ANL-6040
Physics and Mathematics
(TID-4500, 14th Ed.)
AEC Research and
Development Report

ARGONNE NATIONAL LABORATORY
P. O. Box 299
Lemont, Illinois

BASIS AND DIMENSION IN ABSTRACT MODULE THEORY

by

Richard Chichester, Jr.

August, 1959

Operated by The University of Chicago
under
Contract W-31-109-eng-38

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

TABLE OF CONTENTS

	<u>Page</u>
I. MOTIVATION AND OUTLINE OF RESULTS	3
II. NOTATIONAL ORIENTATION AND BASIC CONCEPTS	4
III. SEMISIMPLE MODULES	7
IV. SEMISIMPLE ISOTYPIC MODULES	13
V. CYCLICALLY SIMPLE MODULES AND MODULAR DOMAINS OF INTEGRITY	15

BASIS AND DIMENSION IN ABSTRACT MODULE THEORY

Richard Chichester, Jr.

I. MOTIVATION AND OUTLINE OF RESULTS

A (classical) linear (vector) space is a unitary Δ -module, where Δ is a division ring. Linear spaces enjoy the following well-known properties:

- 1) A basis, in the sense of a maximal linearly independent subset, always exists.
- 2) The cardinal numbers (finite or infinite) of any two bases are equal. This uniquely determined cardinal number is usually called the dimension of the space.
- 3) The dimension determines the linear space up to a Δ -isomorphism.

The standard proofs of these properties of linear spaces depend strongly upon the existence of inverses in the operator ring Δ . A natural question - indeed, the motivation for this paper - is just this: Is it really the division ring that "makes" the linear space, that is, does there exist a class of unital rings $\mathcal{R}$, larger than the class of division rings, such that any unitary R -module, with $R \in \mathcal{R}$, satisfies 1), 2), and 3)? If so, such modules truly deserve the title of generalized linear spaces. Further, a study of the ring of linear transformations of these generalized linear spaces could well lead to some remarkable results in the theory of matrix rings for which the "ground" ring is quite general in nature.

This paper by no means answers all of the above questions. I do believe, however, that it provides a reasonably good foundation for future researches. The approach here is a module theoretic one, that is, we shall study a sequence of progressively stronger impositions on the module structure of a unitary R -module M , without regard to the nature of the operator ring R . Hence the plan is to place certain conditions on the module structure of M which will guarantee 1), 2), and 3) above, and then determine the nature of the ring R which will insure that the first conditions hold good.

The principal results of the paper are as follows:

- 1) A semi-simple module always has a minimal system of generators, but this set of generators need not be a linearly independent set. Further, two minimal systems of generators do not, in general, have the same cardinal number (finite or infinite). This precludes any definition of dimension in the usual sense.
- 2) A "weak dimension" is defined for semi-simple modules, and it is shown that a module which is both semi-simple and isotypic is "almost" uniquely determined by its weak dimension.
- 3) An example is given of a semi-simple isotypic module for which a minimal system of generators is not a linearly independent set (such examples seem particularly difficult to find). Hence such modules cannot serve as generalized linear spaces.
- 4) The notion of a cyclically simple domain of integrity is introduced, and it is shown that such modules do enjoy all three of the above-mentioned properties of ordinary vector spaces.
- 5) The operator ring of a cyclically simple domain of integrity must be a division ring. This is somewhat disappointing; nevertheless, as a consequence, a new module theoretic characterization of ordinary vector spaces is obtained.

II. NOTATIONAL ORIENTATION AND BASIC CONCEPTS

Let R be any ring with a unit. A left unitary R -module is an Abelian group $(M, +)$ together with a scalar multiplication $\mu: R \times M \rightarrow M$ such that:

- A. $\mu(a + b, x) = \mu(a, x) + \mu(b, x)$; $a, b \in R$ and $x \in M$.
- B. $\mu(a, x + y) = \mu(a, x) + \mu(a, y)$; $a \in R$ and $x, y \in M$.
- C. $\mu(ab, x) = \mu(a, \mu(b, x))$; $a, b \in R$ and $x \in M$.
- D. $\mu(1, x) = x$; $x \in M$.

We shall write $ax = \mu(a, x)$ for simplicity. If, in C, we have $(ab)x = b(ax)$, then M is a right unitary R -module. As is well known, left and right modules may be combined to form two-sided modules. In this paper, we shall deal exclusively with left unitary R -modules, and we shall refer to these simply as R -modules. It should be noted that all of our results carry over to the right and two-sided cases.

Let M be an R -module. A set $N \subset M$ is an R -submodule of M if N is closed under subtraction and scalar multiplication. Any R -submodule N is an R -module in the trivial fashion. A module M is said to be simple if $\{0\}$ and M are its only submodules.

Let $N \subset M$ be any submodule, and form the factor group M/N . Define $\mu: R \times M/N \rightarrow M/N$ by $\mu(a, (x)) = (ax)$. Then μ is well-defined, and in this way M/N can be regarded as an R -module. We call it the factor R -module of M by N .

Let M_1 and M_2 be R -modules. An R -homomorphism $\phi: M_1 \rightarrow M_2$ is a group homomorphism such that $\phi(ax) = a\phi(x)$ for all $a \in R$ and all $x \in M_1$. If ϕ is one-one, we call ϕ a monomorphism; if ϕ is onto, we call ϕ an epimorphism. If ϕ is one-one and onto, then ϕ is an isomorphism, and M_1 and M_2 are R -isomorphic modules (notation: $M_1 \approx M_2$). The sets $\text{Ker } \phi = \{x \mid \phi(x) = 0\}$ and $\text{Im } \phi = \{\phi(x) \mid x \in M_1\}$ are called the kernel and image of ϕ . It is trivial to see that they are submodules of M_1 and M_2 , respectively. It is also clear that $\eta: M_1/\text{Ker } \phi \rightarrow \text{Im } \phi$ defined by $\eta((x)) = \phi(x)$ is an isomorphism.

If A is any collection of submodules of a module M , then $\cap A$ is again a submodule of M . In particular, if $H \subset M$ is any set,

$$m(H) = \cap \{N \mid N \subset M \text{ a submodule and } N \supset H\}$$

is a submodule of M . We call it the submodule generated by H . It is the smallest submodule of M containing H , and is characterized as the set of all finite sums $\sum a_i x_i$, where $a_i \in R$ and $x_i \in H$. It may happen that $m(H) = M$. In this case, we call H a set of generators for M . If, in addition, $M \neq \{0\}$ and $M \not\subset m(I)$ for any proper subset $I \subset H$, then we say that H is a minimal system of generators for M . A minimal system of generators for M is a basis for M when, for any finite sum $\sum a_i x_i$, where $a_i \in R$ and $x_i \in H$, $\sum a_i x_i = 0$ implies that every $a_i = 0$.

Suppose $\mathcal{B}$ is any collection of submodules of a module M . Then $m(\cup \mathcal{B})$ is a submodule of M ; we call it the join of the modules of the collection $\mathcal{B}$. If $\mathcal{B} = \{M_\alpha \mid \alpha \in A\}$, we shall write $m(\cup \mathcal{B}) = \vee (M_\alpha \mid \alpha \in A)$. If $A = \{1, 2\}$, it will be convenient to write $M_1 \vee M_2 = \vee (M_i \mid i = 1, 2)$.

The least upper bound notation $\vee$ is pleasantly suggestive. The class $\mathcal{L}$ of submodules of a module M is partially ordered under set inclusion $\subset$, and $\vee$ indeed acts as a least upper bound in $\mathcal{L}$ relative to $\subset$. Similarly, the logical intersection $\cap$ acts as a greatest lower bound. Hence $(\mathcal{L}, \vee, \cap)$ is a lattice (with a zero and an all element). As is well known, $\mathcal{L}$ is not distributive. $\mathcal{L}$ is, however, modular in the sense that, if $N_1, N_2, N_3 \in \mathcal{L}$ are such that $N_1 \supset N_2$, then $N_1 \cap (N_2 \vee N_3) = N_2 \vee (N_1 \cap N_3)$. The trivial verification of these details is left to the reader.¹

¹See, for example, Jacobson, N., Lectures in Abstract Algebra: II, Linear Algebra, D. Van Nostrand Co., Inc., New York (1953).

Quite frequently a join of modules enjoys a property known as directness. Let $\{M_\alpha \mid \alpha \in A\}$ be any collection of submodules of a module M ,² and suppose $M = \bigvee (M_\alpha \mid \alpha \in A)$. We say that M is the direct join of the M_α if, for any $\beta \in A$,

$$\bigvee (M_\alpha \mid \alpha \in A \sim \{\beta\}) \cap M_\beta = \{0\}.$$

Obviously equivalent formulations are these:

1. $\bigvee (M_\alpha \mid \alpha \in F)$ is a direct join for every finite, nonempty subset $F \subset A$.
2. For any well-ordering $\prec$ of A and for every $\beta \in A$,

$$\bigvee (M_\alpha \mid \alpha \in A \text{ and } \alpha \prec \beta) \cap M_\beta = \{0\}.$$

If $A = \{1, 2, \dots, n\}$, then still other formulations are the following:

$$1' \quad X = \sum_{i=1}^n x_i, \quad x_i \in M_i, \text{ uniquely for every } x \in M.$$

$$2' \quad 0 = \underbrace{0 + 0 + \dots + 0}_{n \text{ times}} \text{ uniquely.}$$

The proofs of these statements are obvious (or at any rate trivial).³ If $M = \bigvee (M_\alpha \mid \alpha \in A)$ is a direct join, we shall indicate this by writing $M = \bigvee^0 (M_\alpha \mid \alpha \in A)$. If $A = \{1, 2\}$, we put $M = M_1 \bigvee^0 M_2$.

Let N, L be submodules of the R -module M . It is clear that the epimorphism $\phi: L \rightarrow (L \vee N)/N$ defined by $\phi(m) = (m)$ has kernel $L \cap N$. Hence $(L \vee N)/N \approx L/(L \cap N)$. In particular, if $M = N \bigvee^0 L$, then $M/N \approx L$.

Finally, it is necessary to recall the notion of a projection of a submodule. Let M be any module, and denote by $E(M)$ the totality of module endomorphisms $f: M \rightarrow M$. We regard $E(M)$ as a ring by defining an addition and a multiplication in $E(M)$ in an obvious way:

$$\begin{aligned} (f + g)(x) &= f(x) + g(x), \\ (fg)(x) &= f(g(x)). \end{aligned}$$

²We always choose A such that the function $\alpha \rightarrow M_\alpha$ is 1-1.

³Consult Zariski, O., and Samuel, P., Commutative Algebra, I, D. Van Nostrand Co., Inc., New York, (1958).

Denote the zero endomorphism ($x \rightarrow 0$ for all $x \in M$) by O and the identity by I . Now if $N \subset M$ is any submodule, then a mapping $p \in E(M)$ such that $p(M) = N$ and $p^2 = p$ is called a projection of N .

Concerning projections and direct joins, we have the following theorem, which is sometimes useful:

Theorem: Let $\{M_\alpha \mid \alpha \in A\}$ be a collection of distinct and proper submodules of a module M . Then $M = \bigvee (M_\alpha \mid \alpha \in A)$ if, and only if, there exists a collection of mappings $\{p_\alpha \mid \alpha \in A\} \subset E(M) \sim \{O, I\}$ having the following properties:

- A. p_α is a projection of M_α for each $\alpha \in A$.
- B. $p_\alpha p_\beta = O$ if $\alpha \neq \beta$.
- C. For each $x \in M$, there exists a finite subset $F_x \subset A$ such that $p_\alpha(x) = O$ if $\alpha \notin F_x$.
- D. $x = \sum_{\alpha \in F_x} p_\alpha(x)$ for every $x \in M$.

We omit the proof of the theorem.

III. SEMI-SIMPLE MODULES

The first class of R -modules that we shall consider is the class of semi-simple modules. Throughout this section, no additional assumptions are made about R other than it have a unit.

Definition 1: A module M is semi-simple (completely reducible) if the lattice $\mathcal{L}$ of submodules of M is complemented.

Thus a module M is semi-simple if, and only if, for any submodule $N \subset M$, there exists another submodule $L \subset M$ such that $M = N \bigvee L$. Semi-simple modules exist, since any classical linear space is semi-simple. An example of a module which is not semi-simple is the ring of integers Z , considered as a module over itself in the obvious manner.

One should note that, if M is semi-simple and $N \subset M$ is any submodule, then N is also semi-simple. This is clear, since relative complements always exist in a complemented modular lattice.

The property of semi-simplicity is much more remarkable than one might at first suppose. Of particular importance is the fact that any semi-simple module is the direct join of simple submodules. We prepare for the proof of this assertion with a couple of simple lemmas.

Lemma 1A: Let M be semi-simple and $N \subset M$ any submodule. If $N \neq \{0\}$, there exists a nonzero simple submodule $P \subset N$.

Proof: Let $x \in N$, $x \neq 0$. If $m(\{x\})$ is simple, then we are done. Suppose, therefore, that there exists a proper submodule $L \subset m(\{x\})$. Consider the class $\mathcal{C}$ of all proper submodules of $m(\{x\})$ which do not contain x . Clearly $\mathcal{C} \neq \emptyset$, and it is obvious that $\mathcal{C}$ is an inductively ordered set under $\subset$. By Zorn's lemma, let $M \in \mathcal{C}$ be maximal. By semi-simplicity, there is a submodule $P \subset m(\{x\})$ such that $m(\{x\}) = M \dot{\vee} P$. It is now clear that, if $m(\{x\})$ is not simple, then P is the desired simple submodule of N . Q.E.D.

Lemma 1B: Let M be any module and $\{M_\alpha | \alpha \in A\}$ the class of all (distinct) simple submodules of M . If $M = \bigvee (M_\alpha | \alpha \in A)$ and $N \subset M$ is any submodule, then there exists a set $B \subset A$ such that $M = N \dot{\vee} [\bigvee (M_\beta | \beta \in B)]$.

Proof: If $N = M$, choose $B = \emptyset$. Now suppose $N \neq M$. For convenience, if $C \subset A$ and $C \neq \emptyset$, write $M(C) = \bigvee (M_\gamma | \gamma \in C)$. To prove the lemma, let $\mathcal{P}$ be the class of all nonempty subsets of A having the following properties: 1. $M(C)$ is a direct join for each $C \in \mathcal{P}$, and 2. $N \cap M(C) = \{0\}$ for every $C \in \mathcal{P}$. It is easy to show that $\mathcal{P} \neq \emptyset$. First of all, if $\alpha \in A$, then $N_\alpha \cap N = \{0\}$ or N_α . Suppose $N_\alpha \cap N = N_\alpha$ for every $\alpha \in A$ such that $N_\alpha \neq \{0\}$. Then $M = M(A) \subset N \subset M$, contrary to hypothesis. Hence, for some $\gamma_1 \in A$, $N_{\gamma_1} \neq \{0\}$ while $N_{\gamma_1} \cap N = \{0\}$. Clearly $\{\gamma_1\} \in \mathcal{P}$. Next observe that $\mathcal{P}$ is a partially ordered set under set inclusion $\subset$. Let $\mathcal{S} \subset \mathcal{P}$ be any simply ordered subset, and set $C_1 = \bigcup \mathcal{S}$. It is not altogether trivial to see that $C_1 \in \mathcal{P}$. We first show that $M(C_1)$ is a direct join. Let $F \subset C_1$ by any finite subset. Since $\mathcal{S}$ is simply ordered, $F \subset D$ for some $D \in \mathcal{S}$. But $M(D)$ is a direct join, so that $M(F)$ is also a direct join. Hence $M(C_1)$ is direct. We next prove that $N \cap M(C_1) = \{0\}$. Let $x \in N \cap M(C_1)$. Then there exists a finite, nonempty subset $F \subset C_1$ and $x_\alpha \in M_\alpha$ for each $\alpha \in F$ such that $x = \sum x_\alpha$. As before, there exists a $C_2 \in \mathcal{S}$ such that $F \subset C_2$. Thus $x \in N \cap M(C_2) = \{0\}$, and hence $x = 0$. We now apply Zorn's lemma to the inductively ordered set $\mathcal{P}$. If $B \in \mathcal{P}$ is maximal, then certainly $N \dot{\vee} M(B)$ is a direct join. Let us suppose that $M \neq N \dot{\vee} M(B)$. Then, by an argument exactly like the one used to prove that $\mathcal{P} \neq \emptyset$, there is a $\beta \in A$ such that $N_\beta \neq \{0\}$ while $N_\beta \cap (N \dot{\vee} M(B)) = \{0\}$. An elementary calculation shows that $N_\beta \dot{\vee} (N \dot{\vee} M(B)) = N \dot{\vee} (\bigvee (M_\alpha | \alpha \in B \cup \{\beta\}))$. Hence $B \cup \{\beta\} \in \mathcal{P}$ and $B \cup \{\beta\} \supset B$ properly, which contradicts the maximality of B in $\mathcal{P}$. Consequently, $M = N \dot{\vee} M(B)$, and the lemma is proved.

Lemmas 1A and 1B provide the necessary machinery for the proof of the fundamental structure theorem for semi-simple modules. This is the following:

Theorem 1: Let M be a module. Then the following conditions on M are equivalent:

- A. M is semi-simple.
- B. M coincides with its socle.¹
- C. M is the direct join of simple submodules.

Proof: Clearly C implies B. By lemma 1B, B implies C and B implies A. The proof will therefore be complete if we show that A implies B. The case $M = \{0\}$ is trivial, so we suppose $M \neq \{0\}$. By lemma 1A, M contains a simple submodule $\neq \{0\}$. Let $N \neq \{0\}$ be the socle of M , and assume that $M \neq N$. Then there exists a submodule $N_1 \subset M$ such that $M = N \vee N_1$. It follows that $N \cap N_1 = \{0\}$, so that $N_1 \neq \{0\}$ contains no nonzero simple submodule of M . This contradicts lemma 1A, so $M = N$ as required. Q.E.D.

We have remarked earlier that the class of semi-simple modules includes the class of classical linear spaces. It is therefore natural, in our attempt to construct a generalized linear space, to find out which properties of linear spaces, if any, carry over to semi-simple modules. We shall now use Theorem 1 to ascertain in what respects semi-simple modules constitute a class of generalized linear spaces. We recall the crucial questions from Section I: Must a semi-simple module have a minimal set of generators? Is any minimal system of generators a basis? Need the cardinal numbers of any two minimal systems of generators (and hence of any two bases) be equal? We answer these questions now.

Theorem 2: Every nonzero semi-simple module M has a minimal system of generators.

Proof: Let M be any nonzero semi-simple R -module. By Theorem 1, M is the direct join of nonzero simple submodules, say $M = \vee (N_\alpha \mid \alpha \in A)$. Since any simple module is necessarily cyclic (with any nonzero element as generator), there exists, for each $\alpha \in A$, an $x_\alpha \neq 0$ such that $N_\alpha = m(\{x_\alpha\})$. Clearly $x_\alpha \neq x_\beta$ if $\alpha \neq \beta$.² Define $H = \{x_\alpha \mid \alpha \in A\}$. I assert that H is a minimal system of generators for M . Let $x \in M$. Then there is a finite, nonempty subset $F \subset A$ and a $y_\alpha \in N_\alpha$ for each $\alpha \in F$ such that $x = \sum y_\alpha$. Now $y_\alpha = r_\alpha x_\alpha$ for some $r_\alpha \in R$. Thus $x \in m(H)$, so that H is certainly a system of generators for M . We proceed to show the minimal property. Let $\gamma \in A$ be arbitrary, and set $I = H \sim \{x_\gamma\}$. Assume that $x_\gamma \in m(I)$. Then there is a finite subset $F \subset A \sim \{\gamma\}$ and an $S_\alpha \in R$ for each $\alpha \in F$ such that $x_\gamma = \sum S_\alpha x_\alpha$. Now it is a simple matter to see that $\vee (N_\alpha \mid \alpha \in F \cup \{\gamma\})$ is a direct join. Since $0 = x_\gamma - \sum S_\alpha x_\alpha \in \vee (N_\alpha \mid \alpha \in F \cup \{\gamma\})$, we have that $x_\gamma = 0$, which is impossible. Hence $x_\gamma \notin m(I)$, and $M \not\subset m(I)$. Q.E.D.

¹Recall that the socle of a module M is the join of all its simple submodules.

²We assume that the function $\alpha \rightarrow N_\alpha$ is 1-1.

Theorem 3: There exists (at least) a denumerable infinity of semi-simple modules for which the following statements are true:

- A. There are at least two minimal sets of generators.
- B. Two minimal sets of generators need not have the same cardinal number.
- C. A minimal system of generators may fail to be a basis.

Proof: Let p_1, p_2 be distinct prime integers ≥ 2 , and let $Z_{p_1 p_2}$ denote the factor ring of integers Z module the principal ideal $(p_1 p_2)$ generated by $p_1 p_2$. We shall show that $Z_{p_1 p_2}$, considered as a module over itself in the obvious manner, is semi-simple. Let us set $Z_{p_1 p_2} = \{\bar{0}, \bar{1}, \dots, \overline{(p_1 p_2 - 1)}\}$, where $\bar{m}$ in general denotes the equivalence class of $m \in Z$ relative to $(p_1 p_2)$. Define $N_1 = \{n \bar{p}_1 \mid n \in Z \text{ and } 0 \leq n < p_2\}$ and $N_2 = \{n \bar{p}_2 \mid n \in Z \text{ and } 0 \leq n < p_1\}$. It is trivial to see that N_1 and N_2 are submodules of $Z_{p_1 p_2}$. They are also simple submodules, since N_1 and N_2 are finite groups of prime orders p_2 and p_1 , respectively. Now let $k \in Z$. There exist integers $\beta, \gamma \in Z$ such that

$$k = k\beta p_1 + k\gamma p_2.$$

There exist $\delta, \epsilon, \zeta, \eta \in Z$ such that

$$\begin{aligned} k\beta &= \delta p_2 + \epsilon; \quad 0 \leq \epsilon < p_2, \\ k\gamma &= \zeta p_1 + \eta; \quad 0 \leq \eta < p_1. \end{aligned}$$

Making substitutions and forming equivalence classes, we see that $\bar{k} = \epsilon \bar{p}_1 + \eta \bar{p}_2 \in N_1 \vee N_2$. Now it is obvious that $N_1 \cap N_2 = \{\bar{0}\}$. From these remarks, it is clear that $Z_{p_1 p_2} = N_1 \vee N_2$, so by Theorem 1, $Z_{p_1 p_2}$ is semi-simple. To prove Theorem 3, note that $H_{m,n} = \{m \bar{p}_1, n \bar{p}_2\}$, where $0 < m < p_2$ and $0 < n < p_1$, is a minimal system of generators for $Z_{p_1 p_2}$. Trivially $H = \{\bar{1}\}$ is a minimal set of generators. Nevertheless, $\text{card } H_{m,n} \neq \text{card } H$ always. Finally, $H_{m,n}$ is not a basis for $Z_{p_1 p_2}$ for any m and n , since $\bar{p}_2(m \bar{p}_1) + \bar{p}_1(n \bar{p}_2) = \bar{0}$ while $\bar{p}_1, \bar{p}_2 \neq \bar{0}$. Q.E.D.

From Theorem 3, we conclude that, unless further restrictions be placed on the operator ring R , semi-simple modules cannot qualify as generalized linear spaces.

We conclude this section with a discussion of the weak dimension of a semi-simple module. This notion will be particularly useful when we come to discuss isotypic modules. We begin with some almost obvious lemmas.

Lemma 4A: Let M and N be simple modules and $f: M \rightarrow N$ any homomorphism such that $\text{Ker } f \neq M$. Then f is an isomorphism.

Proof: Trivial.

Lemma 4B: Let N_1, N_2 be submodules of a module M_1 and suppose the function $f: N_1 \rightarrow M/N_2$ defined by $f(x) = (x)$ for all $x \in N_1$ is an isomorphism. Then $M = N_1 \vee N_2$.

Proof: If $y \in M$, there is an $x \in N_1$ such that $(x) = (y)$, so that $y - x \in N_2$. Since $y = x + (y - x) \in N_1 \vee N_2$, it is clear that $M = N_1 \vee N_2$. Let $x \in N_1 \cap N_2$. Then $f(x) = 0$, and therefore $x = 0$. Q.E.D.

We can now state an important theorem about isomorphic semi-simple modules.

Theorem 4: Let M and N be semi-simple modules. If $M = \bigvee (M_\alpha | \alpha \in I_1)$ and $N = \bigvee (N_\beta | \beta \in I_2)$ where $\{M_\alpha | \alpha \in I_1\}$ and $\{N_\beta | \beta \in I_2\}$ are collections of nonzero simple submodules, then $M \approx N$ only if $\text{card } I_1 = \text{card } I_2$.

Proof: The proof is divided into two parts:

Case I. Assume $\text{card } I_1 = n < \aleph_0$. We consider the statement as a propositional function $E(n)$ on the natural numbers $n \geq 1$. The case $n = 1$ is obvious. Now suppose $E(\gamma - 1)$ is true, where γ is any integer > 1 . We show that $E(\gamma)$ is true, thus completing the induction. Let $\text{card } I_1 = \gamma$, and let $g: M \rightarrow N$ be an isomorphism. If $b_0 \in I_2$, then $g^{-1}(N_{b_0}) \neq \{0\}$, M is a simple submodule of M . Hence there is a proper submodule $\bar{M} \subset M$ such that $M = g^{-1}(N_{b_0}) \vee \bar{M}$, and consequently $M/\bar{M} \approx g^{-1}(N_{b_0})$. Let $h: M \rightarrow M/\bar{M}$ be defined by $h(x) = (x)$ for all $x \in M$. Since $M \neq \bar{M}$, $h(M_{a_0}) \neq \{\bar{M}\}$ for some $a_0 \in I_1$. Hence $h(M_{a_0}) = M/\bar{M}$ by simplicity of $M/\bar{M}$, and therefore h induces a nontrivial homomorphism $K: M_{a_0} \rightarrow M/\bar{M}$ in the obvious fashion. By Lemma 4A, K is an isomorphism. Hence $M = M_{a_0} \vee \bar{M}$ by Lemma 4B. Now $M = M_{a_0} \vee \left[\bigvee (M_\alpha | \alpha \in I_1 \sim \{a_0\}) \right]$ and $N = N_{b_0} \vee \left[\bigvee (N_\beta | \beta \in I_2 \sim \{b_0\}) \right]$. Hence, if we set $P = \bigvee (M_\alpha | \alpha \in I_1 \sim \{a_0\})$ and $\bar{P} = \bigvee (N_\beta | \beta \in I_2 \sim \{b_0\})$, we obtain the chains of isomorphisms

$$M/g^{-1}(N_{b_0}) \approx \bar{M} \approx M/M_{a_0} \approx P \text{ and}$$

$$N/N_{b_0} \approx \bar{P}.$$

Next observe that the function $f: M \rightarrow N/N_{b_0}$ defined by $f(x) = (g(x))$ for all $x \in M$ is an onto homomorphism with Kernel $\text{Ker } f = g^{-1}(N_{b_0})$. Thus

$$M/g^{-1}(N_{b_0}) \approx N/N_{b_0},$$

and in view of the above isomorphisms, evidently $P \approx \bar{P}$. Since $\text{card}(I_1 \sim \{a_0\}) = \gamma - 1$, it follows by the induction hypothesis that $\text{card}(I_2 \sim \{b_0\}) = \gamma - 1$. Thus $\text{card } I_2 = \gamma$, and $E(\gamma)$ holds good.

Case II. Assume that $\text{card } I_1 \geq \aleph_0$. Then necessarily $\text{card } I_2 \geq \aleph_0$. Let $g: M \rightarrow N$ be an isomorphism. Denote by I_2^F the set of all finite, nonempty subsets of I_2 . If $G \in I_2^F$, define $N(G) = \bigvee (N_\beta \mid \beta \in G)$. Let $a \in I_1$ and $x \in M_a$ with $x \neq 0$. Now there is a finite nonempty subset $G \subset I_2$ and a $y_b \in N_b$ for each $b \in G$ such that $g(x) = \sum y_b$. Certainly $g(M_a) \cap N(G) \neq \{0\}$, and therefore $g(M_a) \subset N(G)$. Now for each $a \in I_1$, let $J_a \in I_2^F$ be such that $g(M_a) \subset N(J_a)$. Set $J = \{J_a \mid a \in I_1\}$ and let $I_3 = \bigcup J$. Suppose there is a $C \in I_2$ such that $C \notin I_3$. Then $g(M) \subset \bigvee (g(M_\alpha) \mid \alpha \in I_1) \subset \bigvee (N(J_\alpha) \mid \alpha \in I_1) \subset \bigvee (N_\beta \mid \beta \in I_2 \sim \{C\})$, and this last join is properly contained in N . Hence g is not an isomorphism, which is impossible. Thus $I_2 = \bigcup J$. It now follows easily from standard theorems in the theory of transfinite cardinal numbers that $\text{card } J = \text{card } I_2$.³ Clearly $\text{card } J \leq \text{card } I_1$. Hence $\text{card } I_2 \leq \text{card } I_1$. Reversing the roles of I_1 and I_2 (this time using g^{-1}), we see that $\text{card } I_1 \leq \text{card } I_2$. By Bernstein's lemma, $\text{card } I_1 = \text{card } I_2$. Q.E.D.

Of present interest in Theorem 4 is the case in which M and N are the same module. This permits

Definition 2: Let M be any semi-simple module, and let $M = \bigvee (M_\alpha \mid \alpha \in I)$ where $\{M_\alpha \mid \alpha \in I\}$ is a collection of nonzero simple submodules of M . By the weak dimension of M , we mean the cardinality of I ; in symbols, $\text{wdim } M = \text{card } I$. We make the convention that the weak dimension of the zero module is zero.

One should note that the weak dimension is not a "dimension" in the customary sense. Indeed, $\text{wdim } M$ does not even determine the semi-simple R -module M up to an R -isomorphism. To show this, consider the ring of polynomials $Z_6[X]$. We regard $Z_6[X]$ as a Z_6 -module in the usual manner. Let $M = \{0, 3, 3X, 3 + 3X\} \subset Z_6[X]$. M is clearly a Z_6 -submodule of $Z_6[X]$, and it is easy to see that every cyclic submodule of M is simple. Therefore, by Theorem 1, M is semi-simple. Since $H = \{3, 3X\}$ is a minimal set of generators for M , it follows that $\text{wdim } M = 2$. Now regard Z_6 as a Z_6 -module, using the ring multiplication. By Theorem 3, $Z_6 \approx Z_2 \bigvee Z_3$, whence $\text{wdim } Z_6 = 2$. Nevertheless, M and Z_6 are not Z_6 -isomorphic as semi-simple Z_6 -modules; indeed, M and Z_6 are not even cardinally equivalent as sets.

³If A is any set with $\text{card } A \geq \aleph_0$, and if $\mathcal{A}$ is any collection of finite subsets of A such that $A = \bigcup \mathcal{A}$, then $\text{card } \mathcal{A} = \text{card } A$. For proof, see Sierpiński, W., Lecons sur les nombres transfinis, Paris, (1928).

IV. SEMI-SIMPLE ISOTYPIC MODULES

We proceed now to place more restrictions on the module structure of a semi-simple module.

Definition 3: Let M be an R -module. We call M isotypic if all of the nonzero simple submodules of M are R -isomorphic.

One should observe that any (classical) linear space is isotypic. On the other hand, the semi-simple module Z_6 is not isotypic. Indeed, the class of semi-simple isotypic modules is properly contained in the class of semi-simple modules and properly contains the class of ordinary vector spaces.

The first result concerning semi-simple isotypic modules is already at hand. It states that such a module is "almost" uniquely determined by its weak dimension.

Theorem 5: Let M and N be semi-simple isotypic R -modules. Then M and N are R -isomorphic if, and only if, the following conditions hold:

- A. There exist nonzero simple submodules $\overline{M} \subset M$ and $\overline{N} \subset N$ such that $\overline{M} \approx \overline{N}$.
- B. $\text{wdim } M = \text{wdim } N$.

Proof: Write $M = \bigvee (M_\alpha | \alpha \in I_1)$ and $N = \bigvee (N_\beta | \beta \in I_2)$ where $\{M_\alpha | \alpha \in I_1\}$ and $\{N_\beta | \beta \in I_2\}$ are collections of nonzero simple submodules of M and N , respectively. To show necessity, let $g: M \rightarrow N$ be an isomorphism. If $\alpha_0 \in I_1$, then g induces a one-one homomorphism $h: M_{\alpha_0} \rightarrow N$ in the obvious manner. Since N is isotypic, $h(M_{\alpha_0}) \approx N_{\beta_0}$ for any $\beta_0 \in I_2$. Hence $M_{\alpha_0} \approx N_{\beta_0}$, and A. is proved. B. follows at once from Theorem 4. Now let us assume that both conditions hold good. We may suppose that the M_α and the N_β are all proper submodules; for otherwise, $M = \overline{M} \approx \overline{N} = N$, and the proof is complete. Let $\{p_\alpha | \alpha \in I_1\} \subset E(M) \sim \{0, 1\}$ and $\{\overline{p}_\beta | \beta \in I_2\} \subset E(N) \sim \{0, 1\}$ be the mappings of the theorem of Section II, and let $f: I_1 \rightarrow I_2$ be any one-one, onto mapping inducing the cardinal equivalence of I_1 and I_2 . Now it is clear that $M_\alpha \approx N_\beta$ for any α, β . Hence, for each $\alpha \in I_1$, there exists an isomorphism $f_\alpha: M_\alpha \rightarrow N_{f(\alpha)}$. Define a function $g: M \rightarrow N$ by

$$g(x) = \sum f_\alpha p_\alpha(x)$$

for all $x \in M$. The summation is of course meaningful, since $p_\alpha(x) = 0$ for almost all $\alpha \in I_1$. We are going to show that g is an isomorphism. Let $x, y \in M$ and $\gamma \in R$. Then

$$g(x + y) = \sum f_{\alpha} p_{\alpha}(x + y) = \sum f_{\alpha} p_{\alpha}(x) + \sum f_{\alpha} p_{\alpha}(y) = g(x) + g(y), \text{ and}$$

$$g(rx) = \sum f_{\alpha}(r p_{\alpha}(x)) = \sum r f_{\alpha} p_{\alpha}(x) = r \sum f_{\alpha} p_{\alpha}(x) = r g(x).$$

Next let $x \in \text{Ker } g$. Then $\sum f_{\alpha} p_{\alpha}(x) = 0$, whence $f_{\alpha} p_{\alpha}(x) = 0$ for every $\alpha \in I_1$. Now $\text{Ker } f_{\alpha} = \{0\}$, so that $p_{\alpha}(x) = 0$ for all α . Thus $x = \sum p_{\alpha}(x) = 0$, and g is a monomorphism. Finally, let $y \in N$. If we set

$$x = \sum (f_{\alpha})^{-1} \bar{p}_f(\alpha)(y),$$

then a simple calculation shows that $g(x) = y$. This completes the proof of the theorem.

The above theorem shows a remarkable relationship between a semi-simple isotypic module and its weak dimension. It is only fair to ask how many of the properties of a vector space stated in Section I hold good for these modules. I do not yet know whether or not the cardinal numbers of any two minimal systems of generators are equal. If this question can be answered in the affirmative, there follows the problem of discovering the relationship, if any, between the (ordinary) dimension and the weak dimension. These two dimensions are of course identical in the case of a linear space, but analysis in the present, far more general situation seems difficult. On the other hand, it is fairly easy to give examples of semi-simple isotypic modules for which a minimal system of generators is not a basis. In view of the underlying matrix motivation, this alone, regardless of the above unanswered question, proves that the semi-simple isotypic module (over a unital ring) cannot qualify as a generalized linear space.

Theorem 6: There exists (at least) a denumerable infinity of semi-simple isotypic modules for which a minimal system of generators is not a basis.

Proof: Let N be any integer ≥ 2 , and let $Z_{2N} = \{0, 1, \dots, (2N-1)\}$ be the factor ring of integers modulo the principal ideal $(2N)$. We consider the ring $Z_{2N}[X]$ of polynomials in one indeterminate over Z_{2N} . It is clear that $Z_{2N}[X]$ can be regarded as a Z_{2N} -module, and it is in this manner that $Z_{2N}[X]$ is to be regarded for the duration of the proof. Define

$$M = \left\{ f \mid f = \sum_0^n b_i X^i \in Z_{2N}[X] \text{ and } b_i = 0 \text{ or } N \right\}.$$

First of all, it is clear that, if $f, g \in M$, then $f + g \in M$ and $f + f = 0$. Moreover, if $r \in Z_{2N}$ then

$$rf = \begin{cases} f & r = 2k-1; k = 1, 2, \dots, N \\ 0 & r = 2k-2; k = 1, 2, \dots, N \end{cases}.$$

These relations are clear, since $(2k-1)N \equiv N \pmod{2N}$ and $(2k-2)N \equiv 0 \pmod{2N}$ if $k = 1, 2, \dots, N$. Hence M is a Z_{2N} -submodule of $Z_{2N}[X]$. We shall show that M is semi-simple and isotypic. Let $f \in M$. Then $m(\{f\}) = \{0, f\}$, so that every cyclic submodule is simple. Hence M coincides with its socle and is therefore semi-simple by Theorem 1. Let $f, g \in M$ with $f, g \neq 0$. Define $\phi: m(\{f\}) \rightarrow m(\{g\})$ by $\phi(f) = g$ and $\phi(0) = 0$. It is immediate that ϕ is an isomorphism, whence M is isotypic. Now $H = \{NX^i \mid 0 \leq i < \infty\}$ is a minimal set of generators for M but is not a basis; for $\sum 2(NX^i) = 0$, yet $2 \neq 0$. Q.E.D.

V. CYCLICALLY SIMPLE MODULES AND MODULAR DOMAINS OF INTEGRITY

We continue the search for a generalized linear space with the consideration of a certain subclass of the class of semi-simple isotypic modules.

Definition 4: A module M is said to be cyclically simple in case any nonzero cyclic submodule $N \subset M$ is generated by every nonzero element of N .

As an obvious consequence of the definition, we see that, if M is cyclically simple, then any cyclic submodule $N \subset M$ is simple. Since a simple module is always cyclic, it follows that the class of simple submodules of M coincides with the class of cyclic submodules. Hence a cyclically simple module is always contained in its socle, and we have established (see Theorem 1) the

Proposition: A cyclically simple module is necessarily semi-simple.

We proceed now to introduce a module theoretic generalization of the classical notion of an integral domain.

Definition 5: An R -module M is said to be an R -domain of integrity if for any $a \in R$ and $x \in M$, $ax = 0$ implies either $a = 0$ or $x = 0$.

In terms of the (left) ideals of R , the condition of Definition 5 simply states that the order ideal of every nonzero element of M is the zero ideal of R .

Note that, if R is any unital ring and we regard R as an R -module in the obvious manner, then the statement that R is a domain of integrity as a ring is consistent with the statement that R is an R -domain of integrity as an R -module.

Proposition: Any domain of integrity M is isotypic.

Proof: Let M_1 and M_2 be nonzero simple submodules of M . Then $M_1 = m(\{x_1\})$ and $M_2 = m(\{x_2\})$, where $x_1, x_2 \neq 0$. Define a function $f: M_1 \rightarrow M_2$ by $f(ax_1) = ax_2$. Since M is an integral domain, f is well-defined and one-one, and it is obvious that f is an epimorphism. Hence $M_1 \approx M_2$. Q.E.D.

Clearly, any linear space is a cyclically simple domain of integrity. Hence the class of cyclically simple integral domains contains the class of (classical) vector spaces and is (properly) contained in the class of semi-simple isotypic modules. We now show that this particular class of modules possesses all those properties desirable of a generalized linear space.

Theorem 7: Let $M \neq \{0\}$ be any cyclically simple R -domain of integrity. Then M has the following properties:

- A. M has a minimal system of generators.
- B. Every minimal set of generators is a basis for M .
- C. Any two bases for M have the same cardinal number (finite or infinite).
- D. The uniquely defined cardinal number in C determines M up to an R -isomorphism.

Property A follows from semi-simplicity and Theorem 2. Properties B, C, and D are restated below as separate lemmas.

Lemma 7A: Suppose that $H = \{x_\alpha | \alpha \in A\}$ is a minimal set of generators for a cyclically simple module M . Then $M = \bigvee (m(\{x_\alpha\}) | \alpha \in A)$.

Proof: For convenience, put $M_\alpha = m(\{x_\alpha\})$. Since H constitutes a minimal system of generators for M , $M = m(H) \subset m(\bigcup_{\alpha \in A} M_\alpha) = \bigvee (M_\alpha | \alpha \in A) \subset M$. To show the directness of the join, let $\beta \in A$ be arbitrary, and suppose that $L = \bigvee (M_\alpha | \alpha \in A \sim \{\beta\}) \cap M_\beta \neq \{0\}$. Then $L = M_\beta$, by the simplicity of M_β . Hence $M_\beta \subset \bigvee (M_\alpha | \alpha \in A \sim \{\beta\})$, and this implies that $m(I) = M$, where $I = \{x_\alpha | \alpha \in A \sim \{\beta\}\}$. This is impossible if H is a minimal system of generators for M , and so $M = \bigvee (M_\alpha | \alpha \in A)$. Q.E.D.

Lemma 7B: If $H = \{x_\alpha | \alpha \in A\}$ is a minimal system of generators for the cyclically simple R -domain of integrity M , then H is a basis for M .

Proof: Let $F \subset A$ be any finite subset, and suppose that $\sum_F a_\alpha x_\alpha = 0$, where $a_\alpha \in R$ and $x_\alpha \in H$. By Lemma 7A, $M = \bigvee (M_\alpha | \alpha \in A)$, and hence, a fortiori, $\bigvee (M_\alpha | \alpha \in F)$ is a direct join. Therefore $a_\alpha x_\alpha = 0$ for every $\alpha \in F$. But every $x_\alpha \neq 0$. Hence $a_\alpha = 0$ for all $\alpha \in F$, since M is an integral domain. Q.E.D.

Lemma 7C: Let M be cyclically simple, and suppose that $H_1 = \{x_\alpha | \alpha \in A\}$ and $H_2 = \{y_\beta | \beta \in B\}$ are minimal sets of generators for M . Then $\text{card } H_1 = \text{card } H_2$.

Proof: Clearly $x_{\alpha_1} \neq x_{\alpha_2}$ if $\alpha_1 \neq \alpha_2$, and a similar statement holds for the y_β 's. Hence we focus our attention on the equality $\text{card } A = \text{card } B$. First of all, $M_\alpha = m(\{x_\alpha\})$ and $N_\beta = m(\{y_\beta\})$ are simple for every $\alpha \in A$ and $\beta \in B$, by cyclic simplicity. Moreover, by Lemma 7A, $M = \bigvee (M_\alpha | \alpha \in A) = \bigvee (N_\beta | \beta \in B)$. Hence, by semi-simplicity and Theorem 4, $\text{card } A = \text{card } B$ ($= {}^w\dim M$). Q.E.D.

We thus see that the cardinal numbers of any two minimal systems of generators (and hence also of any two bases) for a cyclically simple module M are the same. We call this uniquely determined cardinal number ($= {}^w\dim M$) the dimension of M (notation: $\dim M$). As usual, we make the convention that $\dim M = 0$ if $M = \{0\}$.

Lemma 7D: Let M_1 and M_2 be R -domains of integrity. If $N_1 \subset M_1$ and $N_2 \subset M_2$ are nonzero simple submodules, then $N_1 \approx N_2$.

Proof: The proof of this lemma is entirely analogous to the proof of the already established proposition that any integral domain is isotypic.

We now complete the proof of Theorem 7 with

Lemma 7E: Let M and N be cyclically simple R -domains of integrity. Then M and N are R -isomorphic if, and only if, $\dim M = \dim N$.

Proof: Condition A of Theorem 5 is clearly superfluous, in view of Lemmas 1A and 7D. Q.E.D.

Theorem 7 proves that the cyclically simple integral domain apparently can qualify as a generalized linear space. Now we have already remarked that the class of cyclically simple domains of integrity contains the class of classical vector spaces. Thus a natural question is whether or not there exist cyclically simple domains of integrity that are not ordinary vector spaces. We present the (unfortunate) answer to this question in

Theorem 8: Let $M \neq \{0\}$ be any cyclically simple R -domain of integrity. Then R is a division ring.

Proof: Let $I \subset R$, $I \neq \{0\}$, be any left ideal of R , and choose $x \in M$, $x \neq 0$, arbitrarily. The set $N = \{rx \mid r \in I\}$ is clearly a nonzero submodule of $m(\{x\})$, so that $N = m(\{x\})$. Let $s \in R$. Then $sx \in N$ and $sx = rx$ for some $r \in I$. Since $x \neq 0$, $s = r \in I$, whence $I = R$. Hence the ring R has no proper left ideals. Since R has a unit, it follows that R is a division ring.¹ Q.E.D.

Needless to say, Theorem 8 affords a new characterization of ordinary vector spaces. Also, as a corollary to the proof of this theorem, we have the following interesting result:

Corollary 8A: For a modular integral domain $M \neq \{0\}$, the following statements are equivalent:

- A. M is semi-simple.
- B. M is cyclically simple.
- C. M contains a simple submodule $N \neq \{0\}$.

In particular, an R -module $M \neq \{0\}$ is a vector space if, and only if, M is a semi-simple R -integral domain.

Proof: The chain of implications $C \Rightarrow B \Rightarrow A \Rightarrow C$ is clear.

¹This is a well-known characterization of a division ring. See, for example, Jacobson, N., Lectures in Abstract Algebra, I, Basic Concepts, D. Van Nostrand Co., Inc., New York, (1951).