JOURNAL OF ALGEBRA 7, 343-362 (1967)

Stable Range in Commutative Rings

DENNIS ESTES[1]

AND

JACK OHM*

Louisiana State University, Baton Rouge, Louisiana 70803

Communicated by Marshall Hall, Jr.

Received January 20, 1967

INTRODUCTION

Let R' be a ring with identity. Bass's main criterion for determining the stable range of R' is the following theorem ([*1*], p. 29, Theorem 11.1):

If R' is a finite R-algebra, R being a commutative ring with identity, such that Spm (R) is Noetherian, then $\dim \operatorname{Spm}(R) = d$ implies $d + 1$ defines a stable range for $\mathbf{GL}(R')$.

Here Spm (R) denotes the maximal spectrum of R. (We review the definitions in detail in Section 1.)

In Section 2 we reprove Bass's theorem for the case $R = R'$, showing that it is then an elementary result. Section 3 is concerned with establishing the inequality $\dim \operatorname{Spm}(R) \leqslant \dim \operatorname{Spm}(R')$, under certain assumptions on these rings. We apply this result in Section 4 to show that for any integer $n \geqslant 0$ there exists an integral domain D such that $\dim \operatorname{Spm}(D) = n$ and 1 is in the stable range. The device used in this construction is the Kronecker function ring. The Kronecker function ring is a Bezoution domain having 1 in the stable range, and in Section 5 we give a characterization of such rings. We also show in Section 5 that a principal ideal domain with 1 in the stable range is Euclidean.

Section 6 is devoted to some general theorems on homomorphisms and quotient rings, and these results are used in Section 7 to investigate overrings R (contained in the rational numbers) of the integers Z. For any semilocal overring R of Z, $\dim \operatorname{Spm}(R) = 0$; so 1 is in the stable range. At the other extreme, we prove that 1 is not in the stable range of any finite extension

---

[1] Present address: California Institute of Technology, Pasadena, California.

* Partially supported by a grant from the National Science Foundation.

of Z. Intermediate to these two extremes we exhibit classes of rings which have 1 in the stable range and classes of rings which do not.

Up to this point our main concern has been with stable range 1. In Section 8 we venture slightly further to the question of when 2 is in the stable range of $R[X]$, where R is a principal ideal domain and X is an indeterminate. The main result here asserts that unimodular sequences (a_1, a_2, a), with $a_i \in R[X]$ and $a \in R$, are stable.

1. Notation and Basic Concepts

We shall use R to denote a commutative ring with identity, and we observe the conventions of Bourbaki ([2], Chapt. 5, p. 9) regarding such rings. An ideal of R means an ideal $\neq R$. If A is an ideal of R, $J(A)$ denotes the Jacobson radical of A, i.e., the intersection of the maximal ideals containing A. $\subset$ denotes containment and $<$ denotes proper containment.

Let $J = \{\text{ideals } A \text{ of } R \mid J(A) = A\}$. By a chain of ideals of length n, we mean a sequence of ideals $A_0 < A_1 < \cdots < A_n$. The Krull dimension of R, written dim R, is the sup of the lengths of chains of prime ideals of R; whereas the dimension of the maximal spectrum, denoted by $\dim_J R$, is the sup of the lengths of chains of prime ideals *from* J. Then $\dim_J R \leqslant \dim R$.

For any ideal A of R, a prime ideal P in J which contains A is called a *component* of A if P is minimal among the primes of J which contain A. Every $A \in J$ is the intersection of its components. We say that R is *J-Noetherian* if the ideals of J satisfy the ascending chain condition. R is J-Noetherian implies that every ideal of R has only finitely many components (and the statements are equivalent when $\dim_J R$ is finite). Moreover, any prime of J which contains A also contains a component of A.

We refer the reader to Grothendieck ([5], p. 6, Paragr. 14) for a proper perspective of these concepts. There both dim and $\dim_J$ are treated simultaneously by considering spec $(R) = \{$prime ideals of R, with Zariski topology$\}$ and the subspace Spm (R) consisting of the maximal ideals of R. Our set J corresponds to the collection of closed subsets of Spm (R), and $\dim_J R$ is the combinatorial dimension of Spm (R) in Grothendieck's terminology.

We shall call a sequence $(a_1, ..., a_s, a_{s+1})$, $s \geqslant 1$, of elements of R *stable* if there exist $b_1, ..., b_s \in R$ such that

$$(a_1, ..., a_s, a_{s+1}) = (a_1 + b_1 a_{s+1}, ..., a_s + b_s a_{s+1}).^2$$

The sequence $(a_1, ..., a_s, a_{s+1})$ is called *unimodular* if $(a_1, ..., a_s, a_{s+1}) = R$.

[2] We use $(a_1, ..., a_{s+1})$ to denote both a sequence and the ideal generated by the elements of the sequence; but the context will always make our meaning clear.

We shall say that *n is in the stable range of R* if for every $s \geqslant n$, every unimodular sequence $(a_1, \ldots, a_s, a_{s+1})$, $a_i \in R$, is stable. [With some misgivings, we have abbreviated Bass's terminology ([1], p. 14). He says "n defines a stable range for $\mathbf{GL}(R)$"]. It follows that if n is in the stable range of R, then also m is in the stable range of R for any $m \geqslant n$.

2. Bass's Theorem for $R = R'$

Let $a_0, \ldots, a_{s+1}$ be elements of R, and let $P_1, \ldots, P_t$ be prime ideals of R such that $P_i \not\subset P_j$ for $i \neq j$.

Lemma 2.1. *If $a_{s+1} \notin P_1, \ldots, P_t$, then for any j, $1 \leqslant j \leqslant s$, there exist $b_j \in R$ such that if $a_j' = a_j + b_j a_{s+1}$, then $a_j' \notin P_1, \ldots, P_t$.*

Proof. Suppose $a_j \in P_1, \ldots, P_i, \notin P_{i+1}, \ldots, P_t$, $i \geqslant 0$. Choose $b_j \in P_{i+1}, \ldots, P_t, \notin P_1, \ldots, P_i$; and let $a_j' = a_j + b_j a_{s+1}$. Such a b_j exists, since we can take $b_j \in P_{i+1} \cdot \cdots \cdot P_t$ and $\notin P_1 \cup \cdots \cup P_i$.

Corollary 2.2. *Let R be J-Noetherian. Then there exist $b_1, \ldots, b_s \in R$ such that if $a_j' = a_j + b_j a_{s+1}$, then for any i $1 \leqslant i \leqslant s$, any component of $(a_0, a_1', \ldots, a_{i-1}')$ which contains a_i' also contains a_{s+1}.*

Proof. Apply Lemma 2.1 s times.

Theorem 2.3. *Suppose R is J-Noetherian and $\dim_J R < s$. Then any unimodular sequence $(a_1, \ldots, a_{s+1})$, $a_i \in R$, is stable.*

Proof. Let $a_0 = 0$ and choose b_i as in 2.2. Suppose $(a_0, a_1', \ldots, a_s') < R$, and let P be a component of this ideal. $a_{s+1} \notin P$ since

$$(a_0, a_1', \ldots, a_s, a_{s+1}) = (a_1, \ldots, a_{s+1}) = R.$$

Therefore

$$(a_0, a_1', \ldots, a_s') \supset (a_0, a_1', \ldots, a_{s-1}') \supset \cdots \supset (a_0, a_1') \supset (a_0)$$

implies there exists a sequence of primes $P \supset P_{s-1} \supset \cdots \supset P_1 \supset P_0$, where P_i is a component of $(a_0, a_1', \ldots, a_i')$. By 2.2, the inclusions are proper, a contradiction to the hypothesis that $\dim_J R < s$. Q.E.D.

The above theorem is the case of Bass's theorem when $R = R'$ (in the terminology of the introduction).[3] The device used in its proof is analogous to the process of cutting down with hypersurfaces in algebraic geometry.

3. An Inequality for $\dim_J$

Let R and R' be commutative rings with identity, and suppose we are given a homomorphism $f: R \to R'$ (i.e., R' is an R-algebra). If A' is an ideal of R', we let $(A')^c = f^{-1}(A')$; and if A is an ideal of R, we let $A^e = f(A) \cdot R'$. By the *lying over* and *going up* conditions, we mean the following:

(LO): For any prime ideal P of R, there exists a prime P' of R' such that $(P')^c = P$.

(GU): For any primes $P_1 \subset P_2$ of R, if P_1' is a prime of R' such that $(P_1')^c = P_1$, then there exists a prime P_2' of R' such that $P_1' \subset P_2'$ and $(P_2')^c = P_2$.

Lemma 3.1. *Suppose* (GU) *holds for* $R \to R'$, *and let* P' *be a prime ideal of* R' *and* $P = (P')^c$. *Then* $(J(P'))^c = J(P)$. *Moreover,* $J(P) = P$ *implies there exists a prime ideal* P_1' *of* R' *such that* $P_1' \supset P'$, $(P_1')^c = P$, *and* $J(P_1') = P_1'$.

Proof. Let $a \in (J(P'))^c$, and let M be a maximal ideal containing P. By (GU), there exists a prime $P_1' \supset P'$ such that $(P_1')^c = M$. Let M' be a maximal ideal of R' such that $P_1' \subset M'$. Then $a \in (M')^c = M$; so $(J(P'))^c \subset J(P)$. Conversely, let M' be a maximal ideal containing P'. Choose M to be a maximal ideal of R such that $(M')^c \subset M$. By (GU) there exists a prime ideal M_1' of R' such that $M' \subset M_1'$ and $(M_1')^c = M$. But then $M' = M_1'$; so also $(M')^c = (M_1')^c = M$. Therefore $a \in M$ implies $a \in (M')^c$. Hence $J(P) = (J(P'))^c$.

For the second assertion, choose P_1' to be maximal with respect to the properties that $P_1' \supset P'$ and $P_1' \cap f(R - P) = \phi$. Then P_1' is prime by [*12*], p. 4, (2.1), and $(P_1')^c = P$. But also, by the first assertion, $(J(P_1'))^c = J(P) = P$; so by the maximality of P_1', we have $P_1' = J(P_1')$.

Theorem 3.2. *Suppose* (GU) *and* (LO) *hold for* $R \to R'$. *Then* $\dim_J R \leqslant \dim_J R'$.

[3] The proof given here has recently been extended [by Ohm and Pendleton, *Commutative rings with Noetherian spectrum*—to appear] to an elementary proof of Bass's theorem for the case where R' is an arbitrary commutative R-algebra. The missing link is provided by their theorem: if $\dim_J R$ is finite and R is J-Noetherian, then any finite integral extension of R is also J-Noetherian.

Proof. Let $P_0 < \cdots < P_n$ be a chain of prime ideals of R such that $J(P_i) = P_i$. By applying (LO) + 3.1 + (GU), one constructs a chain of primes $P'_0 < \cdots < P'_n$ of R' such that $(P'_i)^c = P_i$ and $J(P'_i) = P'_i$. Q.E.D.

4. The Kronecker Function Ring

Let D be an integrally closed domain with quotient field K, and let X be an indeterminate. The Kronecker function ring of D is a domain D^* having quotient field $K^* = K(X)$, and Krull ([9], pp. 558-561) gives the following construction for D^*:

Write $D = \cap R_v$, where $\{R_v\}$ is the set of all valuation rings of K which contain D. Let v^* denote the trivial extension of v to $K(X)$ [i.e., define $v^*(a_0 + a_1X + \cdots + a_nX^n) = \inf_{i=0,\dots,n} \{v(a_i)\}$], and let R_{v^*} be the valuation ring of v^*. Then $D^* = \cap R_{v^*}$.

Krull's main theorem on D^* asserts that any valuation ring of K^* which contains D^* is one of these R_{v^*}. Moreover,

Proposition 4.1. *If* $a_1^*, a_2^* \in D^*$, *then* $(a_1^*, a_2^*) = (a_1^* + X^m a_2^*)$ *for some* $m \geqslant 0$.

Proof ([9], p. 559). If $a_1^* = a_1/d$, $a_2^* = a_2/d$, with $a_1, a_2, d \in D[X]$, choose $m > \deg a_1(X)$. Q.E.D.

Thus, in particular, it follows that 1 is in the stable range of D^*, and also that D^* is Bezoutian (i.e., every finitely generated ideal is principal). Since every Bezoutian domain is also a Prüfer domain (i.e., every quotient ring with respect to a prime ideal is a valuation ring), the set $\{R_{v^*}\}$ then coincides with the set of rings $D^*_{P^*}$, where P^* is a prime ideal of D^*. (For these concepts, see for instance [2], Chapt. 7, pp. 94-95).

In [6] (or [7]), Jaffard defines the valuative dimension of a domain D, denoted $\dim_v D$, to be the sup of the ranks of the valuation rings of K which contain D. Moreover, he shows that $\dim_v D \geqslant \dim D$, and when D is Noetherian, then $=$ holds. For a Prüfer domain D^*, $=$ also obviously holds. Thus, for the Kronecker function ring D^*, we have $\dim D \leqslant \dim_v D = \dim_v D^* = \dim D^*$; and when D is Noetherian, then the first equality is also valid.

We continue to use D to denote an integrally closed domain having D^* as its Kronecker function ring.

Theorem 4.2. $D \to D^*$ *satisfies* (LO) *and* (GU).

Proof. (LO): If P is any prime ideal of D, there exists a valuation ring R_v of K which is centered on P (see [12], p. 37, (11.9)). Then R_{v^*} is centered on a prime P^* of D^* lying over P.

(GU): Suppose $P_1 \subset P_2$ are prime ideals of D and P_1^* is a prime ideal of D^* such that $(P_1^*)^c = P_1$. Let R_1^* be a valuation ring of K^* centered on P_1^*, and let $R_1 = R_1^* \cap K$. Then R_1 is a valuation ring of K centered on P_1. There exists a valuation ring R_2 of K such that $R_2 \subset R_1$ and R_2 is centered on P_2 (apply [*12*], p. 35, (11.4)). Then the corresponding valuation ring R_2^* of K^* has the property that R_2^* is centered on a prime P_2^* of D^* lying over P_2; and $R_2^* \subset R_1^*$ implies $P_1^* \subset P_2^*$.

COROLLARY 4.3. $\dim_J D \leqslant \dim_J D^*$.

Proof. Use 3.2 and 4.2. Q.E.D.

From the above corollary and the preceding discussion, we can conclude that if D is Noetherian and $\dim D = \dim_J D$, then $\dim_J D^* = \dim D$ also. Consider then $D = k[X_1, ..., X_n]$, k a field and the X_i indeterminates. Dim $D = \dim_J D = n$, so $\dim_J D^* = n$ for this ring. Thus, we have proved the following:

THEOREM 4.4. *For any $n \geqslant 0$ there exists a domain D^* such that $\dim_J D^* = n$ and 1 is in the stable range of D^*.*

Instead of $k[X_1, ..., X_n]$, one could more generally choose D to be any Noetherian Jacobson ring of dim n (see Krull [*11*]).

We conclude this section by giving an example to show that $<$ can occur in 4.3.

EXAMPLE 4.5. Of a domain D having Kronecker function ring D^* such that $\dim_J D = 0$, $\dim D = \dim_J D^* = 1$, and $\dim D^* = 2$.

Let $K = k(x, y)$, k a field and x, y indeterminates; and let v be the x-adic valuation of K over $k(y)$. Then R_v is the additive direct product of $k(y)$ with M_v, where M_v is the maximal ideal of R_v. Let $D = k + M_v$. D is 1-dim, quasi-local, with maximal ideal M_v. (See [*10*], pp. 670-671.) Therefore $\dim_J D = 0$.

If $\{R_{w_1}\}$ is the set of nontrivial valuation rings of $k(y)$ over k and R_w denotes the inverse image of R_{w_1} under the canonical homomorphism $f: R_v \to R_v/M_v$, then the R_w are rank-2 valuation rings of K which are contained in R_v. Since $\cap R_{w_1} = k$, $\cap R_w = D$. Moreover, if R_u is a nontrivial valuation ring of K such that $D \subset R_u$, then $R_u = R_v$ or $R_u = R_w$ for some w. For, R_u must have center M_v on D, since M_v is the only prime $\neq 0$ of D. Then $\xi \in R_u$, $\notin R_v$ implies $1/\xi \in M_v \subset M_u$, which is impossible. Therefore $R_u \subset R_v$, so $R_u = R_v$ or $f(R_u) = R_{u_1}$ is a nontrivial valuation ring of $k(y)$ over k and hence equals R_{w_1} for some w_1. But then $R_u = R_w$ since $M_v = \ker (f) \subset R_u$.

It follows that $\dim_v D = 2$ and hence that $\dim D^* = 2$. Therefore

$\dim_J D^* \leqslant 2$. To show $\dim D^* = 1$, we need only see then that $\cap M_{w^*} = M_{v^*}$, where M_{w^*}, M_{v^*} are the centers of the R_{w^*}, R_{v^*}, respectively, on D^*.

First observe that any unit of R_v has value $\neq 0$ for only finitely many w, since the w_1 have a similar finiteness property in $k(y)$. Thus, also any finite set of units of R_v will be units in almost all R_w. Let then $d^* \in \cap M_{w^*}$. $d^* = a/b$, $a, b \in K[X]$; and we may assume $a, b \in R_v[X]$ and that at least one coefficient of a or b is a unit in R_v. Then $v^*(a) > 0$ implies $d^* \in M_{v^*}$, and we are done; so we may assume that $v^*(a) = 0$. Then $v^*(b) = 0$ also, and hence both have at least one coefficient which is a unit in R_v. But by our initial remark, we can find a w which has value 0 at all coefficients of a, b which are units in R_v, and which then has value > 0 at the other coefficients. Therefore $w^*(a) = w^*(b) = 0$; so $w^*(d^*) = 0$, a contradiction to $d^* \in M_{w^*}$. Thus, $d^* \in M_{v^*}$ and $\cap M_{w^*} = M_{v^*}$. Q.E.D.

Note that this example gives a D^* which is of $\dim_J = 1$ and which is J-Noetherian. Whether there exist Kronecker function rings of arbitrary $\dim_J$ which are J-Noetherian is an open question.[4]

5. Bezoutian Domains with 1 in the Stable Range

A Bezoutian domain is a domain in which every finitely generated ideal is principal. As we have observed, the Kronecker function ring is an example of such a domain. Moreover, we saw in 4.1 that *any* 2-sequence of a Kronecker function ring is stable. The next proposition shows that this property characterizes Bezoutian domains with 1 in the stable range.

Proposition 5.1. *The following are equivalent for an integral domain D:*

(i) *1 is in the stable range of D and D is Bezoutian.*

(ii) *For any $a_1, a_2 \in D$ and $b \in (a_1, a_2)$, there exist $c, d \in D$ such that $b = c(a_1 + da_2)$.*

(iii) *For any $a_1, a_2 \in D$, there exists $d \in D$ such that $(a_1, a_2) = (a_1 + da_2)$.*

Proof. (i) $\Rightarrow$ (ii): $b \in (a_1, a_2) = (a)$ implies $a_i = a_i'a$, $b = b'a$, where $(a_1', a_2') = D$. Therefore 1 is in the stable range of D implies there exists $d \in D$ such that $u = a_1' + da_2'$ is a unit. Therefore $bu = b'(a_1 + da_2)$, so $b = (b'/u)(a_1 + da_2)$.

(ii) $\Rightarrow$ (iii): $a_2 \in (a_1, a_2)$ implies there exist $c, d \in D$ such that $a_2 = c(a_1 + da_2)$. But then $a_1 = (1 - cd)(a_1 + da_2)$, so $(a_1, a_2) = (a_1 + da_2)$.

[4] William Heinzer, Louisiana State University, has recently shown the existence of Kronecker function rings of arbitrary $\dim_J$ which are J-Noetherian.

(iii) $\Rightarrow$ (i): If $(a_1, ..., a_{s+1})$ is any ideal of D, then there exist $b_i \in D$ such that $(a_i + b_i a_{s+1}) = (a_i, a_{s+1})$, $i = 1, ..., s$. Therefore

$$(a_1, ..., a_{s+1}) = (a_1 + b_1 a_{s+1}, ..., a_s + b_s a_{s+1}). \qquad \text{Q.E.D.}$$

It would be interesting to know if there is some statement similar to (i) $\Leftrightarrow$ (iii) which holds for the case of a domain having stable s-sequences, $s \geqslant 2$.

COROLLARY 5.2. *Let D be a Bezoutian domain with quotient field K, and let D' be a domain such that $D \subset D' \subset K$. If 1 is in the stable range of D, then 1 is in the stable range of D'.*

Proof. $D' = D_S$ for some multiplicative system (abbreviated henceforth to m.s.) S of D(see [4], p. 99, Corollary 2.4). For any elements $a_1', a_2' \in D'$, if $b' \in (a_1', a_2')$, then there exist $m_1, m_2 \in S$ such that $b' = b/m_1$, $a_i' = a_i/m_1$, $b, a_i \in D$, and such that $m_2 b \in (a_1, a_2)$. Therefore by 5.1(ii), there exist $c, d \in D$ such that $m_2 b = c(a_1 + da_2)$. Thus, $b' = (c/m_2)(a_1' + da_2')$; so again by 5.1, 1 is in the stable range of D'. Q.E.D.

In particular, 5.2 implies that 1 is in the stable range of every overring (in K^*) of a Kronecker function ring. See Corollary 6.8 for other examples of rings with the property that 1 is in the stable range of R_S whenever 1 is in the stable range of R.

We conclude this section by considering the case of a Noetherian Bezoutian domain, i.e., let now D be a principal ideal domain. For any $a \neq 0$ in D, we can write $a = up_1^{t_1} \cdot \cdots \cdot p_s^{t_s}$, where u is a unit of D and p_i are distinct primes. Then we define $|a|$ to be the integer $\sum_{i=1}^{s} t_i$. Then $|a|$ depends only on a and $|a| \geqslant 0$, $|ab| = |a| + |b|$.

THEOREM 5.3. *Let D be a principal ideal domain. Then* 1 *is in the stable range of D implies D is a Euclidean domain with $|\ |$ as its Euclidean function.*

Proof. Let $a_1, a_2 \in D$ with $a_2 \neq 0$. By 5.1(ii) there exist $c, d \in D$ such that $a_2 = c(a_1 + da_2)$. Therefore $|a_2| = |c| + |a_1 + da_2|$, so either $|a_1 + da_2| < |a_2|$ or $|c| = 0$; and if $|c| = 0$, then c is a unit and $a_2 \mid a_1$. Q.E.D.

One sees immediately that the converse to this theorem is not valid; for example, take $D = k[x]$, k an algebraically closed field.

COROLLARY 5.4. *A semilocal principal ideal domain is Euclidean.*

6. Homomorphisms, Quotient Rings, and Stable Unimodular Pairs

We denote $\mathscr{U}(R)$ the multiplicative group of units of R. If A is an ideal of R, then the canonical homomorphism $R \to R/A$ induces a homomorphism $\varphi_A : \mathscr{U}(R) \to \mathscr{U}(R/A)$. We denote the kernel $\varphi_A^{-1}(1)$ by $\mathscr{K}(A)$. The following lemma is immediate from the definitions.

Lemma 6.1. *φ_A is surjective for every ideal A of R if and only if every unimodular sequence (a_1, a_2), $a_i \in R$, is stable.*

As an application of this observation, one sees that 1 is not in the stable range of the integers Z by taking $A = (p)$, p a prime $\neq 2, 3$; and similarly, if k is a field and X an indeterminate, then that 1 is not in the stable range of $k[X]$ is seen by taking $A = (1 - X^2)$. The following proposition and its corollaries shed further light on this phenomenom.

Proposition 6.2. *Let A, B be ideals of R, and suppose that every unimodular sequence (a_1, a_2), $a_i \in R$, is stable. Then $\mathscr{K}(A) \subset \mathscr{K}(B)$ implies either* (i) $A \subset B$, *or* (ii) $A \not\subset J(B)$ *and for every maximal ideal M such that $B \subset M$ and $A \not\subset M$, we have $R/M \cong Z/(2)$.*

Proof. Suppose first that $A \subset J(B)$ and $A \not\subset B$. Then there exists $a \in A, \notin B$; and no maximal ideal can contain $(1 + a, AB)$. Thus, $(1 + a, AB) = R$, so $1 + a \in \mathscr{U}(R/AB)$. By 6.1, there exists $u \in \mathscr{U}(R)$ such that $u \equiv (1 + a) \bmod AB$. Therefore $u \equiv 1 \bmod A$ and $u \not\equiv 1 \bmod B$, so $u \in \mathscr{K}(A)$ and $\notin \mathscr{K}(B)$, a contradiction.

Suppose then that $A \not\subset J(B)$, and let M be a maximal ideal such that $B \subset M$, $A \not\subset M$. If $R/M \not\cong Z/(2)$, then there exists $c \in R$ such that $c \not\equiv 0, 1 \bmod M$. Since $A \not\subset M$, there exists $a \in A$ such that $a \equiv 1 \bmod M$; and then $c \equiv ac \bmod M$. Therefore $ac \equiv 0 \bmod A$ and $ac \not\equiv 1, 0 \bmod M$; so if $d = 1 - ac$, then $d \equiv 1 \bmod A$ and $d \not\equiv 0, 1 \bmod M$. Therefore $d \notin M$, so $(d, AM) = R$ and $\varphi_{AM}(d) \in \mathscr{U}(R/AM)$. By 6.1 there exists $u \in \mathscr{U}(R)$ such that $u \equiv d \bmod AM$. Therefore $u \equiv 1 \bmod A$ and $u \not\equiv 1 \bmod M$. Hence $\mathscr{K}(A) \not\subset \mathscr{K}(M)$, so, *a fortiori*, $\mathscr{K}(A) \not\subset \mathscr{K}(B)$. Q.E.D.

Note that $B \subset A$ implies $\mathscr{K}(B) \subset \mathscr{K}(A)$. Thus,

Corollary 6.3. *Suppose any unimodular sequence (a_1, a_2) of R is stable, and let A, B be ideals of R such that $B < A \subset J(B)$. Then $\mathscr{K}(B) < \mathscr{K}(A)$.*

Corollary 6.4. *Suppose any unimodular sequence (a_1, a_2) of R is stable, and suppose a is a nonunit of R which is not a 0-divisor. Then $\mathscr{K}(a)$ is infinite.*

Proof. $(a) > (a^2) > \cdots$, since a is not a 0-divisor. Therefore by 6.3, $\mathscr{K}(a) > \mathscr{K}(a^2) > \cdots$. Q.E.D.

Thus, if 1 is in the stable range of a domain D and D is not a field, then $\mathscr{U}(D)$ must be infinite. This immediately excludes a number of domains from having 1 in the stable range, e.g. the integers of an imaginary quadratic field (see [3], p. 96, Theorem 3). We shall show at the end of Section 7 that, in fact, 1 is not in the stable range of any ring of algebraic integers. {Thus, Bass's assertion ([1], p. 18) that 1 is in the stable range of any ring of algebraic integers can be corrected by inserting the word "not".}

In 6.2, case (ii) actually can occur, as one sees by taking $R = Z/(6)$, for example. Then 1 is in the stable range of R since $\dim_J R = 0$. If $B = (0)$, then $\mathscr{K}(B) = 1$. However if $A = (3)$, then $\mathscr{K}(A) = 1$ also. This example also shows that the assumption in 6.4 that a is not a 0-divisor is necessary in order to insure that $\mathscr{K}(a)$ be infinite.

We now expand 6.1 into a criterion for stability of unimodular pairs of a quotient ring of R. Let then S be a m.s. in R, and let $h : R \to R_S$ be the canonical homomorphism. The *saturation of* S, denoted $\mathscr{S}(S)$, is given by $\mathscr{S}(S) = \{a \in R \mid$ there exists $b \in R$ such that $ab \in S\}$. $\mathscr{S}(S)$ may also be characterized by $\mathscr{S}(S) = \{a \in R \mid h(a) \in \mathscr{U}(R_S)\}$. Moreover S is said to be saturated if $\mathscr{S}(S) = S$. In particular then, $\mathscr{S}(S)$ contains all units of R; and $R_{\mathscr{S}(S)} = R_S$ {actually canonically isomorphic ([2], Chapt. 2, p. 154}.

We define the quasi-saturation of S, denoted $\mathscr{Q}(S)$, by $\mathscr{Q}(S) = \{a \in R \mid$ there exists $m \in S$ such that $am \in S\}$. Then $S \subset \mathscr{Q}(S) \subset \mathscr{S}(S)$, and these inclusions can be proper (take $R = Z$, $S = \{6^i, i \geqslant 2\}$, for example).

LEMMA 6.5. *$\mathscr{S}(S) = \mathscr{Q}(S)$ if and only if $\mathscr{U}(R_S) = \{h(m_1)/h(m_2), m_i \in S\}$,* [i.e., if and only if the multiplicative group generated by $h(S)$ is $\mathscr{U}(R_S)$].

Proof. $\mathscr{Q}(S)$ is always contained in $\mathscr{S}(S)$, so we need only consider the lemma for $\mathscr{S}(S) \subset \mathscr{Q}(S)$.

$\Rightarrow$: Let $u' \in \mathscr{U}(R_S)$. Then there exists $u \in R$, $m \in S$ such that $u' = h(u)/h(m)$; and then $h(u) \in \mathscr{U}(R_S)$. Therefore $u \in \mathscr{S}(S) \subset \mathscr{Q}(S)$, so there exists $m_1 \in S$ such that $m_1 u = m_2 \in S$. Then $u' = h(m_2)/h(mm_1)$.

$\Leftarrow$: Let $a \in \mathscr{S}(S)$. Then $h(a) \in \mathscr{U}(R_S)$; so $h(a) = h(m_1)/h(m_2)$, $m_i \in S$. Therefore $h(m_2 a - m_1) = 0$, so there exists $m \in S$ such that $m(m_2 a - m_1) = 0$. Hence $mm_2 a \in S$ and $a \in \mathscr{Q}(S)$.

COROLLARY 6.6. *If S is a multiplicative group (and hence $\subset \mathscr{U}(R)$), then $\mathscr{S}(S) = \mathscr{Q}(S)$ if and only if $S = \mathscr{U}(R)$.*

The m.s. S is said to be *prime to the ideal* A if $bm \in A$ for some $m \in S$ implies $b \in A$ (i.e., no element of S is congruent to a 0-divisor mod A). Let f_A denote the canonical homomorphism $R \to R/A$, let $R' = R/A$, and let

$S' = f_A(S)$. If S is prime to A, we then have the following commutative diagram ([*16*], p. 226):

$$\begin{array}{ccc} R_S & \xrightarrow{f'} & R'_{S'} \\ h \uparrow & & \uparrow h' \\ R & \xrightarrow{f_A} & R' \end{array}$$

THEOREM 6.7. *Let S be a m.s. of R such that $\mathscr{Q}(S) = \mathscr{S}(S)$. Then every unimodular sequence (x_1, x_2), $x_i \in R_S$, is stable if and only if $\mathscr{Q}(f_A(S)) = \mathscr{S}(f_A(S))$ for every ideal A of R such that S is prime to A.*

Proof. $\Rightarrow$: If $u' \in \mathscr{U}(R'_{S'})$, then there exists $u \in \mathscr{U}(R_S)$ such that $f'(u) = u'$, by 6.1. Since $\mathscr{Q}(S) = \mathscr{S}(S)$, $u = h(m_1)/h(m_2)$, $m_i \in S$, by 6.5. Therefore $u' = f'(u) = f'h(m_1)/f'h(m_2) = h'(m'_1)/h'(m'_2)$, where $m'_i = f_A(m_i) \in S'$. Thus, $\mathscr{S}(S') = \mathscr{Q}(S')$ by 6.5.

$\Leftarrow$: Any ideal of R_S is of the form $h(A) R_S$, where A is an ideal of R which is prime to S. If $u' \in \mathscr{U}(R'_{S'})$, then $u' = h'(m'_1)/h'(m'_2)$, $m'_i \in S'$, by 6.5. There exist $m_i \in S$ such that $f_A(m_i) = m'_i$. If $u = h(m_1)/h(m_2)$, then $u \in \mathscr{U}(R_S)$ and $f'(u) = u'$. Now apply 6.1. Q.E.D.

Note that the above proof shows that the implication $\Rightarrow$ is actually valid for every ideal A such that $A \cap S = \emptyset$.

We give the following corollary as an immediate application of this theorem. When R is Noetherian, the corollary includes the result of 5.2.

COROLLARY 6.8. *If* $\dim R \leqslant 1$ *and every nonunit* $(\neq 0)$ *of R is in only finitely many prime ideals, then* 1 *is in the stable range of R implies* 1 *is in the stable range of R_S for any m.s. S.*

Proof. We may take S saturated, so $S = \mathscr{Q}(S) = \mathscr{S}(S)$. $\dim_J R_S \leqslant \dim R_S \leqslant \dim R \leqslant 1$ implies 2 is in the stable range of R_S, by 2.3; and hence we need only show that unimodular pairs are stable. If $A \neq 0$ is any ideal prime to S, then $f_A(S)$ consists of non-0-divisors in R/A. But R/A is quasi-semilocal of dim 0 so every nonunit of R/A is a 0-divisor,—see [*12*], p. 19, (7.1). Therefore $f_A(S) \subset \mathscr{U}(R/A)$. But S is saturated implies $\mathscr{U}(R) \subset S$; and 1 is in the stable range of R implies $\mathscr{U}(R) \to \mathscr{U}(R/A)$ is surjective so $\mathscr{U}(R/A) \subset f_A(S)$. Thus, $\mathscr{U}(R/A) = f_A(S)$, and the corollary follows from 6.6 and 6.7. Q.E.D.

In 6.7 one might hope to conclude that unimodular pairs are stable whenever $\mathscr{Q}(f_A(S)) = \mathscr{S}(f_A(S))$ for every *prime* ideal A such that S is prime to A rather than for every A such that S is prime to A. That this is not the case can be seen from $R = k[X]$, k an algebraically closed field and X an indeterminate. Take $S = \{\alpha X^i, i \geqslant 0, \alpha \neq 0 \in k\}$. Then S is saturated and $R_S = k[X, 1/X]$. Moreover, $f_A(S) = k - \{0\}$ for every prime ideal A of R such that S is prime to A, so $\mathscr{Q}(f_A(S)) = \mathscr{S}(f_A(S))$ for any such prime $A \neq 0$. However 1 is not in the stable range of R_S:

Proof. Let $P = (X - 1)$, $A = P^2$. Then $f_A(S) = \{\alpha[nX - (n-1)] \mid n$ an integer $\geqslant 0$, $\alpha \neq 0$ in $k\}$. $(1 + X)^2 \equiv 4X \bmod A$, so $1 + X \in \mathscr{S}(f_A(S))$. Suppose then $1 + X \in \mathscr{Q}(f_A(S))$, so that there exist $m_1, m_2 \in S$ with $m_1(1 + X) \equiv m_2 \bmod A$. Then there exist integers $n_1, n_2 \geqslant 0$ and $\beta \in k$ such that $(2n_1 + 1)X - 2n_1 + 1 \equiv \beta[n_2 X - (n_2 - 1)]$. Therefore $2n_1 + 1 = \beta n_2$ and $-2n_1 + 1 = \beta(-n_2 + 1)$. Eliminating β, $2n_1 = 2n_2 - 1$, which is impossible. Thus, $\mathscr{Q}(f_A(S)) < \mathscr{S}(f_A(S))$, so 1 is not in the stable range of R_S. Q.E.D.

7. Overrings of Z

We consider now overrings of the integers Z which are contained in the rationals Q. We shall refer to such rings merely as "overrings of Z", understanding thereby a ring $\subset Q$. By a prime in Z we shall, of course, mean an integer $p > 1$ such that (p) is a prime ideal. If $\{p_\alpha\}$ is a collection of primes, then the saturated m.s. generated by the $\{p_\alpha\}$ will consist of all integers of the form $\pm p_1 \cdot \cdots \cdot p_t$, $p_i \in \{p_\alpha\}$. Such a set of primes uniquely determines an overring Z_S of Z. Conversely, any overring of Z is a quotient ring with respect to a m.s.; and if the m.s. is taken to be saturated, then it is uniquely specified by the primes which it contains (see, for example, [4]).

There are two possible extremes among the overrings: (i) S contains *almost all* primes of Z (i.e., all but a finite number of primes), (ii) S contains only finitely many primes. If S is of type (i), then the Z_S are exactly the semilocal overrings; while if S is of type (ii), the Z_S are exactly the finite extensions of Z. As one might then expect, 1 is in the stable range of Z_S of type (i) (since $\dim_J Z_S = 0$); and we prove in 7.2 that 1 is not in the stable range of any Z_S of type (ii). However, we shall construct examples of overrings which are neither of type (i) or (ii) and which show that for such rings both possibilities can occur. Thus, the problem of a complete classification of overrings of Z having 1 in the stable range remains open.

Finally note that for any overring R of Z, $\dim_J R \leqslant \dim R \leqslant 1$; so by

2.3, 2 is in the stable range of R. Therefore we need only check unimodular pairs in determining if 1 is in the stable range of R.

If a is a nonunit of Z, we denote the canonical homomorphism $Z \to Z/(a)$ by f_a. The next theorem provides examples of overrings which do not have 1 in the stable range.

THEOREM 7.1. *Let S be a saturated m.s. of Z. If there exists a nonunit $a \in Z$ such that $f_a(S) < \mathcal{U}(Z/(a))$, then* 1 *is not in the stable range of Z_S.*

Proof. $f_a(S)$ is a multiplicative group in $Z/(a)$, since $m' \in f_a(S)$ implies $(m')^i = 1$ for some i; and then $(m')^{i-1} = (m')^{-1} \in f_a(S)$. Moreover, $f_a(S) \subset \mathcal{U}(Z/a)$ implies (a) is prime to S. Therefore, since $f_a(S) \neq \mathcal{U}(Z/(a))$ by hypothesis, we can apply 6.6 and 6.7 to conclude that 1 is not in the stable range of Z_S.

COROLLARY 7.2. 1 *is not in the stable range of any finite extension of Z.*

Proof. Any finite extension of Z is of the form Z_S, where S is the saturated m.s. determined by primes $p_1, ..., p_t$. By 7.1 it is thus sufficient to see that there exists a prime $p \neq p_i$ such that $\pm 1, p_1, ..., p_t$ do not generate, mod (p), the multiplicative group of the field $Z/(p)$. Since this group is cyclic, it suffices then to exhibit a prime $p > 2$ such that $-1, p_1, ..., p_t$ are quadratic residues mod (p). For example, by quadratic reciprocity ([3], p. 19), a prime of the form $p = 1 + 8p_1 \cdot \cdots \cdot p_t m$ works. Q.E.D.

Note that the proof of 7.1 only uses the fact that $\mathcal{U}(Z/(a))$ is a torsion group; so it seems likely that at least part of what follows will extend to more general rings.

We can apply 7.1 to construct other Z_S which do not have 1 in the stable range. For example, if a is a prime > 3, let $S(a)$ be the saturation of the m.s. generated by $\{\text{primes } p \mid p \equiv 1 \bmod (a)\}$. Then $m \in S(a)$ implies $m \equiv \pm 1 \bmod (a)$; so $2 \in \mathcal{U}(Z/(a)), \notin f_a(S)$. Thus, 1 is not in the stable range of Z_S. One can more generally, for a given a, take all primes congruent to the elements of a *proper* m.s. of $\mathcal{U}(Z/(a))$ containing -1, and then let S be the saturation of the m.s. generated by these primes. Again by 7.1, 1 is not in the stable range of Z_S.

We now turn to the construction of overrings which do have 1 in the stable range.

LEMMA 7.3. *Let D be a principal ideal domain and let S be a saturated m.s. of D. Then the following are equivalent:*

(i) 1 *is in the stable range of D_S;*

(ii) *if* (a_1, a_2) *is a unimodular sequence of* D *such that the* a_i *are relatively prime to every element of* S, *then there exist* $m \in S$, $b \in D$ *such that* $a_1 m + a_2 b \in S$.

Proof. (i) $\Rightarrow$ (ii): immediate.

(ii) $\Rightarrow$ (i): Since $\dim_J D_S \leqslant \dim D_S \leqslant 1$, we need only check that unimodular pairs are stable. Suppose then $(a_1', a_2') = D_S$, $a_i' \in D_S$. Then $a_i' = a_i/m_i$, $a_i \in D$, $m_i \in S$. $(a_1, a_2) = (a)$; and $(a_1, a_2) D_S = D_S$ implies $(a_1, a_2) \cap S \neq \emptyset$, so $a \in S$ since S is saturated. Now write $a_i = b_i n_i a$, where $(b_1, b_2) = D$ and $n_i \in S$, and the b_i are relatively prime to the elements of S. By (ii) there exists $m \in S$, $b \in D$ such that $b_1 m + b_2 b \in S$. Therefore, multiplying by $n_1 n_2 a$, $a_1(mn_2) + a_2(bn_1) \in S$. Thus, $a_1 + (bn_1/mn_2)\, a_2$ is a unit of D_S.

THEOREM 7.4. *Suppose* S *is a saturated m.s. of* Z *and there exist* $a \neq 0$, $u \in Z$ *such that*

(i) $f_a(S) \supset \mathscr{U}(Z/(a))$,

(ii) $f_a(u) \in \mathscr{U}(Z/(a))$,

and $p \equiv u \bmod (a)$ *implies* $p \in S$ *for almost all primes* p. *Then* 1 *is in the stable range of* Z_S.

Proof. By 7.3 it is sufficient to show that for every unimodular sequence (a_1, a_2) of Z such that the a_i are relatively prime to the elements of S there exist $m \in S$, $b \in Z$ such that $a_1 m + a_2 b \in S$. By Dirchlet's theorem there exists a prime $p_1 \equiv a_1 \bmod a_2$ such that $p_1 \nmid a$. If $p_1 \in S$, we are done; so suppose $p_1 \notin S$. Since $p_1 \nmid a$, p_1 is a unit mod (a). Therefore by (i), there exists $m_1 \in S$ such that $(p_1 u)\, m_1 \equiv 1 \bmod (a)$. Then $(p_1 m_1, aa_2) = Z$; so again by Dirchlet's theorem, there exists a prime p not in the finite exceptional set of (ii) such that $p_1 m_1 p \doteq 1 \bmod (aa_2)$. Then a fortiori $p_1 m_1 p \equiv 1 \bmod (a)$; so $p \equiv u \bmod (a)$, and hence by (ii), $p \in S$. Thus, $a_1(m_1 p) \equiv 1 \bmod (a_2)$ is the required expression. Q.E.D.

Observe that any semi-local overring of Z satisfies the conditions of 7.4; for if $p_1, \ldots, p_t$ are the primes which are nonunits of such a ring, then one need only choose $a = p_1 \cdot \cdots \cdot p_t$. Theorem 7.4 can be used to construct other Z_S having 1 in the stable range as follows:

Let a be an integer > 1, and choose $u \in Z$ such that $f_a(u) \in \mathscr{U}(Z/(a))$. Let S be the saturation of the m.s. generated by *all* primes p such that $p \equiv u \bmod (a)$ and enough other primes $p_1, \ldots, p_t$ such that $f_a(S) = \mathscr{U}(Z/(a))$. Then 1 is in the stable range of Z_S.

Instead of taking all primes $p \equiv u \bmod (a)$, we could delete a finite number of such primes; and 7.4 would still apply. In such a way, one constructs an infinite descending chain of overrings of Z having 1 in the stable range; and moreover, such a chain of overrings can be chosen to have intersection Z.

Let us consider a special case. For example, let $a = 5$, and let S be the saturation of the m.s. generated by 2 and all primes p such that $p \equiv 1 \bmod (5)$. Then $S = \{\pm 1, \pm 2, \pm p\}$ $p \equiv 1 \bmod (5)$. By the above, 1 is in the stable range of Z_S. Note however that by 7.1, 1 is not in the stable range of $Z_{S'}$, where S' is the saturation of the m.s. generated by the primes $\equiv 1 \bmod (5)$. Moreover, $Z_S = Z_{S'}[\frac{1}{2}]$; so Z_S is even a finite extension of $Z_{S'}$: In particular then, 7.2 does not even generalize to overrings of Z.

This last observation can be put more generally:

COROLLARY 7.5. *Suppose S is a saturated m.s. of Z and there exist $a \neq 0$, $u \in Z$ which satisfy* (ii) *of 7.4. Then* 1 *is in the stable range of a finite extension of Z_S.*

Proof. Let $p_1, ..., p_t$ be a set of primes $< a$ which with 1 generate $\mathcal{U}(Z/(a)$, mod (a); and let S' be the saturation of the m.s. generated by S and the p_i. By 7.4, 1 is in the stable range of $Z_{S'} = Z_S[1/p_1 \cdots p_t]$.

Q.E.D.

We conclude this section by proving that 1 is not in the stable range of any ring of algebraic integers.

PROPOSITION 7.6. *Let D be an integrally closed domain with quotient field K, and let D' be the integral closure of D in a finite separable extension K' of K. Then there exists an integer n such that if (a, b) is a unimodular sequence of D which is stable in D', then (a^n, b) is stable in D.*

Proof. By going to a possibly larger field, we may assume that K' is a normal extension of K. (a, b) is stable in D' implies there exists $d' \in D'$ such that $a + d'b$ is a unit of D'. Therefore, if d_i', $i = 1, ..., n$, are the conjugates of d' over K, then $\prod_{i=1}^{n} (a + d_i'b) = a^n + db$ is a unit of D. Moreover, $d \in K \cap D' = D$; so we are done.

COROLLARY 7.7. 1 *is not in the stable range of the ring of algebraic integers of any finite algebraic number field.*

Proof. Take $a = 2$ and b an odd integer which does not divide $a^n \pm 1$.

Q.E.D.

Throughout this section we have used specific properties of the integers, e.g., Dirchlet's theorem, or that $Z/(a)$ is finite. Question: Do analogous results exist for $k[X]$?

8. Stable Triples

If R is a principal ideal domain and X is an indeterminate, then $\dim_J R[X] \leqslant \dim R[X] \leqslant 2$; so 3 is always in the stable range of $R[X]$. We are concerned in this section with the question of when 2 is in the stable range of $R[X]$. To begin, we let R denote an arbitrary ring (of course, commutative with identity), and we fix the following notation: If s, t are positive integers with $s \leqslant t$, $\mathbf{M}(R, s \times t)$ is the set of $s \times t$ matrices with entries from R, $\mathbf{GL}(R, s \times t)$ is the set of $s \times t$ matrices whose $s \times s$ subdeterminants generate the unit ideal and $\mathbf{SL}(R, s \times s)$ denotes the $s \times s$ matrices of determinant 1. By an elementary matrix of $\mathbf{M}(R, s \times s)$, we mean a matrix of the form $I + aE_{ij}$, $i \neq j$, where $I = s \times s$ identity matrix and $E_{ij} = s \times s$ matrix with 0 everywhere except in the (i, j)th place, and 1 there.

If $M_1 \in \mathbf{M}(R, s_1 \times t)$ and $M_2 \in \mathbf{M}(R, s_2 \times t)$, we shall use the notation $M_1 \times M_2$ to denote the matrix of $\mathbf{M}(R, (s_1 \times s_2) \times t)$ having its first s_1 rows equal to those of M_1 and its bottom s_2 rows equal to those of M_2. We now consider the following condition on R, which merely says that every unimodular s-vector, $s \geqslant 2$, can be filled out to an $s \times s$ matrix of determinant 1:

(Condition s^*). For every $\alpha \in \mathbf{GL}(R, 1 \times s)$ there exists $M \in \mathbf{M}(R, (s-1) \times s)$ such that $\alpha \times M \in \mathbf{SL}(R, s \times s)$.

Any R satisfies 2^*. Moreover, Kaplansky ([8], p. 469, Theorem 3.7) has shown that a Bezoutian domain satisfies s^* for all s; Seshadri [14] has shown that $R[X]$ satisfies s^* for all s when R is a principal ideal domain and X an indeterminate; and it is a famous open question of Serre ([13], 23, p. 12) whether $k[X_1, ..., X_n]$ satisfies s^* for all s (the answer being "yes" for $n = 1, 2$).

Proposition 8.0. *If R satisfies s^* and s is in the stable range of R, then R satisfies t^* for all $t \geqslant s$.*

Proof. If $a_i' = a_i + ab_i$, $i = 1, ..., s$, then

$$\det \begin{bmatrix} a_1' & \cdots & a_s' \\ & M & \end{bmatrix} = \det \begin{bmatrix} a_1 & \cdots & a_s & a \\ & M & & \\ -b_1 & \cdots & -b_s & 1 \end{bmatrix}$$

Q.E.D.

Example. Let k = reals, $k_n = k[X_1, ..., X_n]$, $n \geqslant 2$, and let $k_n' = k[X_1, ..., X_n]/(p_n(X))$, where $p_n(X) = X_1^2 + \cdots + X_n^2 - 1$. It is known ([15], p. 270) that k_n' does not have property n^* for $n \neq 2, 4, 8$; and, in fact, the unimodular vector $(X_1', ..., X_n')$ of k_n' cannot be filled out to an $n \times n$ matrix of determinant 1 for these n.

CLAIM. *If* $(X_1, ..., X_n, p_n)$ *is stable in* k_n, *then* k_n *does not have property* m^*, *for all* $m \geqslant n \geqslant 2$.

Proof. First observe that $(X_1, ..., X_n, p_n)$ is stable in k_n implies that $(X_1, ..., X_m, p_m)$ is stable in k_m, for all $m \geqslant n$; for

$$(X_1 + a_1 p_n, ..., X_n + a_n p_n) \subset (X_1 + a_1 p_m, ..., X_n + a_n p_m, X_{n+1}, ..., X_m)$$

if $a_i \in k_n$. Thus it is sufficient to show that k_n does not have property n^*.

Suppose k_n does have n^*. Since $(X_1, ..., X_n, p_n)$ is stable, there exist $a_i \in k_n$ such that if $Y_i = X_i + a_i p_n$, then $1 \in (Y_1, ..., Y_n)$. By n^*, $(Y_1, ..., Y_n)$ can be filled out to a matrix of determinant 1 over k_n; and then reducing mod p_n, we can fill out $(X_1', ..., X_n')$ to a matrix of determinant 1 in k_n'. By our introductory remarks, this implies $n = 2$, 4, or 8. However,

$$1 = \det \begin{bmatrix} Y_1 & \cdots & Y_n \\ & M & \end{bmatrix} = \det \begin{bmatrix} X_1 & \cdots & X_n & p_n, & X_{n+1} \\ & M & & 0 & 0 \\ -a_1 & \cdots & -a_n & 1 & 0 \\ 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

$$= \det \begin{bmatrix} X_1 & \cdots & X_n & X_{n+1} & p_{n+1} \\ & M & & 0 & 0 \\ X_{n+1}a_1 & \cdots & X_{n+1}a_n & 1 & 0 \\ -a_1 & \cdots & -a_n & 0 & 1 \end{bmatrix},$$

the sequence of events being (i) col. $(n + 1) + X_{n+1}$ col. $(n + 2)$, (ii) col. $(n + 1) \leftrightarrow$ col. $(n + 2)$, (iii) row $(n + 1) \leftrightarrow$ row $(n + 2)$, (iv) row $(n + 1) - X_{n+1}$ row $(n + 2)$. Now reduce mod p_{n+1} to conclude that $X_1', ..., X_{n+1}'$ can be filled out to a matrix of determinant 1 over k_{n+1}. However, $n + 1 \neq 2$, 4, 8; so this is impossible. Q.E.D.

Since any ring has property 2^*, we conclude:

COROLLARY 8.1. $(X_1, X_2, X_1^2 + X_2^2 - 1)$ *is not stable in* $k[X_1, X_2]$, *k the real numbers.*

If a is a nonunit of R, the homomorphism $R \to R/(a)$ induces a map of $\mathbf{M}(R, s \times t) \to \mathbf{M}(R/(a), s \times t)$. We shall use $'$ for elements of $R/(a)$; and when we remove the $'$ with no reservations, we are merely denoting an arbitrary element of the inverse image.

PROPOSITION 8.2. $\mathbf{SL}(R, s \times s) \to \mathbf{SL}(R/(a), s \times s)$ *is surjective if and only if* $\mathbf{GL}(R, (s - 1) \times s) \to \mathbf{GL}(R/(a), (s - 1) \times s)$ *is surjective.*

Proof. $\Rightarrow$: If $M' \in \mathbf{GL}(R/(a), (s - 1) \times s)$, then

$$M' \times \alpha' \in \mathbf{SL}(R/(a), s \times s)$$

for some $\alpha' \in \mathbf{M}(R/(a), 1 \times s)$. Now lift to an element $M \times \alpha \in \mathbf{SL}(R, s \times s)$. Then M is the required matrix.

$\Leftarrow$: Let $M' \in \mathbf{SL}(R/(a), s \times s)$. $M' = M_1' \times \alpha'$, $M_1' \in \mathbf{GL}(R/(a), (s-1) \times s)$, $\alpha' \in \mathbf{M}(R/(a), 1 \times s)$. By hypothesis, M_1' lifts to an element $M_1 \in \mathbf{GL}(R, (s-1) \times s)$. Then $M_1 \times \alpha \equiv M \bmod (a)$ implies $\det(M_1 \times \alpha) = 1 + ba$, $b \in R$. But since $M_1 \in \mathbf{GL}(R, (s-1) \times s)$, there exists $\beta \in \mathbf{M}(R, 1 \times s)$ such that $\det(M_1 \times \beta) = b$. Therefore $\det(M_1 \times (\alpha - a\beta)) = 1$, so $M_1 \times (\alpha - a\beta)$ is the required matrix. Q.E.D.

At the present we are only concerned with these things for $s = 2$. Since $\mathbf{GL}(R, 1 \times s) \to \mathbf{GL}(R/(a), 1 \times s)$ is surjective if and only if every unimodular sequence $(a_1, ..., a_s, a)$ is stable, we have the following corollary.

COROLLARY 8.3. *$SL(R, 2 \times 2) \to SL(R/(a), 2 \times 2)$ is surjective if and only if every unimodular sequence (a_1, a_2, a) is stable, $a_i \in R$.*

LEMMA 8.4. *If $M = (m_{ij}) \in GL(R, s \times s)$, then $(a_1, ..., a_s, a)$ is stable if and only if $(a_1', ..., a_s', a)$ is stable, where $a_i' = \sum m_{ij} a_j$.*

Proof. If $b_i' = \sum m_{ij} b_j$, then

$$(a_1' + ab_1', ..., a_s' + ab_s') \subset (a_1 + ab_1, ..., a_s + ab_s).$$

The reverse inclusion follows by using M^{-1}.

LEMMA 8.5. *Let (a_1, a_2, a) be a unimodular sequence from R, and let n be an integer $\geqslant 1$. Then (a_1, a_2, a) is stable implies (a_1, a_2, a^n) is stable.*

Proof. (a_1, a_2, a) is stable implies there exist $b_1, b_2 \in R$ such that $(a_1 + b_1 a, a_2 + b_2 a) = R$. Then $\det M = 1$ for some

$$M = \begin{bmatrix} d_1 & d_2 \\ -a_2 - b_2 a & a_1 + b_1 a \end{bmatrix}, \qquad d_i \in R.$$

Let (a_1', a_2') be the result of applying M to the column vector (a_1, a_2). Then $(a_1', a_2') \equiv (1, 0) \bmod (a)$; and by 8.4, (a_1, a_2, a) is stable if and only if (a_1', a_2', a) is stable. But $a_1' = 1 - c_1 a$, $a_2' = c_2 a$, $c_i \in R$. Therefore let $b_2' = -c_1^{n-1} c_2 + a$. Then $a_2' + b_2' a^n \equiv a^{n+1} \bmod (a_1')$; so any maximal ideal containing $(a_1', a_2' + b_2' a^n)$ also contains (a_1', a_2', a). Thus $(a_1', a_2' + b_2' a^n) = R$.

LEMMA 8.6. *If $(a_1, ..., a_s, a)$ is a unimodular stable sequence and $b \mid a$, then $(a_1, ..., a_s, b)$ is also stable.*

Proof. $(a_1 + b_1 a, ..., a_s + b_s a) = R$ and $a = a'b$ imply

$$(a_1 + (b_1 a')\, b, ..., a_s + (b_s a')\, b) = R.$$

COROLLARY 8.7. *Let* $(a_1, a_2, b_1^{t_1} \cdot \ldots \cdot b_s^{t_s})$ *be a unimodular sequence. Then* $(a_1, a_2, b_1^{t_1} \cdot \ldots \cdot b_s^{t_s})$ *is stable if and only if* $(a_1, a_2, b_1 \cdot \cdots \cdot b_s)$ *is stable.*

Proof. $\Rightarrow$: Apply 8.6.

$\Leftarrow$: $(a_1, a_2, b_1 \cdot \ldots \cdot b_s)$ is stable implies $(a_1, a_2, b_1{}^t \cdot \ldots \cdot b_s{}^t)$ is stable, by 8.5. Choosing t sufficiently large and applying 8.6, we get $(a_1, a_2, b_1^{t_1} \cdot \ldots \cdot b_s^{t_s})$ stable. Q.E.D.

THEOREM 8.8. *Let R be a principal ideal domain, and let* (a_1, a_2, a) *be a unimodular sequence with* $a_1, a_2 \in R[X]$ *and* $a \in R$. *Then* (a_1, a_2, a) *is stable.*

Proof. By 8.7 it is sufficient to consider the case where $a = p_1 \cdot \ldots \cdot p_s$, p_i distinct primes; and by 8.3 we must show that for such an a, $\mathbf{SL}(R[X], 2 \times 2) \to SL(R[X]/(a), 2 \times 2)$ is surjective. Since $R/(a) \cong k_1 \oplus \cdots \oplus k_n$, k_i a field, $R[X]/(a) \cong k_1[X] \oplus \cdots \oplus k_n[X]$. Thus, $R[X]/(a)$ is a direct sum of Euclidean domains. By a well known proof, if E is a Euclidean domain, then any element of $\mathbf{SL}(E, s \times s)$ can be written as a product of elementary matrices; and this property immediately extends to a direct sum of Euclidean domains. In particular then, any element of $\mathbf{SL}(R[X]/(a), 2 \times 2)$ is a product of elementary matrices. Since an elementary matrix lifts trivially we can then lift any element of $\mathbf{SL}(R[X]/(a), 2 \times 2)$ to an element of $\mathbf{SL}(R[X], 2 \times 2)$. Q.E.D.

Remark. Conversations with William Heinzer after this paper was prepared have led to the following observation:

Let D_0, D be integral domains with quotient fields K_0, K respectively. Assume D_0 is integrally closed and D is integral over D_0 and that $[K : K_0]$ is finite. Then the argument of 7.6 yields: if $a, b \in D_0$ and (a, b) is stable in D, then (a^q, b) is stable in D_0 for some $q \leqslant [K : K_0]$. Applying the normalization theorem ([*16*], Vol. 2, p. 200), we have the following theorem: *If a domain D is a finitely generated extension of a field k such that the transcendence degree of D over k is* $\geqslant 1$, *then* 1 *is not in the stable range of D.*

REFERENCES

1. BASS, H. K-theory and stable algebra. *Publ. Inst. Hautes Etudes Sci.*, No. 22 (1964).
2. BOURBAKI, N. "Algébre Commutative." Chapters 1–7. Hermann, Paris, (1961–1965).
3. COHN, H. "A Second Course in Number Theory." Wiley, New York, 1962.
4. GILMER, R. AND OHM, J. Integral domains with quotient overrings. *Math. Ann.* **153** (1964), 97-103.
5. GROTHENDIECK, A. *Publ. Inst. Hautes Etudes Sci.*, No. 20 (1964).

6. Jaffard, P. Dimension des anneaux de polynomes. I. *Sem. Dubreil*, No. 20, (1957-58).
7. Jaffard, P. Théorie de la dimension dans les anneaux de polynomes. *Mem. Sci. Math.*, No. 136 (Gauthier-Villars, Paris, 1960).
8. Kaplansky, I. Elementary divisors and modules. *Trans. Am. Math. Soc.* **66** (1949), 464-491.
9. Krull, W. Beitrage zur Arithmetik kommutativer Integritatsbereiche. I. *Math. Z.* **41** (1936), 544-577.
10. Krull, W. Beitrage zur Arithmetik kommutativer Integritatsbereiche. II. *Math. Z.* **41** (1936), 665-679.
11. Krull, W. Jacobsonsche Ringe, Hilbertscher Nullenstellensatz, Dimensiontheorie. *Math. Z.* **54** (1951), 354-387.
12. Nagata, M. "Local Rings." Interscience, New York, 1962.
13. Serre, J.-P. Modules projectifs et éspaces fibres á fibre vectorielle, *Sem Dubreil*, No. 23 (1957-58).
14. Seshadri, C. S. Trivality of vector bundles over the affine space K^2, *Proc. Natl. Acad. Sci. U.S.* **44** (1958).
15. Swan, R. G. Vector bundles and projective modules, *Trans. Am. Math. Soc.* **105** (1962).
16. Zariski, O. and Samuel, P. "Commutative Algebra," Vol. I. van Nostrand, Princeton, New Jersey, 1958.