PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 100, Number 2, June 1987

ON CHOOSING GENERATING SETS FOR IDEALS

BUDH NASHIER

ABSTRACT. For an ideal I in a ring R the choice of a generating set with some interesting properties depends on how I sits inside R.

1. Preliminaries. Let R denote a commutative Noetherian ring with identity. For a finitely generated R-module M over R, let $\mu(M)$ denote the least number of elements in M required to generate M as an R-module. If I is an ideal in R then $\mu(I/I^2)$ and $\mu(I)$ are closely related. To be precise we have the following folklore result.

PROPOSITION. *Let I be an ideal in R. Then $\mu(I/I^2) \leqslant \mu(I) \leqslant \mu(I/I^2) + 1$.*

PROOF. The first inequality is trivial. For the second one, let $\mu(I/I^2) = n$. Choose elements $a_1, a_2, \dots, a_n$ in I such that $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n$ generate I/I^2. Let $J = (a_1, a_2, \dots, a_n)$. Then $I = J + I^2$. Let $S = 1 + I$. Then $S^{-1}I = S^{-1}J + (S^{-1}I)(S^{-1}I)$. Note that $S^{-1}I$ lies in the Jacobson radical of $S^{-1}R$. Hence $S^{-1}I = S^{-1}J$ by Nakayama's lemma. We can find a single element s in S such that $sI \subset J$. If $s = 1 + a$, $a \in I$, then $I = (J, a)$. Hence $\mu(I) \leqslant n + 1$.

Which one of the above inequalities becomes an equality is a question of interest. A lovely argument of Mohan Kumar [2] shows that if $\mu(I/I^2) > \dim(R)$ (Krull dimension of R), then $\mu(I) = \mu(I/I^2)$. From the equation $I = J + I^n$ it follows that an extra generator for I, if needed, can be chosen to lie in any power of I. Sometimes it is possible to select a set of generators with quite interesting properties. One such situation is offered by the following theorem.

THEOREM. *Let K be a field and let R be an affine K-domain of dimension d. Let M be a regular maximal ideal of R such that the residue field $L = R/M$ is a finite separable extension of K. Given an arbitrary nonzero element a in M^n, where n is an integer at least two, there exist elements $X_1, X_2, \dots, X_d$ in R with the following properties*:

(1) *$L = K[\overline{X}_1]$, where $\overline{X}_1$ denotes the residue class of X_1 modulo M.*

(2) *M is generated by $f(X_1)$, $X_2, \dots, X_d$ and a, where f denotes the minimal polynomial of $\overline{X}_1$ over K.*

(3) *The ring $A = R/(a)$ is integral over the polynomial ring $K[x_1, x_2, \dots, x_{d-1}]$, where x_i is the residue class of X_i modulo (a).*

Received by the editors April 14, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 13F20.

2. Proof of the Theorem. Since A is an affine K-algebra of dimension $d-1$, by Noether's Normalization Theorem [**1**, 14.g], there exist elements $y_1, y_2, \dots, y_{d-1}$ in A such that $B = K[y_1, y_2, \dots, y_{d-1}]$ is a polynomial ring and that A is an integral ring extension of B. Let $\mathfrak{m} = M/(a)$. Since $\mathfrak{m}$ is a maximal ideal in A, $\mathfrak{m} \cap B$ is maximal in B. By the height consideration it follows that $(\mathfrak{m} \cap B) \cap K[y_i] = \mathfrak{m} \cap K[y_i]$ is a nonzero prime ideal in $K[y_i]$ for $i = 1, 2, \dots, d-1$. If $\mathfrak{m} \cap K[y_i]$ is generated by the monic polynomial $g_i(y_i)$ for each $i = 1, 2, \dots, d-1$, then, replacing the y_i's by the g_i's, we assume that A is integral over $K[y_1, y_2, \dots, y_{d-1}]$ and that

$$\mathfrak{m} \cap K[y_1, y_2, \dots, y_{d-1}] = (y_1, y_2, \dots, y_{d-1}).$$

Since L is a finite separable extension of K, it is a simple extension. Let $L = R/M = K(\bar{\alpha})$, where $\alpha \in R$. Let f denote the minimal polynomial of $\bar{\alpha}$ over K. Since L is a separable extension of K, $f'(\alpha) \notin M$ (f' denotes the derivative of f). If $f(\alpha) \in M^2$, then $f(\alpha + t) \notin M^2$ for any $t \in M \setminus M^2$. Hence we may replace α by $\alpha + t$, if need be, and assume that $f(\alpha) \notin M^2$. Thus $f(\alpha)$ is part of a minimal basis for $M \pmod{M^2}$.

If z_1 denotes the residue class of α in A then $f(z_1) \in \mathfrak{m} \setminus \mathfrak{m}^2$, because $a \in M^2$. Hence $f(z_1)$ is part of a minimal basis for $m \pmod{\mathfrak{m}^2}$. Set $x_1 = z_1 + y_1^{t_1}$ where t_1 is an integer at least 2. As $z_1 = x_1 - y_1^{t_1}$ is integral over $K[y_1, y_2, \dots, y_{d-1}]$, by taking a sufficiently large value for t_1, it is easily checked that y_1 is integral over $K[x_1, y_2, \dots, y_{d-1}]$. Hence A is integral over $K[x_1, y_2, \dots, y_{d-1}]$ and $f(x_1)$ is a part of a minimal basis for $\mathfrak{m} \pmod{\mathfrak{m}^2}$.

Now we choose $z_2 \in A$ such that $f(x_1)$ and z_2 are part of a minimal basis for $\mathfrak{m}$ $\pmod{\mathfrak{m}^2}$. Set $x_2 = z_2 + y_2^{t_2}$ where t_2 is an integer at least 2. Then by taking a large value of t_2, as done above, we conclude that A is integral over $K[x_1, x_2, y_3, \dots, y_{d-1}]$ and $f(x_1)$, x_2 are part of a minimal basis for $\mathfrak{m} \pmod{\mathfrak{m}^2}$. We continue replacing the y_i's by x_i's and eventually obtain elements $x_1, x_2, \dots, x_{d-1}$ in A such that A is integral over $K[x_1, x_2, \dots, x_{d-1}]$ and that $f(x_1), x_2, \dots, x_{d-1}$ are part of a minimal basis for $\mathfrak{m} \pmod{\mathfrak{m}^2}$.

Note that $\mu(\mathfrak{m}/\mathfrak{m}^2) = \mu(M/M^2)$ as $a \in M^2$. Since M is a regular maximal ideal of R, we have $\mu(M/M^2)$ $(= \mu(MR_M)) = \dim(R_M) = \dim(R) = d$. Let I be the ideal in A generated by $f(x_1), x_2, \dots, x_{d-1}$. Let $C = A/I$ and $\mathfrak{n} = \mathfrak{m}/I$. Then C is a zero-dimensional ring (being integral over a field isomorphic to L). Note that $\mu(\mathfrak{n}/\mathfrak{n}^2) = \mu(\mathfrak{m}/\mathfrak{m}^2) - (d-1) = 1$. Hence $\mu(\mathfrak{n}) = 1$. We choose x_d in A such that $\mathfrak{m} = (I, x_d)$. If $X_1, X_2, \dots, X_d$ are lifts in R of the elements $x_1, x_2, \dots, x_d$ respectively, then the properties (1), (2), and (3) are satisfied. Thus the proof is complete.

Examples of rings as in the above theorem are readily available in algebraic geometry. The coordinate ring of a smooth irreducible algebraic variety over a perfect field enjoys this property.

References

1. H. Matsumura, *Commutative algebra* (2nd ed.), Benjamin, New York, 1980.
2. N. Mohan Kumar, *On two conjectures about polynomial rings*, Invent. Math. **46** (1978), 225–236.

Department of Mathematics, Florida State University, Tallahassee, Florida 32306 - 3027