MONIC POLYNOMIALS AND GENERATING IDEALS EFFICIENTLY

BUDH NASHIER

ABSTRACT. If $I$ is an ideal containing a monic polynomial in $R[T]$ where $R$ is a semilocal ring, then $I$ and $I/I^2$ require the same minimal number of generators. An ideal containing a monic polynomial in a polynomial ring need not possess any minimal set of generators having a monic as a part of it.

1. Introduction. We are concerned with rings which are commutative and Noetherian with identity. By the dimension of a ring we mean the Krull dimension and we shall have occasion only to deal with rings of finite dimension. Let $A$ be a ring and let $M$ be a finitely generated $A$-module. We define $\mu(M)$ to be the least number of elements in $M$ required to generate $M$ as an $A$-module. The conormal bundle of an ideal $I$ in a ring $A$ is the group $I/I^2$ viewed as an $A/I$-module. Many algebraic properties of this module are intertwined with those of the ideal $I$. For instance, the content of an easily verifiable result is that $\mu(I/I^2) \leq \mu(I) \leq \mu(I/I^2) + 1$. To see when the lower inequality becomes an equality has been the theme of many papers in the literature; and this equality depends heavily on how the ideal $I$ sits inside $A$. In this article we embark on the following problem: Let $A = R[T]$ be a polynomial ring. Let $I$ be an ideal in $A$ such that $I$ contains a monic polynomial. Is it true that $\mu(I) = \mu(I/I^2)$?

In a lovely paper [4] Satyagopal Mandal has shown that if $\mu(I/I^2) \geq \dim(A/I) + 2$ and $I$ contains a monic polynomial then indeed $\mu(I) = \mu(I/I^2)$. While it is not difficult to obtain a positive answer to the question above in the case when $R$ is semilocal, we suspect of no situation where the desired equality between $\mu(I)$ and $\mu(I/I^2)$ will fail. We cite examples of ideals without monic polynomials for which the equality does not hold. One may be curious to know whether a monic polynomial should appear as a part of some minimal set of generators for $I$ given that $I$ does contain monic polynomials. In general, the answer turns out to be in the negative.

2. Cases when equality holds. Let us begin with a simple but useful lemma.

**Lemma 2.1.** If an ideal $I$ in a ring $A$ is contained in all but finitely many maximal ideals of $A$, then $\mu(I) = \mu(I/I^2)$.

**Proof.** Let $\mu(I/I^2) = n$. Choose elements $a_1, \ldots, a_n$ in $I$ which generate $I$ mod $I^2$. If $I$ is contained in all the maximal ideals of $A$, then $(a_1, \ldots, a_n) = I$. Otherwise, let

Received by the editors December 17, 1984.
1980 Mathematics Subject Classification. Primary 13F20.

©1985 American Mathematical Society
0002-9939/85 $1.00 + .25 per page

338
Monic polynomials

Let $M_1, \ldots, M_r$ be all those maximal ideals of $A$ that do not contain $I$. We can rearrange these $M_i$’s to assume that $a_1$ is in $M_1, \ldots, M_i$ but not in $M_{i+1}, \ldots, M_r$. Then the ideal $J = I^2 \cap M_{i+1} \cap \cdots \cap M_r$ is not contained in $M_1 \cup M_2 \cup \cdots \cup M_r$. We can find an element $b$ in $J$ such that $b$ is outside $M_1 \cup M_2 \cup \cdots \cup M_r$. Replace $a_1$ by $a_1 + b = a$. Then $a, a_2, \ldots, a_n$ generate $I$ since they do so locally.

Corollary 2.2. Let $A$ be a semilocal ring. Then $\mu(I) = \mu(I/I^2)$ for any ideal $I$ in $A$.

As a consequence we obtain

Theorem 2.3. Let $A = R[X]$ where $R$ is a semilocal ring. Let $I$ be an ideal in $A$ such that $I$ contains a monic polynomial. Then $\mu(I) = \mu(I/I^2)$. Further, we can find a minimal set of generators for $I$ such that one (hence all) elements in this set are monic polynomials.

Proof. Let $\mu(I/I^2) = n$. Let $a$ be a part of a minimal set of generators for $I \mod I^2$. Let $f$ be a monic polynomial in $I$. Replace $a$ by $a + f^n$ for suitable $n$ to assume that $a$ is monic. Then $I_1 = I/(a)$ is an ideal in $A_1 = A/(a)$ and $\mu(I_1/I_1^2) = n - 1$. Now $A_1$ is semilocal as it is integral over $R$. By Corollary 2.2 $\mu(I_1) = n - 1$. Hence, $\mu(I) = n$. Further, since $a$ appears as a part of a minimal set of generators for $I$ we can add powers of $a$ to the other generators to obtain that each one of them is monic.

Corollary 2.4. If $R$ is a semilocal ring and if $I$ is an ideal containing a monic polynomial in $R[X]$ such that projective dimension of $I$ is finite and $I/I^2$ is a free $R[X]/I$-module, then $I$ is generated by a regular sequence.

Proof. By Ferrand [1] or Vasconcelos [5] the grade of $I$ equals $\text{rank}(I/I^2)$. By Theorem 2.3, $\mu(I) = \mu(I/I^2) = \text{grade of } I$, therefore $I$ is generated by a regular sequence [see 2, 11.11].

The following example shows that Theorem 2.3 does not extend to ideals that do not contain a monic polynomial.

Example 2.5. Let $R = k[[t^2, t^3]]$. Let $M$ be the ideal in $R[X]$ generated by $t^2 - t^3X$ and $1 - t^2X^2$. One easily verifies that $M$ is a maximal ideal of height 1 in $R[X]$. Since $M \cap R = (0)$, $\mu(M/M^2) = 1$. But $M$ cannot be generated by a single element as can be seen without much ado.

The above example involves an element of Pic($R[X]$) which is not extended from $R$.

Example 2.6. Let $D = R[X, Y]/(X^2 + Y^2 - 1) = R[x, y]$. Then $D$ is a Dedekind domain. Consider the ideal $I$ generated by $(1 + y)T - x$ and $xT - 1 + y$ in $D[T]$. Then $I$ is in Pic($D[T]$) such that $\mu(I/I^2) = 1$ and $\mu(I) = 2$.

Proof. Let us first see that $I/I^2$ is a free $D[T]/I$-module of rank 1. For this, we observe that $(I, 1 + y) = D[T]$. Hence $1 + y$ becomes a unit in $D[T]/I$. Then it is easy to see that $I \mod I^2$ is generated by the image of $(1 + y)T - x$. Now $\mu(I/I^2) = 1$ implies that $I$ is a projective ideal of rank one and hence an element of
Pic\((D[T])\). Suppose that \(I\) is principal. Whence it follows that the constant terms of the elements of \(I\) generate a principal ideal. But the ideal generated by the constant terms of elements of \(I\) is the maximal ideal \((x, y - 1)\) which, being a real point on \(S^1\), requires two generators. Therefore, \(\mu(I) = 2\). Furthermore, \(I\) as an element of Pic\((D[T])\) is extended from \(R\) since \(D\) is normal.

The following remark shows that neither of the ideals in the examples above contains a monic polynomial.

**Remark 2.7.** Let \(A = R[T]\) be a polynomial ring. Let \(I\) be an ideal containing a monic polynomial in \(A\). If \(\mu(I/I^2) = 1\) then \(\mu(I) = 1\).

**Proof.** The given hypothesis implies that \(I\) is a projective ideal of rank 1. Since \(I\) contains a monic polynomial, by a theorem of Quillen and Suslin (see [3]), \(I\) must be principal.

While the presence of a monic polynomial in an ideal \(I\) plays such an important role in determining the cardinality of a minimal set of generators for \(I\), one may ask the following: Suppose that an ideal \(I\) in a polynomial ring \(R[T]\) contains a monic polynomial and \(\mu(I) = n\). Is it possible to find a set of \(n\) generators for \(I\) such that one of them is monic? Curiously enough, the following example illustrates that the answer is no.

**Example 2.8.** Take a Dedekind domain \(D\) whose class group has elements of infinite order. To wit, the coordinate ring of the smooth elliptic curve: \(Y^2 + Y = X^3 - X\). Choose a prime \(P\) in \(D\) of infinite order. Then \((P, T) = M\) is a maximal ideal in \(D[T]\) such that \(\mu(M) = 2\) [2, 16.1]. We claim that \(M\) cannot be generated by two polynomials such that one of them is monic. Suppose, if possible, that \(M\) is generated by \(f\) and \(g\) in \(D[T]\) and that \(f\) is monic.

It is a well-known fact that the ideal generated in \(D\) by the resultant of \(f\) and \(g\) is primary to \(P\). Hence \(P\) should have finite order-contradiction. It is a pleasure for me to thank Warren Nichols for steady and useful conversations.

**References**


**Department of Mathematics, Florida State University, Tallahassee, Florida 32306**