ELEMENTARY DIVISORS AND MODULES

BY

IRVING KAPLANSKY

1. **Introduction.** Let A be a matrix over a given ring R. Is it possible to find unimodular matrices P, Q such that PAQ is diagonal? This question, and the application to modules, constitutes the main theme of the present paper. An affirmative answer is classical when R is the ring of integers, or polynomials in one variable, and Jacobson and Teichmüller extended this to any principal ideal ring without divisors of 0. Such rings of course satisfy the ascending chain condition. Our chief purpose has been to expel chain conditions from the subject, to as great an extent as possible, but lesser skirmishes are also fought on the battle-fields of non-commutativity and divisors of 0. In compensation, virtually all rings considered will satisfy at least the condition that finitely generated ideals are principal. Thus the investigations for algebraic number rings in [28][1] are not included, nor of course the still more general theory in [27] and the references given there. Suitable extension of these results to rings without chain condition remains a task for the future, although in this connection the work of Fitting [9] should be mentioned, and also our Theorem 10.5 covers some of the work just cited.

We now summarize the contents of the paper. In §3 we study rings in which the reduction of 1 by 2 matrices is possible; we have called these Hermite rings since in them the Hermite triangular form can be achieved (Theorem 3.5). In §5 we turn to diagonal reduction. In Theorem 5.1 it is shown that all new difficulties are already embodied in the 2 by 2 case. Theorem 5.2 gives a necessary and sufficient condition for diagonal reduction for commutative rings whose divisors of 0 are in the radical. An immediate corollary is a generalization (Theorem 5.3) of Helmer's theorem [12]. The standard reduction of alternate matrices under congruence is possible in an Hermite ring (Theorem 6.1). In §9 we study the uniqueness of the decomposition of a module into cyclic modules—this carries with it the uniqueness of the invariant factors of a matrix. This is applied in §10 to valuation rings, which are allowed to be non-commutative and have divisors of 0. A device due to Krull makes it possible to extend the results in part to an arbitrary integrally closed integral domain (Theorem 10.5). As explained in §9, the ability to reduce finite matrices does not carry with it results on all finitely generated modules, but only those whose "relations" are also finitely generated. In §11 we undertake the study of finitely generated modules without such a restriction, but only over valuation rings. We obtain a complete result

---

(Theorem 11.1) which seems somewhat surprising; and the attendant complications presumably give an indication of what a general theory would be like. In §12 we investigate principal ideal rings, and in §13 we turn to infinite matrices and modules, where in compensation we allow ourselves the descending chain condition on the ring.

2. **Definitions.** R will always denote a ring (associative but not necessarily commutative). Except in §8, it will be assumed that R has a unit element. We shall write R_n for the ring of n by n matrices with elements in R. By a *unit* of a ring we shall mean an element with a two-sided inverse. Units of R_n will be said to be *unimodular*. If $b = ca$ we say that a is a *right divisor* of b; equivalent conditions are $b \in Ra$ and $Rb \subseteq Ra$. We say that a is a *total divisor* of b if $RbR \subseteq Ra \cap aR$, or in words: everything in the two-sided ideal generated by b is right and left divisible by a. It is be observed that an element is not necessarily a total divisor of itself. If R is commutative then right, left, and total divisibility all coincide.

We shall write diag $(d_1, d_2, \cdots)$ for a matrix (it may be rectangular) having $d_1, d_2, \cdots$ down the main diagonal and zeros elsewhere. (By the main diagonal we mean the one beginning at the upper left corner.) We say that the matrix A *admits diagonal reduction* if there exist unimodular matrices P, Q such that

(1) $$PAQ = \text{diag } (d_1, d_2, \cdots)$$

where d_i is a total divisor of d_{i+1}. If every matrix over R admits diagonal reduction, we call R an *elementary divisor ring*.

Particularly attention will be devoted to the diagonal reduction of a matrix consisting of single row or column. In that case either P or Q in (1) is a 1 by 1 matrix, and may be deleted. Thus the diagonal reducibility of $(a\ b)$ hinges on the existence of a unimodular 2 by 2 matrix Q such that

(2) $$(a\ b)Q = (d\ 0).$$

If every 1 by 2 matrix admits diagonal reduction, we shall call R a *right Hermite* ring; if 2 by 1 matrices admit diagonal reduction, R is a left Hermite ring, and if both, R is an Hermite ring. It is to be noted that (2) entails $aR + bR = dR$, so that in a right Hermite ring all finitely generated right ideals are necessarily principal.

We shall now discuss the question of the uniqueness of the generators of principal right ideals. If $a = bu$ where u is a unit, we say that a and b are *right associates*. Clearly right associates are right multiples of each other, or (which comes to the same thing) they generate the same principal right ideals aR and bR. We raise the converse question: If $aR = bR$, are a and b necessarily right associates? It is well known that the answer is affirmative if there are no divisors of 0, and this may be extended to a slightly more general case. (We are using the term "radical" in the sense of Perlis-Jacobson [14].)

LEMMA 2.1. *Let R be a ring in which all right divisors of 0 are in the radical. Then $aR = bR$ implies that a, b are right associates.*

Proof. We have $a = by$, $b = ax$, so $a = axy$. If a, $b = 0$ there is nothing to prove. Otherwise $a(1 - xy) = 0$ shows that $1 - xy$ is in the radical, whence x and y are units.

The answer is also affirmative for commutative principal ideal rings, in the light of the structure theorem of §12. In [10] an affirmative answer is given for another special class of commutative rings. Finally it is not difficult to see that the answer is affirmative for commutative rings with the descending chain condition. But in general the answer is negative: a celebrated counter-example is the ring of all linear transformations in an infinite-dimensional vector space. However the literature does not seem to record any counter-examples in the commutative case, and so it is perhaps worth while to mention the following two.

(a) The ring of all continuous real functions on $(0, 3)$. Define both $a(t)$ and $b(t)$ to be $1 - t$ on $(0, 1)$ and 0 on $(1, 2)$ and set $a(t) = -b(t) = t - 2$ on $(2, 3)$. Then $a(t)$ and $b(t)$ are mutual multiples but not associates.

(b) This example satisfies the ascending chain condition. Take the set of all pairs $(n, f(x))$, where n is an integer, $f(x)$ a polynomial with coefficients in $GF(5)$, and the constant term of f is congruent to n mod 5. Addition and multiplication are componentwise. Then $(0, x)$ and $(0, 2x)$ are mutual multiples but not associates.

It is appropriate to point out the intimate connection between this question of the generation of principal ideals and the main theme of our investigation. Suppose that in a ring R we have $aR + bR = dR$; then $(a\ b)$ and $(d\ 0)$ are right multiples of each other. Thus in seeking a diagonal reduction of $(a\ b)$ to $(d\ 0)$ we are asking precisely whether this implies that they are right associates. (If desired, one can add a row of zeros to both $(a\ b)$ and $(d\ 0)$ and thereby have all matrices under discussion in R_2.) This remark points to the relevance of the following question: if principal ideals are uniquely generated (up to associates) in R, is this property inherited by R_n? A partial affirmative answer is given in Theorem 3.8 below.

The following special case deserves mention: if a has a right inverse, is it a unit? (This is indeed a special case, for if a has a right inverse, then a and 1 are right multiples of each other.) This milder question at least has an unreservedly affirmative answer in the commutative case. The answer is also affirmative for any ring which can be embedded in a ring with either chain condition, or under sundry weaker hypotheses [3]. Moreover in both these cases the property is inherited by R_n. It would be of interest to know whether it is always inherited by R_n. With the additional hypothesis that R is a right Hermite ring, it is in fact inherited by R_n (Theorem 3.9 below).

3. **Triangular reduction.** We begin our discussion with a set of sufficient conditions for a ring to be a right Hermite ring.

THEOREM 3.1. *Let R be a ring satisfying the following conditions*: (1) *all divisors of* 0 *are in the radical*, (2) *the union and intersection of any two principal right ideals is a principal right ideal*, (3) *the union of any two principal left ideals is a principal left ideal*, (4) *in R_2 a matrix with a one-sided inverse is unimodular. Then R is a right Hermite ring.*

Proof. For a, b in R write $aR+bR=dR$, $d=ap+bq$, $a=da_1$, $b=db_1$, $a_1R\cap b_1R=cR$, $c=a_1r=-b_1s$, $Rr+Rs=Rt$, $r=xt$, $s=yt$. If $d=0$, then $a=b=0$ and there is nothing to prove. So we assume henceforth that $d\neq 0$. The equation $d(a_1p+b_1q-1)=0$ then shows that a_1p+b_1q-1 is in the radical, whence

(3) $$a_1p + b_1q = \text{a unit } u.$$

Since we may replace p, q by pu^{-1}, qu^{-1}, there is no loss of generality in assuming $u=1$. Write $z=a_1pb_1=b_1(1-qb_1)$. Then $z\in a_1R\cap b_1R=cR$, say $z=cw=-b_1sw$. If b_1 is in the radical, then (3) shows that a_1 is a unit. It follows that b is a right multiple of a, a trivial case that need not detain us. We therefore assume that b_1 is not in the radical. Then the equation $b_1(1-qb_1+sw)=0$ leads to

(4) $$1 - qb_1 + sw = 0.$$

If s is in the radical, (4) tells us that b_1 is a unit, which we again dismiss. We are thus entitled to assume that t is not in the radical, and from $a_1xt=-b_1yt$ we deduce $a_1x=-b_1y=$ say $ch=a_1xth$. If $a_1x=0$ we have $c=0$, whence $z=b_1(u-qb_1)=0$ and we are led to b_1 being either 0 or a unit, possibilities already ruled out. So from $a_1x(1-th)=0$ we may conclude that t is a unit. Hence finally $Rr+Rs=R$ (this desired conclusion was the sole object of all this maneuvering). Write $er+fs=1$, $g=ep+fq$. Then

(5) $$\begin{pmatrix} a_1 & b_1 \\ e-ga_1 & f-gb_1 \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

From hypothesis (4) it follows that the matrices in (5) are unimodular. The proof of the theorem is completed by observing

(6) $$(a\ b)\begin{pmatrix} p & r \\ q & s \end{pmatrix} = (d\ 0).$$

Theorem 3.1 becomes perceptibly simpler in the commutative case: hypothesis (4) is superfluous, and (3) gets absorbed in (2). But even more: no assumption need be made about the intersection of principal ideals, this being in fact a consequence of the other hypotheses.

THEOREM 3.2. *Let R be a commutative ring in which divisors of* 0 *are in the radical, and the union of any two principal ideals is principal* (*that is, all finitely generated ideals are principal*). *Then R is an Hermite ring.*

Proof. Write $aR+bR=dR$, $ap+bq=d$, $a=sd$, $b=-rd$. Then $d(ps-qr-1)$ $=0$. We dismiss the case $d=0$, and thus have that $ps-qr$ is a unit. The observation (6) completes the proof.

It was remarked in §2 that diagonal reducibility of $(a\ b)$ is possible only if $aR+bR$ is principal. In certain cases we can also conclude that $aR\cap bR$ is principal. The argument is substantially due to Stewart [29].

LEMMA 3.3. *Suppose that $(a\ b)$ is diagonally reducible to $(d\ 0)$ where either (1) d is in the center or (2) d is not a left divisor of 0. Then $aR\cap bR$ is principal.*

Proof. Suppose that the reduction is given by (6) and write $m=ar=-bs$. We contend $aR\cap bR=mR$. To prove this, let z be an element in $aR\cap bR$, $z=ax=-by$, and write

$$U = \begin{pmatrix} p & r \\ q & s \end{pmatrix}, \qquad V = \begin{pmatrix} p & x \\ q & y \end{pmatrix}, \qquad U^{-1}V = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Then $(a\ b)V=(d\ 0)$, $(d\ 0)U^{-1}V=(d\ 0)$, whence $df=0$. Under either of our hypotheses we can deduce that $apf=0$. Since $x=pf+rh$, we have $z=ax=arh$ $\in mR$. Hence $aR\cap bR\subseteq mR$. The inclusion the other way is trivial.

If we go so far as to assume no divisors of 0, we can obtain necessary and sufficient conditions for a ring to be an Hermite ring.

THEOREM 3.4. *Let R be a ring without divisors of 0. Then a necessary and sufficient condition for R to be an Hermite ring is that the union and intersection of any two principal right or left ideals be principal.*

Proof. The necessity follows from Lemma 3.3. The sufficiency will follow from Theorem 3.1 as soon as we verify hypothesis (4) of that theorem. This verification is made by observing that R satisfies the condition of Ore for embeddability in a division ring—cf. [13, p. 31].

The main theorem on reduction of matrices in an Hermite ring asserts the possibility of reduction to triangular form.

THEOREM 3.5. *For any matrix A with elements in a right Hermite ring, we can find a unimodular matrix U such that AU is triangular (that is, has zeros above the main diagonal).*

REMARK 1. It is clear by symmetry that we can equally well arrange to get zeros below the diagonal which begins at the lower right corner. Thus if A is a square matrix we can achieve either of the two possible triangular forms.

REMARK 2. Further normalizations are possible until a canonical form (the Hermite form) is reached [23, pp. 32–33].

Proof. Let A be an m by n matrix. First we treat the case $m=1$ (A is a single row). Write $A=(a\ B)$, B being a row of length $n-1$. By induction we can find a unimodular matrix V such that $BV=(b\ 0\ \cdots\ 0)$. Then we find a

unimodular 2 by 2 matrix W such that $(a\ b)W = (d\ 0)$. Set

$$U = \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix} \begin{pmatrix} W & 0 \\ 0 & I \end{pmatrix}$$

and $AU = (d\ 0\ \cdots\ 0)$.

We now proceed to the general case. Right-multiply A by a unimodular matrix V which reduces the first row. Then

$$AV = \begin{pmatrix} a & 0 \\ B & C \end{pmatrix}$$

where C is an $m-1$ by $n-1$ matrix. By induction there is a unimodular matrix W such that CW is triangular. Then

$$AV \begin{pmatrix} 1 & 0 \\ 0 & W \end{pmatrix}$$

is triangular.

As an immediate corollary we have the following result.

THEOREM 3.6. *If R is a right Hermite ring, so is R_n.*

Proof. For A, B in R_n we can find a unimodular $2n$ by $2n$ matrix U such that $(A\ B)U$ is triangular and hence has the form $(D\ 0)$.

In commutative rings there is a well known variant of the 1 by n case of Theorem 3.5, which we now prove for completeness.

THEOREM 3.7. *Let $a_1, \cdots, a_n$ be elements in a commutative Hermite ring R. Then we can find an n by n matrix with first row $(a_1\ \cdots\ a_n)$ and a determinant d satisfying $dR = a_1R + \cdots + a_nR$.*

Proof. To facilitate the induction, let us prove a little more, namely that we can choose the additional $n-1$ rows in such a fashion that they can be completed to a unimodular matrix by adjunction of a suitable nth row. Let then B be an $n-2$ by $n-1$ matrix which when adjoined to $(a_1\ \cdots\ a_{n-1})$ yields a determinant e with $eR = a_1R + \cdots + a_{n-1}R$; and let C denote the extra row which makes B unimodular. Effect the reduction of $(e\ a_n)$:

$$(e\ a_n) \begin{pmatrix} p & r \\ q & s \end{pmatrix} = (d\ 0).$$

Then we have

$$\begin{vmatrix} a_1 \cdots a_{n-1} & a_n \\ B & 0 \\ (-)^{n-1}qC & p \end{vmatrix} = d,$$

and we successfully continue the induction by observing that

$$\begin{bmatrix} B & 0 \\ (-)^{n-1}qC & p \\ (-)^{n-1}sC & r \end{bmatrix}$$

is unimodular.

The reduction to triangular form enables us to prove the following two results, which show to some extent that properties of R are inherited by R_n.

THEOREM 3.8. *Let R be a right Hermite ring with no divisors of 0, and let A_1, A_2 be (possibly rectangular) matrices over R which are right multiples of each other. Then A_1, A_2 are right associates.*

Proof. There is no harm in right-multiplying A_i by unimodular matrices, and so we may assume that A_i are in triangular form:

$$A_i = \begin{pmatrix} a_i & 0 \\ B_i & C_i \end{pmatrix}.$$

Then we have that a_1 and a_2 are mutual right multiples, whence $a_2 = a_1 u$, u a unit. If $a_i = 0$ we can simply ignore the first row and apply induction. So we suppose $a_i \neq 0$. Then from the equation

$$(7) \qquad \begin{pmatrix} a_1 & 0 \\ B_1 & C_1 \end{pmatrix}\begin{pmatrix} u & R \\ Q & S \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ B_2 & C_2 \end{pmatrix}$$

we find $a_1 R = 0$, whence $R = 0$, $C_2 = C_1 S$. Thus C_1, C_2 are mutual right multiples and by induction $C_2 = C_1 U$ where U is unimodular. If we replace S by U in (7), it will do no harm, and we shall have achieved a unimodular matrix.

THEOREM 3.9. *Let R be a right Hermite ring in which $ab = 1$ implies $ba = 1$. Then the same is true in R_n.*

Proof. Suppose $AB = I$ in R_n. Then $(AU)(U^{-1}B) = I$ where AU is triangular. Write

$$AU = \begin{pmatrix} a & 0 \\ B & C \end{pmatrix}, \qquad U^{-1}B = \begin{pmatrix} p & Q \\ R & S \end{pmatrix}.$$

Then $ap = 1$, whence $pa = 1$; and $aQ = 0$ whence $Q = paQ = 0$. So CS is the identity matrix and by induction C is unimodular, as is A.

4. A weaker triangular reduction. Something can be done in rings which merely satisfy the condition that finitely generated ideals are principal. The idea is based on the following remark, valid in any ring([2]): if a and b are right multiples of each other, then $(a\ 0)$ and $(b\ 0)$ are right associates. In fact if

---

([2]) This remark is similar to, but not the same as the fundamental device in [8].

$b = ax$, $a = by$, then

$$(a\ 0)\begin{pmatrix} x & 1 - xy \\ 1 & -y \end{pmatrix} = (b\ 0),$$

$$\begin{pmatrix} x & 1 - xy \\ 1 & -y \end{pmatrix}^{-1} = \begin{pmatrix} y & 1 - yx \\ 1 & -x \end{pmatrix}.$$

The device extends as follows. Suppose $a_1R + \cdots + a_nR = dR$, so that $d = \sum a_i x_i$, $a_i = dy_i$. Write X, Y for the column and row vectors $(x_1, \cdots, x_n)$, $(y_1, \cdots, y_n)$ respectively. Then

$$(a_1 \cdots a_n\ 0)\begin{pmatrix} X & I - XY \\ 1 & -Y \end{pmatrix} = (d\ 0 \cdots 0).$$

Thus at the expense of adjoining a single zero we can effect the reduction of a row matrix. By induction it follows readily that the addition of m colunms of zeros will permit the reduction of an m-rowed matrix. The precise result is stated in the following theorem.

THEOREM 4.1. *Let R be a ring in which every finitely generated right ideal is principal. Let A be an m-rowed matrix over R, and A_1 the matrix obtained by adjoining m columns of zeros to A. Then we can find a unimodular matrix U such that A_1U is triangular (that is, has zeros above the main diagonal).*

A further consequence of some interest may be noted: if $(a\ b)$ admits reduction to $(d\ 0)$, then it admits reduction to any $(d_1\ 0)$ with $d_1R = dR$, and similarly in Theorem 3.7 any determinant d may be obtained with $dR = a_1R + \cdots + a_nR$.

5. **Diagonal reduction.** We recall the definition: a matrix A admits diagonal reduction if there exist unimodular matrices P, Q such that (1) holds with d_i a total divisor of d_{i+1}. For row or column matrices, diagonal reduction of course coincides with the triangular reduction already discussed. The following theorem shows that the new difficulties are essentially already embodied in the 2 by 2 case.

THEOREM 5.1. *If all 1 by 2, 2 by 1, and 2 by 2 matrices over R admit diagonal reduction, then all matrices admit diagonal reduction and R is an elementary divisor ring.*

REMARK. If R has no divisors of 0, we need only assume the possibility of reduction for 2 by 2 matrices. For we can readily infer the reducibility of $(a\ b)$ from that of the same with a row of zeros added.

Proof. Let A be an m by n matrix. Choose notation so that $m \geq n$. We may suppose by induction that we know diagonal reduction to be possible for smaller m, and for the given m if n is smaller. It is to be observed that m is at least 3. Write A_1 for the first row of A and A_2 for the remaining $m-1$ rows.

We can find unimodular matrices P_1, Q_1 such that $B = P_1 A_2 Q_1 = \text{diag}(x, \cdots)$. Then also

$$C = \begin{pmatrix} 1 & 0 \\ 0 & P_1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} Q_1 = \begin{pmatrix} A_1 Q_1 \\ B \end{pmatrix}.$$

Now write D for the first two rows of C and E for the remainder. Applying induction again we have $F = P_2 D Q_2 = \text{diag}(y, \cdots)$ and then

$$H = \begin{pmatrix} P_2 & 0 \\ 0 & I_{m-2} \end{pmatrix} \begin{pmatrix} D \\ E \end{pmatrix} Q_2 = \begin{pmatrix} F \\ G \end{pmatrix}.$$

Now y is a total divisor of all the elements of F and also of all the elements of D, as appears from $D = P_2^{-1} F Q_2^{-1}$; in particular y is a total divisor of x, the latter being one of the elements of D. The elements of G are linear combinations of those of E, and hence they are totally divisible by x and a fortiori by y. Thus y is a total divisor of every element of H. We may now use elementary transformations to sweep out the first column of H and we reach

$$\begin{pmatrix} y & 0 \\ 0 & K \end{pmatrix}$$

where y is still a total divisor of every element of K. Applying induction to K, we complete the reduction.

Under rather restrictive assumptions we are able to state necessary and sufficient conditions for a ring to be an elementary divisor ring.

THEOREM 5.2. *Let R be a commutative ring whose divisors of 0 are in the radical. Then necessary and sufficient conditions for R to be an elementary divisor ring are* (1) *all finitely generated ideals are principal,* (2) *if $(a, b, c) = 1$, there exist p and q such that $(pa, pb + qc) = 1$*[3].

Proof. We know that (1) is necessary even for R to be an Hermite ring. To prove the necessity of (2), let

(8) $$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

and suppose PAQ effects the diagonal reduction of A. It is clear that PAQ has a unit u in its upper left corner. Suppose the first row of P consists of p, q and the first column of Q consists of x, y. Then $pax + pby + qcy = u$, whence $(pa, pb + qc) = 1$.

To prove the sufficiency we first observe (Theorem 3.2) that R is an Hermite ring. Given a 2 by 2 matrix, we may thus arrange to get a zero,

---

[3] The parentheses here denote greatest common divisor (unique up to a unit under the hypothesis).

say in the lower left corner. We thus reach the matrix A of (8). Write $(a, b, c) = d$, $d = xa + yb + zc$, $a = a_1d$, $b = b_1d$, $c = c_1d$. We dismiss the case $d = 0$ and thus find that $xa_1 + yb_1 + zc_1$ is a unit; without loss of generality we may change notation and assume $(a, b, c) = 1$. We now take the p and q offered us in hypothesis (2), observe that necessarily $(p, q) = 1$, complete the row p, q to a unimodular matrix, and use it to left-multiply A. The result is a matrix with pa, $pb + qc$ for its first row. Right multiplication by a suitable unimodular matrix converts this to 1, 0. We sweep out the element in the lower left corner and thus complete the reduction.

Helmer [12] has defined an *adequate*([4]) ring R to be a commutative ring in which every finitely generated ideal is principal, and which further satisfies the following condition: for any a, $c \in R$ with $a \neq 0$ we can write $a = rs$ with $(r, c) = 1$ and $(s', c) \neq 1$ for any non-unit divisor s' of s. The ring of entire functions forms an excellent example of such a ring. The following generalizes Helmer's theorem.

THEOREM 5.3. *An adequate ring whose divisors of 0 are in the radical is an elementary divisor ring.*

Proof. We are given $(a, b, c) = 1$, and we seek to verify hypothesis (2) of Theorem 5.2. The case $a = 0$ presents no trouble, so we assume $a \neq 0$ and shall then actually produce q with $(a, b + qc) = 1$, thus doing more than needed. Write $a = rs$ with the property asserted above. Since $(r, c) = 1$, the congruence

$$b + qc \equiv 1 \pmod{r}$$

can be solved for q. Write $d = (a, b + qc)$. Then $(d, r) = 1$, and it follows from $a = rs$ that d divides s. If d is not a unit then by hypothesis $(d, c) \neq 1$. This contradicts $(a, b, c) = 1$.

We shall conclude this section by observing what can be accomplished with chain conditions. We pose the question as follows: granted that R is an Hermite ring, what chain condition will suffice to assure us that R is an elementary divisor ring? It appears that the ordinary ascending chain condition is not strong enough and must be reinforced to what we shall call the *mixed ascending chain condition*: no infinite sequence $\{a_i\}$ can exist, where for each i either $a_i R \subset a_{i+1} R$ or $R a_i \subset R a_{i+1}$ (proper inclusion). It is to be observed that this implies the ascending chain condition for principal right ideals and that for principal left ideals, and in a ring whose finitely generated ideals are principal, it implies these chain conditions unrestricted to principal ideals. In a commutative ring it is simply the ordinary ascending chain condition on principal ideals.

THEOREM 5.4. *An Hermite ring which satisfies the mixed ascending chain*

([4]) Helmer's adequate rings have no divisors of 0.

condition is an elementary divisor ring.

Proof. We are given a 2 by 2 matrix A. Consider the totality of equivalent matrices (matrices of the form PAQ with P, Q unimodular). On the authority of the mixed ascending chain condition we can find one, say

$$W = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$$

whose upper left element w satisfies the following condition: if B is any equivalent matrix and b its upper left element, then wR is not properly contained in bR, and Rw is not properly contained in Rb. It follows that w must left-divide x, for we can pass to an equivalent matrix whose upper left element generates $wR+xR$. Similarly w right-divides y. We may sweep away x and y and reach a matrix of the form

$$\begin{pmatrix} w & 0 \\ 0 & t \end{pmatrix}.$$

Now we argue further that w must be a left divisor of any left multiple of t, for

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} w & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} w & at \\ 0 & t \end{pmatrix}.$$

Likewise w right-divides any right multiple of t. In short, w is a total divisor of t.

From Theorems 3.1 and 5.4 we can deduce the theorem of Jacobson-Teichmüller that any principal ideal ring without divisors of 0 is an elementary divisor ring, as soon as we verify the mixed ascending chain condition. This is done by showing that for $a \neq 0$, composition series from R to Ra and from R to aR are finite and have the same length; we refer to [13, p. 34] for details. A more general result on principal ideal rings will be proved in §12.

The theorems proved in this section, and those in some later sections, do not exhaust the class of elementary divisor rings. One particular fact worth mentioning is that a Boolean ring (with unit) is an elementary divisor ring. This is perhaps proved most readily by the observation that a finitely generated Boolean ring is the direct sum of a finite number of fields of two elements. There are two generalizations that can be proved by exploiting the methods and results in [2]: (1) the ring of continuous functions from a compact zero-dimensional space to a (discrete) elementary divisor ring is an elementary divisor ring, (2) any strongly regular ring (in the sense of [2]) is an elementary divisor ring.

6. **Congruence of alternate matrices.** Following Albert [1], we define a square matrix to be *alternate* if $a_{ij} = -a_{ji}$, $a_{ii} = 0$. If $2a = 0$ implies $a = 0$, the

second condition is of course redundant. If P is unimodular, we say that $P'AP$ is *congruent* to A (P' is the transpose of P). In a commutative ring it may be verified by computation that a matrix congruent to an alternate matrix is alternate; or we may observe that A being alternate is equivalent to an invariant property of a scalar product in an n-dimensional vector space over R.

In the following theorem the notation $\dotplus$ is used to denote the direct sum of matrices [23, p. 47].

THEOREM 6.1. *Let R be a commutative Hermite ring and A an n by n alternate matrix over R. Then A is congruent to a matrix of the form*

$$(9) \qquad \begin{pmatrix} 0 & a_1 \\ -a_1 & 0 \end{pmatrix} \dotplus \begin{pmatrix} 0 & a_2 \\ -a_2 & 0 \end{pmatrix} \dotplus \cdots$$

where a_i divides a_{i+1}. In case n is odd a final 1 by 1 matrix 0 is to be adjoined.

Proof. We follow in outline the proof of Cahen [23, p. 52], with a modification to avoid the use of chain conditions. No essential change is needed in the first part of the proof; by reduction of rows (using the 1 by $n-1$ case of Theorem 3.5) we pass from A to a congruent matrix B having zeros everywhere except for elements $b_1, \cdots, b_{n-1}$ on the diagonal next above the main diagonal, and of course their negatives on the symmetrically opposite diagonal. Now effect the reduction

$$(b_1 \cdots b_{n-1})U = (d \quad 0 \cdots 0)$$

with U unimodular. To the ith row of U ($2 \leq i \leq n-2$) add the sum of the first $i-1$ rows; the first and last rows of U are to be left unchanged. The resulting matrix V is still unimodular. Now we enlarge V to an n by n matrix as follows: place a row of $n-1$ zeros above V, and then place to the left a column consisting of $n-1$ ones followed by a zero. If Q is the resulting matrix, computation shows that $C = Q'BQ$ begins with $0, d, \cdots$. The element d divides every element in C, and we may proceed to sweep out the first and second rows and columns, reaching a matrix

$$\begin{pmatrix} 0 & d \\ -d & 0 \end{pmatrix} \dotplus D,$$

where d still divides every element of D. Induction completes the proof.

We add a few words on necessary conditions for a reduction to (9). It is easy to see that congruence of

$$\begin{bmatrix} 0 & a & b \\ -a & 0 & 0 \\ -b & 0 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & d & 0 \\ -d & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

is possible only if $aR+bR=dR$. Thus it is necessary that finitely generated ideals be principal. I have not determined whether it is necessary for R to be an Hermite ring. However, if divisors of 0 are in the radical, then we can assert that a necessary and sufficient condition for congruence to (9) is that all finitely generated ideals be principal.

7. **Elementary matrices.** We refer to [13, p. 42] for the definition of elementary matrices and the elementary transformations they induce. We raise the following question: to what extent can the reductions of §§3–6 be effected by elementary transformations? The following is a more or less satisfactory answer.

THEOREM 7.1. *Let R be a right Hermite ring in which the reduction $(a\ b)U = (d\ 0)$ can be effected with U a product of elementary matrices. Then every unimodular matrix over R is a product of elementary matrices.*

Proof. Following the first part of the proof of Theorem 3.5 virtually verbatim, we show that any 1 by n matrix admits reduction by a product of elementary matrices. Let then A be a unimodular matrix, and U a product of elementary matrices reducing the first row of A, say to $(a\ 0\ \cdots\ 0)$. Then a is necessarily a unit. Elementary transformations on the left will convert AU to the form

$$\begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}.$$

By induction B is a product of elementary matrices and so is A.

Examples satisfying the hypothesis of Theorem 7.1 are furnished by rings admitting a right Euclidean algorithm [32]; such rings are necessarily right principal ideal rings. If a ring R admits both a right and a left Euclidean algorithm, then the standard proof shows that R is an elementary divisor ring, divisors of 0 being irrelevant.

8. **You can do it without a unit.** We have assumed up to this point that all rings under discussion have a unit element. This restriction was however not necessary. One could adjoin a unit in the usual way, prove a given theorem, and then translate it back to the original ring; but this is both inelegant and technically awkward. If rings without unit are to be investigated, it is possible and preferable to do so directly. As a sample, we formulate the definition of equivalence: two matrices A, B are equivalent if there exist quasi-regular matrices P, Q such that $B=PAQ+PA+AQ+A$ (P is quasi-regular if there exists P_1 with $P+P_1+PP_1=P+P_1+P_1P=0$). Then the theorems on diagonal reduction in §5 go through, with certain slight modifications in handling principal ideals. It did not seem worth while to grapple with these added complications, and so we have relegated the discussion of rings without unit to these brief remarks.

When we come to the treatment of R-modules, however, it is not so easy

to dispense with a unit element, and we shall constantly assume one which moreover acts as unit operator. It is well known that if R does in fact have a unit element 1, then it is a spurious generalization to omit the assumption that it acts as unit operator, for an R-module decomposes into the direct sum of a trivial module and a module having 1 as unit operator. It would be interesting to work out a successful theory of modules over rings having "approximate" unit elements in some sense, a good example being Boolean rings. However, one must not expect too much of such a theory, as the following theorem shows.

THEOREM 8.1. *Let R be a ring having the property that for every right R-module M, MR is a direct summand of M. Then R has a left unit element.*

Proof. Let S be the ring obtained from R by the usual formal adjunction of a unit; S consists of pairs (a, n) where $a \in R$ and n is an integer, and is a right R-module in a natural way. Write $S = SR \oplus T$. The elements of SR all have second component 0. Hence in the direct sum, the element $(0, 1)$ has components $(e, 0)$ and $(-e, 1)$. Then for any x in R, $(-e, 1)x = (x - ex, 0) \in T \cap SR = 0$. Hence e is a left unit element.

Theorem 8.1 provides a short proof for a theorem of Goldman [11, Theorem III].

9. **Modules.** We shall always be speaking of right R-modules, and R is assumed to have a unit element which acts as unit operator.

Let us note the connection between modules and matrices. Any R-module can be represented as a difference module $F - G$, where F is a free module. Let $\{u_i\}$ be a basis for F and $\{v_j\}$ a set spanning G. Write $v_j = \sum u_i a_{ij}$. We arrange the elements a_{ij} in a matrix, for convenience well-ordering the rows and columns; there will be only a finite number of nonzero elements in each column. In this fashion we attach a matrix to any R-module, and conversely any column-finite matrix names a module. It is clear that equivalent matrices name isomorphic modules; for in setting $B = PAQ$ (with P, Q column-finite matrices with two-sided inverses), we are merely changing bases in F and G. We observe that a diagonal matrix names a direct sum of cyclic modules; more generally, any matrix with at most one nonzero entry in each row and column names a direct sum of cyclic modules. We may then state the following theorem.

THEOREM 9.1. *Let R be an elementary divisor ring, F a free R-module with finite basis, and G a finitely generated submodule of F. Then $F - G$ is isomorphic to a direct sum of cyclic modules $R - a_i R$ where a_i is a total divisor of a_{i+1}.*

A word of warning is in order. Theorem 9.1 does not give us the structure of an arbitrary finitely generated module M over an elementary divisor ring R, for though we may represent M as $F - G$ with F a free module with a finite basis, there is no assurance that G is finitely generated (in other words, we

may have a matrix with a finite number of rows but an infinite number of columns). If R further satisfies the ascending chain condition on right ideals, then G will be finitely generated, and in this case Theorem 9.1 does give us the structure of any finitely generated R-module. Further remarks on this point are made in §11.

We have remarked that equivalent matrices give rise to isomorphic modules. It is not true conversely that matrices which name isomorphic modules are necessarily equivalent, for among other things they may not even have the same size. However the following more modest converse has been proved by Fitting [8]: if A and B name isomorphic modules, then

$$\begin{pmatrix} A & 0 & 0 \\ 0 & I & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} B & 0 & 0 \\ 0 & I' & 0 \end{pmatrix}$$

are equivalent, where the adjoined identity and zero matrices are of suitable sizes.

We shall now consider questions of uniqueness. We remark first on the essential equivalence of uniqueness theorems for matrices and modules. It is clear that a suitable uniqueness theorem, on the expression of a module as a direct sum of cyclic modules, implies the same uniqueness for the invariant factors of matrices (we follow customary terminology in referring to the diagonal elements of a reduced matrix as its invariant factors). Conversely, suppose we have some uniqueness result for the invariant factors of matrices, and let us make the modest supposition that in particular the uniqueness asserts that units correspond only to units. Then Fitting's result readily enables us to translate the uniqueness over to modules. From this remark, and the well known uniqueness of invariant factors of matrices over an integral domain, we can derive a uniqueness theorem for modules over integral domains. However the stronger Theorem 9.3 yields to direct module arguments.

LEMMA 9.2. *Let M be the direct sum of cyclic modules $R - S_i$ ($i = 1, \cdots, n$), where S_i is a right ideal. Suppose further that $S_1 + \cdots + S_n$ is contained in a proper two-sided ideal W with the property that matrices over $R - W$ are unimodular if they have one-sided inverses. Then M cannot be spanned by fewer than n elements.*

REMARK. In the case $S_1 = \cdots = S_n = 0$, the conclusion gives us the invariance of the number of basis elements of a free R-module. In the light of [3, Theorem 5], this lemma includes the results to be found in [6] and [7].

Proof. The proof is virtually the same as that in [13, p. 32], but we give it for completeness. Suppose M is spanned by $y_1, \cdots, y_m$ ($m < n$), and let x_i be the generator of $R - S_i$ (that is, the coset $1 + S_i$). Writing (x_i) and (y_j) as row vectors, we have $(y_j) = (x_i)A$, $(x_i) = (y_j)B$, where A is n by m and B is

m by n. From $(x_i)AB = (x_i)$ we deduce that AB must be congruent mod W to the n by n identity matrix. Let A', B' denote the result of appending $n-m$ columns and rows respectively to A, B. Then also $A'B' \equiv I \pmod{W}$. By hypothesis $B'A' \equiv I \pmod{W}$, a manifest absurdity.

THEOREM 9.3. *Let R be a ring in which every one-sided ideal is two-sided. In particular, R may be any commutative ring. Suppose the R-module M is isomorphic to the direct sum of cyclic modules $R - S_1, \cdots, R - S_m$, and also to the direct sum of $R - T_1, \cdots, R - T_n$, where S_i, T_j are ideals each containing its successor, S_1, $T_1 \neq R$. Then: $m = n$ and $S_i = T_i$.*

Proof. We begin with some simple remarks on the effect of multiplying modules by scalars. It is to be noted that, by our hypothesis, any right multiple of an element c in R can be written as a left multiple of c. It follows that for any R-module M, Mc is again an R-module. Also: (1) $(M_1 \oplus \cdots \oplus M_r)c$ is isomorphic to $M_1 c \oplus \cdots \oplus M_r c$. (2) If M is cyclic, so is Mc. In fact, if M is generated by x, then Mc is generated by xc. (3) If further I is the annihilating ideal of x (or of M—they are identical in this context), then $Mc = 0$ if and only if c is in I. More generally, the annihilating ideal of Mc is precisely the ideal of all a in R with $ca \in I$. From this we deduce our final remark. (4) Suppose we have the cyclic modules $M = R - I$ and $N = R - J$ with I containing J; then the annihilating ideal of Mc contains that of Nc.

The hypothesis that all ideals in R are two-sided can be seen to imply that matrices over R are unimodular if they have one-sided inverses. Since any homomorphic image of R inherits the property that all ideals are two-sided, it follows that Lemma 9.2 is applicable.

We turn now to the proof of Theorem 9.3. That $m = n$ is a consequence of Lemma 9.2. Suppose $S_i \neq T_i$ and select an element c which is, say, in S_i but not in T_i. Then (by the remarks above) Mc is on the one hand the direct sum of fewer than $n - i + 1$ nonzero cyclic modules, and on the other hand the direct sum of at least that many. Moreover in each decomposition the annihilating ideals still contain their successors. By induction (say on $m+n$) we have a contradiction.

10. Valuation rings. We generalize Krull's definition of valuation rings [20] by admitting divisors of 0 and non-commutativity. If we were to restrict ourselves to the case of no divisors of 0, we could use Schilling's formulation [25].

DEFINITION. A ring R is said to be a *valuation ring* if for any a, $b \in R$, either a is a total divisor of b or b is a total divisor of a.

In particular a is a total divisor of itself. Hence any left multiple of a is a right multiple; every ideal is two-sided. Left and right divisibility coincide and we may use the term "divide" unambiguously. It is easy to see that the sum of any two non-units is a non-unit. Thus the non-units form the unique maximal ideal which is the radical, and modulo the radical we have a division

ring. In particular, all divisors of 0 are in the radical, and we may use any-
thing we have proved under that hypothesis. For example (Theorem 2.1)
generators of principal ideals are unique. It follows also that left and right
associates coincide, and we use "associate" unambiguously. The elements
group themselves into equivalence classes of associates; these classes are pre-
served under multiplication and are naturally ordered by divisibility. In
short, we have a valuation on an ordered semi-group (the reader may invent
his own postulates for an ordered semi-group).

We may take it as obvious that a valuation ring is an elementary divisor
ring: place an element dividing everything in the upper left corner, sweep out
the first row and column, and so on. Theorem 9.3 is applicable to any valua-
tion ring. It follows that over a valuation ring the invariant factors of matrices
are unique up to associates, and we shall use this fact in the sequel.

For valuation rings a stronger result than Theorem 9.3 can be proved: as
Theorem 10.1 shows, we can do something with infinite direct sums. It would
be of interest to know if Theorem 10.1 can be extended to a wider class of
rings, but one must formulate it carefully: observe that the direct sum of a
countable number of replicas of a cyclic group of order 6 is isomorphic to the
direct sum of itself and a cyclic group of order 2. However Theorem 10.1 is
strong enough to yield a conclusive result for commutative principal ideal
rings, as follows from §12 and standard considerations on the decomposition
of a module into its primary parts: we get a uniqueness theorem for the ex-
pression of a module as a direct sum of (any number of) indecomposable
cyclic modules.

THEOREM 10.1. *Let a_1, a_2, $\cdots$ be a sequence of non-units in a valuation
ring R, each properly dividing its successor. Write M_i for the R-module $R - a_i R$.
Suppose the module M is the direct sum of modules M_i in two ways, having re-
spectively α_i and β_i summands M_i. Then: $\alpha_i = \beta_i$ for each i.*

Proof. If a divides b, $b \neq 0$, let us write b/a for any element c with $b = ac$;
it is readily seen that b/a is determined up to a unit, and that much am-
biguity need not concern us. This "division" has the following desirable prop-
erties: (1) b/a is a unit if and only if a and b are associates, (2) $(c/b)(b/a)$
and c/a are associates, (3) the module $(R - bR)a$ is isomorphic to $R - (b/a)R$.

We need some remarks on annihilators of scalars. If M is a module and c
any element in R, then the subset of M annihilating c is evidently a sub-
module of M; also the submodule of a direct sum thus obtained is the direct
sum of the corresponding submodules. Finally, if a divides b ($b \neq 0$), then
the annihilator of a in the module $R - bR$ is precisely the submodule
$(R - bR)(b/a)$.

Consider the following two operations on an R-module: (1) taking the
submodule annihilating a_1, (2) taking the submodule annihilating a_2 and then
multiplying by a_2/a_1. By suitably combining the observations above, we see
that these two operations yield precisely the same result when applied to

the module M_i ($i>1$), to wit, they both yield $M_i(a_i/a_1)$. When applied to the module M_1, the first operation does nothing, while the second passes us to the submodule $N=M_1(a_2/a_1)$. Since a_2/a_1 is not a unit, $N\neq M_1$. If we let P and Q respectively denote the results of applying the two operations to the module M, we see that $P-Q$ is isomorphic to α_1 and also to β_1 replicas of M_1-N. If α_1 and β_1 are both finite, Theorem 9.3 tells us they are equal. If either is infinite, a theorem valid under very general conditions asserts that they are both infinite and equal [4, p. 20, Ex. 13].

Next consider the module Ma_{i-1}. This multiplication wipes out M_r for $r<i$, and for $r\geqq i$ it converts M_r into a module isomorphic to $R-(a_r/a_{i-1})R$. The elements a_r/a_{i-1} still have the property that each properly divides its successor. Our set-up is thus unaltered, and hence the argument that proved $\alpha_1=\beta_1$ is applicable to prove that $\alpha_i=\beta_i$. This concludes the proof of Theorem 10.1.

We return now to the consideration of finite matrices, and we pass from the question of the uniqueness of the invariant factors to that of their behaviour under multiplication.

LEMMA 10.2. *Let* $C=(A\ B)$ *be matrices over a valuation ring, with* $A=\mathrm{diag}\ (d_1,\ \cdots,\ d_r)$, d_i *a divisor of* d_{i+1}. *Then the ith invariant factor of* C *divides* d_i ($i=1,\ \cdots,\ r$).

Proof. Let x be an element of C dividing all others, and use elementary transformations to sweep out its row and column. This will leave A unchanged if x is d_1 or if it falls below d_r. If x is in the same row as d_j, the operations will place sundry elements on the column of d_j and otherwise will not affect A. Of course x is the first invariant factor of C. The remaining ones are the invariant factors of $(A'\ B')$ where $A=\mathrm{diag}\ (d_1,\ \cdots,\ d_{j-1},\ d_{j+1},\ \cdots,\ d_r)$ and B' collects what is left after the deletion of the row and column of x. The lemma now follows by induction.

THEOREM 10.3. *Over a valuation ring, the invariant factors of* $C=AB$ *are multiples of those of* A. *To be more precise, if* C *has fewer invariant factors than* A, *they are multiples as long as they last; if* C *has more invariant factors than* A, *the extra ones are* 0.

Proof. The columns of C are linear combinations of those of A. Thus $(A\ C)$ is equivalent to $(A\ 0)$ and its invariant factors are evidently those of A with perhaps some extra zeros. On the other hand, we may pass to $(A'\ C')$ where C' has its invariant factors down its main diagonal. The result now follows from Lemma 10.2.

We may pass from valuation rings to more general rings by a device due to Krull, which is embodied in the following lemma.

LEMMA 10.4. *Let* R *be a ring which is an intersection of valuation rings* S_i, *and suppose that for* a, b *in* R, a *is a total divisor of* b *if it divides* b *in every* S_i.

Let $A = \mathrm{diag}\ (d_1,\ \cdots)$ and $B = \mathrm{diag}\ (e_1,\ \cdots)$ be matrices of the same size over R[5], *with B a multiple of A, $B = PAQ$. Then d_i is a total divisor of e_i.*

The hypothesis of Lemma 10.4 is notably fulfilled in the case of any integrally closed integral domain [21, p. 552], and the conclusion is accordingly valid. Actually the commutativity permits us to do something more general: we may form the determinantal ideals (the ith determinantal ideal is generated by the i by i subdeterminants). Following Krull, there is no difficulty in proving the following statements, which constitute a generalization of results of Steinitz [28].

THEOREM 10.5. *Let R be an integrally closed integral domain and A, A' matrices of the same size*[5] *over R with $A' = PAQ$. Let D_i, D_i' denote the determinantal ideals of A, A'. Then any principal ideal containing $D_{i+1}D_i'$ also contains $D_i D_{i+1}'$. If R is further a multiplication ring (that is if every finitely generated ideal is invertible) we form the invariant factor ideals $E_i = D_i D_{i-1}^{-1}$ and E_i divides E_i'* [6].

Another generalization of known results can be proved.

THEOREM 10.6. *Let R be an elementary divisor integral domain, and A, B matrices of the same size over R which are multiples of each other. Then A, B are equivalent.*

Proof. By Theorem 10.5 the invariant factors are multiples of each other and hence associates[7]. The theorem then becomes evident on passage to the diagonal form.

We conclude this discussion of divisibility with a theorem on one-sided divisibility. Systems of linear equations correspond to the case where B is a single column.

THEOREM 10.7. *Let R be an elementary divisor ring in which all ideals are two-sided and the invariant factors of a matrix are unique up to associates. Let A, B be matrices over R with the same number of rows. Then a necessary and sufficient condition for B to be a right multiple of A is that A and $(A\ B)$ have the same nonzero invariant factors.*

Proof. We may suppose A in the form $\mathrm{diag}\ (d_1,\ \cdots)$. Then d_1 must divide every element of B and in particular its first row. It follows that $d_2, d_3,\ \cdots$ are the invariant factors of $(A'\ B')$ where $A' = \mathrm{diag}\ (d_2, d_3,\ \cdots)$ and B' is B with its first row deleted. By induction B' is a right multiple of A' and consequently B is a right multiple of A.

---

[5] This can be generalized, with the same precautions as in Theorem 10.3.

[6] In the same way we can prove that E_i divides E_{i+1}.

[7] It is necessary to observe that R is integrally closed; this is true for any integral domain whose finitely generated ideals are principal.

It is perhaps worth mentioning that if R is merely an Hermite ring, we can base a systematic discussion of one-sided divisibility on the triangular reduction, and we can even fall further back on Theorem 4.1. The results are comparable with von Neumann's theory of linear equations in regular rings [24, pp. 15–17].

11. **Modules over valuation rings.** The fact that a valuation ring R is an elementary divisor ring does not suffice to determine the structure of a finitely generated R-module, as we have remarked earlier. Nevertheless we might still ask whether such a module is a direct sum of cyclic modules, although we of course abandon the idea that the annihilating ideals are principal. It turns out that this will be so if and only if a certain strong condition is imposed on R. This condition is of a technical nature, and we refer the reader to [16] for the definitions relevant for the following theorem. To avoid excessive complications, we have taken R to be an integral domain and confined ourselves to modules with two generators.

THEOREM 11.1. *For a valuation integral domain R the following two statements are equivalent*: (1) *every R-module with two generators is a direct sum of cyclic modules*, (2) *every pseudo-convergent set of nonzero breadth in R has a limit in R.*

REMARK. By [16, Theorem 4] condition (2) is implied by maximality. As is fitting and proper, it imposes no restriction on R in case R has the ascending chain condition (that is, when the value group is the group of integers).

Proof. We first prove that (2) implies (1). Represent the given module M as $F-G$ where F is the free module with basis x, y. It will be convenient to agree that the letters a, b always stand for the coefficients of an element $xa+yb$ in G. If it is always true that xa, yb are separately in G, then it is evident that $F-G$ is a direct sum of cyclic modules. So we suppose we have an element xa_1+yb_1 in G with neither xa_1 nor yb_1 in G. Let us suppose for definiteness that a_1 divides b_1, or as we shall henceforth write, $Va_1 \leq Vb_1$, V denoting the valuation attached to R. If all elements of G are proportional to this element xa_1+yb_1, we again see that the conclusion is obvious. So let there be a second linearly independent element xa_2+yb_2 in G. Then $yf \in G$ where $f = a_1b_2 - a_2b_1 \neq 0$.

We define $c_1 = b_1/a_1$, $z_1 = x+yc_1$, and we suppose that for every ordinal ρ less than λ we have defined c_ρ and $z_\rho = x+yc_\rho$ with the following properties:

(a) $z_\rho a \in G$ implies $z_\sigma a \in G$ for $\rho < \sigma$,

(b) $z_\rho a$, $z_\rho a' \notin G$ imply $V(c_\rho - b/a) < V(b'/a' - b/a)$,

(c) For $\rho < \sigma$ and $z_\sigma a \notin G$ we have

$$(10) \qquad\qquad V(c_\sigma - b/a) > V(c_\rho - b/a),$$

(d) $\{c_\rho\}$ is pseudo-convergent. We write γ_ρ for $V(c_\sigma - c_\rho)$ $(\rho < \sigma)$.

(e) $\gamma_\rho < Vf$.

Case I. λ not a limit ordinal. If for every a, $z_{\lambda-1}a \in G$, the process stops (see below). If not, suppose $z_{\lambda-1}a^* \notin G$ and define $c_\lambda = b^*/a^*$, $z_\lambda = x + yc_\lambda$. (a) If $z_{\lambda-1}a \in G$, then necessarily $Va^* < Va$, and $z_\lambda a = (z_\lambda a^*)(a/a^*) \in G$. (b) To prove this for λ, suppose for definiteness that $Va' \leqq Va$. Then

$$(xa + yb) - (xa' + yb')a/a' = y[(c_\lambda - b'/a') - (c_\lambda - b/a)]a \in G.$$

This equation shows that the difference between $c_\lambda - b/a$ and $c_\lambda - b'/a'$ must have higher value than either, for otherwise

$$xa + yb = z_\lambda a + y(b - c_\lambda a)$$

leads to the contradiction $z_\lambda a \in G$. (c) Apply (b) with $\rho = \lambda - 1$, $a' = a^*$ and we have $V(c_{\lambda-1} - b/a) < V(c_\lambda - b/a)$. For any $\rho < \lambda - 1$ we have $V(c_{\lambda-1} - b/a) > V(c_\rho - b/a)$ by induction. We deduce (10) for $\sigma = \lambda$. (d) From (c) with a, b replaced by a^*, b^* we have $V(c_\lambda - c_\sigma) > V(c_\lambda - c_\rho)$. It follows that $V(c_\lambda - c_\sigma) > V(c_\sigma - c_\rho)$. (e) If $V(c_\lambda - c_{\lambda-1}) \geqq Vf$, then

$$y(b^* - c_{\lambda-1}a^*) = y(c_\lambda - c_{\lambda-1})a^* \in G$$

since $yf \in G$, and this contradicts $z_{\lambda-1}a^* \notin G$.

Case II. λ a limit ordinal. We define c_λ to be a limit of $\{c_\rho\}$; note that the induction hypothesis (e) is used here. The perseverance of conditions (d) and (e) is evident, and the proof of (b) above is valid. To prove (a), suppose $z_\rho a \in G$. Then also $z_{\rho+1}a \in G$ and

$$z_{\rho+1}a - z_\rho a = y(c_{\rho+1} - c_\rho)a \in G.$$

Now $V(c_\lambda - c_\rho) = V(c_{\rho+1} - c_\rho)$ so we have $y(c_\lambda - c_\rho)a$ in G. It follows that $z_\lambda a$ is in G. Finally to verify (c) we note that by (10), $V(c_\rho - b/a) = \gamma_\rho$ and then

$$V(c_\lambda - b/a) = V(c_\lambda - c_\rho + c_\rho - b/a) \geqq \gamma_\rho.$$

The conclusion of this transfinite induction must be the appearance of an element $z = x + yc$ such that $za \in G$ for all a. We now claim that M is indeed the direct sum of two cyclic modules, namely those with basis elements y and z (or more precisely, their images mod G). To see this we merely have to observe

$$xa + yb = za + y(b - ac).$$

We now turn to the reverse implication $(1) \to (2)$; we give the proof without full details. Suppose that on the contrary there is a pseudo-convergent set $\{u_\rho\}$ in R with no limit in R but with nonzero breadth. Write $V(u_{\rho+1} - u_\rho) = \gamma_\rho$, let α be an element of the value group exceeding all γ's, and let v_ρ be any element of value $\alpha - \gamma_\rho$. Take F to be the free module with basis x, y and G the submodule spanned by $\{xv_\rho + yu_\rho v_\rho\}$. It can be seen that the elements of the form yb in G are precisely those with $Vb \geqq \alpha$. Now let it be alleged

that $F-G$ is the direct sum of cyclic modules. It is out of the question that there be more than two of these modules, and we may take their generators to be y and $x+yc$. Then for every ρ there must exist a relation

$$(x + yu_\rho)v_\rho = yd_\rho + (x + yc)e_\rho.$$

Necessarily $e_\rho = v_\rho$ and $u_\rho = c + d_\rho / v_\rho$. Since $Vd_\rho \geqq \alpha$, we have $V(c - u_\rho) \geqq \gamma_\rho$. This makes c a limit of $\{u_\rho\}$, a contradiction.

12. **Principal ideal rings.** In this section we shall discuss principal ideal rings (rings in which every left or right ideal is principal). Although our main concern is with the commutative case, we obtain some subsidiary results without this restriction.

THEOREM 12.1. *Let R be a principal ideal ring for which divisors of 0 are in the radical. Then R either has no divisors of 0 or is a valuation ring with descending chain condition.*

Proof. Any two-sided ideal I of R is of the form $aR = Ra'$. Then $a = ua'$, $a' = av$, $ua = aw$, $a = uav = awv$. If $a \neq 0$, then $1 - wv$ is in the radical, v is a unit. Similarly u is a unit and we see that a is both a left and right generator of I.

This applies in particular to the radical $S = sR = Rs$ and to $T = S \cap S^2 \cap S^3 \cap \cdots = tR = Rt$. Write $t = st_1$. We claim $t_1 \in T$. For if not, t_1 could be written $t_1 = s^n t_2$ with t_2 not in S. Also $t = s^{n+2} t_3$, so that $s^{n+1}(t_2 - st_3) = 0$. Either $s^{n+1} = 0$ which means $t = 0$ or $t_2 \in S$, a contradiction. So $t_1 \in T$, say $t_1 = t_4 t$, $t(1 - st_4) = 0$, $t = 0$. It follows that any nonzero element can be written as a power of s times an element not in the radical.

Let us now assume that divisors of 0 really are present and show that some power of s is 0. Let $ab = 0$ where a, b are different from 0. Write $a = s^m a_1$, $b = s^m b_1$, with a_1, b_1 not in S. If $a_1 s^n = 0$ we conclude $s^n = 0$. Otherwise $a_1 s^n = s^n a_2$ where a_2 is not 0. We have $s^{m+n} a_2 b_1 = 0$ and $a_2 b_1 \neq 0$. Write $a_2 b_1 = s^p a_3$, a_3 not in S, and we have finally $s^{m+n+p} a_3 = 0$, $s^{m+n+p} = 0$. Let s^k be the lowest power of s that vanishes.

Let us note that any divisor of s is either a unit or in the radical. For if $s = ab$, then $abs^{k-1} = 0$. If a is not in the radical, $bs^{k-1} = 0$, $b \in S$, $b = cs$ and $s = acs$ shows that a is a unit.

Let a be any element not in the radical and write $aR + sR = bR$. Then b is a divisor of s. We cannot have b in the radical, hence b is a unit, and $ax + sy = 1$ shows that a is a unit. It is now clear that the only (right or left) ideals in R are the powers of S, and R is a valuation ring with descending chain condition.

Theorem 12.1 shows that principal ideal rings with divisors of 0 in the radical either fall under the Jacobson-Teichmüller theory or under the theory of §10. In either event they are elementary divisor rings, and the structure of finitely generated modules over them may be considered as known.

LEMMA 12.2. *Let I, J be two-sided ideals in a ring R such that neither contains*

*the other, and $R-I$, $R-J$ are principal ideal rings with divisors of 0 in the
radical. Then R is the only principal left ideal containing $I+J$.*

Proof. Suppose $I+J$ is contained in Rc. We first treat the case where $R-I$
has no divisors of 0. In the ring $R-J$ the ideal $(I+J)-J$ has a two-sided
generator. Let $a \in I$ be an element mapping on this generator. We can write
$a = bc$, and either b or c must be in I. The possibility $c \in I$ leads to $J \subset I$,
and so we have $b \in I$. Let us denote images mod J by asterisks. Then $a^* = b^* c^*$,
$b^* = a^* d^*$ (since b is in I), hence $a^* = a^* d^* c^*$. Either $a^* = 0$ which means $I \subset J$,
or c^* is a unit which means $Rc = R$.

There remains the case where both $R-I$, $R-J$ are valuation rings with
descending chain condition. Let M, N be the inverse images of the radicals
of $R-I$, $R-J$. If $M \neq N$, then $M+N = R$. Since suitable powers of M, N lie
in I, J respectively, we deduce $I+J = R$. So we assume $M = N$. We may
without loss of generality suppose $I \cap J = 0$, and we then have a nilpotent
radical M with $R-M$ a division ring. In particular all non-units are in M.
Let s be in M but not M^2. Then s generates M mod I, that is, $M \subset Rs + I$.
Now if c is not a unit, $c = xs + i$ ($i \in I$). Since $I \subset Rc$, we have $i = yc$ where y
cannot be a unit since that would mean $I \supset Rc \supset J$. So y is a non-unit, $1-y$ is
a unit, $c \in Rs$, $I \subset Rs$, whence $M = Rs$. From this we find that every element of
M is expressible as a unit times a power of s. It follows that R is a valuation
ring with descending chain condition. But in such a ring any two ideals are
comparable. This contradiction shows that c is a unit, $Rc = R$.

The two preceding results are admirably adapted to yield a structure
theorem on commutative principal ideal rings. Conceivably they might also
work in "mildly" non-commutative cases. But at any rate we can derive the
theorem of Krull [19] and even a slightly more general theorem([8]).

THEOREM 12.3. *Let R be a commutative ring with the ascending chain
condition, and suppose that every maximal ideal in R is principal. Then R is a
principal ideal ring and moreover it is the direct sum of a finite number of
integral domains and valuation rings with descending chain condition.*

Proof. First suppose that divisors of 0 are in the radical. We shall show
that R is a principal ideal ring. For this purpose it will suffice to show that
for any a, b, $aR + bR$ is principal. If $aR + bR = R$ there is nothing to prove.
Otherwise $aR + bR$ is contained in a maximal ideal cR. Write $a = a_1 c$, $b = b_1 c$.
We note that aR is properly contained in $a_1 R$, for otherwise (since divisors of
0 are in the radical) c would be a unit. If $a_1 R + b_1 R = R$, then $aR + bR = cR$.
If not, we repeat the operation. After a finite number of steps we shall find

---

([8]) Krull's theorem asserts that any commutative principal ideal ring has the structure
described in Theorem 12.3. His later papers contain more general results. Another theorem that
can be stated is the following: if every prime ideal in R is principal, then R is a principal ideal
ring. For I. S. Cohen has shown (unpublished) that if every prime ideal is finitely generated,
then the ascending chain condition holds.

that $aR+bR$ is principal.

Now let R be any ring satisfying the hypothesis of our theorem. Write 0 as an irredundant intersection of primary ideals: $0 = Q_1 \cap Q_2 \cap \cdots \cap Q_n$. Each $R - Q_i$ has divisors of 0 in the radical (they are even nilpotent). The preceding paragraph shows that $R - Q_i$ is a principal ideal ring. Theorem 12.1 shows that it is either an integral domain or a valuation ring with descending chain condition. Lemma 12.2 shows that $Q_i + Q_j = R$. Hence R is the direct sum of the rings $R - Q_i$.

With this structure theorem at hand, commutative principal ideal rings may be considered to be fully under control. In particular, they are elementary divisor rings. A useful application is to the case of a ring with the classical Noether ideal theory, modulo a nonzero ideal.

13. Infinite matrices and modules. We recall that with every module we have associated a matrix with only a finite number of nonzero elements in each column. We now consider the reduction theory for such matrices, and we begin with the case of matrices which are infinite only one way.

If there are only a finite number of columns, then there are only a finite number of nonzero elements in all, and it is evident that this case is essentially identical with that of finite matrices. It corresponds to the case of a free module reduced by only a finite number of relations; cf. [26].

Matrices with only a finite number of rows correspond to a finite free module reduced by any set of relations. As may be expected, it requires the ascending chain condition to accomplish matrix reduction here.

THEOREM 13.1. *The following two statements are equivalent for a ring R:* (a) *R is a right Hermite ring satisfying the ascending chain condition on right ideals*, (b) *for any row matrix A over R there exists a unimodular matrix U such that AU has at most one nonzero element.*

Proof. The ability to reduce a 1 by 2 matrix shows that R is a right Hermite ring. Further, if $A = (a_1\ a_2 \cdots)$, the reduction shows that the right ideal generated by the a's is principal. Conversely, given the row $(a_1\ a_2 \cdots)$, we know that the a's generate a principal right ideal dR. In fact a finite number of the a's suffice to generate dR. A unimodular reduction of them will introduce d, which may then be used to sweep out the row.

Theorem 13.1 extends in evident fashion to the case of a finite number of rows. Under the stated conditions we can get a triangular reduction, and if R is further an elementary divisor ring we can reach diagonal form.

We turn now to the consideration of matrices which are infinite both ways. Here even the ascending chain condition will not suffice; we need the descending chain condition. Moreover simple examples show that we cannot hope in general to put a matrix in diagonal form, and that the business of having elements divide their successors has to be dropped. We shall content ourselves with achieving matrices with a most one nonzero element in each

row and column; for the module interpretation this is adequate. However even this modest program does not admit fulfilment in the presence of direct sums.

LEMMA 13.2. *Let R be a ring in which left and right inverses coincide, and suppose it is a direct sum of rings S, T with unit elements u, v. Then the matrix*

$$
A = \begin{pmatrix}
u & & & & 0 \\
v & u & & & \\
& v & u & & \\
& & & \cdot & \cdot \\
0 & & & & \cdot & \cdot
\end{pmatrix}
$$

is not equivalent to a matrix with at most one nonzero element in each row and column.

Proof. Suppose on the contrary that PAQ does effect such a reduction. We first look at this in the component S. There A is the identity matrix, so PAQ is unimodular. Thus a nonzero element must actually appear in each row and column of PAQ. By applying a permutation matrix we may suppose that PAQ is in diagonal form. Now let us look at the T-component: there A has a left inverse but no right inverse. The same is true for PAQ, but (under our assumptions) this is impossible for a diagonal matrix.

We thus see that direct sums cause difficulties in manipulating infinite matrices; but on the other hand, they are no trouble at all in discussing modules. This remark is relevant as we proceed to the study of principal ideal rings with descending chain condition. Asano has shown [13, pp. 75–76] that they are direct sums of primary rings, and for the purpose of modules we reduce at once to that case. In the primary case we establish a matrix reduction.

THEOREM 13.3([9]). *Let R be a primary principal ideal ring with descending chain condition. Then any matrix over R is equivalent to one having at most one nonzero element in each row and column.*

COROLLARY. *If R is a principal ideal ring with descending chain condition, any R-module is a direct sum of cyclic modules.*

Proof. We consider first the case where R is a division ring; the theorem is then known (cf. [18] and the references given there), but for completeness we

---

([9]) Theorem 13.3 is believed to be new. Its module corollary was proved by Köthe in [17], and special cases can be found elsewhere in the literature—[15, Theorem 5.1], [5], and the references given in the latter. In the countable case, Theorem 13.3 is a special case of results of Ulm [30]—or rather, it would be a special case if Ulm's work were suitably extended to more general rings. The non-countable case is however definitely not included in Ulm's work, for the theorem he is proving is then false [31].

give a brief proof. Use letters v_i for the columns and write

$$(11) \qquad\qquad v_i = \sum u_j a_{ij},$$

where u_j index the rows. We introduce new variables u', v' as follows. Set $u_i' = v_i' = v_i$ if v_i is linearly independent of the preceding v's; but if v_i is a linear combination of preceding v's, set $v_i' = (v_i$ minus that linear combination). Note that we can solve backward for the v_i in terms of the v_i'. The u_i' are linearly independent elements of the linear space spanned by the u_i; complete them (changing notation) to a basis having the same ordinal type as the u_i. In terms of the new bases, the equation (11) becomes $v_i' =$ either u_j' or 0. Hence the matrix has been converted into one having at most one nonzero element in each row and column.

We now return to the general case. The primary ring R is a matrix ring (of finite order) over a completely primary ring S. We can blow up our given matrix to a larger one over S, and it is thus sufficient to prove our theorem for matrices over S. The ring S has a radical generated by an element r with $r^{n+1} = 0$, and $S - (r)$ is a division ring; S is in fact a valuation ring. We assume by induction that the theorem is known for smaller n.

At this point we pause to make two simple remarks on "convergence." (It is a matter of taste whether one takes the convergence purely formally, or actually introduces a suitable weak topology.) (1) If U is a square matrix (one whose rows and columns have the same ordinal type) mapping modulo r onto a unimodular matrix, then U is unimodular. One proves this by taking the (finite) power series expansion. A more general theorem is proved in [22]. (2) Let E_i be a well ordered array of square matrices, each having only one nonzero element and that divisible by r, and such that for any fixed column, only a finite number of the E's have a nonzero entry. Then the products $(I+E_1)(I+E_2) \cdots$ and $\cdots (I+E_2)(I+E_1)$ are well defined and unimodular, for we shall have to deal only with products of at most n elements, and the sums involved are readily seen to converge. The limit is unimodular by remark (1).

We return now to the business of reducing our matrix A. Let us pass to the ring $T = S - (r^n)$, and write A^* for the image of A. By induction we can find in T unimodular matrices P^*, Q^* such that $P^*A^*Q^*$ has at most one nonzero element in each row and column. Choose matrices P, Q mapping on P^*, Q^*, and choose them column-finite, of course. By remark (1) above, P and Q are unimodular. Our remaining task is to remove from PAQ the sundry terms in r^n that spoil it. First we sweep out the rows, that is, if a row contains both terms in r^n and a (unique) term properly dividing it, we sweep out the former with the latter. Excision of an element in the jth column means right-multiplication by a matrix of the form

$$(12) \qquad\qquad I + ar^k e_{ij}.$$

Since there are only a finite number of elements to be swept out of any column, these multiplications satisfy the conditions of remark (2) above. We similarly sweep out the columns; here we use (12) on the left if we are sweeping with an element in the jth row, and there is at most one such element. Having accomplished all this, we still have on our hands some rows and columns decorated solely by terms in r^n. We treat these by the division ring case of the theorem, leaving the other rows and columns unchanged. This completes the proof of Theorem 13.3.

In the commutative case we can prove a converse to Theorem 13.3.

THEOREM 13.4. *Let R be a commutative ring with the property that every matrix over R is equivalent to one with at most one nonzero element in each row and column. Then R is a valuation ring with descending chain condition*([10]).

Proof. By Theorem 13.1, R is a principal ideal ring. Then Theorem 12.3 and Lemma 13.2 show that we have only to exclude the case where R is an integral domain. Now the hypothesis of our theorem assures us that any R-module is a direct sum of cyclic modules. This applies in particular to the quotient field of R, and is possible only if R is that quotient field.

Extension of Theorem 13.4 to the non-commutative case must await further information on non-commutative principal ideal rings.

We conclude with a remark on matrices vs. modules. The study by matrix methods of modules, over rings not satisfying the descending chain condition, leads to normal forms that are comparatively complicated and to correspondingly complex convergence questions. The investigators who followed Ulm have consequently preferred direct group-theoretic methods. However we have considered Theorem 13.3 worth proving because the normal form involved is simple, and because the proof is comparatively transparent.

BIBLIOGRAPHY

1. A. A. Albert, *Symmetric and alternate matrices in an arbitrary field*, Trans. Amer. Math· Soc. vol. 43 (1938) pp. 386–436.

2. R. Arens and I. Kaplansky, *Topological representation of algebras*, Trans. Amer. Math. Soc. vol. 63 (1948) pp. 457–481.

3. R. Baer, *Inverses and zero-divisors*, Bull. Amer. Math. Soc. vol. 48 (1942) pp. 630–638.

4. N. Bourbaki, *Éléments de mathématique*, VI, *Algèbre linéaire*, Actualités Scientifiques et Industrielles, no. 1032, Paris, 1947.

5. J. Brenner, *The decomposition theorem for abelian groups*, Bull. Amer. Math. Soc. vol. 47 (1941) pp. 116–117.

6. J. Dieudonné, *Sur le nombre de dimensions d'un module*, C. R. Acad. Sci. Paris vol. 215 (1942) pp. 563–565.

7. C. J. Everett, *Vector spaces over rings*, Bull. Amer. Math. Soc. vol. 48 (1942) pp. 312–316.

8. H. Fitting, *Über den Zusammenhang zwischen dem Begriff der Gleichartigkeit zweier Ideale und dem Äquivalenzbegriff der Elementarteilertheorie*, Math. Ann. vol. 112 (1936) pp. 572–582.

([10]) Köthe has a similar but independent theorem in [17].

9. ———, *Die Determinantenideale eines Moduls*, Jber. Deutschen Math. Verein. vol. 46 (1936) pp. 195–228.

10. A. Fraenkel, *Über die Teiler der Null und die Zerlegung von Ringen*, Journal für Mathematik vol. 145 (1915) pp. 139–176.

11. O. Goldman, *A characterization of semi-simple rings with the descending chain condition*, Bull. Amer. Math. Soc. vol. 52 (1946) pp. 1021–1027.

12. O. Helmer, *The elementary divisor theorem for certain rings without chain condition*, Bull. Amer. Math. Soc. vol. 49 (1943) pp. 225–236.

13. N. Jacobson, *The theory of rings*, Mathematical Surveys, vol. 2, American Mathematical Society, New York, 1943.

14. ———, *The radical and semi-simplicity for arbitrary rings*, Amer. J. Math. vol. 67 (1945) pp. 300–320.

15. R. E. Johnson, *On structures of infinite modules*, Trans. Amer. Math. Soc. vol. 53 (1943) pp. 469–489.

16. I. Kaplansky, *Maximal fields with valuations*, Duke Math. J. vol. 9 (1942) pp. 303–321.

17. G. Köthe, *Verallgemeinerte Abelsche Gruppen mit Hypercomplexem Operatorenring*, Math. Zeit. vol. 39 (1935) pp. 31–44.

18. G. Köthe and O. Toeplitz, *Theorie der halbfiniten unendlichen Matrizen*, Journal für Mathematik vol. 165 (1931) pp. 116–127.

19. W. Krull, *Die verschiedenen Arten der Hauptidealringe*, Sitzungsberichte der Heidelberg Akademie (1924) no. 6.

20. ———, *Allgemeine Bewertungstheorie*, Journal für Mathematik vol. 167 (1932) pp. 160–196.

21. ———, *Beiträge zur Arithmetik kommutativer Integritätsbereiche*, Math. Zeit. vol. 41 (1936) pp. 545–577.

22. ———, *Linearformenmoduln und lineare Gleichungssysteme in unendlich vielen Variablen über einem diskret bewerteten, perfekten Körper*, Monatshefte für Mathematik und Physik vol. 43 (1936) pp. 463–476.

23. C. C. MacDuffee, *The theory of matrices*, Ergebnisse der Mathematik, vol. 2, Berlin, 1933.

24. J. v. Neumann, *Continuous geometry*, vol. 2, Princeton, 1937.

25. O. F. G. Schilling, *Noncommutative valuations*, Bull. Amer. Math. Soc. vol. 51 (1945) pp. 297–304.

26. W. Schmeidler, *Bemerkungen zur Theorie der abzählbaren Abelschen Gruppen*, Math. Zeit. vol. 6 (1920) pp. 274–280.

27. E. Snapper, *Polynomial matrices in several variables*, Amer. J. Math. vol. 69 (1947) pp. 622–652.

28. E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern*, Math. Ann. vol. 71 (1912) pp. 328–354.

29. B. M. Stewart, *A note on least common left multiples*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 587–591.

30. H. Ulm, *Zur Theorie der abzählbar-unendlichen Abelschen Gruppen*, Math. Ann. vol. 107 (1933) pp. 774–803.

31. ———, *Zur theorie der nicht-abzählbaren primären Abelschen Gruppen*, Math. Zeit. vol. 40 (1935) pp. 205–207.

32. B. L. van der Waerden, *Moderne Algebra*, 1st ed., vol. 2, Berlin, 1931, §106.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.