[JT]/P, C) \to \mathrm{Ext}^1_{R[JT]}(R[JT]/P, R[JT]),$$

where the modules in the top row vanish by natural reasons and

$$\mathrm{Ext}^1_{R[JT]}(R[JT]/P, R[JT]) = 0,$$

because grade $P \geq 2$. This shows that $P = \mathfrak{m}R[JT]$ and establishes that if $C \neq 0$ then its Krull dimension must be 2.

As the final step, tensoring (5) with $R/\mathfrak{m}$ we get the exact sequence

$$F(J) \overset{\varphi}{\to} F(I) \to C/\mathfrak{m}C \to 0.$$

Note that φ must be an embedding as $F(J)$ is a polynomial ring of dimension 2 and $F(I)$ is finite (integral) over it of the same dimension. Since the rank of $F(I)$ over $F(J)$ is $e_0 = 1$, $C/\mathfrak{m}C$ must be a module of rank 0 over $F(J)$, that is the Krull dimension of $C/\mathfrak{m}C$ is less than 2.

Suppose that $\dim C/\mathfrak{m}C < 2$, which means that there is an ideal $L \subset R[JT]$ such that $L \not\subset \mathfrak{m}R[JT]$ with $L \cdot C \subset \mathfrak{m}C$. Localizing at $\mathfrak{m}R[JT]$ and using Nakayama lemma, we get that there exists $h \notin \mathfrak{m}R[JT]$ such that $hC = 0$. This contradicts the assertion above that $\mathfrak{m}R[JT]$ was the only associated prime of C.

Finally, with $c(f) = I = J = (a, b)$, we appeal to Proposition 2.3 to complete the proof. ∎

Putting Theorems 3.1 and 4.2 together, we have:

THEOREM 4.4. *If R is a Noetherian normal domain then Conjecture* 1.1 *holds*.

Remark 4.5. If R is not integrally closed one may still say something about the content of a Gaussian polynomial $f(t)$, after noting that $f(t)$ is still Gaussian as a polynomial over the integral closure S of R. If S is Noetherian, one can easily see that $e_0 = 0$ (the "old" and "new" e_0's coincide). If S is not Noetherian, S is still a Krull domain and its prime spectrum is Noetherian [5]. These conditions may be sufficient to allow for modifications in the proof that lead to $e_0 = 0$.

REFERENCES

1. D. D. Anderson, Some problems in commutative ring theory, *in* ''Zero-Dimensional Commutative Rings,'' M. Dekker Lecture Notes in Pure & Applied Math., Vol. 171, pp. 363–372. Dekker, New York, 1995.
2. D. D. Anderson and B. G. Kang, Content formulas for polynomials and power series and complete integral closure, preprint.
3. W. Bruns and J. Herzog, ''Cohen-Macaulay Rings,'' Cambridge Univ. Press, Cambridge, 1993.
4. R. Gilmer, Some applications of the Hilfssatz von Dedekind-Mertens, *Math. Scand.* **20** (1967), 240–244.
5. W. Heinzer, Minimal primes of ideals and integral ring extensions, *Proc. Amer. Math. Soc.* **40** (1973), 370–372.
6. C. Huneke, The theory of *d*-sequences and powers of ideals, *Adv. Math.* **46** (1982), 249–279.
7. D. G. Northcott, A generalization of a theorem on the contents of polynomials, *Proc. Cambridge Phil. Soc.* **55** (1959), 282–288.
8. D. G. Northcott and D. Rees, Reductions of ideals in local rings, *Proc. Camb. Phil. Soc.* **50** (1954), 145–158.
9. H. T. Tsang, ''Gauss' Lemma,'' Ph.D. thesis, University of Chicago, 1965.
10. H. T. Tsang, Gauss' lemma, *Proc. Amer. Math. Soc.* **35** (1972), 372–376.
11. W. V. Vasconcelos, Hilbert functions, analytic spread and Koszul homology, *Contemp. Math.* **159** (1994), 401–422.
12. W. V. Vasconcelos, ''Arithmetic of Blowup Algebras,'' London Math. Soc., Lecture Note Series 195, Cambridge Univ. Press, Cambridge, 1994.