(11) $$KM \equiv 0 \pmod{2^{n-1}\cdot 9}.$$

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 $n\geqq 4$.

If, in addition,* M is divisible by every prime p where $3<p\leqq n$, 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 θ 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 ϵ $(\epsilon a=a, a \in M)$. Designate by Ω_M the set of all such operators, $0, \epsilon, \alpha, \beta, \cdots$. It is well known that if operations of $\oplus$ and $\odot$ be defined in Ω_M by $(\theta+\eta)a=\theta a+\eta a$ and $(\theta\eta)a=\theta(\eta a)$, $(a \in M)$, Ω_M forms a ring with unit element ϵ (*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 $2^w n!M$, $(w\geqq n-3)$.

† 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 Ω_M a subring Γ such that*

$$R(M) \sim \Gamma \quad (\oplus, \odot; \Gamma),$$

*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 α of Ω_M. Let Γ be the set of all such α, 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:

$$\begin{aligned}(a+b)h &= ah+bh = \alpha h+\beta h = (\alpha+\beta)h,\\ (ab)h &= a(bh) = a(\beta h) = \alpha(\beta h) = (\alpha\beta)h,\\ (\gamma a)h &= (ga)h = g(ah) = (\gamma\alpha)h, \qquad \text{all } h \in M.\end{aligned}$$

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

THEOREM 2. *If in Ω_M there exists a subring Γ such that $M\sim\Gamma$ $(\oplus;\Gamma)$ then there exists a ring $R(M)$ over M such that*

$$R(M) \sim \Gamma \quad (\oplus, \odot; \Gamma).$$

We define $ab=\alpha b$. Then

$$(1) \qquad a(b+c) = \alpha(b+c) = \alpha b+\alpha c = ab+ac,$$

$$(2) \qquad (a+b)c = (\alpha+\beta)c = \alpha c+\beta c = ac+bc,$$

$$(3) \qquad (ab)c = (\alpha b)c = (\alpha\beta)c = \alpha(\beta c) = \alpha(bc) = a(bc),$$

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

COROLLARY. *If $M\sim\Gamma$ $(\oplus)$, Γ a submodule of Ω_M, there exists a (non-associative) ring $R^*(M)$ over M, where ab is defined as αb, $(a\rightarrow\alpha)$.*

The relation between associativity of $R(M)$ and the Γ-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 $R_1\supset R$ for which $N_1=(0)$; 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

$$\begin{pmatrix}\alpha_1\\ \cdot\\ \cdot\\ \cdot\\ \alpha_n\end{pmatrix} = (\alpha_i) = \sum \alpha_i d_i, \qquad (\alpha_i) + (\beta_i) = (\alpha_i + \beta_i), \qquad \alpha(\alpha_i) = (\alpha\alpha_i).$$

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

$$v = \sum \alpha_i d_i \to \sum \left(\sum \alpha_i \alpha_{ji}\right) d_j = Av,$$

where A is the matrix (α_{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) $\alpha(uv) = u(\alpha v)$ and (ii) $\alpha(uv) = (\alpha u)v$. 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, $u \to U$; and by (ii), $\alpha u \to \alpha U$, ($\alpha \in F$). Thus

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

where Γ is a subalgebra of the total $n \times n$ matrix algebra $\mathfrak{M}$ 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 Γ-operator property of the correspondence is significant in the light of the following remark, which is in part a result of Theorem 2:

If $V \sim \Gamma$ $(\oplus; \Gamma, F)$, Γ any subalgebra of $\mathfrak{M}$, then there exists an algebra $A(V)$ over V such that

$$A(V) \sim \Gamma \quad (\oplus, \odot; \Gamma, F).$$

That not every matrix representation of an algebra possesses the Γ-operator property is evinced by the example

$$A(V)\colon \quad \begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix}, \quad \begin{pmatrix}\alpha_1\\ \alpha_2\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix} = \begin{pmatrix}\alpha_1 & \beta_1\\ \alpha_1 & \beta_2\end{pmatrix},$$

for

$$\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix} \cong \begin{pmatrix}\beta_1 & \beta_2\\ 0 & 0\end{pmatrix} \quad (\oplus, \odot)$$

but the relation

* See van der Waerden, loc. cit., vol. 2, p. 111.

$$\begin{pmatrix}\alpha_1 & \alpha_2\\ 0 & 0\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix} \to \begin{pmatrix}\alpha_1 & \alpha_2\\ 0 & 0\end{pmatrix}\begin{pmatrix}\beta_1 & \beta_2\\ 0 & 0\end{pmatrix}$$

does not hold. However

$$\begin{pmatrix}\beta_1\\ \beta_2\end{pmatrix} \sim \Gamma \equiv \begin{pmatrix}\beta_1 & 0\\ 0 & \beta_1\end{pmatrix} \quad (\oplus, \odot; \Gamma).$$

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, $B_i = C_{i1} + \cdots + C_{il_i}$, where C_{ij} is cyclic of order $p_i^{b_{ij}}$, $\sum_{j=1}^{l_i} b_{ij} = a_i$. The endomorphism ring Ω_M of M is a direct sum of endomorphism rings of the B_i:

$$\Omega_M = \Omega_1 + \cdots + \Omega_n,$$

Ω_i a two-sided ideal in Ω_M, $\Omega_i \cap \Omega_j = \delta_{ij}\Omega_j$, $\Omega_i\Omega_j = \delta_{ij}\Omega_i^2$. Further, if $B = C_1 + \cdots + C_l$, C_j of order p^{b_j}, be represented as a vector space

$$\begin{pmatrix}x_1\\ \cdot\\ \cdot\\ \cdot\\ x_l\end{pmatrix}, \quad x_j \ (\mathrm{mod}\ p^{b_j}), \quad b_1 \leqq \cdots \leqq b_l,$$

then Ω_B may be represented* by the ring of all matrices $(\beta_{jk}) = (\alpha_{jk}p^{b_j - b_k})$, $p^{b_j - b_k}$ defined as 1 for $j < k$, β_{jk} reduced (mod p^{b_j}). Thus if M is represented as a vector space, Ω_M is a ring of matrices with blocks along the diagonal, the Ω_i-blocks having the (β_{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* Γ, *and*

$$B_i \sim \Gamma_i \subset \Omega_i \ (\oplus; \Gamma_i).$$

Let Γ_i be the map of B_i. Then Γ_i is a two-sided ideal in Γ, and every $\gamma \in \Gamma$ is a sum of $\gamma_i \in \Gamma_i$. Moreover $\Gamma_i \subset \Omega_i$. For let $b_i \to \lambda_i \in \Gamma_i$, $(\lambda_i = (\theta_1 + \cdots + \theta_n), \theta_i \in \Omega_i)$. Since $b_i \in B_i$,

$$p_i^{a_i} b_i = 0 \to p_i^{a_i}(\theta_1 + \cdots + \theta_n) = 0.$$

Hence $p_i^{a_i}\theta_j = 0$, $(j = 1, \cdots, n)$. From the structure of Ω_i already indicated, $\theta_j = 0$, $(j \neq i)$. Thus Γ is a direct sum.

* K. Shoda, *Über die Automorphismen einer endlichen Abelschen Gruppe*, Mathematische Annalen, vol. 100 (1928), p. 676.

† Note that B is admissible relative to Ω_M, that is, $\Omega_M B_i \subset B_i$.

THEOREM 4. *If* $M = B_1 + \cdots + B_n$, $B_i \sim \Gamma_i$ $(\oplus;\Gamma_i)$, Γ_i *a subring of* Ω_i, *then* $\Gamma = \Gamma_1 + \cdots + \Gamma_n$ *is direct,* Γ_i *a two-sided ideal in* Γ, *and*

$$M \sim \Gamma \subset \Omega_M \ (\oplus;\Gamma).$$

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

$$\begin{aligned}\rho m &= \rho b_1 + \cdots + \rho b_n = \mu_1 b_1 + \cdots + \mu_n b_n \to \mu_1\gamma_1 + \cdots + \mu_n\gamma_n \\ &= (\mu_1 + \cdots + \mu_n)(\gamma_1 + \cdots + \gamma_n).\end{aligned}$$

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

$$R(M) \cong \Omega_M \ (\oplus, \odot;\Omega_M)$$

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

$$R(M) \cong \Gamma \subset \Omega_M \ (\oplus, \odot;\Gamma),$$

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

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

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

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

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

THEOREM 7. *If M is elementary, the units of Ω_M are in the centrum of Ω_M.**

For the endomorphism $\sigma^{-1}\Omega_M\sigma$ of the additive group of Ω_M (σ a unit) must be defined by a ring multiplier ρ: $\sigma^{-1}\Omega_M\sigma = \rho\Omega_M$. 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 Ω_V.

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

For a cyclic M, Ω_M is represented by the $n \times n$ matrices $(\delta_{ij}\alpha_j)$, α_j (mod $p_j^{a_j}$). Hence under

$$\begin{pmatrix} \alpha_1 \\ \cdot \\ \cdot \\ \cdot \\ \alpha_n \end{pmatrix} \to \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix},$$

M is elementary. If there are repeated primes in the type of M, then the order of Ω_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 $(\gamma_i\alpha_i\beta_i)$, $(0 \leqq \gamma_i < p_i^{a_i})$.

UNIVERSITY OF WISCONSIN

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