JOURNAL OF ALGEBRA 27, 278–305 (1973)

Generating Modules Efficiently: Theorems from Algebraic K-Theory

DAVID EISENBUD AND E. GRAHAM EVANS, JR.*

Department of Mathematics, Brandeis University, Waltham, Massachusetts 02154
Department of Mathematics, University of Illinois, Urbana, Illinois 61801

Communicated by D. Buchsbaum

Received December 15, 1971

1. INTRODUCTION

Several of the fundamental theorems about algebraic K_0 and K_1 are concerned with finding unimodular elements, that is, elements of a projective module which generate a free summand. In this paper we use the notion of a basic element (in the terminology of Swan [22]) to extend these theorems to the context of finitely generated modules. Our techniques allow a simplification and strengthening of existing results even in the projective case.

Our main theorem, Theorem A, is an extension to the nonprojective case of a strong version of Serre's famous theorem on free summands of projective modules. It has as its immediate consequences (in the projective case) Bass's theorems about cancellation of modules and stable range of rings [1, Theorems 9.3 and 11.1] and the theorem of Forster and Swan on "the number of generators of a module." In the non-projective case it implies a mild strengthening of Kronecker's well-known result that every radical ideal in an n-dimensional noetherian ring is the radical of $n + 1$ elements. (If the ring is a polynomial ring, then n elements suffice [7]; this can be proved by methods similar to those of Theorem A.) Theorem A also contains the essential point of Bourbaki's theorem [4, Theorem 4.6] that any torsion-free module over an integrally closed ring is an extension of an ideal by a free module.

We also prove a theorem which gives an improvement of the Forster-Swan theorem already mentioned. The Forster-Swan theorem gives a bound (in terms of some local information) on the number of elements required to generate certain modules over a nice ring A. Our Theorem B says that, if g is the number of generators for a module M which the Forster-Swan theorem

* Both authors were partially supported by the N.S.F. during the preparation of this paper.

predicts, then a set of g generators for M can be obtained from any set of generators for M by suitable elementary transformations. Bass's stable range theorem is nothing but the special case of this in which $M = A$.

There are three techniques which we use throughout this paper, and which are perhaps worthy of note:

The first has already been mentioned—it is the systematic use of basic elements in place of unimodular elements. The definition is this: If R is a commutative ring, A an R-algebra finitely generated as an R module, and M a finitely generated A-module, then we will say that an element $m \in M$ is basic if for all primes p of R the image of m in M_p is part of a minimal system of generators of M_p over A_p. The element $m \in M$ is said to be j-basic if the above condition is satisfied just for maximal ideals p (see Section 2 for more precise definitions).

The use of basic (rather than unimodular) elements is necessary to produce a good result in the non-projective case. But in the projective case the two notions almost coincide. Unimodular elements of a projective module are obviously basic, and any basic element of a projective module generates a direct summand. If the projective is free (or in case $A = R$) the direct summand will be free. See Lemma 1 for the details.

The second technique on which our theorems rest is the use of j-prime ideals, which were also introduced by Swan in [22]. A j-prime ideal of a commutative ring is by definition a prime ideal which is an intersection of maximal ideals. The use of j-prime ideals avoids the clumsiness of working with closed sets in the maximal spectrum, and is helpful in the formulation of the proofs of our non-projective extensions.

The last technical point we will mention is an extremely simple, but effective, version of the Chinese remainder theorem that works for any finite set of prime ideals, even with containment relations. Its use goes back at least to Forster's paper [11, Hilfssatz *l*]. We use it constantly, but it is perhaps most clearly visible in the proof of Lemma 2.

The plan of this paper is as follows:

Section 2 is concerned with the fundamental definitions we will use.

Theorem A is stated in Section 3. Before proving it, we spell out its applications to the results mentioned in the second paragraph of this introduction. We have included full proofs of these results so that our paper could be read as an introduction to this part of K-theory and module theory.

The proof of Theorem A, modulo 3 lemmas, is given in Section 4. The lemmas themselves are proved in Sections 5–6. (The rather technical result on semisimple artinian rings, which is proved in Section 6, is required only for the non-commutative case of the theorems.)

Section 7 is devoted to Theorem B, our strengthening of the Forster-Swan theorem.

In Section 8 we have collected some of the open problems in this area that seem to us most interesting. We have also included an example which has obstructed our attempts to improve Bass's cancellation theorem.

We are very grateful to M. Artin, who suffered with us through early versions of this material. In particular, he pushed us toward Theorem A by showing us an unpublished manuscript in which he proved the commutative case of the first statement of Theorem A (this was a conjecture of D. Rees). We are also grateful to Artin for his patience in trying to explain to us that we were merely "trying to put a general position argument in general position."

We are pleased to express our debt to H. Bass and I. Kaplansky. Bass showed us a technical trick which rescued the non-commutative case of Theorem B, while the original impetus for Theorem B (indeed, for undertaking the work that led to this paper) came from Kaplansky's elegant exposition of the proof of the Stable Range Theorem given in [9, Theorem 2.3].

2. Hypotheses and Definitions

In this section we establish the basic hypotheses, definitions, and symbols that will be used throughout the paper.

R will always denote a commutative j-noetherian ring (see definition below). A will be an R algebra which is finitely generated as an R module, and M will be a finitely generated A module.

A reader who is not completely at home in this field may find it helpful, for a first reading, to assume that R is noetherian and that $A = R$. A further simplification in language can be achieved without too much loss by dropping all the "j" prefixes.

Definition. A *j-ideal* of a commutative ring is an ideal which is an intersection of maximal ideals. A commutative ring is j-noetherian if it satisfies the ascending chain condition on j-ideals.

The name j-ideal is suggested by the fact that R has zero Jacobson radical modulo a j-ideal. The notions connected with j-ideals were used by Swan in [22] in order to avoid some of the complications of working with the maximal spectrum, which has no generic points.

In [1], the hypothesis for Serre's theorem and related results was that the ring R has noetherian maximal spectrum, that is, that the closed subsets of the maximal spectrum of R satisfy the descending chain condition. Since these closed sets correspond to j-ideals of R, we see that R has a noetherian maximal spectrum if and only if R is j-noetherian. We will adhere to the ideal theoretic language throughout the paper. We record some details:

A prime j-ideal of R will be called a *j-prime* of R. The *j-dimension of* R is the length of a maximal chain of j-primes of R. The *j-height* of a j-prime p is the maximal length of a chain of j-primes contained in p. We note that the j-dimension of R coincides with the dimension of the maximal spectrum of R.

We also require some ideas connected with the number of generators of a module. If A is a ring and M a finitely generated A module we will write $\mu(A, M)$ for the minimal number of generators of M as an A-module.

The following definition is central to this paper:

DEFINITION. If A is an R algebra, p a prime ideal of R, M a finitely generated A-module, and M' an A-submodule of M, we will say that *M' is basic in M at p* if $\mu(A_p, (M/M')_p) < \mu(A_p, M_p)$ and *M' is t-fold basic in M at p* if $\mu(A_p, (M/M')_p) \leqslant \mu(A_p, M_p) - t$.

If $m_1, \ldots, m_t \in M$, then we will say that $m_1, \ldots, m_t$ are u-fold basic in M at p if the submodule $\sum_{i=1}^{t} Am_i$, is u-fold basic in M at p.

An element $m \in M$ is *j-basic* if it is basic at all the j-primes of R. We remark that m is j-basic if m is basic at every maximal ideal of R.

In expositions of Serre's theorem, there is usually a lemma which says that the set of primes at which a given element is unimodular is open. This becomes false if we replace unimodular by basic.

However, the set of primes where M requires at least $k + 1$ generators does play an important role. To preserve the ideal-theoretic language we imitate Kaplansky's unpublished treatment of Swan's theorem on the number of generators of a module and make the following definition:

DEFINITION. Let A be an R-algebra and M an A-module. For the purpose of this definition, we let $\mathscr{N}_t$ be the set of all A submodules $M' \subset M$ which can be generated by t elements. We define $I_t(A, M) = \sum_{M' \in \mathscr{N}_t} \operatorname{ann}_R(M/M')$ where ann_R denotes the annihilator in R. We note that $I_t(A, M)$ is an ideal of R. It follows readily from the definition that, for any prime ideal p of R, $p \supset I_t(A, M)$ if and only if $\mu(A_p, M_p) > t$. We remark that, if $\mu(A, M) = t$, then $I_u(A, M) = R$ for all $u \geqslant t$. Thus there are only finitely many distinct ideals $I_t(A, M)$. Since R is j-noetherian, the collection of j-primes, each of which is minimal over some $I_t(A, M)$, is finite. The finiteness of this set of primes is the elementary but crucial fact needed in the proofs of our theorems.

3. The Extension of Serre's Theorem and Its Consequences

In this section we state our extension of Serre's theorem. We also record a number of results, some already well known, which easily follow from it.

Theorem A. *Let R be a commutative J-noetherian ring with j-* dim $R = d < \infty$, *A an R-algebra which is a finitely generated R module, and M a finitely generated A-module.* Then:

(i) If, for every minimal j-prime p of R, $\mu(A_p, M_p) > d$, then M contains a j-basic element.

(ii)(a) More generally, let $M' \subseteq M$ be an A-submodule. If, for every j-prime p of R, M' is (j- dim(p) + 1)-fold basic in M at p, then M' contains a basic element of M.

(b) If, furthermore, $m_1, ..., m_u \in M'$ generate M' and if $a \in A$ is given such that $(a, m_1) \in A \oplus M$ is j-basic, then there is a j-basic element of M of the form $m_1 + am'$, where $m' \in \sum_{i=2}^{u} Am_i$.

(iii) If R has a noetherian spectrum, then the statements (i) and (ii) remain true when one deletes all occurrences of "j."

Remark. Let $\mathscr{P}_t$ denote the set of j-primes of R of j-height $\leqslant t$; and, if $p \in \mathscr{P}_t$, write $\dim_t(p)$ for the length of a maximal chain of primes containing p and belonging to $\mathscr{P}_t$. By restricting one's attention to primes belonging to $\mathscr{P}_t$, and using $\dim_t$ in place of j-dim throughout the proof of Theorem A, one can obtain a theorem without hypotheses on the j-dimension of R. For example, in (ii) above, if one weakens the hypothesis, and supposes only that M is ($\dim_t(p)$ + 1)-fold basic in M for all $p \in \mathscr{P}_t$, then the element M obtained in Theorem A will be basic at all primes of $\mathscr{P}_t$. We have exploited this stronger version of Theorem A in Corollaries 2 and 3 in Section 6.

We will now record some results, several of them already well known, which follow easily from Theorem A. We will assume, as always, that R is a commutative j-noetherian ring, A is an R algebra which is a finitely generated R-module, and M is a finitely generated A-module.

Corollary 1. (a) Serre's theorem ([20, Theorem 1] and [1, Theorem 8.2]): *Let j*-dim *$R = d$. If P is a finitely generative projective A-module whose rank at each localization is at least $d + 1$, then P has a free direct summand.*

(b) *If R and P are as above, and if P is generated by elements $m_1, ..., m_u$, then the generator of the free direct summand may be chosen to be of the form $m = m_1 + a_2m_2 + \cdots + a_um_u$ with $a_i \in A$.*

Remark. What Serre actually proved was part (a) with $A = R$. Bass proved the non-commutative case of (a) in [1, Theorem 8.2] Part (b) was observed and used by Murthy in [18] for the case $d = 1$, $A = R$.

Proof. It obviously suffices to prove (b). We choose a finitely generated projective A module Q such that $P \oplus Q$ is free. Since P has rank at least $d + 1$ at each localization, we see that P is $(d + 1)$-fold basic in $P \oplus Q$ at each j-prime p of R. Theorem (Aii) with $t = 1$, $a = 1$ gives us the existence of an element $m \in P$ of the required form which is j-basic in $P \oplus Q$. The following lemma finishes the proof:

LEMMA 1. *Let F be a finitely generated free A module, $m \in F$ a j-basic element. Then m generates a free direct summand of F.*

Remark. If $A = R$, the above is true if F is only assumed to be finitely generated and projective.

Proof. Suppose $F \cong A^u$. Multiplication by m induces an epimorphism $A \rightarrow^{\alpha} Am$. We will show that α is an isomorphism and that F/Am is projective. Together, these statements imply that Am is a free direct summand of F. Since F/Am is finitely presented, it suffices to prove these statements locally; thus, we will assume that R is a local ring. Since $m \in F$ is basic, it now follows that F/Am may be generated by $u - 1$ elements, so that there exists an epimorphism $\gamma: A^{u-1} \rightarrow F/Am$. Putting this together with α we obtain the following commutative diagram with exact rows:

(*)
$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"'] & A^u \arrow[r] \arrow[d, "\beta"] & A^{u-1} \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & Am \arrow[r] & F \arrow[r] & F/Am \arrow[r] & 0,
\end{tikzcd}$$

where β is obtained from α and some lifting of γ to a map $A^{u-1} \rightarrow F$. It follows from the diagram that β is an epimorphism. Since A is a finitely generated module over the commutative ring R and $F \cong A^u$, this implies that β is an isomorphism since by a theorem of [25], or [19], epimorphic endomorphisms of finitely generated modules over commutative rings are isomorphisms.

(Since F is free over A, β is split so we can prove that β is an isomorphism more simply. If we put $K = \ker \beta$, we have $F \cong F \oplus K$. Thus, for the maximal ideal p of R, we have

$$(F/pF) \oplus (K/pK) \cong F/pF.$$

Since the summands are finite dimensional vector spaces over R/p, we see that $K/pK = 0$. By Nakayama's lemma, this implies $K = 0$, so β is an isomorphism as claimed.)

Since β is an isomorphism, α is an isomorphism, and F/Am is projective as claimed. ▌

By using the remark following Theorem A, it is possible to prove a somewhat more general result, which we now state. Note that we make no hypothesis on j-dim R. For simplicity, we formulate the statement only in the case $A = R$.

COROLLARY 2. *Suppose that P is a finitely generated projective R module and suppose that at each j-prime p of $\mathscr{P}_t$, P_p has rank at least $t + 1$. Then there is an element $m \in P$ such that the ideal $P^*(m) = \{\alpha(m) \mid \alpha \in \mathrm{Hom}_R(P, R)\}$ of R has j-height at least $t + 1$.*

Proof. It is clear that $P^*(m) = R$ if and only if Rm is a free summand of P or, equivalently, if and only if m is j-basic in P. As in the proof of Corollary 1, we may consider P as a direct summand of a finitely generated free module F. Then P is $(t + 1)$-fold basic in F at each j-prime of R. Thus by Theorem A(ii), with $a = 1$, there is an element $m \in P$ which is basic at every $p \in \mathscr{P}_t$. Thus $(P_p)^*(m) = R_p$ for each such p. But $P_p{}^*(m) = (P^*(m))_p$ since $\mathrm{Hom}_{R_p}(P_p, R_p) = (\mathrm{Hom}_R(P, R))_p$. Thus j-height $(P^*(m)) \geqslant t + 1$ as claimed. ▌

COROLLARY 3 (Bourbaki's theorem [4, Theorem 4.6]). *Let R be an integrally closed noetherian domain and let M be a finitely generated torsion-free R-module. Then there exists a free submodule $F \subseteq M$ such that M/F is isomorphic to an ideal of R.*

Proof. We proceed by induction on $s = \mu(R_{(0)}, M_{(0)})$. If $s = 1$, then M is isomorphic to an ideal of R. Thus it suffices to prove that, if $s \geqslant 2$, there exists an element $m \in M$ such that M/Rm is torsion-free.

We now suppose $s \geqslant 2$. Then for every prime ideal p of R we have $\mu(R_p, M_p) \geqslant 2$. By the remark following Theorem A applied with $t = 1$, there is an element $m \in M$ which is basic at every prime ideal p of R with $ht(p) \leqslant 1$. We will prove M/Rm is torsion-free by showing that it is torsion-free when localized at any prime ideal of R.

Recall that, if N is a module over a local ring R with maximal ideal p, then the depth of N is the smallest integer k such that

$$\mathrm{Ext}^k(R/p, N) \neq 0.$$

See [13, Theorems 217 and 218] or [16, Theorem 26] for details. Furthermore, if R is a noetherian domain, then R is integrally closed if and only if for every prime ideal p of R:

(*)
(1) If $ht(p) = 1$, then R_p is a discrete valuation ring, and
(2) if $ht(p) > 1$, then depth $_{R_p}(R_p) > 1$.

See [15] or [16, Theorem 39] for details.

Now we return to the proof. If $p \subset R$ is a prime ideal of height 1, then, by (*), R_p is a discrete valuation ring, so M_p is free. But m is basic in M at p. Thus, by Lemma 1, $(Rm)_p$ is a direct summand of M_p so $(M/Rm)_p$ is torsion-free.

Next we assume that M/Rm is not torsion-free and let $p \neq 0$ be a prime ideal which is associated to M/Rm. Since $(M/Rm)_p$ is torsion over R_p, we see from the previous paragraph that $ht(p) > 1$. But $\text{depth}_{R_p}(M_p) \geqslant 1$ since M_p is torsion-free, and $\text{depth}_{R_p}(M/Rm)_p = 0$ since p_p is associated to $(M/Rm)_p$. The long exact sequence in $\text{Ext}_{R_p}(R_p/p_p, ——)$ now yields $\text{depth}_{R_p}(R_p) \leqslant 1$, which contradicts (*). Thus M/Rm is torsion-free as desired. ▮

COROLLARY 4 (Bass's cancellation theorem [1, Theorem 9.1]). *Let j-dim $R = d < \infty$, and let P be a finitely generated projective A-module whose rank at each localization is at least $d + 1$. Let Q be any finitely generated projective A-module, and let M be any A-module. If $Q \oplus P \simeq Q \oplus M$, then $P \simeq M$.*

Proof. Let Q' be a projective A module such that $Q \oplus Q'$ is finitely generated and free, say $Q' \oplus Q \simeq A^t$. It follows that $A^t \oplus P \simeq A^t \oplus M$, so it suffices to be able to cancel copies of A. Thus we may assume that $Q = A$. Let $\alpha: A \oplus M \to A \oplus P$ be the given isomorphism, and suppose $\alpha(1, 0) = (a, p_1)$. Then $(a, p_1) \in A \oplus P$ is basic. Let $p_2, \ldots, p_u \subset P$ be such that $p_1, \ldots, p_u$ generate P. Since P has rank at least $d + 1$ at each localization, we may regard P as a $(d + 1)$-fold basic direct summand of a finitely generated free module F, as in the proof of Corollaries 1 and 2. By Theorem A(ii), there is an element of P of the form $p = p_1 + a(\sum_{i=2}^{u} a_i p_i)$ which is basic in F. By Lemma 1, Ap is a free direct summand of F, and therefore of P. Let $\beta: A \oplus P \to A \oplus P$ be given by the matrix

$$\beta = \begin{pmatrix} 1_A & 0 \\ f & 1_P \end{pmatrix},$$

where $f: A \to P$ by $f(1) = \sum_{i=2}^{u} a_i p_i$. The composition $\beta\alpha: A \oplus M \to A \oplus P$ sends $(1, 0)$ to (a, p). Since p generates a free summand of P, there is a map

$\varphi\colon P \to A$ sending p to $1 - a$. Let $\gamma\colon A \oplus P \to A \oplus P$ be the automorphism

$$\gamma = \begin{pmatrix} 1_A & \varphi \\ 0 & 1_P \end{pmatrix}.$$

The isomorphism $\gamma\beta\alpha\colon A \oplus M \to A \oplus P$ sends $(1, 0)$ to $(1, p)$. If we let η be the automorphism $A \oplus P \to A \oplus P$ defined by

$$\eta = \begin{pmatrix} 1_A & 0 \\ -\hat{p} & 1_P \end{pmatrix},$$

where $-\hat{p}$ is the map $A \to P$ sending 1 to $-p$, then the following commutative diagram with exact rows shows that $M \cong P$:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "1"] & A \oplus M \arrow[r] \arrow[d, "\eta\gamma\beta\alpha"] & M \arrow[r] & 0 \\
0 \arrow[r] & A \arrow[r] & A \oplus P \arrow[r] & P \arrow[r] & 0.
\end{tikzcd}$$

∎

The next corollary is the well-known Forster-Swan theorem on the number of generators of a module. In Section 7, we will prove a stronger theorem (Theorem B) on generating a module.

COROLLARY 5 (Forster and Swan [11 and 22]). *Let N be a finitely generated A-module and suppose that*

$$t = \max_{\mathfrak{p}\in\mathscr{P}}((j\text{-dim}\, p) + \mu(A_\mathfrak{p}, N_\mathfrak{p})),$$

where $\mathscr{P}$ is the set of j-primes p of R such that $N_\mathfrak{p} \neq 0$. Then N can be generated by t elements.

Proof. By passing to $A/(\operatorname{ann}(N))$, we may assume that N is faithful, so that $\mathscr{P}$ is the set of all j-primes of R. Suppose that $\mu(A, N) = u > t$. Then there exists an exact sequence

$$0 \to M' \to M \to N \to 0$$

where M is a free A-module on u generators. For each prime p of R, M' is $[u - \mu(A_\mathfrak{p}, N_\mathfrak{p})]$-fold basic in M at p. Since $u > t \geqslant (\mu(A_\mathfrak{p}, N_\mathfrak{p}) + j\text{-dim}(p))$, we have $u - \mu(A_\mathfrak{p}, N_\mathfrak{p}) > j\text{-dim}(p)$ so that, for each $p \in \mathscr{P}$, M' is $(j\text{-dim}(p) + 1)$-fold basic in M at p. By Theorem (Aii), there exists an element $m \in M'$ which is basic in M. By Lemma 1, Am is a free summand of M so $M \cong Am \oplus P$ for some finitely generated projective A-module P. Since $\operatorname{rank}(M) = u > (j\text{-dim}\, R) + 1$, Corollary 4 implies that P is free of rank $u - 1$. But P maps onto N, so N can be generated by $u - 1$ elements. This contradicts the assumption that $\mu(A, N) = u$. ∎

The proof of the Forster-Swan theorem just given mimics a proof of a weaker "number of generators" result found in Bass [2, Corollary 3.8]. We are able to get the full result because of the strength of our version of Serre's theorem.

Theorem B may also be considered a generalization of the following corollary.

COROLLARY 6 (Bass's stable range theorem [1, Theorem 11.1]). *Let $b_1, ..., b_t \in A$ such that $\sum_{i=1}^{t} b_i A = A$ where $t > (j\text{-dim } R) + 1$. Then there exist $a_2, ..., a_t \in A$ such that $\sum_{i=2}^{t} (b_i + b_1 a_i) A = A$.*

Proof. We remark that a list $(b_1, ..., b_t)$ of elements of A may be regarded as an element of the free left A-module A^t. By Lemma 6, the element is j-basic if and only if it generates a free direct summand, that is, if there exists a map of left modules $A^t \to A$ sending $(b_1, ..., b_t)$ to 1. If such a map exists, it is given by a list of maps $\hat{c}_1, ..., \hat{c}_t$, where the map $\hat{c}_i : A \to A$ is right multiplication by c_i. Thus $\sum b_i c_i = 1$. Consequently $(b_1, ..., b_t) \in A^t$ is j-basic if and only if $\sum b_i A = A$.

Now suppose that $\sum_{i=1}^{t} b_i A = A$. We apply Theorem A(ii) in the following setup: $M = A^{t-1}$ (left modules) with canonical basis $m_2, ..., m_t$;

$$m_1 = (b_2, ..., b_t) \in A^{t-1}; \qquad \text{and} \qquad a = b_1 \in A.$$

Since $\sum_{i=1}^{t} b_i A = A$, $(b_1, m_1) \in A \oplus M$ is j-basic. Thus, by the theorem, there exist $a_2, ..., a_t$ such that

$$m_1 + a\left(\sum_{i=2}^{t} a_i m_i\right) = (b_2 + b_1 a_2, ..., b_t + b_1 a_t) \in A^{t-1}$$

is j-basic. Hence $\sum_{i=2}^{t} (b_i + b_1 a_i) A = A$ as desired. ∎

The last corollary is a non-projective application of Theorem A. For convenience, we will work with the commutative case $A = R$, and we will give the version of the corollary without j, since that is closer to the classical result. The first statement of the corollary was stated by Kronecker [14] for the case $R = K[x_1 \cdots x_d]$ with K a field. It was given a much simpler proof, valid for all noetherian rings, by van der Waerden [24]. We have recently been able to improve the result in case R is a polynomial ring over some other ring (see [7]).

COROLLARY 7. *Let R be a commutative ring with noetherian spectrum of* *dimension d, and let $I \subseteq R$ be an ideal. Then there exist $d+1$ elements $x_1, ..., x_{d+1} \in I$ such that, for any prime p of R,*

(1) *$p \supseteq I$ if and only if $p \supseteq (x_1, ..., x_{d+1})$; that is, $\sqrt{I} = \sqrt{(x_1, ..., x_{d+1})}$, and*

(2) *If $p \supseteq I$ and $I_p \neq 0$, then $(x_1, ..., x_{d+1}) \not\subseteq pI$.*

Proof. Let $J \subseteq R$ be the annihilator of I, so that I is a faithful module over R/J. Let I^{d+1} be the direct sum of $d+1$ copies of I. Clearly, for any prime q of R/J, $\mu((R/J)_q, I_q^{d+1}) \geqslant d+1 > \dim R/J$. Thus by part i of Theorem A, I^{d+1} contains a basic element x with components $x_1, ..., x_{d+1}$. We claim that these x_i satisfy the conclusions of the corollary. For (1), note that, if p is a prime ideal of R and $p \supseteq I$, then surely $p \supseteq (x_1, ..., x_{d+1})$. On the other hand, if $p \not\supseteq I$, then, since $IJ = 0 \subseteq p$, we must have $p \supseteq J$. It follows that $I_p^{d+1} = (R/J)_p^{d+1}$. Since x is basic in $(R/J)_p^{d+1}$ we have $x \notin p(R/J)_p^{d+1}$. Thus, for some i, $x_i \notin p$ as required.

To prove (2), suppose $p \supseteq I$ and $I_p \neq 0$. Then $p \supseteq J$, so $x \in I^{d+1}$ is basic at p. In particular $x \notin p(I^{d+1})_p$, so $(x_1, ..., x_{d+1}) \not\subseteq pI$. ▌

4. Proof of Theorem A

In this section, we will prove Theorem A modulo 3 lemmas. The lemmas will be proved in Sections 5–6.

Proof of Theorem A(iii). This follows by deleting the occurrences of "j" from the proofs of (i) and (ii).

(ii) ⇒ (i). Since $\mu(A_p, M_p) > d$ for every minimal j-prime p of R, $\mu(A_q, M_q) > d$ for every j-prime q of R. Thus M is $(d+1)$-fold basic in M at every j-prime of R. Hence the hypothesis of (ii)(a) are satisfied if one takes $M' = M$. This reduces (i) to (ii).

(ii)(a). In order to reduce (ii)(a) to the special case of (ii)(b) in which $a = 1$, we must deal with the (non-noetherian) possibility that M' is not finitely generated. Lemma 2 does this. The result is interesting even in the noetherian case, since it gives a fixed bound on the number of elements needed to generate some submodule M'' of M satisfying the conditions on M' given in (ii)(a).

Lemma 2. *With R, A, M, M' and d as in Theorem* A(ii)(a), *there exists a submodule $M'' \subseteq M'$ such that M'' can be generated by $d+1$ elements, and, such that for every j-prime p of R, M'' is (j-$\dim(p)+1$)-fold basic in M at p.*

Using Lemma 2, and replacing M' by M'' if necessary, we see that (ii)(a) follows from (ii)(b).

(ii)(b). The idea of the proof is to replace the submodule $M' = \sum_{i+1}^{u} Am_i$ with submodules generated by successively fewer elements, the first of which always has the form $m_1 + am''$, and such that all the submodules are sufficiently basic. When we reach a point at which $m_1 + am''$ is the only generator required for such a submodule, the theorem will have been proved.

The next lemma tells us that this shrinking of the number of generators can be done if we are only interested in maintaining basicness at finitely many of the j-primes of R.

LEMMA 3. *Let R, A, M, and M' be as in Theorem* A. *Let $p_1, \ldots, p_v$ be j-primes, and let $w_1, \ldots, w_v$ be positive integers such that M' is w_i-fold basic in M at p_i. Let $m_1, \ldots, m_u \in M$ such that $M' = \sum_{i=1}^{u} Am_i$. If $a \in A$ is given such that $(a, m_1) \in A \oplus M$ is basic at $p_1, \ldots, p_v$, then there exist elements $a_i \in A$ such that $(a, m_1 + aa_1m_u) \in A \oplus M$ is basic at $p_1, \ldots, p_v$, and the submodule $A(m_1 + aa_1m_u) + \sum_{i=2}^{u-1} A(m_i + a_im_u)$ is* $[\min(u-1, w_i)]$*-fold basic in M at p_i for each i.*

The final lemma gives us finite sets of j-primes to use in applying Lemma 3. Lemma 4 will also be used in the proof of Lemma 2, given in the next section.

LEMMA 4. *Let R, A, M be as in Theorem* A, *and let $\mathscr{P} \subseteq j$*-spec *R be any set of primes. Let $M' \subseteq M$ be an A-submodule. Suppose that, for every j-prime p such that there exists a j-prime $q \in \mathscr{P}$ with $p \subsetneqq q$, M' is w-fold basic in M at p. Then M' is w-fold basic in M at all but finitely many of the primes in $\mathscr{P}$.*

We can now finish the proof of Theorem A(ii). We suppose that $M' = \sum_{i=1}^{u} Am_i$ and that (a, m_1) is j-basic in $A \oplus M$. We say that a set of elements $\{n_1, \ldots, n_x\}$ with $n_i \in M'$ is a *basic set* if the submodule $N = \sum_{i=1}^{x} An_i$ is $\{\min(x, j\text{-dim}(p) + 1)]$-fold basic in M at p for all j-primes p.

By hypothesis $\{m_1, \ldots, m_u\}$ is a basic set. On the other hand, if $\{m\}$ is a basic set, then m is j-basic in M.

We will show if $\{n_1, \ldots, n_x\}$ is a basic set with $x > 1$, then there exist elements $a_1, \ldots, a_{x-1} \in A$ such that $\{n_1 + aa_1n_x, n_2 + a_2n_x, \ldots, n_{x-1} + a_{x-1}n_x\}$ is a basic set. If we apply this fact $u - 1$ times starting with the basic set $\{m_1, \ldots, m_u\}$, we obtain a basic set with only one element m; this element will have the form required by Theorem A(ii)(b).

Suppose once again that $N = \sum_{i=1}^{x} An_i$ with $\{n_1, \ldots, n_x\}$ a basic set. We claim that there are only finitely many j-primes p such that N is not $(\min(x, j\text{-dim}(p) + 2))$-fold basic at p. Since j-dim R is finite, we need only show this for j-primes p with a fixed value of $s = j\text{-dim}(p)$. For all j-primes q with $j\text{-dim}(q) > s$, $\min(x, j\text{-dim}(q) + 1) \geqslant \min(x, s + 2)$. Thus Lemma 4 applies with $\mathscr{P} = \{p \text{ a } j\text{-prime of } R \mid j\text{-dim}\, p = s\}$ to show that N is

$[\min(x, j\text{-dim}(p) + 2)]$-fold basic at all but finitely many j-primes p with $j\text{-dim}(p) = s$, as claimed.

Let E be the finite set of j-primes p at which N is not $[\min(x, j\text{-dim}(p)+2)]$-fold basic. By Lemma 3, there exist $a_1, ..., a_{x-1} \in A$ such that

$$N' = A(n_1 + aa_1 n_x) + \sum_{i=2}^{x-1} A(n_i + a_i n_x)$$

is $\min[x - 1, j\text{-dim}(p) + 1]$-fold basic in M at the primes $p \in E$.

On the other hand, if $p \notin E$, then the submodule N' just defined is $\min(x - 1, j\text{-dim}(p) + 1)$-fold basic in M at p for any choice of the elements a_i.

Thus $\{n_1 + aa_1 n_x, n_2 + a_2 n_x, ..., n_{x-1} + a_{x-1} n_x\}$ is a basic set as required. The proof of Theorem A on the basis of Lemmas 2–4 is complete. ∎

5. The Proofs of Lemmas 2 and 4 and the Case $A = R$ of Lemma 3

In this section we complete the proof of Theorem A in the case $A = R$ by proving these lemmas. We will make use of the ideals $I_t(A, M)$ which were defined and discussed in Section 2.

Proof of Lemma 4. We suppose that $M' \subseteq M$ is w-fold basic at all j-primes p such that p is properly contained in some prime of $\mathscr{P}$, and we wish to show that M' is w-fold basic at all but finitely many j-primes in $\mathscr{P}$. We will show that M' is w-fold basic at all j-primes in $\mathscr{P}$ except possibly at those which are minimal over the ideal $I_u(A, M/M')$ for some u. Since there are only finitely many j-primes minimal over each $I_u(A, M/M')$, and only finitely many distinct ideals of the form $I_u(A, M/M')$, the result will be established.

Suppose that $p \in \mathscr{P}$ and that p is not minimal over any $I_u(M/M')$. Suppose that $\mu(A_p, (M/M')_p) = v + 1$. Then $p \supseteq I_v(A, (M/M'))$ but $p \not\supseteq I_x(A, (M/M'))$ for any $x > v$. Since p is not minimal over $I_v(A, (M/M'))$, there is a j-prime q such that $I_v(A, M/M) \subseteq q \not\subseteq p$. By hypothesis, M' is w-fold basic in M at q. Hence

$$\mu(A_p, (M/M')_p) = \mu(A_q, (M/M')_q) \leqslant \mu(A_q, M_q) - w.$$

Since $\mu(A_q, M_q) \leqslant \mu(A_p, M_p)$, we see that $\mu(A_p, (M/M')_p) \leqslant \mu(A_p, M_p) - w$. Thus M' is w-fold basic in M at p. ∎

The proof of Lemma 3 in the non-commutative case involves a technical result on semisimple artinian rings (Lemma 5) which extends the result

[22, Lemma 4]. However, if $A = R$, we require the result only in case the semisimple ring is a field, and for fields it is virtually obvious.

Proof of Lemma 3. For any choice of a_1, $(a, m_1 + aa_1m_u) \in A \oplus M$ is basic at $p_1, \ldots, p_v$. This follows from the fact that, if $\alpha\colon A \to M$ is the map defined by $\alpha(1) = a_1m_u$, then the elementary automorphism

$$\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} \colon A \oplus M \to A \oplus M$$

carries (a, m_1) to $(a, m_1 + aa_1m_u)$ which is basic at $p_1, \ldots, p_2$ by assumption. Thus it suffices to choose elements $a_j \in A$ to fulfill the second condition of the lemma. For those i with $w_i \geqslant u$, the condition is clearly satisfied for any choice of a_j. Therefore we may assume that $w_i < u$ for all i.

The proof is now an induction on the number v of primes involved. The case $v = 0$ is vacuous. Reordering the p_i, if necessary, we may assume that p_v is minimal among $p_1, \ldots, p_v$ and, hence, $p_v \not\supseteq \bigcap_{z=1}^{v-1} p_z$. Suppose that $a_1', \ldots, a_{u-1}' \in A$ have been chosen so that

$$m_1' = m_1 + aa_1m_u\,,\ m_u' = m_2 + a_2'm_u\,, \ldots,\ m_{u-1}' = m_{u-1} + a_{u-1}m_u$$

generate a submodule which is w_i-fold basic at p_i for $i < v$.

We will show that we can choose $a_1'', \ldots, a_{u-1}''$ so that:

$$(*) \qquad \begin{cases} \text{for any } r \in R - p_v \\ m_1'' = m_1' + aa_1''rm_u\,,\ m_2'' = m_2' + a_2''rm_u\,, \ldots,\ m_{u-1}'' = m_{u-1}' + a_{u-1}''rm_u \\ \text{are } w_v\text{-fold basic at } p_v\,. \end{cases}$$

If we choose $r \in \bigcap_{j<v} p_j$, but $r \notin p_v$, then the elements $m'', \ldots, m_{u-1}''$ will be w_i-fold basic at p_i for $i \leqslant v$. For $i < v$, this is true because it was true for the m_i', and $r \in p_i$, while, for $i = v$, it is guaranteed by $(*)$. This completes the induction.

It remains to show we can pick elements a_j'' to satisfy the conditions of $(*)$. We may begin by localizing at p_v. Let J denote the jacobson radical of A_p. Since questions of basicness over A_p are not affected by reducing modulo J, we may factor out J and assume that A is semisimple artinian. This puts us in the position of the following lemma, which will finish the proof of Lemma 3.

In Lemma 5, we will use the language appropriate to the above situation: If A is semisimple, M a finitely generated A module, and $m \in M$, then we will say m is basic in M if $\mu(A, M) > \mu(A, M/Am)$ and that a submodule $M' \subseteq M$ is w-fold basic if $\mu(A, M/M') \leqslant \mu(A, M) - w$.

Lemma 5. *Let A be a semisimple artinian ring, $a \in A$, and let M be a finitely generated A-module. If $m_1, \ldots, m_u \in M$ are such that $(a, m_1) \in A \oplus M$ is basic and $M' = \sum_{i=1}^{u} Am_i$ is w-fold basic in M with $w < u$, then there exist elements $a_1, \ldots, a_{u-1} \in A$ such that for all central units $r \in A$,*

$$A(m_1 + aa_1rm_u) + \sum_{i=2}^{u-1} A(m_i + a_irm_u)$$

is w-fold basic in M.

We have already remarked that for the case $A = R$ of Lemma 3 it is enough to prove Lemma 5 when A is a field. We do this now; we will postpone the proof of Lemma 5 in general to the next section.

Proof of Lemma 5 in Case A is a field. If $\sum_{i=1}^{u-1} Am_i$ is w-fold basic, choose $a_i = 0$ for all i. Otherwise let $x < u$ be the largest integer such that $m_x \in \sum_{i=1}^{x-1} Am_i$. Such an x must exist since $\sum_{i=1}^{u-1} Am_i$ is a vector space of dimension $\leqslant w - 1$ and there are $u - 1 > w - 1$ elements $m_1, \ldots, m_{u-1}$. Choose $a_i = 0$ for $i \neq x$ and $a_x = 1$. This clearly satisfies the lemma if $x \neq 1$. But, if $x = 1$, then, by the choice of x, we have $m_1 = 0$. Because (a, m_1) is basic in $A \oplus M$, we must have $a \neq 0$, and hence the choice is again, satisfactory. ▮

Proof of Lemma 2. We wish to find $d + 1$ elements of M' which generate a (j-dim(p) + 1)-fold basic submodule of M at every j-prime p.

To do this, we introduce some notation:

$\mathscr{P}_t = \{j\text{-primes } p \text{ of } j\text{-height} \leqslant t\}$.

$\dim_t(p)$ = the length of the longest chain of j-primes containing p in $\mathscr{P}_t$.

Since j-dim(R) $= d$, every j-prime belongs to $\mathscr{P}_d$, so j-$\dim_d(p) = j$-dim(p).

We will inductively choose $d + 1$ elements of M' so that, for each $t \leqslant d + 1$, the first $t + 1$ elements generate a [j-dim(p)) + 1]-fold basic submodule at each j-prime $\in \mathscr{P}_t$.

Suppose $m_1, \ldots, m_t$ have been found so that $N = \sum_{i=1}^{t} Am_i$ is ($\dim_{t-1}(p) + 1$)-fold basic at every $p \in \mathscr{P}_{t-1}$. Since $\dim_t(p) \leqslant \dim_{t-1}(p) + 1$, N will be ($\dim_t(p)$)-fold basic for all $p \in \mathscr{P}_{t-1}$.

Fix $s \leqslant t$, and let $\mathscr{P}_{t,s} = \{p \in \mathscr{P}_t \mid \dim_t(p) = s\}$. For any j-prime p' such that p' is properly contained in a prime of $\mathscr{P}_{t,s}$, we have $p' \in \mathscr{P}_{t-1}$, and $\dim_t(p') > s$. Thus N is $(s + 1)$-fold basic in M at p'.

Lemma 4, applied with $\mathscr{P} = \mathscr{P}_{t,s}$, now shows that N is $(s + 1)$-fold basic in M at all but finitely many of the primes in $\mathscr{P}_{t,s}$. Since $\bigcup_s \mathscr{P}_{t,s} = \mathscr{P}_t$, we see that N is ($\dim_t(p) + 1$)-fold basic in M at p for all but finitely many primes $p \in \mathscr{P}_t$. Let $q_1, \ldots, q_u \in \mathscr{P}_t$ be the finitely many exceptional primes.

We now consider M/N. Since N is *not* ($\dim_t(q) + 1$)-fold basic at any q_i, the hypothesis of the lemma shows that M'/N is basic in M/N at each of the primes $q_1, \ldots, q_u$. We will find an element $\bar{m}_{t+1}$ of M'/N which is basic in M/N at each prime $q_1, \ldots, q_u$. If m_{t+1} is any element of M' which reduces to $\bar{m}_{t+1}$ modulo N, it is clear that

$$M'' = \sum_{i=1}^{t+1} Am_i$$

satisfies the conditions of the lemma.

To show the existence of $\bar{m}_{t+1}$, we use induction on the number u. As in the proof of Lemma 3, we may rearrange the primes so that q_u is minimal among the q_i. Now suppose that $\bar{m}'_{t+1} \in M'/N$ has been chosen to be basic at each prime $q_1, \ldots, q_{u-1}$. If $\bar{m}'_{t+1}$ is basic at q_u, we are done. If not, pick $r \in R$ such that $r \in (\bigcap_{i<u} q_i)$ but $r \notin q_u$ and choose $\bar{m}''_{t+1} \in M'/N$ to be basic at q_u. Then $\bar{m}_{t+1} = \bar{m}'_{t+1} + r\bar{m}''_{t+1}$ is basic at each prime $q_1, \ldots, q_u$. ∎

We have now completed the proof of Theorem A in the case $A = R$. For the general case, all that remains is the proof of Lemma 5, which is contained in the next section.

6. A Lemma about Semisimple Artinian Rings

To simplify the proof of Lemma 5, it is useful to isolate a certain special case which occurs (essentially) in [22, Lemma 4]. For the reader's convenience we will reproduce Swan's proof.

Lemma 6. *Let A be a semisimple artinian ring, and let M be a cyclic A module. Suppose $m_1, m_2 \in M$ are such that*

$$M = Am_1 + Am_2.$$

Then there exists $a \in A$ such that for all central units $r \in R$,

$$M = A(m_1 + arm_2).$$

Proof. Since M is cyclic there is an epimorphism $A \to M$. Since A is semisimple, the map splits, and we have

$$A \cong M \oplus M'$$

for some A-module M'. Again, because A is semisimple, $Am_1 \cap Am_2$ is a direct summand of Am_2. Since the complement must be cyclic, it will have the form Abm_2 for some $b \in A$. Thus we have

$$M = Am_1 \oplus Abm_2.$$

Let K be the kernel of the epimorphism $\alpha\colon A \to Am_1$ which sends 1 to m_1. K is isomorphic to $Abm_2 \oplus M'$, so there is a short exact sequence

$$0 \longrightarrow Abm_2 \oplus M' \longrightarrow A \xrightarrow{\alpha} Am_1 \longrightarrow 0.$$

Let $\beta\colon A \to Abm_2 \oplus M'$ be a splitting, and let $\pi\colon Abm_2 \oplus M' \to Abm_2$ be the projection.

If $r \in A$ is a central unit, then multiplication by r induces an automorphism $\hat{r}\colon Abm_2 \to Abm_2$. Since

$$A \xrightarrow{(\alpha,\beta)} Am_1 \oplus (Abm_2 \oplus M')$$

is an isomorphism, the map

$$A \xrightarrow{(\alpha,\hat{r}\pi\beta)} Am_1 \oplus Abm_2 = M$$

is an epimorphism. It sends 1 to $m_1 + a'brm_2$ for some $a' \in A$, so $M = A(m_1 + a'brm_2)$ for all central units $r \in A$. The lemma is thus satisfied by the choice $a = a'b$. ▌

For the proof of Lemma 5, we will use one new piece of notation. If M is a finitely generated module over an artinian ring, we write $\lambda(M)$ for the length of a composition series for M. We remind the reader of the convention we established for Lemma 4: If A is semisimple we say that a submodule $M' \subseteq M$ is w-fold basic if

$$\mu(A, M/M') \leqslant \mu(A, M) - w.$$

Proof of Lemma 5. We may harmlessly assume that A is simple. Because of this assumption, we can replace considerations of basicness by considerations of length. For, setting $\lambda_0 = \lambda(A)$, we may write

$$\lambda(M) = x\lambda_0 + y \qquad \text{with} \qquad y < \lambda_0,$$

where x and y are positive integers. Then, if $N \subseteq M$, N is z-fold basic in M if and only if

$$\lambda(N) \geqslant (z-1)\,\lambda_0 + y.$$

If

$$\lambda\left(\sum_{t=1}^{u-1} Am_t\right) \geqslant (w-1)\lambda_0 + q,$$

we may take $a_i = 0$ for all i, and Lemma 4 will be satisfied. Otherwise, we may replace m_u with a multiple of m_u if necessary and assume that

$$\lambda(M') = (w-1)\,\lambda_0 + q,$$

where $M' = \sum_{t=1}^{u} Am_t$ and that

$$M' = \left(\sum_{t=1}^{u-1} Am_t\right) \oplus Am_u .$$

Furthermore, if $r \in A$ is a central unit, then multiplication by r induces an automorphism $\hat{r}\colon Am_u \to Am_u$, and thus $1 \oplus \hat{r}\colon M' \to M'$ is an automorphism. Consequently, it suffices to prove Lemma 5 under the hypothesis $r = 1$. We will prove:

(**) If $n_1 ,\ldots, n_u$ generate M', and if v is an integer, $1 \leqslant v < u$, such that

$$(1) \quad n_u \notin \sum_{t=1}^{v} An_t$$

and

$$(2) \quad \lambda\left(\sum_{t=1}^{v-1} An_t\right) \geqslant (v-2)\lambda_0 + q,$$

then there exists an $a_v \in A$ such that with

$$N = \begin{cases} \sum_{t=1}^{v-1} An_t + A(n_v + a_v n_u), & \text{if} \quad v > 1, \qquad \text{or} \\ A(n_1 + aa_1 n_u), & \text{if} \quad v = 1, \end{cases}$$

we have $N \supseteq \sum_{t=1}^{v} An_t$ and either (1′) $n_u \in N$, or (2′) $\lambda(N) \geqslant (v-1)\lambda_0 + q$.

We first apply (**) to the sequence of elements $n_1 = m_1 ,\ldots, n_u = m_u$, with $v = 1$, and obtain a sequence of elements

$$n_1' = m_1 + aa_1 m_u , \qquad n_2' = n_2 ,\ldots, n_u' = n_u .$$

If (1′) is satisfied by this choice of a_1, we will have

$$\sum_{t=1}^{u-1} An_t' = M',$$

so the choice of a_1, together with the choice

$$a_2 = a_3 = \cdots = a_{u-1} = 0,$$

satisfies Lemma 5.

If, on the other hand, (1′) is not satisfied but (2′) is, we may apply (**) to the sequence of elements

$$n_1' ,\ldots, n_u'$$

with $v = 2$, and obtain a sequence of elements

$$n_1^{(2)} = n_1', \qquad n_2^{(2)} = n_2' + a_2 n_u', \qquad n_3^{(2)} = n_3',\ldots, n_u^{(2)} = n_u'$$

such that $(**)$ is satisfied. We continue in this way until we reach a case in which (1′) is satisfied, or until we have applied $(**)$ with $v = u - 1$. We obtain a sequence of elements of M' of the form

$$m_1 + aa_1 m_u\,,\ m_2 + a_2 m_2\,,\ldots, m_{u-1} + a_{u-1} m_u\,,\ m_u\,,$$

such that, if we set

$$N = A(m_1 + aa_1 m_u) + \sum_{t=2}^{u-1} A(m_t + a_t m_u),$$

we will have

$$N \supseteq \sum_{t=1}^{u-1} Am_t$$

and either

$$n_u \in N$$

or

$$\lambda(N) \geqslant (u-2)\,\lambda_0 + q \geqslant (w-1)\,\lambda_0 + q = \lambda(M').$$

In either case, we see that $N = M'$, so that the above choice of the elements a_i satisfies Lemma 5.

It remains to prove $(**)$. We may assume, as above, that

$$M' = \left(\sum_{t=1}^{u-1} An_t\right) \oplus An_u\,.$$

Suppose $v > 1$. Set $M'' = (\sum_{1=t}^{v} An_t)/(\sum_{t=1}^{v-1} An_t)$, and let $\bar{n}_v$ be the image of n_v in M'', so that $M'' = A\bar{n}_v$. Choose $b, b' \in A$ so that $An_u = Abn_u \oplus Ab'n_u$ and such that

$$\lambda(Abn_u) = \min(\lambda(An_u), \lambda_0 - \lambda(M'')).$$

Because of this choice,

$$A\bar{n}_v \oplus Abn_u = M'' \oplus Abn_u$$

is cyclic, so, by Lemma 6, there exists an $a_v' \in A$ such that

$$A(\bar{n}_v + a_v' bn_u) = M'' \oplus Abn_u\,.$$

The choice $a_v = a_v'b$ satisfies $(**)$ because either $\lambda(An_u) \leqslant \lambda(M'')$, in which case $n_u \in Abn_u$, or $\lambda(M'' \oplus Abn_u) = \lambda_0$, so that

$$\begin{aligned}\lambda\left(\sum_{t=1}^{v-1} An_t + A(n_v + a_v n_u)\right) \\ &= \lambda\left(\sum_{t=1}^{v-1} An_t\right) + \lambda(A(m_v + a_v m_u)) \\ &\geqslant (v-2)\lambda_0 + q + \lambda_0 \geqslant (V-1)\lambda_0 + q,\end{aligned}$$

as required.

The case $v = 1$ remains; the only difference is that we must work with the element $a \in A$, so things become more complicated. In any case, if $\lambda(An_1) \geqslant q$, then the choice $a_1 = 0$ satisfies $(**)$, so we may assume $\lambda(An_1) < q$. We choose $b, b' \in A$ such that $An_u = Abn_u \oplus Ab'n_u$ and

$$\lambda(Abn_u) = \min(\lambda(An_u), q - \lambda(An_1)).$$

Let e be a idempotent of A which generates the right ideal aA so that $e = ac$, for some $c \in A$, and $ea = a$. The modules $A(a, m_1)$ and $A(e, n_1)$ are isomorphic by the map sending (a, n_1) to $(ac, n_1) = (e, n_1)$. Thus in particular $\lambda(A(a, n_1)) = \lambda(A(e, n_1))$.

Let α: $A(e, n_1) \to An_1$ be the projection onto the second factor. There is an exact sequence

$$0 \longrightarrow (\operatorname{ann} n_1)e \longrightarrow A(e, n_1) \xrightarrow{\alpha} An_1 \longrightarrow 0,$$

where $\operatorname{ann} n_1$ is the left annihilator of n_1, a left ideal. Let β: $Ae \to (\operatorname{ann} n_1)e$ be a splitting of the inclusion map, and let d be the idempotent of A that induces by right multiplication, the map $A \to (\operatorname{ann} n_1)e$ which is given by β on Ae and 0 on $A(1-e)$. Thus

$$Ad = (\operatorname{ann} n_1)e.$$

Since $(1-e)d = 0$, we have $ed = (e + (1-e))\,d = d$. The exact sequence above may now be written

$$0 \longrightarrow Ad \longrightarrow A(e, n_1) \xrightarrow{\alpha} An_1 \longrightarrow 0.$$

Because $\lambda(Ad) \geqslant \lambda(Abn_u)$, there is an epimorphism $Ad \to^{\epsilon} Abn_u$: say it sends d to $a'bn_u$. Since $ed = d$, $a'bn_u = ea'bn_u$. The composite map

$$A(e, n_1) \xrightarrow{(\alpha, \beta)} An_1 \oplus Ad \xrightarrow{(1, \epsilon)} An_1 \oplus Abn_u$$

is onto, and carries (e, n_1) to $n_1 + a'bn_u$, which therefore generates $An_1 \oplus Abn_u$. Since $a'bn_u = ea'bn_u = aca'bn_u$, we see that the choice $a_1 = ca'b$ satisfies Lemma 5, for either

$$\lambda(A(n_1 + aa_1n_u)) = \lambda(An_1) + \lambda(Abn_u) \geqslant q,$$

or $n_u \in Abn_u$, in which case

$$n_u \in A(n_1 + aa_1n_u). \quad \blacksquare$$

7. Generating Modules

In this section we simultaneously improve the Forster-Swan theorem on the number of generators of a module, and generalize Bass's stable range theorems (Corollaries 5 and 6 of Section 3). We show that, if M is an A-module for which the Forster-Swan theorem predicts s generators, then a set of s generators for M may be obtained by starting with any set of generators and applying certain "elementary transformations."

Theorem B. *Let R be a commutative j-noetherian ring, and let A be an R-algebra which is finitely generated as an R-module. Let M be an A module which is generated by finitely many elements $m_1, \ldots, m_t \in M$.*

Suppose that for every j-prime p of R with $m_t \notin pM_p$ we have:

$$t > j\text{-dim}(p) + \mu(A_p, M_p).$$

Then there exist elements $a_1, \ldots, a_{t-1} \in A$ such that

$$M = \sum_{i=1}^{t-1} A(m_i + a_im_t).$$

Proof of Theorem B. Let $\mathscr{P}$ be the set of j-primes p with $m_t \notin pM_p$. We will do an induction on the number

$$u = \max_{p \in \mathscr{P}}(j\text{-dim}(p) + \mu(A_p, M_p)).$$

If $u = 0$, then $m_t \in pM_p$ for *all* j-primes p, so we may take $a_i = 0$ for all i.

If $u > 0$, we will show that, under the hypothesis $t > u$ of the theorem, we can choose $b_2, \ldots, b_t \in A$ with the following property: If we set $m_1' = m_1 + \sum_{i=2}^t b_im_i$ and $N = M/Am_1'$, then we will have

$$(*) \qquad \begin{cases} \mu(A_p, N_p) < \mu(A_p) \\ \text{for all those } p \in P \text{ such that} \\ u = j\text{-dim}(p) + \mu(A_p, M_p). \end{cases}$$

Write $\bar{m}_i$ for the image of m_i in N and let $\mathscr{P}'$ be the set of j-primes p of R such that $\bar{m}_t \notin pN_p$. Note that $\mathscr{P}' \subseteq \mathscr{P}$.

For any prime p of R, we have $\mu(A_p, N_p) \leqslant \mu(A_p, M_p)$ so that, for a choice of $b_2, \ldots, b_t$ satisfying $(*)$ above,

$$u > v = \max(j\text{-}\dim p + \mu(A_p, N_p)).$$

Thus $t - 1 > v$. Since N is generated by the $t - 1$ elements $\bar{m}_2, \ldots, \bar{m}_t$, the inductive hypothesis says that there exist elements $a_2, \ldots, a_{t-1} \in A$ such that

$$N = \sum_{i=2}^{t-1} A(m_i + a_i m_t).$$

Thus

$$M = Am_1' + \sum_{i=2}^{t-1} A(m_i + a_i m_t).$$

Set $a_1 = b_t - \sum_{i=2}^{t-1} b_i a_i$, so that

$$m_1' = m_1 + \sum_{i=2}^{t} b_i m_i$$

$$= m_1 + a_1 m_t + \sum_{i=2}^{t-1} b_i(m_i + a_i m_t).$$

This implies that $m_1' \in \sum_{i=1}^{t-1} A(m_i + a_i m_t)$, so that

$$M = \sum_{i=1}^{t-1} A(m_i + a_i m_t),$$

as required.

It remains to show that $b_2, \ldots, b_t$ may be chosen to satisfy $(*)$. Recall from Section 2 that, for any integer x, $I_x(A, M)$ is an ideal of R with the property that, for every prime ideal p of R,

$$p \supseteq I_x(A, M) \Leftrightarrow \mu(A_p, M_p) > x.$$

Similarly, for an integer y,

$$p \supseteq I_y(R, M) \Leftrightarrow \mu(R_p, M_p) > y.$$

For any integers x and y, set $I_{x,y} = I_x(A, M) + I_y(R, M)$. Since M is finitely generated both as A-module and as R-module, there are only finitely many distinct ideals of the form $I_{x,y}$.

We will show that if $p \in P$ is a j-prime with

$$u = j\text{-}\dim(p) + \mu(A_p, M_p),$$

then p is minimal among the j-primes containing one of the ideals $I_{x,y}$. To this end, suppose that x and y are as large as possible subject to the conditions $I_x(A, M) \subseteq p$, $I_y(R, M) \subseteq p$. Then $I_{x,y} \subseteq p$. If p is not minimal among j-primes containing $I_{x,y}$ then there is a j-prime q such that

$$I_{x,y} \subseteq q \subset p.$$

By the definition of $I_x(A, M)$ we have

$$\mu(A_p, M_p) = x + 1 = \mu(A_q, M_q).$$

Since $j\text{-dim}(q) > j\text{-dim}(p)$, we must have

$$j\text{-dim}(q) + \mu(A_q, M_q) > u.$$

By the definition of u this is a contradiction if $q \in \mathscr{P}$, that is, if $m_t \notin qM_q$.

However, since $p \in \mathscr{P}$, we have $m_t \notin pM_p$. Since $\mu(R_p, M_p) = y + 1$ we may find $n_1, ..., n_y \in M$ such that

$$m_t, n_1, ..., n_y$$

is a set of minimal generators for M_p *as an* R_p*-module.* Since $q \subset p$, these elements also generate M_q as an R_q-module. But $\mu(R_q, M_q) = y$, so $m_t, n_1, ..., n_y$ are actually a minimal set of generators for M_q over R_q. Thus $m_t \notin qM_q$, so $q \in \mathscr{P}$. This gives the desired contradiction, and shows that p is minimal among j-primes containing $I_{x,y}$. Let $p_1, ..., p_z$ be the finitely many j-primes minimal over at least one of the ideals $I_{x,y}$. Since $m_1, ..., m_t$ generates a submodule of M that is at least 1-fold basic at every prime of $\mathscr{P}$, Lemma 3, applied with $a = 1$, shows that there exist elements $b_2, ..., b_t \in A$ such that

$$m_1' = m_1 + \sum_{i=2}^{t} b_i m_i$$

is basic at the primes $p_1, ..., p_z$. This choice of $b_2, ..., b_t$ satisfies $(*)$, so the proof of Theorem B is complete. ∎

8. Some Open Problems and a Counterexample

A. *Relatives of Serre's Theorem*

The most famous problem in the subject of projective modules is Serre's very durable question: Let K be a field $R = K[x_1 \cdots x_d]$ a polynomial ring. Is every projective R-module free? We would like to conjecture a more modest version of this:

Conjecture 1. Let R be a noetherian ring of dimension d, and suppose that $R = S[x]$ for some ring S, where x is an indeterminate. Then every projective R-module of rank d has a free summand.

Here is some evidence to support this assertion: If $d = 1$, then R modulo its nilpotent radical is a principal ideal ring, and the conjecture follows at once. For the case $d = 2$, the conjecture was established by Murthy [17, Theorem 2] under the additional assumption that there are only finitely many maximal ideals p of S such that S_p is not a discrete valuation ring. (This includes Seshadri's theorem). We have been able to establish the result for all d, under the hypothesis that S is a polynomial ring (possibly with 0 indeterminates) over a semilocal ring of positive dimension.

In a different direction, Bass [3] has shown that, if d is odd, then every stably free R-module of rank d has a free summand. This implies our conjecture in case d is odd and S is itself a polynomial ring over some field.

In line with Theorem A, it seems natural to make a stronger conjecture to include non-projective modules:

Conjecture 2. Let R and S be as in Conjecture 1. Suppose M is a finitely generated R-module such that, for every j-prime p of R, $\mu(R_p, M_p) \geqslant d$. *Then M contains a j-basic element.*

It turns out that this is true if M is a direct sum of ideals of R. One gets as a consequence an improved version of Kronecker's theorem (Corollary 7). See [7] for a discussion of this.

Still using Theorem A as a model, one might hope to strengthen this conjecture still further to include the cancellation theorem and the Forster-Swan theorem, both improved by lowering the numerical bound by 1, as corollaries. For a precise version of this, see [8], where it is proved, along with Conjectures 1 and 2, in the case in which S is a polynomial ring (possibly with 0 indeterminates) over a semilocal ring of positive dimension.

A note of warning should be sounded regarding the stable range theorem. Here the bound $d + 1$ cannot be improved when R has the form $K[x_1, ..., x_d]$, with K a field. The following example is due to Vasershtein [26]: Let K be the field of real numbers, and let $R = K[x_1 \cdots x_d]$. Then $x_1, ..., x_d, 1 - \sum x_i^2$ is a unimodular row of $d + 1$ elements over R, and there exist no elements $a_1, ..., a_d \in R$ such that

$$x_1 + a_1\left(1 - \sum x_i^2\right), ..., x_d + a_d\left(1 - \sum x_i^2\right)$$

is unimodular. (The only proof that we know of this fact is topological.) However, it seems to be an open question whether, if R is as in Conjecture 1, $E(d + 1, R)$ is transitive on unimodular rows (see [1] for the connection).

B. *Cancellation*

Here there is a great scarcity of strong results and of counterexamples. One would like to prove under some general hypothesis that, if R is a commutative noetherian ring and $L, M,$ and N are finitely generated R modules such that $L \oplus M \simeq L \oplus N$, then $M \simeq N$. The drawback of Bass's theorem (Corollary 4) is that it requires L to be projective and M (or N) to have a "large" projective summand. Dress in [6] has modified Bass's result to cover the case in which L, M, and N are all summands of sums of a given module. His technique is to force L, M, and N to be projective over a different ring. Some criteria of "largeness" is certainly necessary in general (see Swan [21, Section 4]); but the need for projectivity is not clear. It cannot be completely omitted as we shall see below.

There are various results that do go in the desired direction. For example, it is known that, if R is semilocal, then $M \simeq N$ (see Vasconcelos [25] or Evans [10] where a stronger result is proved). If R is semihereditary and L is projective, then $M \simeq N$ (Kaplansky [12, page 75]). Without any hypothesis on R, if $L = R$ and M is an ideal of R, then $M \simeq N$ (Kaplansky [12, page 76]).

On the other hand, we know of no counterexample to cancellation over any 1-dimensional commutative ring. (But Swan has given an example of failure of cancellation in a finite non-commutative Z-algebra.)

Vasconcelos [25] has shown that, if R is an integrally closed domain, I and J ideals of R, and M a finitely generated R module, then $I \oplus M \simeq J \oplus M$ implies $I \simeq J$.

Bass's cancellation theorem can be extended to cancel modules of finite projective dimension from big projectives. The exact statement is the following: Let R and A be as in Theorem A. Let P be a finitely generated projective module of rank $>j$-dim(R). Let M be a finitely generated module of finite projective dimension. Let P' be any projective module. Then $P \oplus M \simeq P' \oplus M$ implies $P \simeq P'$.

(*Proof.* We know from [23, Corollary 3.6] that K_0(finitely generated projective modules) is isomorphic to K_0(finitely generated modules of finite projective dimension.) Since $[P] = [P']$ in K_0(finitely generated modules of finite projective dimension) we get $[P] = [P']$ in K_0(finitely generated projective modules). It follows from [23, Theorem 1.10] that there exists a finitely generated projective module Q such that $P \oplus Q \simeq P' \oplus Q$. Corollary 3 implies that $P \simeq P'$. ▮)

Chase in [5] has given some very interesting results and examples for $R = K[X, Y]$ with K a field. For instance, if L, M, and N are torsion-free, then $L \oplus M \simeq L \oplus N$ implies $R \oplus M \simeq R \oplus N$. Furthermore, if K is algebraically closed of characteristic 0, then $M \simeq N$. He also gives a counterexample if K is the field of real numbers and a partial answer if K is algebraically closed of characteristic >0. The full result in characteristic >0 is unknown.

We conclude with an example to show that one cannot, in Bass's cancellation theorem, replace the condition that M have a large projective summand, with the condition that M require many generators locally (as Theorem A might lead one to hope) or even with the condition that M be torsion-free of large rank.

EXAMPLE. Let K be the field of real numbers, and let

$$S = K[x_1, x_2, x_3]\Big/\left(1 - \sum x_i^2\right)$$

(this is the coordinate ring of the 2-sphere). Let $R = S[y_1, y_2]$, where the y_i are indeterminants. We will construct, for each i, finitely generated torsion free R-modules M_i and N_i of torsion-free rank $i + 2$ such that $R \oplus M_i \simeq R \oplus N_i$ but $M_i \not\simeq N_i$.

To do this, we first define P to be the S-module which is the cokernel of the map

$$\begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \bar{x}_3 \end{pmatrix} : S \to S^3,$$

where $\bar{x}_i$ is the image of x_i in S. P is in fact projective, because

$$\begin{pmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \bar{x}_3 \end{pmatrix}$$

is split by the map

$$(\bar{x}_1, \bar{x}_2, \bar{x}_3) : S^3 \to S$$

(this is because $\sum \bar{x}_i^2 = 1$). Thus $S \oplus P \simeq S^3 \simeq S \oplus S^2$. It is known (Swan [21, Theorem 3]) that $P \not\simeq S^2$.

Let $Q = R \otimes_S P$, and let $I = (y_1, y_2)$, the ideal of R generated by y_1 and y_2. Let

$$J_i = \underbrace{I \oplus I \oplus \cdots \oplus I.}_{i \text{ times}}$$

Finally, set $M_i = Q \oplus J_i$, $N_i = R^2 \oplus J_i$. Since $S \oplus P \simeq S^3$, it follows that $R \oplus Q \simeq R^3$, so $R \oplus M_i \simeq R \oplus N_i$, and M_i and N_i are torsion-free of rank $i + 2$ as promised.

To conclude, we must show that $M_i \not\simeq N_i$. To do this we will use the following easy lemma:

LEMMA 7. *Let R be any commutative noetherian ring, and let I be an ideal of R that contains an R-sequence of length 2. Then any map*

$$x: I \to R$$

satisfies $x(I) \subseteq I$.

Proof. The exact sequence $0 \to I \to R \to R/I \to 0$ gives rise to an exact sequence

$$\mathrm{Hom}(R, R) \to \mathrm{Hom}(I, R) \to \mathrm{Ext}^1(R/I, R).$$

Since I contains an R-sequence of length 2, $\mathrm{Ext}^1(R/I, R) = 0$ [12, p. 101]. Thus every map from I to R is induced by multiplication by some element of R; in particular every map from I to R carries I into I. ▌

Now suppose, contrary to what we wish to show, that $M_i \cong N_i$ for some i. We will conclude that the S-modules P and S^2 are isomorphic, a contradiction.

Suppose the isomorphism is given by the matrix

$$\varphi = \begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix}: Q \oplus J_i \to R^2 \oplus J_i .$$

Since $y_1, y_2 \in I$ are an R-sequence, it follows from Lemma 7 that $\varphi_{12}: J_i \to R^2$ has image contained in IR^2. Further, since φ is an isomorphism, $(\varphi_{11}, \varphi_{12}): Q \oplus J_i \to R^2$ is an epimorphism, so $R^2 = \varphi_{11}(Q) + IR^2$.

Let $U \subseteq R$ be the multiplicatively closed set $U = \{1 + y \mid y \in I\}$, so that I_U is in the Jacobson radical of R_U. Since $R_U{}^2 = (\varphi_{11}(Q))_U + IR_U{}^2$, Nakayama's lemma implies that $R_U{}^2 = \varphi_{11}(Q)_U$, that is, that

$$\varphi_{11_U}: Q_U \to R_U{}^2$$

is onto. Since Q_U is a projective of rank 2, this implies that $Q_U \cong R_U{}^2$. To finish the proof, note that $R_U/I_U \cong S$, and $Q_U/I_U Q_U \cong P$. Thus from $Q_U \cong R_U{}^2$, it follows that $P \cong S^2$ as S-modules, which is the desired contradiction. ▌

Note added in proof. A very slightly weakened form of Theorem B can be obtained as another corollary of Theorem A. Assume that the condition of Theorem B is satisfied for all j-primes of R, and let

$$F \to A^t \to M \to 0$$

be a free presentation of M using the given generators. Theorem A(ii)(b) can now be applied (with $a = 1$) to the submodule of F^* generated by the images $n_1, \ldots, n_t$ of the dual basis elements in A^*. We get elements $a_1 \cdots a_{t-1} \in A$ such that $n_t + \sum_1^{t-1} a_i n_i$ is basic in F^*. It follows easily that these a_i satisfy Theorem B.

References

1. H. Bass, K-Theory and stable algebra, *Publ. Math. I. H. E. S.* No. 22 (1964), 5–60.
2. H. Bass, "Algebraic K-Theory," Benjamin, Menlo Park, Cal., 1968.
3. H. Bass, Modules which support nonsingular forms, *J. Algebra* 13 (1969), 246–252.
4. N. Bourbaki, Diviseurs ("Algèbre Commutative," Chapter 7), Hermann, Paris, 1965.
5. S. U. Chase, Torsion-free modules over $K[X, Y]$, *Pacific J. Math.* 12 (1962), 437–447.
6. A. Dress, On the decomposition of modules, *Bull. Amer. Math. Soc.* 75 (1969), 984–986.
7. D. Eisenbud and E. G. Evans, Every algebraic set in n-space is the intersection of n hypersurfaces, *Invent. Math.* **19** (1973), 107–112.
8. D. Eisenbud and E. G. Evans, Three conjectures about modules over polynomial rings, in (Lecture Notes in Mathematics 311), Springer-Verlag, New York/Berlin, 1972.
9. D. Estes and J. Ohm, Stable range in commutative rings, *J. Algebra* 7 (1967), 343–362.
10. E. G. Evans, Krull-Schmidt and cancellation over local rings, to appear.
11. O. Forster, Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring, *Math. Z.* **84** (1964), 80–87.
12. I. Kaplansky, "Infinite Abelian Groups," rev. ed., University of Michigan Press, Ann Arbor, 1969.
13. I. Kaplansky, "Commutative Rings," Allyn & Bacon, Boston, 1970.
14. L. Kronecker, Grundzüge eine arithmetischen Theorie der algebraischen Grossen, *J. Reine Angew. Math.* **92** (1882), 1–123.
15. W. Krull, Über die Zerlegung der Hauptideale in algemeinen Ringen, *Math. Ann.* **105** (1931), 1–14.
16. H. Matsumura, "Commutative Algebra," Benjamin, Menlo Park, Cal., 1970.
17. M. P. Murthy, Projective modules over a class of polynomial rings, *Math. Z.* **88** (1965), 184–189.
18. M. P. Murthy, Generators for certain ideals in regular rings of dimension three, *Comment. Math. Helv.* **47** (1972), 179–184.
19. Morris Orzech, Onto endomorphisms are isomorphisms, *Amer. Math. Monthly* **78** (1971), 357–362.
20. J.-P. Serre, "Modules Projectifs et Espaces Fibrés à Fibre Vectorielle," Seminaire P. Dubreil, Expose 23 (1957–58), Paris.
21. R. G. Swan, Vector bundles and projective modules, *Trans. Amer. Math. Soc.* **105** (1962), 264–277.
22. R. G. Swan, The number of generators of a module, *Math. Z.* **102** (1967), 318–322.
23. R. G. Swan, "Algebraic K-Theory" (Lecture Notes in Mathematics 76), Springer-Verlag, New York/Berlin, 1968.
24. B. L. van der Waerden, Review of Perron's article "Über das Vahlensche Beispiel zu einen Satz von Kronecker," in *Zbl. Math.* **24** (1941), 276.
25. W. V. Vasconcelos, On local and stable cancellation, *An. Acad. Brasil. Ci.* **37** (1965), 389–393.
26. L. N. Vasershtein, Stable rank of rings and dimensionality of topological spaces, *Functional Anal. Appl.* **5** (1971), 102–110.