

OUTER PRODUCT RINGS

BY
DAVID LISSNER⁽¹⁾

1. Introduction. Let R be a commutative ring with identity, V an n -dimensional free R -module and $\Lambda(V)$ the exterior algebra on V ; as is customary we identify V with $\Lambda^1(V)$. In this paper we investigate the question of decomposability of vectors in $\Lambda^{n-1}(V)$; in particular we would like to know, for certain classes of rings, whether all $(n-1)$ -vectors are decomposable. Of course $\Lambda^{n-1}(V)$ is isomorphic to V , and if this isomorphism is properly chosen the exterior product $v_1 \wedge \cdots \wedge v_{n-1}$ corresponds to the usual outer product $[v_1, \dots, v_{n-1}]$ in V , so we are in effect asking whether all vectors in V can be expressed as outer products. Rings having this property will be called OP-rings. A well-known theorem of Hermite [2], originally proved for the integers, is valid in all such rings; we will describe the relation between these two properties more precisely in §2. Also in §2 we develop the basic properties of the outer product and use these to show that principal ideal domains are OP-rings. In §3 we give some examples of rings which are not OP-rings, including one to show that this property is not equivalent to the one studied by Hermite. Finally, in an appendix we show that all Dedekind domains are OP-rings.

2. Conventions and elementary properties. Let $W = R^n = R \oplus \cdots \oplus R$ and let $\{e_1, \dots, e_n\}$ be the standard basis for W , i.e., each $e_i = (0, \dots, 0, 1, 0, \dots, 0)$, with the 1 occurring in the i th place. $R_{n \times m}$ will denote the set of $n \times m$ matrices with entries in R , and if $A \in R_{n \times n}$ we use $|A|$ for the determinant of A . For $w_1, \dots, w_k \in W$ we will use $\text{col}(w_1, \dots, w_k)$ to denote the $k \times n$ matrix whose rows are the w_i 's; i.e., if $w_i = (a_{i1}, \dots, a_{in})$ for each i then

$$\text{col}(w_1, \dots, w_k) = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kn} \end{bmatrix}.$$

Again for vectors $w_i \in W$, $[w_1, \dots, w_{n-1}]$ will denote the usual outer product (see, e.g., Graeub [1] for a discussion); that is, $[w_1, \dots, w_{n-1}]$ is the vector in W whose i th component is $(-1)^{i+1}$ times the determinant of the matrix obtained by deleting the i th column from the matrix $\text{col}(w_1, \dots, w_{n-1})$. Finally, we have the usual inner product in W : if

Received by the editors January 6, 1964.

⁽¹⁾ This work was supported in part by a grant from the U. S. Army Research Office to Syracuse University.

$w = (a_1, \dots, a_n)$ and $w' = (b_1, \dots, b_n)$ then

$$\langle w, w' \rangle = a_1 b_1 + \dots + a_n b_n.$$

Now let V be any n -dimensional free R -module and let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for V . As mentioned before we will identify V with the subspace $\Lambda^1(V)$ of $\Lambda(V)$; then the vectors

$$\beta_i = (-1)^{i+1} \alpha_1 \wedge \dots \wedge \alpha_{i-1} \wedge \alpha_{i+1} \wedge \dots \wedge \alpha_n$$

for $i = 1, \dots, n$ form a basis for $\Lambda^{n-1}(V)$, and $\gamma = \alpha_1 \wedge \dots \wedge \alpha_n$ is a basis for $\Lambda^n(V)$. For each $v = \sum a_i \alpha_i \in V$ let $v' = (a_1, \dots, a_n) \in W$ and for $w = (b_1, \dots, b_n) \in W$ let $\phi(w) = \sum b_i \beta_i \in \Lambda^{n-1}(V)$; then the maps $v \rightarrow v'$ and ϕ are isomorphisms of V with W and W with $\Lambda^{n-1}(V)$ respectively, and the following identities hold for all $v_i \in V$:

- (1) $v_1 \wedge \phi(v'_2) = \langle v'_1, v'_2 \rangle \gamma$,
- (2) $v_1 \wedge \dots \wedge v_{n-1} = \phi[v'_1, \dots, v'_{n-1}]$, and
- (3) $v_1 \wedge \dots \wedge v_n = |\text{col}(v'_1, \dots, v'_n)| \gamma = v_1 \wedge \phi[v'_2, \dots, v'_n] = \langle v'_1, [v'_2, \dots, v'_n] \rangle \gamma$.

Two remarks are worth making. First, according to (2) the isomorphism ϕ sends outer products in W into exterior products in $\Lambda^{n-1}(V)$, as mentioned in the introduction; hence a given vector w can be expressed as an outer product if and only if $\phi(w)$ is decomposable. Second, by (3) (or simply by the Laplace expansion) we have

$$|\text{col}(w_1, \dots, w_n)| = \langle w_1, [w_2, \dots, w_n] \rangle;$$

we will often wish to express the determinant in this way.

If $A \in R_{n \times n}$ we will use $A^\#$ to denote the cofactor matrix of A , that is, the $n \times n$ matrix whose i, j entry is the cofactor of the i, j entry of A . In terms of the outer product this can be described very simply: if $A = \text{col}(w_1, \dots, w_n)$ then $A^\#$ is the $n \times n$ matrix whose i th row is $(-1)^{i+1} \cdot [w_1, \dots, w_{i-1}, w_{i+1}, \dots, w_n]$. If $|A|$ is a unit in R then A is invertible and its inverse is given by the familiar formula:

$$A^{-1} = \frac{(A^\#)^T}{|A|};$$

in particular, if $|A| = 1$ then $A^\# = (A^{-1})^T$ so $(A^\#)^\# = A$ and all the rows of A are outer products of the rows of $A^\#$. As a consequence we have

PROPOSITION 2.1. *Let $w_0, w_1 \in W$ and $\langle w_0, w_1 \rangle = 1$. Then w_0 is an outer product if and only if w_1 is.*

Proof. Suppose $w_0 = [w_2, \dots, w_n]$ and let $A = \text{col}(w_1, w_2, \dots, w_n)$. Then

$$|A| = \langle w_1, [w_2, \dots, w_n] \rangle = \langle w_1, w_0 \rangle = 1,$$

so all the rows of A are outer products, and in particular this is true of w_1 .

Of course the proposition has an equivalent formulation in terms of exterior products: if $u_0, u_1 \in \Lambda^{n-1}(V)$ and $\langle \phi^{-1}(u_0), \phi^{-1}(u_1) \rangle = 1$ then u_0 is decomposable if and only if u_1 is.

Let $w = (a_1, \dots, a_n) \in W$. The ideal in R generated by the a_i 's will be denoted by $I(a_1, \dots, a_n)$ or $I(w)$, and w will be called unimodular if $I(w) = R$. For $v \in V$ or $u \in \Lambda^{n-1}(V)$ we define $I(v)$ and $I(u)$ to be $I(v')$ and $I(\phi^{-1}(u))$, respectively, and again v or u is unimodular if the corresponding ideal is R .

COROLLARY. *Let w be a unimodular vector in W . Then $\phi(w)$ is decomposable if and only if there are $w_2, \dots, w_n \in W$ such that*

$$|\operatorname{col}(w, w_2, \dots, w_n)| = 1.$$

Proof. Suppose such w_i 's exist and let $w_0 = [w_2, \dots, w_n]$. Then $\phi(w_0)$ is decomposable, and $\langle w, w_0 \rangle = |\operatorname{col}(w, w_2, \dots, w_n)| = 1$, so $\phi(w)$ is decomposable also. Conversely suppose $\phi(w)$ is decomposable. Since w is unimodular there is a $w_0 \in W$ such that $\langle w, w_0 \rangle = 1$, and then $\phi(w_0)$ is also decomposable so w_0 is an outer product; say $w_0 = [w_2, \dots, w_n]$. Then $|\operatorname{col}(w, w_2, \dots, w_n)| = \langle w, w_0 \rangle = 1$, as desired.

In 1849 Hermite [2] showed that if R is the ring of integers and w is unimodular then there always do exist vectors $w_2, \dots, w_n$ satisfying $|\operatorname{col}(w, w_2, \dots, w_n)| = 1$; we will refer to rings with this property as H-rings. It is easy to show (see, e.g., [4, §2] for a proof) that this holds for any ring for which all finitely generated projective modules are free, and by the previous corollary it certainly also holds for OP-rings; in fact the relation between H-rings and OP-rings can now be easily described: R is an H-ring if all unimodular $(n-1)$ -vectors are decomposable and an OP-ring if all $(n-1)$ -vectors are decomposable. Hence one would expect that there are H-rings which are not OP-rings, and this is indeed the case; we will give an example of such a ring in the next section.

Now let f be an R -module endomorphism of V ; then f induces an endomorphism f^* of $\Lambda^{n-1}(V)$ defined by

$$f^*(v_1 \wedge \dots \wedge v_{n-1}) = (fv_1) \wedge \dots \wedge (fv_{n-1})$$

for all $v_i \in V$. Let P be the matrix for F with respect to the basis $\{\alpha_1, \dots, \alpha_n\}$; then $[f(v)]' = (v')P$ for all $v \in V$, and the matrix for f^* with respect to the basis $\{\beta_1, \dots, \beta_n\}$ is P^* , so we also have

$$f^*(\phi(w)) = \phi(wP^*)$$

for all $w \in W$. Applying this to the defining equation for f^* gives

$$\phi([v'_1, \dots, v'_{n-1}]P^*) = \phi[v'_1P, \dots, v'_{n-1}P]$$

for all $v_i \in V$, or, equivalently,

$$(4) \quad [w_1, \dots, w_{n-1}]P^\# = [w_1P, \dots, w_{n-1}P]$$

for all $w_i \in W$.

Let $\mathcal{H}$ denote the set of all vectors in W which can be expressed as outer products. Then

(5) $(a_1, \dots, a_n) \in \mathcal{H}$ implies $(da_1, \dots, da_{n-1}, a_n) \in \mathcal{H}$ for all $d \in R$,

(6) if P is invertible then $w \in \mathcal{H}$ if and only if $wP \in \mathcal{H}$, and

(7) if $d \in I(a_1, \dots, a_{n-1})$ then $(a_1, \dots, a_n) \in \mathcal{H}$ if and only if

$$(a_1, \dots, a_{n-1}, a_n + d) \in \mathcal{H}.$$

Proofs. (5) is a special case of (4) since $\text{diag}(d, \dots, d, 1) = [\text{diag}(1, \dots, 1, d)]^\#$. In (6) we have $P = (P^{-1})^{-1} = |P|((P^{-1})^T)^\#$, and if $w \in \mathcal{H}$ it again follows from (4) that $w((P^{-1})^T)^\# \in \mathcal{H}$, and hence that $wP \in \mathcal{H}$, since $\mathcal{H}$ is certainly closed under scalar multiplication. Finally if $d = a_1b_1 + \dots + a_{n-1}b_{n-1}$ then (7) is the special case of (6) obtained by taking

$$P = \begin{bmatrix} 1 & & & b_1 \\ & \ddots & & \vdots \\ 0 & & \ddots & \vdots \\ & & & 1 & b_{n-1} \\ 0 & \dots & 0 & 1 \end{bmatrix}.$$

Now let V_0 be the submodule of V generated by $\{\alpha_1, \dots, \alpha_{n-1}\}$ and W_0 the corresponding submodule of W . The vectors $(-1)^{i+1}\alpha_1 \wedge \dots \wedge \alpha_{i-1} \wedge \alpha_{i+1} \wedge \dots \wedge \alpha_{n-1}$ form a basis for $\Lambda^{n-2}(V_0)$, and just as before an element of $\Lambda^{n-2}(V_0)$ will be decomposable in $\Lambda(V_0)$ if and only if its coordinates with respect to this basis form an outer product in W_0 . Let $v_0 = \sum_{i=1}^{n-1} a_i (-1)^{i+1} \alpha_1 \wedge \dots \wedge \alpha_{i-1} \wedge \alpha_{i+1} \wedge \dots \wedge \alpha_{n-1}$ be such a vector. Then since v_0 is decomposable $\phi(a_1, \dots, a_{n-1}, 0) = v_0 \wedge \alpha_n$ is decomposable also; this proves

(8) if $(a_1, \dots, a_{n-1})$ is an outer product in W_0 then $(a_1, \dots, a_{n-1}, 0)$ is an outer product in W .

Now we are ready for

THEOREM 2.2. *Principal ideal domains are OP-rings.*

Proof. Let R be a principal ideal domain, n an integer ≥ 2 and V an n -dimensional free R -module. We wish to show that every $u \in \Lambda^{n-1}(V)$ is decomposable, and this is trivial if $n = 2$ so we may do an induction on n . Let $u = \phi(w)$ where $w = (a_1, \dots, a_n) \in W$, and let $I(a_1, \dots, a_{n-1}) = I(d)$. Then each $a_i = db_i$ and by (5) it will be sufficient to show that $(b_1, \dots, b_{n-1}, a_n) \in \mathcal{H}$. But $I(b_1, \dots, b_{n-1}) = R$ so by (7) it will actually be sufficient to show that $(b_1, \dots, b_{n-1}, 0) \in \mathcal{H}$, and this of course follows from (8) and the induction hypothesis.

COROLLARY. *Let R be a principal ideal domain, n an integer ≥ 2 , $w \in R^n$*

and $d \in I(w)$. Then there are vectors $w_2, \dots, w_n \in R^n$ such that

$$|\operatorname{col}(w, w_2, \dots, w_n)| = d.$$

(This is the result actually obtained by Hermite in [2], but we prefer to reserve the title of H-ring for rings satisfying the somewhat more restricted condition described previously.)

Proof. By the hypothesis on d there is a $w_0 \in R^n$ such that $\langle w, w_0 \rangle = d$, and by the theorem $w_0 = [w_2, \dots, w_n]$ for some $w_i \in R^n$. Then

$$|\operatorname{col}(w, w_2, \dots, w_n)| = d,$$

as desired.

3. Counterexamples. In this section we give some examples of rings in which the various properties under discussion fail. Specifically, we give rings which are not OP-rings, i.e., do not satisfy Theorem 2.2, rings which do not satisfy the corollary to Theorem 2.2, rings which are H-rings but not OP-rings, and finally rings which are not even H-rings. The last example raises an interesting question; we close with a discussion of this problem.

The examples we wish to consider first are polynomial rings over fields, and we will make use of the theory of ideals in such rings, in particular of their primary decomposition and properties relating to their dimension. As usual, if I and J are two ideals in R we use $I:J$ to denote $\{x \in R \mid xJ \subseteq I\}$.

We begin with rings which are not OP-rings.

THEOREM 3.1. *Let F be a field, $R = F[x_1, \dots, x_k]$ and $v \in R^n$, where $k \geq n \geq 3$, and suppose $\dim I(v) = k - n$. Then $v \notin \mathcal{S}$.*

Proof. Let $v = (a_1, \dots, a_n)$; for each $i = 1, \dots, n$ we will use $I(\dots \hat{a}_i \dots)$ to denote the ideal $I(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$. In general if J is an ideal of dimension r and a is any polynomial in R then it follows (Lang [3, p. 36, Theorem 11]) that $\dim(J, a)$ is either r , $r - 1$, or -1 ; hence if $(J, a) \neq R$ we have $\dim(J, a) \leq \dim J \leq \dim(J, a) + 1$. In our case $\dim I(v) = k - n \neq -1$ since $k \geq n$, so $I(v) \neq R$ and so $\dim I(\dots \hat{a}_i \dots) \leq \dim I(v) + 1 = k - (n - 1)$. But $I(\dots \hat{a}_i \dots)$ is generated by $n - 1$ elements, so it follows by a theorem of Macaulay (van der Waerden [10, p. 70]) that $I(\dots \hat{a}_i \dots)$ is in fact an unmixed $(k - n + 1)$ -dimensional ideal; that is, all the prime ideals belonging to $I(\dots \hat{a}_i \dots)$ have dimension $k - n + 1$. For the same reason, of course, $I(v)$ is an unmixed $(k - n)$ -dimensional ideal. Now let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the distinct prime ideals belonging to $I(\dots \hat{a}_i \dots)$; that is

$$I(\dots \hat{a}_i \dots) = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r,$$

where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$ -primary, and the $\mathfrak{p}_i$'s are all distinct. Suppose that

for some j we have $a_i \in \mathfrak{p}_j$. Then $I(v) \subseteq \mathfrak{p}_j$, and $\mathfrak{p}_j$ is a prime ideal, so $\mathfrak{p}_j$ contains one of the prime ideals belonging to $I(v)$. But the prime ideals belonging to $I(v)$ all have dimension $k - n$ and the dimension of $\mathfrak{p}_j$ is $k - n + 1$, so this is not possible. Thus $a_i \notin \mathfrak{p}_j$ for any j , so

$$I(\dots \hat{a}_i \dots): I(a_i) = I(\dots \hat{a}_i \dots)$$

(for a proof of this see Northcott [6, p. 23, Theorem 6]) and this of course holds for all $i = 1, \dots, n$.

Now suppose $v = [v_1, \dots, v_{n-1}]$. Then for any $k = 1, \dots, n-1$ we have

$$\langle v_k, v \rangle = \langle v_k, [v_1, \dots, v_{n-1}] \rangle = |\text{col}(v_k, v_1, \dots, v_{n-1})| = 0,$$

since the matrix in question has two equal rows; hence if $v_k = (b_1, \dots, b_n)$ then $a_1 b_1 + \dots + a_n b_n = 0$ and so $b_i \in I(\dots \hat{a}_i \dots): I(a_i) = I(\dots \hat{a}_i \dots) \subseteq I(v)$ for each i . Thus $I(v_k) \subseteq I(v)$ for all k , and since $v = [v_1, \dots, v_{n-1}]$ implies that $I(v) \subseteq \prod I(v_k)$ it follows that $I(v) \subseteq I(v)^{n-1} \subseteq I(v)^2$ and hence that $I(v) = I(v)^2$. But this is impossible, since the only idempotent ideals in $F[x_1, \dots, x_n]$ are (0) and (1) , both of which are precluded by the restriction on the dimension.

Now let $v, w \in R^n$. Then (v, w) is a vector in R^{2n} and $I(v, w)$ the ideal in R generated by its components, i.e., $I(v, w)$ is the ideal generated by the components of v and the components of w . With this understanding we can state

THEOREM 3.2. *Let F be a field, $R = F[x_1, \dots, x_k]$ and $v, w \in R^n$, where $n \geq 3$ and $k \geq 2n$, and suppose $\dim I(v, w) = k - 2n$. Then there do not exist vectors $v_2, \dots, v_n \in R^n$ such that*

$$|\text{col}(v, v_2, \dots, v_n)| = \langle v, w \rangle,$$

although certainly $\langle v, w \rangle \in I(v)$.

Proof. We have $\dim I(v, w) \neq -1$ since $k - 2n \geq 0$, so $I(v, w) \neq R$. Then it follows from the dimension theorem, just as in the previous proof, that $\dim I(v) \leq \dim I(v, w) + n = k - n$. From this it follows, again by the same sort of argument, that $\dim I(v) = k - n$.

Now suppose there do exist $v_2, \dots, v_n \in R^n$ such that

$$|\text{col}(v, v_2, \dots, v_n)| = \langle v, w \rangle,$$

and let $u = [v_2, \dots, v_n]$. Then $\langle v, u \rangle = |\text{col}(v, v_2, \dots, v_n)| = \langle v, w \rangle$ so $\langle v, u - w \rangle = 0$, and $\dim I(v) = k - n$ so we can apply the argument used in the previous theorem to conclude from this that the coordinates of $u - w$ must all be in $I(v)$. Then $I(v, u) = I(v, w)$, so $\dim I(v, u) = k - 2n$ and it follows as before that $\dim I(u) = k - n$. But then $u \notin \mathcal{H}$ by the previous theorem, and this is a contradiction.

Next let F be a field and $R = F[[x, y, z, \dots]]$, the ring of formal power series in k variables, k finite and ≥ 3 . Then R is of course a local ring, and it is well known that finitely generated projective modules over such rings are free, so R is an H-ring. But we claim that R is not an OP-ring.

Proof. Let $v = (x, y, z) \in R^3$, and suppose $v = [a, b]$, $a = (a_1, a_2, a_3)$, $b = (b_1, b_2, b_3)$, and $a_i, b_i \in R$ for all i . Then $\langle a, v \rangle = \langle b, v \rangle = 0$, i.e.,

$$a_1x + a_2y + a_3z = 0$$

and

$$b_1x + b_2y + b_3z = 0.$$

Computing the linear terms in x, y , and z in these expressions shows that the a_i 's and b_i 's must all have 0 constant terms. Hence $a_2b_3 - b_2a_3$ can have no linear term, so the equation

$$x = a_2b_3 - b_2a_3$$

cannot be satisfied and v cannot be an outer product.

Finally, Kaplansky has given examples of rings which are not H-rings (see Swan [9, §4, Example 1] for a discussion); we will describe one of them here because it leads to an interesting question. Let F be a subfield of the real numbers, p the polynomial $x^2 + y^2 + z^2 - 1$ in $F[x, y, z]$, $\bar{R} = F[x, y, z]/(p)$, and $a \rightarrow \bar{a}$ the natural map of $F[x, y, z]$ onto $\bar{R}$. Then we claim that Hermite's theorem is false for $\bar{R}$; in particular there does not exist a 3×3 matrix over $\bar{R}$ with first row $(\bar{x}, \bar{y}, \bar{z})$ and determinant 1, although certainly $1 \in I(\bar{x}, \bar{y}, \bar{z})$.

Proof. Suppose such a matrix does exist, say

$$\begin{vmatrix} \bar{x} & \bar{y} & \bar{z} \\ \bar{a}_1 & \bar{a}_2 & \bar{a}_3 \\ \bar{b}_1 & \bar{b}_2 & \bar{b}_3 \end{vmatrix} = 1,$$

where $a_i, b_i \in F[x, y, z]$, and let $v = [(x, y, z), (a_1, a_2, a_3)]$. Then

$$\begin{vmatrix} x & y & z \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = 1 + pq$$

for some $q \in F[x, y, z]$, and the coordinates of v are polynomials in x, y , and z so v is a continuous function of the vector (x, y, z) , and of course v is orthogonal to (x, y, z) . If $(x, y, z) \in S^2$ (the unit sphere in R^3) then $p = 0$ so $\langle v, (b_1, b_2, b_3) \rangle = 1$ and so $v \neq 0$. Hence the existence of such a matrix would imply the existence of a nonvanishing tangent field on S^2 , contrary to the well-known theorem.

This raises the following question. Let Q be the rational numbers and $R = Q[x, y, z]$; do there exist polynomials $q_i \in R$ such that

$$1 \in I(x + q_1 p, y + q_2 p, z + q_3 p),$$

where p is the polynomial given in the above example? Suppose such polynomials do exist, and let $v = (x + q_1 p, y + q_2 p, z + q_3 p) \in R^3$. If Hermite's theorem is true for R there will be vectors $v_2, v_3 \in R^3$ such that $|\text{col}(v, v_2, v_3)| = 1$, and then reducing mod p yields a matrix over $Q[x, y, z]/(p)$ with first row $(\bar{x}, \bar{y}, \bar{z})$ and determinant 1, which we have just shown is not possible. Hence the existence of the q_i 's would imply that Hermite's theorem does not hold for $Q[x, y, z]$, which would answer a well-known question raised by Serre in [7].

Appendix. We will show here that Dedekind domains are OP-rings; this generalizes slightly a classical result of Steinitz, who proved in 1912 [8] that Dedekind domains are H-rings. (Of course Steinitz stated his theorem for the ring of integers in an algebraic number field, but his proof is valid in any Dedekind domain.)

Let D be a Dedekind domain and a an element of D which is neither 0 nor a unit. Then $D/(a)$ is a principal ideal ring, and in fact a finite direct sum of local rings R_k whose radicals are principal ideals generated by nilpotent elements. (For a proof of this and a discussion of Dedekind domains in general see [11, Chapter 5].) Hermite's theorem for the R_k 's is clear (since $I(a_1, \dots, a_n) = R_k$ only if one of the a_i 's is a unit) and the theorem carries over immediately to direct sums; hence $D/(a)$ is an H-ring.

We will use some standard terminology from matrix theory. Specifically, $SL_n(R_k)$ will denote the group of $n \times n$ matrices of determinant 1 over R_k , I the $n \times n$ identity matrix and $\{e_{ij} | i, j = 1, \dots, n\}$ the usual basis for $R_{n \times n}$. For $i \neq j$ and any $\lambda \in R$

$$B_{ij}(\lambda) = I + \lambda e_{ij},$$

and for a transposition $(i j) \in \mathfrak{S}_n$ (the symmetric group on n objects) $P_{(ij)}$ is the matrix obtained by performing the permutation $(i j)$ on the rows of I . Finally for any $\lambda \in R$ let $D_i(\lambda) = \text{diag}(1, \dots, 1, \lambda, 1, \dots, 1)$, with the λ occurring in the i th place (i.e., $D_i(\lambda) = I + (\lambda - 1)e_{ii}$). The matrices $B_{ij}(\lambda)$ are certainly in $SL_n(R_k)$; we define $EL_n(R_k)$ to be the subgroup generated by all these matrices, and we note that since $D_i(-1)P_{(ij)} = B_{ji}(1)B_{ij}(-1)B_{ji}(1)$ this group contains matrices equal to the $P_{(ij)}$'s to within a minus sign.

Now if x and y are any two elements of R_k then either x divides y or y divides x ; using this and the fact that $EL_n(R_k)$ contains matrices which act like the $P_{(ij)}$'s one shows by a very standard argument (see, for example,

MacDuffee [5, the proof of Theorem 22.4]) that for any $A \in SL_n(R_k)$ there is a $P \in EL_n(R_k)$ such that PA is a diagonal matrix. But if $i \neq j$ and u is a unit in R then

$$D_i(u)D_j(u^{-1}) = B_{ij}(u - u^2)B_{ji}(-u^{-1})B_{ij}(u - 1)B_{ji}(1),$$

and it follows from this (provided $n \geq 2$) that all diagonal matrices of determinant 1 are in $EL_n(R_k)$; hence $PA \in EL_n(R_k)$. Then $A \in EL_n(R_k)$ also, and A was any matrix of determinant 1, so $SL_n(R_k) = EL_n(R_k)$ for all $n \geq 2$. Now the obvious inclusion of $SL_n(R_k)$ into $SL_n(D/(a))$, namely $A \rightarrow I + \dots + I + A + I + \dots + I$, sends the $B_{ij}(\lambda)$ matrices into matrices of the same form, and hence sends $EL_n(R_k)$ into $EL_n(D/(a))$ for each k . Since $SL_n(D/(a)) = \sum_k \oplus SL_n(R_k) = \sum_k \oplus EL_n(R_k)$ it then follows that $SL_n(D/(a)) = EL_n(D/(a))$, and hence that the map of $SL_n(D)$ into $SL_n(D/(a))$ induced by the natural map of D onto $D/(a)$ is actually onto, since the range of this map certainly contains $EL_n(D/(a))$. With this established we are now ready to prove

THEOREM. *Dedekind domains are OP-rings.*

Proof. (We wish to thank the referee for the following simplification of the author's original proof.) Let $(a_1, \dots, a_n) \in D^n$; we must show that $(a_1, \dots, a_n) \in \mathcal{H}$. If all the a_i 's are 0 this is certainly true, and if one of them is a unit it follows immediately from the corollary to Proposition 2.1. Hence we may assume that some a_i is neither 0 nor a unit, and we may of course take this to be a_1 . Let $\bar{D} = D/(a)$ and $a \rightarrow \bar{a}$ be the natural map of D onto $\bar{D}$. Since $\bar{D}$ is a principal ideal ring there is a $b \in D$ with $I(\bar{a}_1, \dots, \bar{a}_n) = I(\bar{b})$; let $\bar{a}_i = \gamma_i \bar{b}$ ($\gamma_i \in \bar{D}$) for each i . It follows from the representation $\bar{D} = \sum \oplus R_k$ that the γ_i 's can be chosen so that $I(\gamma_1, \dots, \gamma_n) = \bar{D}$; we will suppose that this has been done. We may of course further suppose that $n \geq 3$, the theorem being trivial if $n = 2$. Then since $\bar{D}$ is an H-ring there is a matrix in $SL_{n-1}(\bar{D})$ with first row $(\gamma_2, \dots, \gamma_n)$, and by the previous discussion this lifts to a matrix $M_0 \in SL_{n-1}(D)$; let $(c_2, \dots, c_n)$ be the first row of M_0 . Then $\gamma_i = \bar{c}_i$ for each i so $\bar{a}_i = \bar{c}_i \bar{b}$; hence for each $i = 2, \dots, n$ there is a $d_i \in D$ such that

$$a_i = d_i a_1 + c_i b.$$

Let

$$M = \begin{bmatrix} 1 & d_2 & \dots & d_n \\ 0 & & & \\ \vdots & & M_0 & \\ 0 & & & \end{bmatrix};$$

then $M \in SL_n(D)$ and $(a_1, b, 0, \dots, 0)M = (a_1, a_2, \dots, a_n)$, so by (6) of §2 $(a_1, \dots, a_n) \in \mathcal{K}$ if and only if $(a_1, b, 0, \dots, 0) \in \mathcal{K}$. Since the theorem always holds for $n = 2$ this last statement follows immediately from (8), or for that matter one can easily write down vectors whose outer product is $(a_1, b, 0, \dots, 0)$.

BIBLIOGRAPHY

1. W. Graeb, *Lineare Algebra*, Grundlehren Mathematische Wissenschaften 97, Springer, Berlin, 1958.
2. M. Hermite, *Sur une question relative à la théorie des nombres*, J. Math. Pures Appl. (1) 14 (1849), 21-30.
3. S. Lang, *Introduction to algebraic geometry*, Interscience, New York, 1958.
4. D. Lissner, *Matrices over polynomial rings*, Trans. Amer. Math. Soc. 98 (1961), 295-305.
5. C. C. MacDuffee, *The theory of matrices*, Springer, Berlin, 1933.
6. D. G. Northcott, *Ideal theory*, Cambridge Univ. Press, Cambridge, 1953.
7. J.-P. Serre, *Faisceaux algébriques cohérents*, Ann. of Math. (2) 61 (1955), 197-278.
8. E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern*, Math. Ann. 71 (1912), 328-354.
9. R. Swan, *Vector bundles and projective modules*, Trans. Amer. Math. Soc. 105 (1962), 264-277.
10. B. L. van der Waerden, *Modern algebra*, Vol. II, Ungar, New York, 1950.
11. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Van Nostrand, Princeton, N. J., 1958.

SYRACUSE UNIVERSITY
SYRACUSE, NEW YORK