ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 13, Number 4, Fall 1983

# KRULL-SCHMIDT UNIQUENESS FAILS DRAMATICALLY OVER SUBRINGS OF $Z \oplus \cdots \oplus Z$

LAWRENCE S. LEVY

This paper is dedicated to Professor Goro Azumaya on the occasion of his sixtieth birthday.

**Introduction.** We give a simple set of examples, illustrating the many ways that uniqueness of direct sum decompositions of finitely generated modules fails to hold over certain subrings $R$ of $Z \oplus \cdots \oplus Z$. Specifically, we show the following four results.

(1) For every $m \geqq 2$ there is a module $M$ over one of these rings $R$ such that $M$ can be expressed as the direct sum of $k$ indecomposable modules for every $k$ with $2 \leqq k \leqq m$.

(2) Direct sum cancellation, $M \oplus C \cong N \oplus C \Rightarrow M \cong N$, fails to hold over $R$.

(3) The $n$-th root property, $\oplus^n M \cong \oplus^n N \Rightarrow M \cong N$, fails to hold over $R$.

(4) Interchange of localizations property. There are four non-isomorphic, indecomposable modules $H$, $K$, $M$, $N$ such that $H \oplus K \cong M \oplus N$, and two maximal ideals $P$, $Q$ of $R$ such that

$$H_P \cong M_P \not\cong K_P \cong N_P \text{ but } H_Q \cong N_Q \not\cong K_Q \cong M_Q.$$

Here $Z$ can be taken to be the ring of integers. But the results we obtain are much more general. In Examples (1) and (4), $Z$ can be any integral domain with at least four maximal ideals. If this $Z$ is noetherian, then $R$ will be a module-finite $Z$-algebra. (See "Fixed Notation and Generality" below.)

In order to obtain examples (2) and (3), the ring $Z$ must satisfy an additional non-triviality condition involving non-liftability of units modulo maximal ideals to units of $Z$ itself. The precise conditions needed will be stated in Examples 4.4 and seem to be satisfied by most integral domains with infinitely many maximal ideals.

We also obtain some other related examples, as by-products of the methods used to obtain (1)–(4). The first are the simplest examples I know of modules with properties (5)–(7) below (See §5.)

Received by the editors on December 9, 1981, and in revised form on September 17, 1982.

(5) $M$ is indecomposable but, for some maximal ideal $P$, $M_P$ is not.

(6) $M$ is a projective of rank one such that $(\forall n)\oplus^n M \not\cong \oplus^n R$.

(7) $M$ and $N$ Noetherian modules such that $M_P \cong N_P$ for every maximal ideal $P$, but $M \not\cong N$.

In (6), $Z$ cannot be taken to be the integers. But the polynomial ring $Z = F[x]$ — where $F$ is any field which is not an algebraic extension of a finite field — will do for (6), in fact for all of (1)–(7).

We provide a bit of insight into K. R Goodearl's "power cancellation" by providing an example of a module-finite algebra $R$ over a PID such that the finitely generated $R$-modules fail to satisfy power cancellation. (See §5.)

For non-Noetherian modules $M$ there is a more extreme version of example (1) above, due to B.L. Osofsky **[11]**, which satisfies property (8) below.

(8) For every finite $m \geqq 2$, $M$ is the direct sum of $m$ indecomposable modules, but $M$ is not the direct sum of infinitely many submodules.

In the Appendix we briefly sketch how to obtain this from our methods.

**Background.** The classical Krull-Schmidt theorem states that, if $\oplus_{i=1}^m M_i \cong \oplus_{i=1}^n N_i$ with each $M_i$ and $N_i$ indecomposable and each $M_i$ of finite length, then $m = n$ and (after a suitable renumbering of the $N_i$) each $M_i \cong N_i$.

Azumaya's well-known generalization of this "Krull-Schmidt uniqueness" **[1]** was motivated by a desire to remove the strong finiteness restrictions above. The "finite length" condition is replaced by the condition that the ring of endomorphisms of each $M_i$ be a local ring; and when this is done, the number of direct summands can even be allowed to be infinite.

Our examples are intended to complement Azumaya's theorem by showing that Krull-Schmidt uniqueness can fail very badly, even in the presence of the following strong finiteness conditions: when $Z$ denotes the integers, the additive group of every module occuring in (1)–(4) is free of finite rank; and the rings $R \subseteqq Z \oplus \cdots \oplus Z$ are all commutative Noetherian rings of Krull dimension one.

We remark that bizarre direct-sum behavior of non-Noetherian modules has already been well documented. See **[3, 4, 11]** and the partly expository paper **[14]**.

It seems worthwhile to remark here that the following question of Krull [**9**, p. 38] apparently remains unanswered. To obtain Krull-Schmidt uniqueness, does it suffice to require that each summand $M_i$ satisfy the minimum condition? (For a partial answer see **13**, Proposition 5].)

For readers who would prefer to see our examples over an integral domain $R$, we note the following theorem.

THEOREM 0.1. *Examples* (1)–(5) *can all occur for finitely generated* *modules over the polynomial ring* $R = \mathbf{Z}[x]$, where $\mathbf{Z}$ is *the ring of integers*; *in fact, for modules whose additive group is free of finite rank.*

To prove this, we note that there is a ring homomorphism of $\mathbf{Z}[x]$ onto the integral group ring $\mathbf{Z}G_n$ of the cyclic group $G_n$ of arbitrary order $n$. In **[10]** it is shown that examples (1)–(5) can all be realized as $\mathbf{Z}G_n$-modules, for suitable $n$, hence also as $\mathbf{Z}[x]$-modules.

The methods used here are, in fact, adapted from those in **[10]**. However, the proofs in the present paper are much easier and more general than the long, intricate proofs found in **[10]**.

In connection with the above theorem, I do not know whether $R$ can be chosen to be an integral domain of Krull dimension one in examples of type (1) above. Roger Wiegand has recently shown that cancellation (2) can fail in this setting **[15]**. And failure of $n$-th root uniqueness (3) is well-known over Dedekind domains with torsion class group.

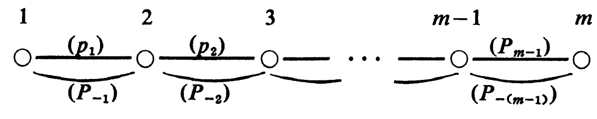
We introduce the rings $R$ which will be used in §1 and the necessary $R$-modules in §2. The examples of (1)–(7) are presented in §§2–5, as immediate applications of the theorems stated in §2, and proved in §§5–8.

The method of proof of the main module isomorphism theorem, 2.1, is to transform it to a problem about matrices over fields, and then actually carry out the necessary matrix reductions. This is done in §8, and is the only complicated part of this paper.

**Fixed notation and generality 0.2.** Throughout the rest of this paper $Z$ denotes a commutative ring such that $Z$ is an indecomposable ring with at least four maximal ideals; and the intersection of these four maximal ideals has zero annihilator in $Z$. This paper is written so that, for a first reading, the reader can take $Z$ to be the ring of integers. The term "module", when used in this paper, always means finitely generated module.

I would like to thank Hyeja Byun, Roger Wiegand, and the referee for many helpful suggestions.

**1.** $R$, $\mathbf{R}$, **graph w**, $S(\mathbf{w})$. The notation introduced in this section will remain in force throughout this paper. Let $m$ be an integer greater than one. Form graph $G$ below, consisting of $m$ vertices, with each pair of consecutive vertices joined by two edges (contrary to the usual definition of "graph", which permits at most one edge to join two vertices).

(G) 


If $Z$ denotes the integers, choose a sequence of distinct maximal ideals, labeled $P_1$, $P_{-1}$, $P_2$, $P_{-2}$, ..., to use as labels of the edges of $G$. Thus, for each $i$, edge $(P_i)$ joins vertex $|i|$ to vertex $|i| + 1$. For more general $Z$, as in 0.2, let $P_1, P_{-1}, P_2, P_{-2}, \ldots$, be any sequence of maximal ideals such that the two or four maximal ideals which meet at each vertex of $G$ are always distinct, and such that $\bigcap_{|i|=1}^{m-1} P_i$ has zero annihilator in $Z$.

Let $R$ be the ring

(1.1) $R = \{(r_1, \ldots, r_m) \in \oplus^m Z \mid r_i \equiv r_{i+1} \pmod{P_i \text{ and } P_{-i}} (\forall i \leqq m-1)\}$.

The graph $G$ is intended to help the reader visualize that for an element $r = (r_1, \ldots, r_m)$ of $\oplus^m Z$ to belong to $R$, $r_1$ must be congruent $r_2$ modulo both ideals $P_1$ and $P_{-1}$, and so on for each pair of consecutive coordinates.

LEMMA 1.2. *Let $b \in \bigcap_{\pm i} P_i$. Then, for every choice of $z_1, z_2, \ldots$, in $Z$, $(bz_1, bz_2, \ldots, bz_m) \in R$.*

PROOF. This follows from the fact that, for any $z \in Z$, $bz \equiv 0$ modulo every $P_i$ and $P_{-i}$.

Next, let $\mathbf{R}$ be the direct sum of all the fields $Z/P_i$ and $Z/P_{-i}$; that is $\mathbf{R} = \bigoplus_{|i|=1}^{m-1} Z/P_i$. We will write elements of $\mathbf{R}$ as boldface letters $\mathbf{w}$. Coordinate $i$ of $\mathbf{w}$—with $i$ positive or negative—will be denoted by $\bar{w}_i$ where $\bar{w}_i \in Z/P_i$.

For each $\mathbf{w} \in \mathbf{R}$ we define graph $\mathbf{w}$ to be the graph obtained from $G$ by deleting edge $P_i$ whenever $\bar{w}_i = 0$. Thus,

(1.3) graph $\mathbf{0}$ consists of $m$ vertices and no edges, and graph $\mathbf{1} = G$.

Finally, for $\mathbf{w}$ in $\mathbf{R}$ we define an $R$-module $S(\mathbf{w}) \subseteqq \oplus^m Z$. For each coordinate $\bar{w}_i$, with $i$ positive or negative, choose a pre-image $w_i$ in $Z$. Then let $S(\mathbf{w})$ be the set of all elements $s = (s_1, \ldots, s_m)$ in $\oplus^m Z$ such that, for $1 \leqq i \leqq m-1$,

$$(1.4) \qquad \begin{aligned} s_i w_i &\equiv s_{i+1} \pmod{P_i} \text{ if } w_i \notin P_i, \text{ and} \\ s_i w_{-i} &\equiv s_{i+1} \pmod{P_{-i}} \text{ if } w_{-i} \notin P_{-i}. \end{aligned}$$

Note that, given $\mathbf{w}$ in $\mathbf{R}$, (1.4) contains one congruence for each edge in graph $\mathbf{w}$. Also note that $S(\mathbf{w})$ is clearly an additive subgroup of $\oplus^m Z$, and is completely determined by $\mathbf{w}$. Observe that

$$(1.5) \qquad S(\mathbf{0}) = \oplus^m Z \text{ and } S(\mathbf{1}) = R.$$

The first of these is true because graph $\mathbf{0}$ has no edges [see (1.3)], so there are no congruences to satisfy. The second is seen to be true by comparing (1.4) and (1.1).

It follows immediately from (1.4) that $S(\mathbf{v}) \cdot S(\mathbf{w}) \subseteqq S(\mathbf{vw})$. Setting $\mathbf{v} = \mathbf{1}$ we see that $R\,S(\mathbf{w}) \subseteqq S(\mathbf{w})$. Hence $S(\mathbf{w})$ is an $R$-module.

**2. Main theorems.** Let $\mathbf{w}(1), \ldots, \mathbf{w}(n)$ be elements of $\mathbf{R}$.

THEOREM 2.1. *A full set of invariants for the R-isomorphism class of any direct sum* $S(\mathbf{w}(1)) \oplus \cdots \oplus S(\mathbf{w}(n))$ *is*

(i) *the number n of summands*;

(ii) (*Graph invariant*) *for each i, positive or negative, the number of* $\mathbf{w}(j)$ *such that coordinate i of* $\mathbf{w}(j)$ *is nonzero* [*that is, for each i, the number of* $\mathbf{w}(j)$ *such that edge* $(P_i)$ *appears in graph* $\mathbf{w}(j)$] *and*

(iii) (*Units invariant*) *the* $\mathcal{U}$*-congurence class* (*defined below*) *of the product* $\mathbf{w}(1)\mathbf{w}(2) \ldots \mathbf{w}(n)$.

Two elements $\mathbf{v}$ and $\mathbf{w}$ of $\mathbf{R}$ are called *congruent modulo liftable units*, notation $\mathbf{v} \equiv \mathbf{w} \pmod{\mathcal{U}}$, provided there exist units $u_i$ in $Z$ such that, for $1 \leqq i \leqq m - 1$,

$$(2.2) \qquad \bar{v}_i = \bar{w}_i u_i \quad (\text{in } Z/P_i) \text{ and } \bar{v}_{-i} = \bar{w}_{-i} u_i \quad (\text{in } Z/P_{-i}).$$

The products in (2.2) make sense because $Z/P$ is a $Z$-module. But note that the subscript attached to $u$ is $+i$ both times. Of course, when $Z$ denotes the integers, then each $u_i = \pm 1$.

Note that the modules $S(\mathbf{w})$ need not be indecomposable. The extreme case is $S(\mathbf{0}) = \bigoplus^m Z$, which is the direct sum of $m$ $R$-modules.

THEOREM 2.3. *For* $\mathbf{w}$ *in* $\mathbf{R}$ *suppose graph* $\mathbf{w}$ *has s connected components. Then* $S(\mathbf{w})$ *is the direct sum of s indecomposable R-modules.*

COROLLARY 2.4. (of Theorem 2.1) *If all coordinates of* $\mathbf{w}$ *are nonzero, then* $S(\mathbf{w})$ *is a projective R-module.*

PROOF. $S(\mathbf{w}) \oplus S(\mathbf{w}^{-1}) \cong S(\mathbf{1}) \oplus S(\mathbf{1}) = R \oplus R$, by Theorem 2.1 and (1.5)

In Proposition 5.6 we sketch a proof of the converse of the this corollary.

**3. Number of indecomposable summands.** Let $E$ be the set of edges of $G$. For any subset $X \subseteqq E$, let $\mathbf{e}(X)$ be the element of $\mathbf{R}$ such that coordinate $i$ of $\mathbf{e}(X) = 1$ if edge $(P_i) \in X$ and $= 0$ if edge $(P_i) \notin X$.

LEMMA 3.1 *For any partition* $E = X \cup Y$ *of* $E$ *into disjoint subsets, we have* $S(\mathbf{e}(X)) \oplus S(\mathbf{e}(Y)) \cong R \oplus S(\mathbf{0})$ *as R-modules.*

PROOF. Recall that $R = S(\mathbf{1})$. Disjointness of $X$ and $Y$ shows that $\mathbf{e}(X)\cdot\mathbf{e}(Y) = \mathbf{0} = \mathbf{1}\cdot\mathbf{0}$. The lemma now follows immediately from Theorem 2.1.

EXAMPLE 3.2. (Recall that $R \subseteqq \bigoplus^m Z$ with $m \geqq 2$.) $R \oplus S(\mathbf{0})$ is the direct sum of $s$ indecomposable $R$-modules for every $s$ in the interval $2 \leqq s \leqq m + 1$.

PROOF. Let $X$ be the set of all edges $(P_i)$ of $G$ for which $i > 0$, and $Y$ the set of edges for which $i < 0$. Then

(1) $$E = X \bigcup Y \qquad \text{(disjoint union).}$$

Moreover, graph $\mathbf{e}(X)$ (all upper edges of $G$) and graph $\mathbf{e}(Y)$ (all lower edges of $G$) are connected graphs, so $S(\mathbf{e}(X))$ and $S(\mathbf{e}(Y))$ are indecomposable $R$-modules by Theorem 2.3. Then Lemma 3.1 establishes the decomposition needed for $s = 2$.

Now modify $X$ and $Y$ by removing edge $(P_{-1})$ from $Y$ and putting it into $X$. Then (1) still holds, and graph $\mathbf{e}(X)$ remains connected. On the other hand, graph $\mathbf{e}(Y)$ has two connected components, so $S(\mathbf{e}(Y))$ is the direct sum of two indecomposable $R$-modules. Lemma 3.1 now establishes the decomposition needed for $s = 3$. Moving edge $(P_{-2})$ from $Y$ to $X$ does $s = 4$. Continuing in this way, we eventually reach $X = E$ and $Y = \varnothing$. This is the case $s = m + 1$.

## 4. Cancellation; n-th roots.

PROPOSITION 4.1. *Suppose every coordinate of* $\mathbf{w}$ *is nonzero. Then* $S(\mathbf{w}) \oplus S(\mathbf{0}) \cong R \oplus S(\mathbf{0})$ *as R-modules.*

PROOF. Recall that $R = S(\mathbf{1})$. Since $\mathbf{w} \cdot \mathbf{0} = \mathbf{0} = \mathbf{1} \cdot \mathbf{0}$, the proposition follows immediately from Theorem 2.1.

Variations of this proposition appear in [**15**, 2.3] and [**8**, 2.10].

EXAMPLE 4.2. Direct sum cancellation fails if $Z$ denotes the integers and every $P_i = p_i Z$ with $p_i \geqq 5$ ($i$ positive or negative).

PROOF. Since no $p_{\pm i}$ equals two, every coordinate of $\mathbf{w} = \mathbf{2}$ is nonzero. So, by Proposition 4.1 it suffices to show

(1) $$S(\mathbf{2}) \ncong R.$$

Suppose, to the contrary, that $S(\mathbf{2}) \cong S(\mathbf{1})$. Then by Theorem 2.1, $\mathbf{2} \equiv \mathbf{1}$ (mod $\mathscr{U}$). In particular, there exists a unit $u_1$ in $Z$ such that

(2) $$\bar{2} = \bar{1} u_1 \text{ in } Z/P_1.$$

Since $Z$ denotes the integers here, $u_1$ can only equal $\pm 1$. But since $p_1 \neq 3$, we have $\bar{2} \neq \pm \bar{1}$.

EXAMPLE 4.3 (Failure of $n$-th root property). Again let $Z$ denote the integers, and assume every $p_{\pm i} \geqq 5$. Let $n$ be the least common multiple of the numbers $\{p_i - 1 \mid 1 \leqq i \leqq m - 1\}$. Then

(1) $$\oplus^n S(\mathbf{2}) \cong \oplus^n R \text{ but } S(\mathbf{2}) \ncong R.$$

PROOF. In the previous proof we showed that all coordinates of $\mathbf{2}$ are nonzero, and $S(\mathbf{2}) \ncong R$. So it suffices to show that

(2) $$\oplus^n S(\mathbf{w}) \cong \oplus^n R$$

whenever all coordinates of **w** are nonzero.

For each $i$, positive or negative, $Z/p_i - \{0\}$ is a group of order $p_i - 1$. Hence $\mathbf{w}^n = \mathbf{1}$. Since $R = S(\mathbf{1})$, we get (2) as an immediate application of Theorem 2.1.

EXAMPLES 4.4 (Failure of cancellation and $n$-th roots for general $R$).

(i) Suppose that there exist units $\bar{t}_1$ in $Z/P_1$ and $\bar{t}_{-1}$ in $Z/P_{-1}$ which cannot be simultaneously lifted to a unit of $Z$. Then direct sum cancellation fails for $R$-modules.

(i) Suppose, in addition to (i), that for some positive integer $n$, $t_1^n \equiv 1 \pmod{P_1}$ and $t_{-1}^n \equiv 1 \pmod{P_{-1}}$. Then the *n-th* root property fails for $R$-modules.

PROOF. Let **w** be the element of **R** which equals $\bar{t}_1$ and $\bar{t}_{-1}$ in coordinates 1 and $-1$ respectively, and equals 1 in all other coordinates. Then the isomorphism in Proposition 4.1 holds. Since $\mathbf{w} \not\equiv \mathbf{1} \pmod{\mathscr{U}}$, we have $S(\mathbf{w}) \not\cong S(\mathbf{1}) = R$. Thus cancellation fails. Failure of $n$-th roots is a minor modification of Example 4.3, obtained by using **w** in place of **2**.

COROLLARY 4.5. *Let $F$ be any field, and let $Z$ be the polynomial ring $Z = F[x]$. Then direct sum cancellation and the n-th root property fail for some subring $R$ of $Z \oplus Z$.*

PROOF. For some maximal ideal $P_1$ of $Z = F[x]$, $F[x]/P_1$ has an element $\bar{t}_1 \neq \bar{1}$ such that $\bar{t}_1^n = \bar{1}$ for some $n \neq 1$. (If $F$ has characteristic $\neq 2$, we can take $P_1 = \langle x - 1\rangle$, $\bar{t}_1 = -1 + P_1$, and $n = 2$.) Taking $P_{-1} = \langle x \rangle$ and $\bar{t}_{-1} = 1 + P_{-1}$ then satisfies the conditions of Examples 4.4.

**5. Localizations, power cancellation.** Let $P$ be the kernel of the ring homomorphism: $R \twoheadrightarrow Z/P_1$ given by $(r_1, \ldots, r_m) \to r_1 + P_1 = r_2 + P_1$. Since $Z/P_1$ is a field, $P$ is a maximal ideal of $R$. Let $R_1$ be the $R$-module whose additive group is $(Z, +)$ with scalar multiplication $(r_1, \ldots, r_m)z = r_1 z$, let $R_2$ be similarly defined, but with $(r_1, \ldots, r_m)z = r_2 z$, and so on for $R_3, \ldots, R_m$.

LEMMA 5.1. *For* **w** *in* **R**, *let $P$ be defined as above.*

(i) *If $\bar{w}_1 \neq 0$, then $S(\mathbf{w})_P \cong R_P$ (as $R_P$-modules).*

(ii) *If $\bar{w}_1 = 0$, then $S(\mathbf{w})_P \cong (R_1)_P \oplus (R_2)_P$ with both terms on the right-hand side nonzero.*

PROOF. Choose $e$ in $Z$ such that $e \equiv 1 \pmod{P_1}$ and $e \equiv 0$ (mod $P_{-1}$ and $P_{\pm 2}$). Then let

$$b = (e, e, 0, 0, \ldots, 0) \in R - P. \tag{1}$$

Since every $S(\mathbf{w}) \subseteqq S(\mathbf{0}) = R_1 \oplus \cdots \oplus R_m$, we can consider $S(\mathbf{w})_P \subseteqq S(\mathbf{0})_P$.

To prove (i), suppose $\bar{w}_1 \neq 0$, and let $\bar{w}_1 = w_1 + P_1$. We show that, for $s = (s_1, \ldots, s_m)$ in $S(\mathbf{0})$,

$$(2) \qquad s/1 \in S(\mathbf{w})_P \Leftrightarrow s_1 w_1 \equiv s_2 \pmod{P_1}.$$

For ($\Leftarrow$), note that $sb \in S(\mathbf{w})$ so $(sb)/1 \in S(\mathbf{w})_P$. But by (1), $b/1$ is invertible in $R_P$. So $s/1 \in S(\mathbf{w})_P$.

For ($\Rightarrow$), we suppose $s/1 = x/d$ with $x$ in $S(\mathbf{w})$ and $d$ in $R - P$. Then there exists $d'$ in $R - P$ such that $d'ds = d'x$, so $d_1' d_1 s_1 = d_1' x_1$ and $d_2' d_2 s_2 = d_2' x_2$. Since $d' \in R - P$, we have $d_1'$ and $d_2' \in Z - P_1$. Therefore $d_1 s_1 \equiv x_1$ and $d_2 s_2 \equiv x_2 \pmod{P_1}$. Since $x_1 w_1 \equiv x_2$, by definition of $S(\mathbf{w})$, we have $d_1 s_1 w_1 \equiv d_2 s_2 \pmod{P_1}$. But $d \in R - P$. So $d_1 \equiv d_2 \not\equiv 0 \pmod{P_1}$. Hence $s_1 w_1 \equiv s_2 \pmod{P_1}$ as desired.

Since $R = S(\mathbf{1})$, we get the following special case of (2).

$$(3) \qquad s/1 \in R_P \Leftrightarrow s_1 \equiv s_2 \pmod{P_1}.$$

Let $f\colon S(\mathbf{w}) \to R$ and $g\colon R \to S(\mathbf{w})$ be multiplication by $(w_1 e, e, 0, 0, \ldots, 0)$ and $(e, w_1 e, 0, 0, \ldots, 0)$ respectively, and let $r = (w_1 e^2, w_1 e^2, 0, 0, \ldots, 0) \in R - P$. Then $f_P$ and $g_P/r$ are mutually inverse $R_P$-isomorphisms between $S(\mathbf{w})_P$ and $R_P$ in view of (2) and (3).

To prove (ii), suppose that $\bar{w}_1 = 0$, and recall that $S(\mathbf{w})_P \subseteqq S(\mathbf{0})_P$. We show, first, that

$$(4) \qquad S(\mathbf{w})_P = S(\mathbf{0})_P.$$

If $s = (s_1, \ldots, s_m) \in S(\mathbf{0})$, then $sb$, $b$ as in (1), belongs to $S(\mathbf{w})$; hence $sb/1 \in S(\mathbf{w})_P$. Since $b/1$ is invertible in $R_P$, we have (4).

To complete the proof of (ii) we only have to show that $(R_i)_P \neq 0 \Leftrightarrow i \leqq 2$. For $i \geqq 3$, we have $bR_i = 0$, so $(R_i)_P = 0$ follows from invertibility of $b/1$. For $i \leqq 2$, merely note that neither $(1, 0, 0, \ldots, 0) \in R_1$ nor $(0, 1, 0, 0, \ldots, 0) \in R_2$ is annihilated by any element of $R - P$.

An example similar to the following one, but for modules over certain integral group rings, was given in [**12**, Theorem 2.2].

Examples 5.2 (Interchange of localizations). Whenever $m \geqq 3$, we produce four indecomposable $R$-modules such that

$$(1) \qquad M \oplus N \cong H \oplus K$$

and two maximal ideals $P$ and $Q$ of $R$ such that

$$(2) \qquad M_P \cong H_P \ncong N_P \cong K_P,$$

$$(3) \qquad M_Q \cong K_Q \ncong N_Q \cong H_Q.$$

Proof. Write elements of $\mathbf{R}$ in the form

$$(a_1, \ldots, a_{m-1}; b_{-1}; \ldots, b_{-(m-1)}) \in \mathbf{R} = (\oplus_{i=1}^{m-1} Z/P_i) \oplus (\oplus_{i=1}^{m-1} Z/P_{-i})$$

Then define elements of **R** by

$$\mathbf{e}_M = (1, 1, 1, 1, \ldots, 1; 0, 0, 0, 0, \ldots, 0),$$
$$\mathbf{e}_N = (0, 0, 0, 0, \ldots, 0; 1, 1, 1, 1, \ldots, 1)$$

Define $\mathbf{e}_H$ by interchanging the second coordinates of each half of $\mathbf{e}_M$, as shown below, and similarly obtain $\mathbf{e}_K$ from $\mathbf{e}_N$.

$$\mathbf{e}_H = (1, 0, 1, 1, \ldots, 1; 0, 1, 0, 0, \ldots, 0),$$
$$\mathbf{e}_K = (0, 1, 0, 0, \ldots, 0; 1, 0, 1, 1, \ldots, 1).$$

Finally, let $M = S(\mathbf{e}_M)$, $N = S(\mathbf{e}_N)$, etc.

The isomorphism in (1) holds because both sides are isomorphic to $R \oplus S(\mathbf{0})$ [Lemma 3.1], and the four modules in (1) are indecomposable because their graphs are connected [Theorem 2.3].

Finally, (2) holds by Lemma 4.1 (and the fact that the local ring $R_P$ is indecomposable), and (3) holds if we build $Q$ analogously to $P$, but use $P_2$ instead of $P_1$.

EXAMPLE 5.3. An indecomposable $R$-module with a decomposable localization at a maximal ideal $S(\mathbf{w})$ where $\bar{w}_1 = 0$ and every other $\bar{w}_{\pm i} = \bar{1}$.

PROOF. $S(\mathbf{w})$ is indecomposable because graph **w** is connected [Theorem 2.3]; and $S(\mathbf{w})_P$ is decomposable by Lemma 5.1 (ii).

EXAMPLE 5.4. (Here $Z$ is not the ring of the integers.) A projective $R$-module $M$ of rank one such that

$$(1) \qquad (\forall n) \oplus^n M \not\cong \oplus^n R.$$

Let $F$ be any field that is not an algebraic extension of a finite field, and let $Z = F[x]$, the polynomial ring. Then let $R$ be the set of all $(f, g)$ in $\oplus^2 F[x]$ such that

$$(2) \qquad f \equiv g \ (\text{mod both } P_1 = \langle x - 1 \rangle \text{ and } P_{-1} = \langle x \rangle).$$

We can identify **R** with $F \oplus F$, where the first $F$ means $F[x]/\langle x-1\rangle$ and the second $F$ means $F[x]/\langle x \rangle$.

Since $F$ is not an algebraic extension of a finite field, there is an element $t \in F$ such that, for every $n \geqq 1$, $t^n \neq 1$. Let $\mathbf{w} = (t, 1)$ and $M = S(\mathbf{w})$, and recall that $R = S(\mathbf{1})$. To prove (1), assume to the contrary that isomorphism holds. Then $\mathbf{w}^n \equiv 1 \pmod{\mathcal{U}}$ by Theorem 2.1. Since $\mathbf{w} = (t, 1)$, so $\mathbf{w}^n = (t^n, 1)$, we have by (2.2).

$$(3) \qquad t^n \cdot u(x) = 1 \ (\text{in } F[x]/\langle x - 1\rangle) \text{ and } 1 \cdot u(x) = 1 \ (\text{in } F[x]/\langle x \rangle)$$

for some unit $u(x) \in F[x]$, hence $u(x) \in F$. Since $t \in F$ also, the equalities in (3) are actually equalities in $F$; so $t^n = 1$, contrary to our choice of $t$. Thus (1) holds.

Finally, $M$ is projective because both coordinates of $\mathbf{w}$ are nonzero [Cor. 2.4]. To see that $M$ has rank one, recall that for finitely generated projective modules $M$, the function $P \to \operatorname{rank} M_P$ is locally constant on spec $R$ [**2**, Chap. 2, §5, Theorème 1]. Since $R = S(\mathbf{1})$ is indecomposable [Thm. 2.3], it therefore suffices to check that rank $M_P = 1$ for a single prime ideal $P$; and this is done in Lemma 5.1(i).

POWER CANCELLATION. The finitely generated modules over a ring $S$ are said to satisfy "power cancellation" provided

$$A \oplus C \cong B \oplus C \Rightarrow (\exists n) \bigoplus^n A \cong \bigoplus^n B$$

for all finitely generated $S$-modules $A$, $B$, $C$.

K. R. Goodearl has proved that such power cancellation holds whenever $S$ is a $Z$-algebra, $Z$ the integers, such that $(S, +)$ is torsion-free of finite rank [**5**]. He was not able to determine whether $Z$ could be replaced by other principal ideal domains. The following example sheds a bit of light on this.

EXAMPLE 5.5. A module-finite algebra $R$, over a principal ideal domain, such that the finitely generated $R$-modules fail to satisfy power cancellation. Let $R$ and $M$ be as in Example 5.4. Then $R$ is a module-finite $F[x]$ – algebra. Moreover, $M \oplus S(\mathbf{0}) \cong R \oplus S(\mathbf{0})$ by Proposition 4.1.

For completeness, we sketch a proof of the converse of Corollary 2.4.

PROPOSITION 5.6. *Let* $\mathbf{w} \in \mathbf{R}$. *If* $S(\mathbf{w})$ *is a projective R-module, then all coordinates of* $\mathbf{w}$ *are nonzero.*

PROOF SKETCH. Suppose, for definiteness, that $\bar{w}_1 = 0$ and let $P$ be as in Lemma 5.1. It suffices to show that $S(\mathbf{w})_P$ is not $R_P$-projective, hence (by 5.1) to check that $(R_1)_P$ is not $R_P$-projective.

Let $\pi\colon R \twoheadrightarrow R_1$ be coordinate projection. Then $\pi_P$ maps $R_P$ onto $(R_1)_P$, has nonzero kernel, and does not split because the local ring $R_P$ is an indecomposable $R_P$-module.

REMARK 5.7. These rings provide the simplest example I know of for Noetherian modules which are locally isomorphic but not isomorphic. When $Z$ denotes the integers and $P_i = p_i Z$ with every $p_i \geqq 5$, we have $S(\mathbf{2}) \not\cong R$, but $S(\mathbf{2})_P \cong R_P$ for every maximal ideal $P$. The first assertion was proved in Example 4.2. The second follows immediately from Example 4.3(2) and the fact that projective modules over local rings are free.

**6. Proof of Theorem 2.3.** Suppose first that graph $\mathbf{w}$ is connected. We show that $S(\mathbf{w})$ is indecomposable by showing that zero and one are the only idempotent elements in its $R$-endomorphism ring.

Let $\pi_i$ be the projection map: $S(\mathbf{w}) \to$ coordinate $i$. For $b$ in $Z$, let $b \cdot 1_R = (b, b, \ldots, b) \in R$; and let $b(\hat{\imath})$ be obtained from $b \cdot 1_R$ by changing coordinate $i$ of $b \cdot 1_R$ to zero. Since the ideal $\bigcap_{\pm j} P_j$ has zero annihilator in $R$ (we chose the $P_{\pm j}$ with this property), we see that for $s$ in $S(\mathbf{w})$,

$$(1) \qquad s \in \ker \pi_i \Leftrightarrow bs = b(\hat{\imath})s \text{ for all } b \in \textstyle\bigcap_{\pm j} P_j.$$

Now let $f$ be any $R$-endomorphism of $S(\mathbf{w})$. We want to show that $f$ equals multiplication by $(z_1, \ldots, z_n)$ for suitable $z_i$ in $Z$. Consider diagram (2).

$$(2) \qquad \begin{array}{ccc} S(\mathbf{w}) & \longrightarrow\!\!\!\!\to & Z \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f_i} \\ S(\mathbf{w}) & \xrightarrow{\;\pi_i\;}\!\!\!\!\to & Z \end{array}$$

To see the existence of $f_i$ making the diagram commute, it suffices to show that $f(\ker \pi_i) \subseteqq \ker \pi_i$; and this follows from (1) since both $b$ and $b(\hat{\imath}) \in R$ when $b \in \bigcap_{\pm j} P_j$. Since $f_i$ is a $Z$-endomorphism of $Z$, it equals multiplication by some $z_i$ in $Z$. Thus $f$ is multiplication by $(z_1, \ldots, z_m)$ as claimed.

Now suppose $f = f^2$. Then each $z_i = z_i^2$. Since $Z$ is an indecomposable ring, each $z_i$ must equal zero or one. To complete the proof of indecomposability, we show that each $z_i = z_{i+1}$. Fix $i \neq m$.

By the Chinese Remainder Theorem we can find $c$ in $Z$ such that

$$(3) \qquad c \to \bar{w}_i \text{ in } Z/P_i \text{ and } c \to \bar{w}_{-1} \text{ in } Z/P_{-1}.$$

The $S(\mathbf{w})$ contains an element $s = (\ldots, 1, c, \ldots)$ whose $i$-th and $(i + 1)$-th coordinates are 1 and $c^2$ respectively. Hence

$$(4) \qquad f(s) = (\ldots, z_i, z_{i+1}c, \ldots,) \in S(\mathbf{w}).$$

Since graph $\mathbf{w}$ is connected, it must have an edge connecting vertex $i$ to vertex $i + 1$, say edge $(P_i)$. Then $\bar{w}_i \neq 0$. Also, $\bar{w}_i = c + P_i$. We see from (4) and the definition of $S(\mathbf{w})$ that

$$(5) \qquad z_i c \equiv z_{i+1} c \pmod{P_i}.$$

Cancelling $c$ from both sides [because $c \not\equiv 0 \pmod{P_i}$], we see $z_i \equiv z_{i+1} \pmod{P_i}$. Since $z_i$ and $z_{i+1}$ each equal zero or one, we now have $z_i = z_{i+1}$. Thus, when graph $\mathbf{w}$ is connected, $S(\mathbf{w})$ must be indecomposable.

Suppose next that graph $\mathbf{w}$ has $s \geqq 2$ conneccted components. The connected component $X$ which contains vertex 1 consists of a set of consecutive vertices, say $1, 2, \ldots, b$. Let $Y$ be the union of the other connected components of graph $\mathbf{w}$.

Since no edges connect vertices of $X$ with vertices of $Y$, $S(\mathbf{w})$ is the direct sum $T \oplus U$ of its projections in coordinates 1 through $b$ and $b + 1$ through $m$ respectively.

Let $R^{(b)}$ and $R^{(b+1)}$ be the projections of $R$ in coordinates 1 through $b$, and $b + 1$ through $m$ respectively.

Then $T$ is an $R^{(b)}$-module of the form $S(\mathbf{w}^*)$ where * indicates deletion of coordinates $\pm i$ with $i \geqq b + 1$. Moreover $X =$ graph $\mathbf{w}^*$ (built from points 1 through b) is connected. By the first case considered above, $S(\mathbf{w}^*)$ is an indecomposable $R^{(b)}$-module, hence an indecomposable $R$-module.

Similarly $U$ has an analogous form $U = S(\mathbf{w}^{**})$ as an $R^{(b+1)}$-module. Since graph $\mathbf{w}^{**}$ has $s - 1$ connected components, we conclude by induction that $U$ is the direct sum of $s - 1$ indecomposable $R^{(b+1)}$-modules, hence $R$-modules. This completes the proof of the theorem.

**7. A Chinese Remainder Theorem.** The following well-known lemma will be required in §8. A sketch of its proof is included for completeness. (For a much more general version of the lemma, see [**15**, Theorem 1.1].)

CHINESE REMAINDER THEOREM FOR MATRICES OF DETERMINANT ONE. *Let $P_1, \ldots, P_t$ be distinct maximal ideals of a commutative ring $Z$. For each $i = 1, 2, \ldots, t$ let $\bar{A}[i]$ be a matrix of determinant* 1, *in $(Z/P_i)_{n\times n}$ (the same $n$ for all $i$). Then there is a matrix $A$ in $Z_{n\times n}$ with* det $A = 1$, *such that, for each $i$, $A \to \bar{A}[i]$* (mod $P_i$).

PROOF SKETCH. We can suppose that $\bar{A}[i]$ an identity matrix, whenever $i \neq 1$: If $A^{(1)}$ denotes the "$A$" that we get in this situation, and if $A^{(i)}$ denotes the analogous "$A$" for each other $\bar{A}[i]$, then the product $\Pi_{i=1}^{t} A^{(i)}$ solves the original problem.

Next, we claim that we can suppose that $\bar{A}[1]$ is an elementary matrix $E_{uv}(\bar{x})$ $(u \neq v)$. (Here $E_{uv}(\bar{x})$ denotes the matrix obtained from the $m \times m$ identity matrix by changing its $(u, v)$-entry to $\bar{x}$.) Since $Z/P_1$ is a field, every matrix of determinant 1 is a product of such elementary matrices.

Finally, suppose $\bar{A}[1] = E_{uv}(\bar{x})$. By the ordinary Chinese Remainder Theorem, we can find $x$ in $Z$ such that $x \to \bar{x}$ in $Z/P_1$ and $x \to 0$ in each other $Z/P_i$. Then $A = E_{uv}(x)$ is the desired matrix of determinant 1 in $Z_{m\times m}$.

**8. Proof of Theorem 2.1.** We prove Theorem 2.1 by transforming it into a problem about matrices over the fields $Z/P_{\pm i}$ and then solving the matrix problem.

DEFINITIONS 8.1. The set $Z_{m\times n}$ of $m \times n$ matrices over $Z$ becomes an $R$-module if we identify each element $\underline{r} = (r_1, \ldots, r_m)$ of $R$ with the

$m \times m$ diagonal matrix $r = \operatorname{diag}(r_1, \ldots, r_m)$, and then define $rv$ ($v$ in $Z_{m\times n}$) to be matrix multiplication. Next we define $R$-submodules

$$S(\mathbf{A}, \mathbf{B}) \subseteqq Z_{m\times n} \tag{1}$$

which generalize the modules $S(\mathbf{w})$ and play a key role in what follows.

In (1), $\mathbf{A}$ and $\mathbf{B}$ denote $n \times n$ matrices over $\mathbf{R}$ whose rows generate the same $\mathbf{R}$-submodule of $\mathbf{R}_{n\times 1}$. In other words, $\mathbf{A}$ and $\mathbf{B}$ are indexed families of $n \times n$ matrices $\bar{A}[i]$ and $\bar{B}[i]$ over the fields $Z/P_i$, $1 \leqq |i| \leqq m - 1$, such that the row space of each $\bar{A}[i]$ equals that of $\bar{B}[i]$.

For $v$ in $Z_{m\times n}$, write $v[\text{row } i]$ for row $i$ of $v$. Then define $S(\mathbf{A}, \mathbf{B})$ to be the set of all $v$ in $Z_{m\times n}$ such that, for $1 \leqq i \leqq m - 1$,

$$\begin{aligned} v[\text{row } i]\cdot \bar{A}[i] &= v[\text{row}(i+1)]\cdot \bar{B}[i] \qquad \text{in } (Z/P_i)_{1\times n},\\ v[\text{row } i]\cdot \bar{A}[-i] &= v[\text{row}(i+1)]\cdot \bar{B}[-i] \qquad \text{in } (Z/P_{-i})_{1\times n}. \end{aligned} \tag{2}$$

To see that $S(\mathbf{A}, \mathbf{B})$ is closed under left multiplication by $R$, recall that for each $r$ in $R$, $r_i \equiv r_{i+1}$ modulo both $P_i$ and $P_{-i}$. The desired closure now follows immediately from (2).

Note that $S(\mathbf{0}_{n\times n}, \mathbf{0}_{n\times n}) = Z_{m\times n}$, because restrictions (2) become vacuous.

For $\mathbf{w}$ in $\mathbf{R}$, let $e(\mathbf{w})$ be the element of $\mathbf{R}$ such that

$$\text{coordinate } i \text{ (positive or negative) of } e(\mathbf{w}) = \begin{cases} \bar{1} \text{ if } \bar{w}_i \neq 0 \\ 0 \text{ if } \bar{w}_i = 0. \end{cases} \tag{3}$$

From now on, write the elements of $S(\mathbf{w})$ as $m \times 1$ columns (instead of rows, as before). Then $S(\mathbf{w})$ equals $S(\mathbf{w}, e(\mathbf{w}))$ if we think of $\mathbf{w}$ and $e(\mathbf{w})$ as $1 \times 1$ matrices. Moreover,

$$S(\mathbf{w}(1)) \oplus \cdots \oplus S(\mathbf{w}(n)) = S\left(\begin{bmatrix} (\mathbf{w}(1) & & 0 \\ & \ddots & \\ 0 & & \mathbf{w}(n) \end{bmatrix}, \begin{bmatrix} e(\mathbf{w}(1)) & & 0 \\ & \ddots & \\ 0 & & e(\mathbf{w}(n)) \end{bmatrix}\right). \tag{4}$$

Although we are only interested in $R$-modules of the form (4), two steps in the proof of Theorem 2.1 will require us to consider the more general $R$-modules $S(\mathbf{A}, \mathbf{B})$.

The next lemma translates the question of when $S(\mathbf{A}, \mathbf{B}) \cong S(\mathbf{C}, \mathbf{D})$ into a purely matrix-theoretic question, because the isomorphisms $\varphi_i$ and $\bar{\varphi}_i$ are all matrix multiplications.

DIAGRAM LEMMA 8.2. *Let $S = S(\mathbf{A}, \mathbf{B})$ and $T = S(\mathbf{C}, \mathbf{D})$ with $\mathbf{A}$ and $\mathbf{B}$ $n \times n$ and $\mathbf{C}$ and $\mathbf{D}$ $t \times t$. Then $S \cong T$ as $R$-modules if and only if there exist $Z$-isomorphisms $\varphi_i$ $(1 \leqq i \leqq m)$ and $\bar{\varphi}_i$ $(1 \leqq |i| \leqq m - 1)$ such that, for each $i$, Diagram (1) commutes. In particular, $S \cong T$ implies $n = t$.*

$$\begin{array}{ccccc} Z_{1\times n} & \xrightarrow{\bar{A}[i]} & (Z/P_i)_{1\times n} & \xleftarrow{\bar{B}[i]} & Z_{1\times n} \\ \downarrow{\scriptstyle \varphi_{|i|}} & & \downarrow{\scriptstyle \bar{\varphi}_i} & & \downarrow{\scriptstyle \varphi_{|i|+1}} \\ Z_{1\times t} & \xrightarrow{\bar{C}[i]} & (Z/P_i)_{1\times n} & \xleftarrow{\bar{D}[i]} & Z_{1\times n} \end{array}$$

DIAGRAM (1)

PROOF. First we show that each projection map

(2) $$\rho_i\colon S \to \text{row } i \text{ of } Z_{m\times n}$$

is onto. For simplicity, let $i = 1$. Take any element of $Z_{1\times n}$ and call it $v$[row 1]. We want to find $v$ in $S$ whose first row is $v$[row 1].

We find one candidate $w'$ for $v$[row 2] by setting $i = 1$ in the first equation of 8.1(2), and using the fact that the row space of $\bar{A}[1]$ equals that of $\bar{B}[1]$. Then find a second candidate $w''$ for $v$[row 2] by using the second equation of 8.1(2), again with $i = 1$. Finally, use the Chinese Remainder Theorem—together with distinctness of $P_1$ and $P_{-1}$—to find $v$[row 2] such that

$$v[\text{row } 2] \equiv w' \pmod{P_1} \text{ and } v[\text{row } 2] \equiv w'' \pmod{P_{-1}}.$$

Continuing in this way, we find all of the rows of $v$.

($\Rightarrow$). Let $\varphi\colon S \cong T$ be any $R$-isomorphism, and choose any positive $i$. We show that there is a unique $Z$-isomorphism $\varphi_i$ making "square 1" of Diagram (3) commute.

$$\begin{array}{ccccc} S & \xrightarrow{\rho_i=\rho_i(S)} & Z_{1\times n} & \xrightarrow{[\bar{A}[i],\,\bar{A}[-i]]=\alpha} & \operatorname{im}\alpha = \operatorname{im}\beta \\ \downarrow{\scriptstyle \varphi} & \text{“square 1”} & \downarrow{\scriptstyle \varphi_i} & \text{“square 2”} & \downarrow{\scriptstyle \bar{\theta}_i} \\ T & \xrightarrow{\rho_i=\rho_i(T)} & Z_{1\times t} & \xrightarrow{[\bar{C}[i],\,\bar{C}[-i]]=\gamma} & \operatorname{im}\gamma = \operatorname{im}\delta \end{array}$$

DIAGRAM (3)

For $b$ in $Z$ let $b(\hat{\imath})$ be the $m \times m$ diagonal matrix whose $i$-th diagonal entry is zero, and whose other diagonal entries equal $b$. Also, let $I_m$ be the $m \times m$ identity matrix. Since $\bigcap_{\pm j} P_j$ has zero annihilator in $\mathbf{Z}$, we have, for $s$ in $S$,

(4) $$\rho_i(s) = 0 \Leftrightarrow (bI_m)s = b(\hat{\imath})s \text{ for all } b \text{ in } \textstyle\bigcap_{\pm j} P_j.$$

Under the identification of $R$ with diagonal matrices described in Definition 8.1, we have $bI_m$ and $b(\hat{\imath}) \in R$ when $b \in \bigcap_{\pm j} P_j$ [Lemma 1.2]. Therefore (4) and its counterpart for $T$ show that $\varphi$ takes the kernel of $\rho_i(S)$ onto the kernel of $\rho_i(T)$. The existence of $\varphi_i$ follows. In addition, $n$ now equals $t$.

The horizontal arrows in "square 2" of Diagram (3) represent right multiplication by the $n \times (2n)$ matrices $\alpha$ and $\gamma$, producing $Z$-homomorphisms (also called $\alpha$ and $\gamma$) taking

$$Z_{1\times n} \longrightarrow (Z/P_i)_{1\times n} \oplus (Z/P_{-i})_{1\times n}.$$

Next we show the existence of a unique $Z$-homomorphism $\bar{\theta}_i$ making "square 2" of Diagram (3) commute, when $1 \leqq i \leqq m-1$. It suffices to show that $\varphi$ takes ker $\alpha\rho_i(S)$ onto ker $\gamma\rho_i(T)$. Since we already know that $\varphi$ takes ker $\rho_i(S)$ onto ker $\rho_i(T)$, it therefore suffices to prove (5) and its counterpart for $T$.

(5) $$\ker(S \twoheadrightarrow \operatorname{im} \alpha) = \ker \rho_i + \operatorname{ket} \rho_{i+1}.$$

Let $K = \ker(S \twoheadrightarrow \operatorname{im} \alpha)$. The inclusion $K \supseteqq \ker \rho_i$ is obvious. The inclusion $K \supseteqq \ker \rho_{i+1}$ follows by drawing the diagram, analogous to Diagram (3), whose top row is

(6) $$\operatorname{im} \beta \xleftarrow{[\bar{B}[i],\, \bar{B}[-i]]=\beta} Z_{1\times n} \xleftarrow{\rho_{i+1}} S$$

and noting that the map $S \twoheadrightarrow \operatorname{im} \beta$ in (6) equals the map $S \twoheadrightarrow \operatorname{im} \alpha$ in Diagram (3) by the definition of $S = S(\mathbf{A}, \mathbf{B})$. Thus the inclusion ($\supseteqq$) holds in (5).

For the inclusion ($\subseteqq$) take $v$ in $K$. Let $w'$ be the element of $Z_{m\times n}$ whose first $i$ rows equal those of $v$, with $i$ as in (5), and whose remaining rows equal zero; and let $w''$ be the element of $Z_{m\times n}$ which equals $v$ in rows $i+1$ through $m$ and equals zero in rows 1 through $i$. Then $w'$ and $w'' \in S$ (because $v \in K$); and $v = w' + w''$ with $w'$ in ker $\rho_{i+1}$ and $w''$ in ker $\rho_i$, as desired.

Thus $\bar{\theta}_i$ exists making "square 2" commute in Diagram (3). This $\bar{\theta}_i$ can be extended to an automorphism, also called $\bar{\theta}_i$, of the finitely generated semisimple $Z$-module in (7).

(7) $$(Z/P_i)_{1\times n} \oplus (Z/P_{-i})_{1\times n}$$

The restrictions of $\bar{\theta}_i$ to the fully invariant $Z$-submodules $(Z/P_i)_{1\times n}$ and $(Z/P_{-i})_{1\times n}$ of (7) now produce the maps $\bar{\varphi}_i$ and $\bar{\varphi}_{-i}$ which together with $\varphi_{|i|}$ and $\varphi_{|i|+1}$ make Diagram (1) commute.

($\Leftarrow$) Given commutative Diagram (1), it is straightforward to verify that $S \cong T$ via $\varphi_1 \oplus \varphi_2 \oplus \cdots \oplus \varphi_m$, where $\varphi_i$ takes row $i$ of $S$ to row $i$ of $T$.

8.3. Proof of theorem 2.1. Let $S = S(\mathbf{A}, \mathbf{B})$ be as on the right-hand side of 8.1(4), and lėt $T = S(\mathbf{C}, \mathbf{D})$ be analogously constructed from elements $\mathbf{x}(1), \ldots, \mathbf{x}(t)$ of $\mathbf{R}$.

($\Rightarrow$) Suppose $S \cong T$. We establish invariants (i), (ii), and (iii) of the theorem by applying the Diagram Lemma.

(i) Equality of the number of summands, $n = t$, has been explicitly stated in the Diagram Lemma.

(ii) (Graph invariant) For each $i$, positive or negative, the number of $\mathbf{w}(j)$ such that coordinate $i$ of $\mathbf{w}(j)$ is nonzero equals the rank of the diagonal matrix $\bar{A}[i]$. Reading Diagram (1) of the Diagram Lemma mod $P_i$ shows that this equals the rank of $\bar{C}[i]$.

(iii) (Units invariant) Each $\varphi_i$ and $\bar{\varphi}_{\pm i}$ in the Diagram Lemma equals right multiplication by an $n \times n$ matrix which we will again call $\varphi_i$ and $\bar{\varphi}_{\pm i}$. Let $u_i = \det \varphi_i$. Then $u_i$ is a unit of $Z$ ($u_i = \pm 1$ if $Z$ denotes the integers).

Now fix any positive $i$, $1 \leqq i \leqq m - 1$. Assume first that $\det \bar{A}[i] \neq 0$. Then $\det \bar{B}[i] = \bar{1}$ by the form 8.1(4) of **A** and **C**. By commutativity of the squares in the Diagram Lemma we see that $\det \bar{C}[i] \neq 0$ and hence $\det \bar{D}[i] = \bar{1}$. So reading the outer square of the Diagram Lemma shows

$$(1) \qquad u_{i+1} \det \bar{A}[i] = \det \bar{C}[i]\, u_i.$$

Note that (1) still holds if $\det \bar{A}[i] = 0$ because both sides then equal zero. Substituting $\det \bar{A}[i] = \bar{w}_i(1)\bar{w}_i(2) \cdots \bar{w}_i(n)$ into (1) we see

$$(2) \qquad \bar{w}_i(1) \cdots \bar{w}_1(n) = \bar{x}_i(1) \cdots \bar{x}_i(n) u_i u_{i+1}^{-1}.$$

Similar reasoning applies when $i$ is negative, so this completes the proof of (iii). (See (2.2))

($\Leftarrow$) Now we assume that invariants (i), (ii), and (iii) of $S$ equal those of $T$. To prove $S \cong T$ we describe a set of transformations of **A** and **B** which do not alter the isomorphism class of $S = S(\mathbf{A}, \mathbf{B})$. Then we apply these transformations to **A**, **B** and to **C**, **D** until we get **A** = **C** and **B** = **D**, hence $S = T$. These transformations are (3)–(6) below. Note that **A** and **B** need not be diagonal matrices in (3)–(6).

(3) Any $\bar{A}[i]$, $i$ postive or negative, can be left multiplied by an arbitrary matrix of determinant $\bar{1}$.

(4) The same for any $\bar{B}[i]$.

(5) Any $\bar{A}[i]$ and $\bar{B}[i]$, $i$ positive or negative, can be simultaneously right multiplied by any invertible matrix (over $Z/P_i$).

(6) Let $u_1, \ldots, u_m$ be arbitrary units of $Z$. Then the first row of each $A[i]$ and $A[-i]$ can be left multiplied by $u_i$ provided we simultaneously left multiply the first row of $B[i]$ and $B[-i]$ by $u_{i+1}$.

(3). For simplicity of notation we show that $\bar{A}[2]$ can be replaced by $\bar{\varphi}_2^{-1}\bar{A}[2]$, where $\bar{\varphi}_2$ is an arbitrary matrix of determinant $\bar{1}$.

By the Chinese Remainder Theorem for matrices of determinant 1 (§7), there is a matrix $\varphi_2 \in Z_{n\times n}$ such that $\det \varphi_2 = 1$, such that $\varphi_2 \to \bar{\varphi}_2$ in $(Z/P_2)_{n\times n}$ and such that $\varphi_2 \to I_n$ in $(Z/P_{-2})_{n\times n}$ and in $(Z/P_{\pm 1})_{n\times n}$.

Noie that Diagram $(7)_2$ commutes.

$$\begin{array}{ccccc} Z_{1\times n} & \xrightarrow{\bar{A}[2]} & (Z/P_2)_{1\times n} & \xrightarrow{\bar{B}[2]} & Z_{1\times n} \\ \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \bar{I}_n} & & \downarrow{\scriptstyle \varphi_3 = I_n} \\ Z_{1\times n} & \xrightarrow{\bar{\varphi}_2^{-1}\bar{A}[2]} & (Z/P_2)_{1\times n} & \xleftarrow{\bar{B}[2]} & Z_{1\times n} \end{array}$$

DIAGRAM $(7)_2$

Applying the Diagram Lemma with $\varphi_2$ as above and every other $\varphi_i$ and $\bar{\varphi}_{\pm i}$ an identity matrix now establishes (3). Note that $\varphi_2$ also appears in Diagrams $(7)_{-2}$ and $(7)_{\pm 1}$. But modulo each of $P_{-2}$ and $P_{\pm 1}$, matrix $\varphi_2$ becomes an identity matrix, hence causes no difficulty.

(4). This is obtained similarly.

(5). For our "typical" $i = 2$, statement (5) is obtained by using an arbitrary invertible matrix $\bar{\varphi}_2$ in place of $\bar{I}_n$ in a modification of Diagram $(7)_2$.

(6). This is obtained by taking every $\varphi_i = \text{diag}(u_i^{-1}, 1, 1, \ldots, 1)$ and every $\bar{\varphi}_{\pm i} = \bar{I}_n$ in the appropriate modifications $(7)_{\pm i}$ of $(7)_2$.

Now suppose **A**, **B**, **C**, **D** are all diagonal matrices of the form shown on the right-hand side of 8.1(4). We claim the following statement.

(7) The diagonal entries of any $\bar{A}[i]$, $i$ positive or negative, can be arbitrarily permuted provided we simultaneously apply the same permutation to the diagonal entries of $\bar{B}[i]$.

It suffices to prove that we can simultaneously permute any pair of consecutive diagonal entries of $\bar{A}[i]$ and $\bar{B}[i]$. So we can assume, for simplicity of notation, that **A** and **B** are $2 \times 2$ matrices. Simultaneously left multiplying $\bar{A}[i]$ and $\bar{B}[i]$ by the matrix

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

of determinant 1 achieves the first change illustrated in (8); then simultaneous right multiplication by

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

finishes the job.

$$(8) \qquad \begin{bmatrix} h & 0 \\ 0 & k \end{bmatrix} \text{ then } \begin{bmatrix} 0 & k \\ -h & 0 \end{bmatrix} \text{ then } \begin{bmatrix} k & 0 \\ 0 & h \end{bmatrix}$$

Because of (7) we can now suppose that all zero entries which occur as diagonal entries of $\bar{A}[i]$ and $\bar{B}[i]$ occur before all nonzero entries. We distinguish two cases for each $i$.

CASE 1. $\det \bar{A}[i] \neq 0$, hence $\bar{B}[i] = \bar{I}_n$. Then we left multiply $A[i]$ by a diagonal matrix of determinant $\bar{1}$ in such a way that all but (possibly) the first diagonal entry $\bar{a}[i]$ of $\bar{A}[i]$ become equal to $\bar{1}$.

CASE 2. det $\bar{A}[i] = 0$. Then the first diagonal entry of $\bar{A}[i]$ equals zero, by the assumption after (8). Here we right multiply $\bar{A}[i]$ by a diagonal matrix of determinant $\bar{1}$ in such a way that all nonzero diagonal entries of $A[i]$ become equal to $\bar{1}$.

Do the same to **C** and **D** that was done above to **A** and **B**. Since modules $S$ and $T$ have the same graph invariant—see (ii)—we get $\mathbf{B} = \mathbf{D}$, and every entry of $\bar{A}[i]$ equals the corresponding entry of $\bar{C}[i]$ except possibly (see Case 1 above) that we may have $\bar{a}[i] \neq \bar{c}[i]$ when one, hence both, of these does not equal zero.

Let **a** be the element of **R** whose $i$-th coordinate equals $\bar{a}[i]$, and similarly define **c**. Since modules $S$ and $T$ have the same units invariant (see (2.2)), **a** and **c** are congruent modulo liftable units. So there exist units $v_1, \ldots, v_{m-1}$ in $Z$ such that, for all $i > 0$,

$$\bar{c}[i] = \bar{a}[i]v_i \text{ in } Z/P_i \text{ and } \bar{c}[-i] = \bar{a}[-i]v_i \text{ in } Z/P_{-i}. \tag{9}$$

Define units $u_1, \ldots, u_m$ in $Z$ as follows: $u_m = 1$, $u_{m-1}u_m^{-1} = v_{m-1}$, $u_{m-2}u_{m-1}^{-1} = v_{m-2}, \ldots, u_1u_2^{-1} = v_1$. Then (9) becomes

$$\bar{c}[i] = \bar{a}[i]u_iu_{i+1}^{-1} \text{ and } \bar{c}[-i] = \bar{a}[-i]u_iu_{i+1}^{-1}. \tag{10}$$

To get every $\bar{a}[\pm i] = \bar{c}[\pm i]$ use (6) to simultaneously replace each $\bar{a}[\pm i]$ and $\bar{b}[\pm i]$ by $\bar{a}[\pm i]u_i$ and $\bar{b}[\pm i]u_{i+1}$. Then use (5) to change these to $\bar{a}[\pm i]u_iu_{i+1}^{-1}$ and $\bar{b}[\pm i]\cdot 1$ respectively. Because of (10), we now have $\mathbf{A} = \mathbf{C}$, so the proof is complete.

**9. Appendix: non-Noetherian example.** Our non-Noetherian example of non-uniqueness of the number of indecomposable summands will be a ring considered as a module over itself. It (Example 9.1) was proved by Barbara L. Osofsky for the case that $K$ is the field of two elements [**11**]. We include it here because it follows immediately from our earlier results, for readers familiar with ultraproducts. See [**6**, p. 97; **7**, p. 179].

EXAMPLE 9.1. Let $K$ be any integral domain. Then there is a countably generated $K$-algebra $E$ such that

(i) for every integer $m \geqq 2$, $E$ has $m$ primitive, orthogonal idempotents $e_{mj}$ such that $e_{m1} + \cdots + e_{mm} = 1$; and

(ii) $E$ has no infinite set of orthogonal idempotents.

PROOF. First we construct an infinite sequence of $K$-algebras $R^1$, $R^2$, .... If $K$ has at least four maximal ideals, let $Z = K$, and then let $R^m$ be the subring $R$ of $\oplus^m Z$ constructed, as in §1 (using some pecific set of maximal ideals of $Z$).

Otherwise let $Z$ be the polynomial ring $K[x]$. $Z$ now has at least four maximal ideals, in fact, infinitely many. Again let $R^m$ be the subring $R$ of $\bigoplus^m Z$ constructed in §1.

By Example 3.2, $R^m$ has a module $M^m = R^m \oplus S(\mathbf{0})$ such that (i)′ holds (and we prove (ii)′ below).

(i)′ For every integer $s$ with $2 \leqq s \leqq m + 1$, $M^m$ can be written as the direct sum of $s$ indecomposable $R^m$-modules; and

(ii)′ $M^m$ cannot be written as the direct sum of more than 2m submodules. To obtain (ii)′, note that $M^m = R^m \oplus S(\mathbf{0})$, which is contained in the $Z$-module $\bigoplus^{2m} Z$.

Next, let $E^m$ be the endomorphism ring of the $R^m$-module $M^m$, so $E^m$ is a $Z$-algebra. From (i)′ and (ii)′ we get

(i)″ for every $s$, $2 \leqq s \leqq m + 1$, $E^m$ has $s$ primitive, orthognal, idempotents whose sum equals 1; and

(ii)″ $E^m$ has no set of more that $2m$ orthogonal idempotents.

Let $E'$ be any non-principal ultra-product of $E^1, E^2, \ldots$. Then $E'$ has all of the properties demanded in (i) and (ii), except for countable generation. Call the desired idempotents of $E'$, $e_{mj}$. The $K$-subalgebra $E$ of $E'$ generated by the (countable set of) idempotents $e_{mj}$ then has all the properties demanded in (i) and (ii).

## References


**1.** G. Azumaya, *Corrections and supplementaries to my paper concerning Krull-Remak-Schmidt's Theorem*, Nagoya J. Math. **1** (1950), 117–124.

**2.** N. Bourbaki, *Algèbre Commutative*, Chap. 2, Hermann, Paris, 1961.

**3.** S. Brenner and C.M. Ringel, *Pathological modules over tame rings*, J. London Math. Soc. (2) **14** (1976), 207–215.

**4.** A.L.S. Corner, *Every countable reduced torsion-free ring is an endomorphism ring*, Proc. London Math. Soc. (3) **13** (1963), 687–710.

**5.** K.R. Goodearl, *Power cancellation of groups and modules*, Pacific J. Math. **64** 1(976), 387–411.

**6.** I.N. Herstein, *Topics in ring theory*, Univ. of Chicago Press, Chicago and London, 1969.

**7.** ———, *Non-commutative Rings*, Carus Monographs, Amer. Math. Soc. 1968.

**8.** H. Jacobinski, *Genera and decompositions of lattices over orders*, Acta, Maty. **121** (1968), 1–29.

**9.** W. Krull, *Matrizen, Moduln und verallgemeinerte Abelsche Gruppen im Bereich der ganzen algebraischen Zahlen*," S.B. Heidelberger Academie der Wissenschaften **2** (1932), 13–38.

**10.** L.S. Levy, *Modules over Dedekind-like rings*, Preprint.

**11.** B.L. Osofsky, *A remark on the Krull-Schmidt-Azumaya theorem*, Canad. Math. Bull. **13** (1970), 501–505.

**12.** I. Reiner, *Failure of the Krull-Schemidt theorem for integral representations*, Mich. Math. J. **9** (1962), 225–231.

**13.** R.B. Warfield, Jr., *A Krull-Schmidt theorem for infinite sums of modules*, Proc. Amer. Math. Soc. **22** (1969), 460–465.

**14.** ———, *Large modules over Artinian rings*, in *Representation Theory of Algebras*, ed. R. Gordon, Marcel Dekker, New York, 1978, 451–463.

**15.** R. Wiegand, *Cancellation over commutative rings of dimension one and two*, J. Algebra (to appear).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WI 53706