Conversely (11) implies (9). Since (9) holds for the modulus $2^{n-2}\cdot 9M$, it follows similarly that (11) holds for the modulus $2^{n-2}\cdot 9$ with $M=2^{n-4}M_1$. Hence (11) will be true for the given modulus if $M=2^{n-3}M_1$. This supplies a proof by induction that (8) is a universal form for every $n \geq 4$.

If, in addition, $M$ is divisible by every prime $p$ where $3 < p \leq n$, we satisfy the necessary condition given by Dickson for the form (8) to represent at least one set of $n$ primes. The proof of the sufficiency of this condition still remains a challenge to the ingenuity of number theorists.

NEW YORK, N. Y.

RINGS AS GROUPS WITH OPERATORS

C. J. EVERETT, JR.

1. Introduction. A module $M(0,a,b,\cdots)$ is a commutative group, additively written. Every correspondence of $M$ onto itself, or part of itself, such that $a \rightarrow a'$, $b \rightarrow b'$ implies $a + b \rightarrow a' + b'$ defines an endomorphism of $M$. An endomorphism may be regarded as an operator $\theta$ on $M$ subject to the postulates (i) $\theta a = a'$ is uniquely defined as an element of $M$, (ii) $\theta(a + b) = \theta a + \theta b$, $(a, b \in M)$. In particular, there exist a null operator $0$ ($0M = 0$) and a unit operator $e$ ($ea = a, a \in M$). Designate by $\Omega_M$ the set of all such operators, $0, e, \alpha, \beta, \cdots$. It is well known that if operations of $\oplus$ and $\odot$ be defined in $\Omega_M$ by $(\theta + \eta)a = \theta a + \eta a$ and $(\theta\eta)a = \theta(\eta a)$, $(a \in M)$, $\Omega_M$ forms a ring with unit element $e$ (endomorphism ring of $M$).† The equation $\theta = \eta$ means $\theta a = \eta a$ (all $a \in M$). A ring $R(M)$ is called a ring over $M$ in case $M$ is the additive group of $R(M)$. Correspondence of a set $P$ onto a set $Q$ (many-one) is written $P \sim Q$; if specifically one-one, $P \cong Q$. Corresponding operations in $P$, $Q$ preserved under the map are indicated in parentheses; for example, $P \sim Q$ (+). If a set $T$ has the property that $TP$ is defined in $P$, $TQ$ in $Q$, and if, under a correspondence $P \sim Q$, $p \rightarrow q$ implies $tp \rightarrow tq$ ($t \in T$, $p \in P$, $q \in Q$), we write $P \sim Q$ ($T$) ($T$-operator correspondence). If $R$ is a ring, the two-sided ideal $N$ of elements $z$ of $R$ such that $zr = 0$ (all $r \in R$), is called the left annulling ideal of $R$.

* For example, replace $6M$ in (8) by $2^{n-1}M$, $(w \geq n-3)$.
† Loc. cit., p. 156.
‡ van der Waerden, Moderne Algebra, vol. 1, 2d edition, p. 146.
2. **Fundamental theorems.** We prove first the following theorem:

**Theorem 1.** If \( R(M) \) is a ring over \( M \), there exists in \( \Omega_M \) a subring \( \Gamma \) such that

\[
R(M) \sim \Gamma \ (\oplus, \odot; \Gamma),
\]

this correspondence being one-one if and only if \( N = (0) \) for \( R(M) \).*

For \( R(M) \) consists of the elements of \( M \) on which a multiplication has been defined so that (i) \( ab \in M \), (ii) \( a(b+c) = ab + ac \), (iii) \( (a+b)c = ac + bc \), (iv) \( (ab)c = a(bc) \). By (i), every \( a \) of \( M \) defines a map of \( M \) into \( M \) which by (ii) is an endomorphism. Hence to every \( a \) of \( M \) corresponds an operator \( \alpha \) of \( \Omega_M \). Let \( \Gamma \) be the set of all such \( \alpha \), whence \( R(M) \sim \Gamma \), where \( a \rightarrow \alpha \) is defined by \( ag = \alpha g \) (all \( g \in M \)). We have that \( a + b \rightarrow \alpha + \beta \), \( ab \rightarrow \alpha \beta \) and \( \gamma a \rightarrow \gamma \alpha \) from the following:

\[
\begin{align*}
(a + b)h &= \alpha h + \beta h = \alpha h + \beta h = (\alpha + \beta)h, \\
(ab)h &= a(\beta h) = \alpha (\beta h) = (\alpha \beta)h, \\
(\gamma a)h &= g(a h) = g(\alpha h) = (\gamma \alpha)h, \\
\end{align*}
\]

all \( h \in M \).

Since, under the correspondence, \( N \rightarrow 0 \), proof of the theorem is complete.

**Theorem 2.** If in \( \Omega_M \) there exists a subring \( \Gamma \) such that \( M \sim \Gamma \ (\oplus; \Gamma) \) then there exists a ring \( R(M) \) over \( M \) such that

\[
R(M) \sim \Gamma \ (\oplus, \odot; \Gamma).
\]

We define \( ab = \alpha b \). Then

\[
\begin{align*}
(1) \quad a(b + c) &= \alpha(b + c) = ab + \alpha c = ab + ac, \\
(2) \quad (a + b)c &= (\alpha + \beta)c = ac + \beta c = ac + bc, \\
(3) \quad (ab)c &= (\alpha \beta)c = \alpha \beta c = \alpha bc = a(bc),
\end{align*}
\]

and \( M \) with this multiplication is a ring \( R(M) \). Since \( ab = \alpha b \rightarrow \alpha \beta \), the theorem follows.

**Corollary.** If \( M \sim \Gamma \ (\oplus) \), \( \Gamma \) a submodule of \( \Omega_M \), there exists a (non-associative) ring \( R^*(M) \) over \( M \), where \( ab \) is defined as \( \alpha b \), \( (a \rightarrow \alpha) \).

The relation between associativity of \( R(M) \) and the \( \Gamma \)-operator character of the correspondence seems to indicate a point of departure for the study of rings with associativity not assumed.

* In case \( N \neq (0) \), there exists a ring \( R \supset R \) for which \( N = (0) \); thus \( R \) is always isomorphic with a subring of the endomorphism ring of some module. See, for example, A. A. Albert, *Modern Higher Algebra*, University of Chicago Press, 1937, p. 22, Theorem 5.
3. On linear algebras. Let $V$ be a vector space of $n$ dimensions over a field $F$. Elements of $V$ satisfy

$$
\left(\begin{array}{c}
\alpha_1 \\
\vdots \\
\alpha_n
\end{array}\right) = (\alpha_i = \sum \alpha_id_i), \quad (\alpha_i + \beta_i) = (\alpha_i + \beta_i), \quad \alpha(\alpha_i) = (\alpha\alpha_i).
$$

It is well known* that every $F$-operator endomorphism of $V$ ($v \rightarrow v'$ implies $\alpha v \rightarrow \alpha v'$) is represented by an $n \times n$ matrix over $F$ operating on $V$. For under such a map, $d_i \rightarrow \sum \alpha_id_i$, and

$$
v = \sum \alpha_id_i \rightarrow \sum (\sum \alpha\alpha_{ij}d_j = Av,
$$

where $A$ is the matrix $(\alpha_{ij})$. Now a linear associative algebra of order $n$ over the field $F$ is simply a ring $A(V)$ over $V$ subject to the axioms

(i) $a(uv) = u(av)$ and (ii) $a(uv) = (au)v$. Condition (i) requires that the endomorphism defined by the multiplier $u$ be an $F$-operator map, that is, $uv = Uv$, where $U$ is a matrix of the type just indicated. Hence in the correspondence of Theorem 1, $u \rightarrow U$; and by (ii), $\alpha u \rightarrow \alpha U$, $(\alpha \in F)$. Thus

$$
A(V) \sim \Gamma \ (\oplus, \ominus ; \Gamma, F)
$$

where $\Gamma$ is a subalgebra of the total $n \times n$ matrix algebra $M$ over $F$. This correspondence (which is the classical one) is biunique if and only if the left annulling ideal $N$ of $A(V)$ is $(0)$, a much weaker condition than the possession of unit element usually required. The $\Gamma$-operator property of the correspondence is significant in the light of the following remark, which is in part a result of Theorem 2:

* See van der Waerden, loc. cit., vol. 2, p. 111.
\[
\begin{pmatrix}
\alpha_1 & \alpha_2 \\
0 & 0
\end{pmatrix}
\begin{pmatrix}
\beta_1 \\
\beta_2
\end{pmatrix}
\rightarrow
\begin{pmatrix}
\alpha_1 & \alpha_2 \\
0 & 0
\end{pmatrix}
\begin{pmatrix}
\beta_1 & \beta_2 \\
0 & 0
\end{pmatrix}
\]
does not hold. However
\[
\begin{pmatrix}
\beta_1 \\
\beta_2
\end{pmatrix}
\sim \Gamma \equiv \begin{pmatrix}
0 \\
\beta_1
\end{pmatrix}
(\oplus, \ominus; \Gamma).
\]

4. **Reduction theorems for finite rings.** Let \( M \) be a module of order \( m = p_1^{a_1} \cdots p_n^{a_n} \). Then \( M = B_1 + \cdots + B_n \) is a direct sum, \( B_i \) of order \( p_i^{a_i} \), containing all elements of period dividing \( p_i^{a_i} \). Moreover, \( B_i = C_{i1} + \cdots + C_{i\ell_i} \), where \( C_{ij} \) is cyclic of order \( p_i^{b_{ij}}, \sum_{j=1}^{\ell_i} b_{ij} = a_i \). The endomorphism ring \( \Omega_M \) of \( M \) is a direct sum of endomorphism rings of the \( B_i \):
\[
\Omega_M = \Omega_1 + \cdots + \Omega_n,
\]
\( \Omega_i \) a two-sided ideal in \( \Omega_M \), \( \Omega_i \cap \Omega_j = \delta_{ij} \Omega_i \), \( \Omega_i \Omega_j = \delta_{ij} \Omega_j \). Further, if \( B = C_1 + \cdots + C_i, \ C_i \) of order \( p_i^{b_i} \), be represented as a vector space
\[
\begin{pmatrix}
x_1 \\
\vdots \\
x_i
\end{pmatrix}, \ x_j \pmod{p_i^{b_i}}, \ b_1 \leq \cdots \leq b_i,
\]
then \( \Omega_B \) may be represented* by the ring of all matrices \( (\beta_{jk}) = (\alpha_{jk} p_i^{b_i-b_k}), \ p_i^{b_i-b_k} \) defined as 1 for \( j < k \), \( \beta_{ik} \) reduced \( \pmod{p_i^{b_i}} \). Thus if \( M \) is represented as a vector space, \( \Omega_M \) is a ring of matrices with blocks along the diagonal, the \( \Omega_i \)-blocks having the \( (\beta_{jk}) \) structure described.†

**Theorem 3.** If \( M \sim \Gamma \subset \Omega_M \,(\oplus; \Gamma) \), then \( \Gamma = \Gamma_1 + \cdots + \Gamma_n \), a direct sum of two-sided ideals in \( \Gamma \), and
\[
B_i \sim \Gamma_i \subset \Omega_i \,(\oplus; \Gamma_i).
\]

Let \( \Gamma_i \) be the map of \( B_i \). Then \( \Gamma_i \) is a two-sided ideal in \( \Gamma \), and every \( \gamma \in \Gamma \) is a sum of \( \gamma_i \in \Gamma_i \). Moreover, \( \Gamma_i \subset \Omega_i \). For let \( b_i \rightarrow \lambda_i \in \Gamma_i, \ (\lambda_i = (\theta_1 + \cdots + \theta_n), \ \theta_i \in \Omega_i) \). Since \( b_i \in B_i \),
\[
\hat{p}^a b_i = 0 \rightarrow \hat{p}^a (\theta_1 + \cdots + \theta_n) = 0.
\]
Hence \( \hat{p}^a \theta_j = 0 \), \( (j = 1, \cdots, n) \). From the structure of \( \Omega_i \) already indicated, \( \theta_j = 0 \), \( (j \neq i) \). Thus \( \Gamma \) is a direct sum.

† Note that \( B \) is admissible relative to \( \Omega_M \), that is, \( \Omega_M B \subset B \).
THEOREM 4. If \( M = B_1 + \cdots + B_n \), \( B_i \sim \Gamma_i \) (\( \oplus ; \Gamma_i \)), \( \Gamma_i \) a subring of \( \Omega_i \), then \( \Gamma = \Gamma_1 + \cdots + \Gamma_n \) is direct, \( \Gamma_i \) a two-sided ideal in \( \Gamma \), and

\[
M \sim \Gamma \subset \Omega_M \ (\oplus ; \Gamma).
\]

Since \( \Gamma_i \subset \Omega_i \), \( \Gamma \) is a direct sum, and \( \Gamma_i \) is a two-sided ideal in \( \Gamma \). Define \( M \sim \Gamma \) by \( m = b_1 + \cdots + b_n \rightarrow \gamma_1 + \cdots + \gamma_n \) (where \( b_i \rightarrow \gamma_i \)). Then addition is preserved. Let \( \rho \in \Gamma \), \( \rho = \mu_1 + \cdots + \mu_n \) (\( \mu_i \in \Gamma_i \)). Then

\[
\rho m = \rho b_1 + \cdots + \rho b_n = \mu_1 b_1 + \cdots + \mu_n b_n \rightarrow \mu_1 \gamma_1 + \cdots + \mu_n \gamma_n
\]

THEOREM 5. Every ring over \( M = B_1 + \cdots + B_n \) is a direct sum of rings over the \( B_i \); hence to construct all rings over \( M \) it is only necessary to construct all rings over the \( B_i \).

5. On elementary modules. \( M \) is said to be elementary in case there exists an isomorphism

\[
M \cong \Omega_M \ (\oplus ; \Omega_M).
\]

THEOREM 6. \( M \) is elementary if and only if there exists a ring with unit element, \( R(M) \) over \( M \), such that every endomorphism of \( M \) is defined by a left multiplier of \( R(M) \).

For if \( M \) is elementary, there exists a ring \( R(M) \) such that

\[
R(M) \cong \Omega_M \ (\oplus ; \Omega_M)
\]

where \( ab \) is defined as \( \alpha b \), \( (a \rightarrow \alpha) \). Let \( m \rightarrow \theta m \) be an endomorphism of \( M \). In the above isomorphism let \( t \leftarrow \theta \). Then \( tm = \theta m \), \( (t \in R(M)) \). Conversely, if \( R(M) \) is of this type,

\[
R(M) \cong \Gamma \subset \Omega_M \ (\oplus ; \Omega ; \Gamma),
\]

and if one assumes \( \theta \in \Omega_M \), there exists a \( t \in R(M) \) such that \( ta = \theta a \), \( (a \in M) \). Hence \( \theta \in \Gamma \) and \( \Gamma = \Omega_M \); whence \( M \) is elementary.

COROLLARY. The modules of rational numbers, and of rational integers \( C \) (the infinite cyclic group) are elementary.

For it is readily shown that the only solution of the functional equation \( \Phi = (a + b) = \Phi(a) + \Phi(b) \) in the field of rationals and the ring of integers is of the type \( \Phi(a) = ra \) where \( r \) is a multiplier of the domain.

COROLLARY. The only rings \( R(C) \) over \( C \) are given by the multiplication \( a \cdot b \), defined as any fixed positive integral multiple of the ordinary product \( ab \) in the ring of rational integers.
To define a ring $R(C)$ we must obtain a homomorphism

$$C \sim \Gamma (\oplus; \Gamma)$$

where $\Gamma$ is a subring of $\Omega_C$, setting $a \cdot b = ab (a \rightarrow \alpha)$. But $\Omega_C$ is the ordinary ring of rational integers, its only subrings being principal ideals \( \{m\} \). Hence we must have

$$C \sim \{m\} (\oplus; \{m\})$$

where $1 \rightarrow m, a \rightarrow ma$.

**Theorem 7.** If $M$ is elementary, the units of $\Omega_M$ are in the centrum of $\Omega_M$.*

For the endomorphism $\sigma^{-1}\Omega_M\sigma$ of the additive group of $\Omega_M$ (\(\sigma\) a unit) must be defined by a ring multiplier $\rho: \sigma^{-1}\Omega_M\sigma = \rho\Omega_M$. Then in particular $\sigma^{-1}\epsilon\sigma = \rho\epsilon$ and $\rho = \epsilon$.

**Corollary.** A vector space $V$ of order greater than or equal to $2$ is not elementary.

For there always exist nonsingular matrices not commutative with the total matrix algebra, and hence not in the centrum of $\Omega_V$.

**Theorem 8.** A finite module $M$ is elementary if and only if it is cyclic.

For a cyclic $M$, $\Omega_M$ is represented by the $n \times n$ matrices $(\delta_i, \alpha_i), \alpha_i (\mod p^{e_i})$. Hence under

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \rightarrow \begin{pmatrix} \alpha_1 \\ \vdots \\ 0 \\ \alpha_n \end{pmatrix},$$

$M$ is elementary. If there are repeated primes in the type of $M$, then the order of $\Omega_M$ is greater than that of $M$ and $M$ is not elementary (see §4).

Thus the rings $R(M)$ over elementary finite $M$ are completely known, $(\alpha_i)(\beta_i)$ being defined as $(\gamma_i, \alpha_i\beta_i), (0 \leq \gamma_i < p^{e_i})$.

**University of Wisconsin**

* A stronger theorem holds: If $M$ is elementary, its endomorphism ring is commutative.