1963

Fundamental theory of modules over rings

James Thomas Sedlock
Lehigh University

FUNDAMENTAL THEORY OF MODULES OVER RINGS

by

James Thomas Sedlock

A THESIS

Presented to the Graduate Faculty

of Lehigh University

in Candidacy for the Degree of

Master of Science

Lehigh University

1963

(ii)

CERTIFICATE OF APPROVAL

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science.

May 15, 1963
(date)

Gerhard Rayna
Professor in charge

Ernst Pitcher
Head of the Department

TABLE OF CONTENTS

CHAPTER I - MODULES AND SUBMODULES

A set M is called a left module over a ring R if:

1) (M,+) is an abelian group
2) there exists a scalar multiplication between elements of M and R such that for each m in M and r in R there is a unique element rm in M
3) this scalar multiplication satisfies the conditions

$$r(m + m') = rm + rm'$$
$$(r + r')m = rm + r'm$$
$$(rr')m = r(r'm)$$

for all r,r' in R and m,m' in M.

If, in addition, R has an identity 1 and

$$1m = m$$

for all m in M, then M is called a unitary module. When condition 2) above is fulfilled, we simply say M has a ring R as a set of left operators. One may similarly define a right module over a ring R.

In a left R-module as defined above the product mr has no meaning, since R operates only on the left. Hence, defining

$$mr = rm$$

for all r in R and m in M, we claim

Theorem 1: If mr is defined by the preceding equation, then any left module M over a commutative ring R is a right R-module.

Proof: By definition of left R-module M, (M,+) is an abelian group. If R is a set of left operators and

$$mr = rm,$$

then it is also a set of right operators. Lastly,

$$(m + m')r = r(m + m') = rm + rm' = mr + m'r$$

$$m(r + r') = (r + r')m = rm + r'm = mr + mr'$$

$$m(rr') = (rr')m = (r'r)m = r'(rm) = (rm)r' = (mr)r'.$$

Note that the commutativity of R was used in the last step only.

Some examples of modules:

1) Any vector space over a field or skew-field is a unitary module over a ring, where the ring is that field (or, as the case may be, skew-field)

2) Given any ring R, we may consider the additive abelian group (R,+) as a left R-module where R acts as a set of left operators, and as a right R-module when R operates on the right

3) Any abelian group (G,+) may be considered as a unitary module over the ring of integers Z if we define

$ng = g + \ldots + g$ (n times) for n positive

$0g$ = zero of the group

$ng = -g - \ldots -g$ (-n times) for n negative.

The last two examples imply that any subsequent statements pertaining to modules also apply to abelian groups and general rings when interpreted in this light.

A <u>submodule</u> N of a module M over ring R is a subset of M which is itself a module over R. For example, every left ideal in a ring, when the ring is considered as a left module over itself, is a submodule. Thus, any assertions about the submodules of a given module may be translated into ones about the ideals of a ring.

<u>Theorem 2</u>: If $N_1, \ldots, N_m$ are submodules of a module M over a ring R, then

$$\sum_{i=1}^{m} N_i = \left\{ \sum_{i=1}^{m} n_i \;\middle|\; n_i \text{ in } N_i \right\},$$

which we shall denote by N*, is also a submodule of M.

<u>Proof</u>: In proving a subset of a module to be a submodule all we need show is that it is a subgroup of the additive group of the module, and closed with respect to the scalar multiplication.

A) For any a,b in N*

$$a - b = \sum_{i=1}^{m} n_i - \sum_{i=1}^{m} n_i' = \sum_{i=1}^{m} (n_i - n_i')$$

which belongs in N* since each $(n_i - n_i')$ is in N_i. Therefore, N* is a subgroup of M.

B) Let r belong to R. For any a in N*

$$ra = r \sum_{i=1}^{m} n_i = \sum_{i=1}^{m} rn_i .$$ This is an element of N* since each rn_i belongs to N_i.

In the case of this theorem, we say that N* is the smallest submodule of M containing $N_1, \ldots, N_m$ in the sense that N* contains each N_i, and any other submodule containing each N_i must also contain N*.

Theorem 3: If $N_1, \ldots, N_m$ are submodules of a module M over a ring R, then

$$\bigcap_{i=1}^{m} N_i = \{ n \mid n \text{ in } N_i; \; i = 1, \ldots, m \}$$

which we shall denote by N**, is also a submodule of M.

Proof:

A) If n, n' belong to N**, then both are elements of each N_i

==> n - n' belongs to each N_i

==> n - n' belongs to N**

B) For any r in R and n in N**, n is an element of each N_i

==> rn belongs to each N_i

==> rn belongs to N** .

Theorem 4: (Dedekind Modular Law) If K, L, N are submodules of an R-module M such that $L \subset K$, then

$$K \cap (L + N) = L + (K \cap N) .$$

Proof: Let x belong to $K \cap (L + N)$. Then x = 1 + n for some 1 in L and n in N. Now x in K and 1 in $L \subset K$

==> n = x - 1 is in K

==> n is in $K \cap N$

==> x = 1 + n is in $L + (K \cap N)$.

Hence, $K \cap (L + N) \subset L + (K \cap N)$.

Conversely, let x belong to $L + (K \cap N)$. Then $x = l + k$ for some l in L and k in $K \cap N$. But $L \subset K$ and k in K

$\Longrightarrow$ $x = l + k$ is in K, and k in N

$\Longrightarrow$ $x = l + k$ is in $L + N$

$\Longrightarrow$ x is in $K \cap (L + N)$.

That is, $L + (K \cap N) \subset K \cap (L + N)$.

<u>Theorem 5</u>: Let R be a commutative ring. If either N is a submodule of an R-module M and S is an arbitrary subset of R, or N is an arbitrary subset of M and S is a left ideal in R, then

$$SN = \left\{ \sum_{i=1}^{m} s_i n_i \;\middle|\; s_i \text{ in } S,\ n_i \text{ in } N,\ m \text{ in } Z \text{ arbitrary} \right\}$$

is a submodule of M.

<u>Proof</u>:

A) If a, b belong to SN, then

$$a + b = \sum_{i=1}^{m} s_i n_i + \sum_{i=1}^{k} s_i' n_i' = \sum_{i=1}^{m+k} s_i n_i \quad \text{is in SN.}$$

For an arbitrary $a = \sum_{i=1}^{m} s_i n_i$ in SN, either

$$a' = \sum_{i=1}^{m} (-s_i) n_i \quad \text{or} \quad a' = \sum_{i=1}^{m} s_i (-n_i)$$

belongs to SN, depending on whether S is an ideal or N a submodule respectively. In either case,

$$a + a' = 0 .$$

B) For any r in R and a in SN,

$$ra = r\sum_{i=1}^{m} s_i n_i = \sum_{i=1}^{m} (rs_i)n_i \quad \text{belongs to SN if S is an ideal}$$

$$\sum_{i=1}^{m} s_i(rn_i) \quad \text{belongs to SN if N is a submodule}$$

The commutativity of R was used only in the last line of the proof.

CHAPTER II - HOMOMORPHISMS

A function $f: M \longrightarrow M^*$, where both M and M* are R-modules, is called an R-homomorphism of M into M* if for all m, m' in M and r, r' in R

$$f(m + m') = f(m) + f(m')$$

and

$$f(rm) = rf(m) .$$

Theorem 1: If M and M* are R-modules and $f: M \longrightarrow M^*$ is an R-homomorphism, then

A) $f(0) = 0^*$ (the zero of M*) and $f(-m) = -f(m)$

B) if $A \subset R$ and $L \subset M$, then $f(AL) \subset Af(L)$

C) $\ker f = \{ m \mid m \text{ in } M \text{ and } f(m) = 0^* \}$ is an R-submodule of M

D) f is one-to-one if and only if $\ker f = (0)$

E) if $L \subset M$ and $L^* \subset M^*$ are submodules, then $f(L)$ and $f^{-1}(L^*)$ are submodules of M* and M respectively .

Proof:

A) $f(0) = f(0 + 0) = f(0) + f(0)$

$$\Longrightarrow \quad f(0) = f(0) - f(0) = 0^*$$

$f(m - m) = f(m) + f(-m) = 0^*$

$$\Longrightarrow \quad f(-m) = 0^* - f(m) = -f(m)$$

B) Since any element of AL can be written as $\sum a_i b_i$ for some set of a_i in A and some set of b_i in L, then

$f(\sum a_i b_i) = \sum f(a_i b_i) = \sum a_i f(b_i)$ is in $Af(L)$

$\Longrightarrow \quad f(AL) \subset Af(L)$.

C) For any k, k' in ker f and r in R,

$f(k - k') = f(k) - f(k') = 0^* - 0^* = 0^*$

$\Longrightarrow$ $k - k'$ is in ker f

$f(rk) = rf(k) = r0^* = 0^*$ $\Longrightarrow$ rk is in ker f

D) If f is one-to-one, then $f(m) \neq f(m')$ for all $m \neq m'$ in M. But $f(0) = 0^*$

$\Longrightarrow$ $f(m) \neq 0^*$ for all $m \neq 0$ in M

$\Longrightarrow$ ker f = (0).

Conversely, let ker f = (0) and suppose there exist $m \neq m'$ in M such that $f(m) = f(m')$. Then

$$0^* = f(m) - f(m') = f(m) + f(-m') = f(m-m')$$

where $m - m' \neq 0$ since $m \neq m'$

$\Longrightarrow$ ker $f \neq (0)$, a contradiction.

Thus, f is one-to-one.

E) Let m,m' belong to $f^{-1}(L^*)$. Then $f(m)$, $f(m')$ in L^*

$\Longrightarrow$ $f(m) - f(m') = f(m - m')$ is in L^*

$\Longrightarrow$ $m - m'$ is in $f^{-1}(L^*)$.

For any r in R, $rf(m) = f(rm)$ is in L^* since $f(m)$ is an element of L^*

$\Longrightarrow$ rm belongs to $f^{-1}(L^*)$.

A similar argument holds for submodule $f(L)$ of M^*.

<u>Theorem 2</u>: Given an R-module M, then $L \subset M$ is an R-submodule if and only if there exists an R-homomorphism

$$f: M \longrightarrow M^*$$

such that $L = \ker f$.

Proof: The "if" case has been proved in part C) of the preceding theorem.

Now, let $L \subset M$ be an R-submodule. Then L is a subgroup of the abelian group $(M,+)$, and M/L is an abelian group. We assert:

A) For any r in R and $m + L$ in M/L (where $m + L$ denotes the coset of m in M/L), if we define

$$r(m + L) = rm + L$$

then M/L is an R-module. For,

i. M/L is an abelian group

ii. $r(m + L) = rm + L$ is in M/L since rm belongs to M. To exhibit the uniqueness of this product, let $m + L = m' + L$. Then $m - m'$ in L

$\Longrightarrow$ $r(m - m') = rm - rm'$ in L

$\Longrightarrow$ $(rm - rm') + L = L$, or $rm + L = rm' + L$

iii. $r[(m + L) + (m' + L)] = r[(m + m') + L]$

$$= r(m + m') + L = (rm + rm') + L$$

$$= (rm + L) + (rm' + L) = r(m + L) + r(m' + L)$$

$$(r + r')(m + L) = [(r + r')m + L] = (rm + r'm) + L$$

$$= (rm + L) + (r'm + L) = r(m + L) + r'(m + L)$$

$$(rr')(m + L) = (rr')m + L = r(r'm) + L$$

$$= r[r'm + L] = r[r'(m + L)] .$$

B) If we define $f: M \longrightarrow M/L$ in a natural way by

$$f(m) = m + L$$

then f is an R-homomorphism. For, given any r in R and m, m' in M

$$f(m + m') = (m + m') + L = (m + L) + (m' + L)$$
$$= f(m) + f(m')$$

$$f(rm) = (rm) + L = r(m + L) = rf(m).$$

Clearly, $\ker f = L$.

Theorem 3: (Fundamental Theorem of Homomorphisms of Modules) If $f\colon M \longrightarrow M^*$ is an R-homomorphism of R-modules M and M^*, then

$$M/\ker f \cong_R f(M)$$

(where "$\cong_R$" is to be read "is R-isomorphic to") .

Proof: Define $g\colon M/\ker f \longrightarrow f(M)$ by

$$g(m + \ker f) = f(m).$$

Note that if φ is the natural homomorphism from M to $M/\ker f$, then $g = f\varphi^{-1}$. We claim that g as defined is an R-isomorphism.

A) g is well-defined

Let $m + K = m' + K$, where $K = \ker f$. Then, $m - m'$ is in K and

$$g(m + K) - g(m' + K) = f(m) - f(m')$$
$$= f(m - m') = 0^*$$

$$\Longrightarrow \quad g(m + K) = g(m' + K)$$

B) g is an R-homomorphism

$$g[(m + K) + (m' + K)] = g[(m + m') + K] = f(m + m')$$
$$= f(m) + f(m') = g(m + K) + g(m' + K)$$

$$g[r(m + K)] = g(rm + K) = f(rm) = rf(m) = r[g(m + K)]$$

C) g is one-to-one

Let $g(m + K) = g(m' + K)$ be in $f(M)$. Then

$$0^* = g(m + K) - g(m' + K) = g[(m - m') + K]$$
$$= f(m - m')$$

$\Longrightarrow$ $m - m'$ belongs in K

$\Longrightarrow$ $(m - m') + K = K$, or $m + K = m' + K$

D) g is onto

Let f(m) be in f(M). Then certainly m is in M and $m + K$ is in M/K, and by definition

$$g(m + K) = f(m) .$$

The following two results are the Dedekind-Noether Isomorphism Theorems.

Theorem 4: If $f: M \longrightarrow M^*$ is an R-homomorphism of an R-module M onto an R-module M*, then

A) there exists a one-to-one correspondence between the submodules of M containing $K = \ker f$ and the submodules of M*

B) if $L \subset M$ corresponds to $L^* \subset M^*$, then

i. $f(L) = L^*$ and $f^{-1}(L^*) = L$

ii. f induces an R-homomorphism of L onto L*

iii. $L/K \cong_R L^*$

iv. $M/L \cong_R M^*/L^*$

Proof:

A) If $L \subset M$ is a submodule containing K, then $f(L) = L^*$ is a submodule of M* by Theorem 1 (II). To show that two distinct submodules of M cannot give rise to the same submodule of M*, assume there exist an L and an L' both containing K such that $f(L) = f(L')$. Then l in L

$\Longrightarrow$ there exists an l' in L' such that $f(l) = f(l')$

$\Longrightarrow$ $f(l - l') = 0$

$\Longrightarrow$ $l - l'$ belongs to $K \subset L'$

$\Longrightarrow$ $(l - l') + l' = l$ is in L'.

Hence, $L \subset L'$. Similarly, $L' \subset L$, so that $L = L'$.

Also, every submodule $L^* \subset M^*$ arises from a submodule of M containing the kernel: for, $f^{-1}(L^*)$ is a submodule of M by Theorem 1 (II), $K \subset f^{-1}(L^*)$ by definition of the inverse function, and $f(f^{-1}(L^*)) = L^*$ since f is onto.

B) i. Verified above

ii. Follows from i. and the fact that f is an R-homomorphism from $L \subset M$ onto $M^* \supset L^*$

iii. Since $f: L \longrightarrow L^*$ is an R-homomorphism with kernel K, then by Theoren 3 (II) $L/K \cong_R L^*$

iv. Since the natural R-homomorphism $\varphi: M^* \longrightarrow M^*/L^*$ is onto, then $\varphi f: M \longrightarrow M^*/L^*$ is an R-homomorphism onto. We wish to show that $\ker \varphi f = L$.

k belongs to $\ker \varphi f \iff \varphi f(k) = 0^*$

$\iff f(k)$ is in L^*

$\iff k$ is in $f^{-1}(L^*) = L$.

Thus, by the Fundamental Theorem, $M/L \cong_R M^*/L^*$.

Theorem 5: If N and L are submodules of an R-module M, then

$$(L + N)/N \cong_R L/(L \cap N).$$

Proof: From previous work we know that $(L + N)$ and $(L \cap N)$ are submodules of M such that $N \subset (L + N)$ and $(L \cap N) \subset L$. Therefore, we may consider the factor modules $(L + N)/N$ and $L/(L \cap N)$.

Let $f: (L + N) \longrightarrow (L + N)/N$ be the natural homomorphism, which is onto. Then f induces an R-homomorphism $g: L \longrightarrow (L + N)/N$ which we claim is also onto. For, let $x + N$ belong to $(L + N)/N$, where x is in $L + N$. Then $x = l + n$ for some l in L and n in N

$\Longrightarrow$ $x + N = l + N$. But, $g(l) = l + N$

$\Longrightarrow$ g is an R-homomorphism of L onto $(L + N)/N$. Since $\ker g = L \cap N$, by Theorem 3 (II) we have

$$L/(L \cap N) \cong_R (L + N)/N .$$

CHAPTER III - FINITENESS CONDITIONS

An R-module M is called Noetherian if it satisfies the ascending chain condition; that is, if every strictly ascending chain of submodules

$$N_1 \subset N_2 \subset \ldots$$

is finite. On the other hand, if the descending chain condition is fulfilled so that every strictly descending chain of submodules

$$N_1 \supset N_2 \supset \ldots$$

is finite, then M is called Artinian. For example, considered as a Z-module, the additive group of integers is Noetherian but not Artinian.

M is said to satisfy the maximum condition if every non-empty set of submodules contains an element not contained in any other submodule of that particular set. It satisfies the minimum condition if every non-empty set of submodules contains an element which does not properly contain any other submodule of the set.

To indicate the relationships between these definitions, we shall state the following purely set-theoretic result whose proof will be omitted.

Theorem 1: An R-module M is Noetherian if and only if it satisfies the maximum condition; M is Artinian if and only if it satisfies the minimum condition.

<u>Theorem 2</u>: If N is a submodule of R-module M, then M is either Noetherian or Artinian if and only if both M/N and N are likewise.

<u>Proof</u>: We shall consider only the Noetherian case.

If the A.C.C. holds for M, certainly if does also for N. The correspondence between submodules of M/N and those of M containing N assures that M/N satisfies the A.C.C.

Now suppose the converse and let $L_1 \subset L_2 \subset \ldots$ be an ascending chain of submodules of M. Then

$$(L_1 \cap N) \subset (L_2 \cap N) \subset \ldots$$

is a chain of submodules of N, so by hypotheses there exists an integer $n \geq 1$ such that

$$(L_n \cap N) = (L_{n+1} \cap N) = \ldots$$

Likewise, $(L_1 + N) \subset (L_2 + N) \subset \ldots$

is an ascending chain of submodules of M containing N, hence in one-to-one correspondence with the submodules of M/N, which satisfies the A.C.C. Therefore, for some integer $m \geq 1$,

$$(L_m + N) = (L_{m+1} + N) = \ldots$$

Let h be the greater of the integers m and n. Then we

have $(L_h \cap N) = (L_{h+1} \cap N) = \ldots$

and $(L_h + N) = (L_{h+1} + N) = \ldots$

where $L_h \subset L_{h+1} \subset \ldots$

However, for any integer $k \geq h$ we have

$$L_{k+1} = L_{k+1} \cap (L_{k+1} + N) = L_{k+1} \cap (L_k + N)$$

$$= L_k + (L_{k+1} \cap N) \quad \text{by the Modular Law}$$

$$= L_k + (L_k \cap N) = L_k$$

Q.E.D.

Theorem 3: If $N_1, \ldots, N_k$ are Noetherian submodules of an R-module M such that $M = N_1 + \ldots + N_k$, then M is also Noetherian.

Proof: Let k = 2. By theorem 5 (II)

$$M/N_1 = (N_1 + N_2)/N_1 \cong_R N_2/(N_1 \cap N_2) .$$

By the preceding theorem $N_2/(N_1 \cap N_2)$ satisfies the A.C.C., hence M/N_1 is Noetherian. Since the A.C.C. holds for N_1 also, the conclusion follows, again from the preceding theorem. The proof may be completed by induction.

(Remark: An analogous theorem is true for Artinian submodules)

A set of elements $\{ m_\alpha \mid \alpha \text{ in an index set } A \}$ of an R-module M is said to be a basis of M if for every element m in M there exist elements r_α in R and integers k_α such that

$$m = \sum_{\alpha \text{ in } A} (r_\alpha m_\alpha + k_\alpha m_\alpha),$$

where all but finitely many terms of this sum are zero. If M is unitary, the integral coefficients become unnecessary and it suffices that

$$m = \sum_{\alpha \text{ in } A} r_\alpha m_\alpha$$

for some r_α in R. If, in addition, the r_α are uniquely determined by m, then M is called R-free.

Theorem 4: R-module M is Noetherian if and only if every submodule of M has a finite basis.

Proof: First, assume M Noetherian. Let N be an arbitrary submodule of M, and $\mathcal{L}$ the set of all submodules of N having finite bases. Note that $\mathcal{L}$ is not empty since (0) is always such a submodule. Let L' in $\mathcal{L}$ be maximal; we already know that $L' \subset N$. For any n in N, $(n) = \{ rn \mid r \text{ in } R \}$ is a submodule of N having $\{ n \}$ as a basis, so that the submodule $L' + (n)$ of N is in $\mathcal{L}$ since both L' and (n) have finite bases. But $L' \subset L' + (n)$ and L' maximal

$\Longrightarrow$ $L' = L' + (n)$

$\Longrightarrow$ n belongs in L', since n is in $L' + (n)$

$\Longrightarrow$ $N \subset L'$.

Thus, N = L', the latter having a finite basis by hypothesis.

Conversely, suppose each submodule of M has a finite basis, and let $N_1 \subset N_2 \subset \ldots$ be an ascending chain of submodules. Then $N = \bigcup \{ N_i \}$ is a submodule of M, hence has a finite basis, say $\{ n_1, \ldots, n_m \}$. For each basis element n_i there exists an integer k_i such that n_i belongs to N_{k_i}. Let k be maximum of these m integers. For such a k each basis element of N is contained in N_k

$\Longrightarrow$ $N \subset N_k$ $\Longrightarrow$ $N = N_k$.

That is, the given sequence terminates at N_k, which is the desired conclusion.

Theorem 5: If M is a unitary R-module having a finite basis, and the ring R is left Noetherian (or Artinian), then M is also Noetherian (or Artinian).

Remark: Since the submodules of R, when R is considered as a left R-module, are its left ideals, then the chain conditions when referred to R pertain to sequences of left ideals in R.)

<u>Proof</u>: Let R satisfy the A.C.C. If $\{ m_1, \ldots, m_n \}$ is a finite basis for M, then

$$M = Rm_1 + \ldots + Rm_n \quad .$$

By Theorem 3 (III) it suffices to show that each submodule Rm_i of M satisfies the A.C.C.

So, let m be an arbitrary basis element, and $N_1 \subset N_2 \subset \ldots$ an ascending chain of submodules of Rm. Form the sequence $I_1, I_2, \ldots$ where

$$I_i = \{ r \mid r \text{ in } R \text{ and } rm \text{ in } N_i \} \quad .$$

For any r in R and r', r" in I_i

$$(r' - r'')m = r'm - r''m \quad \text{is in } N_i$$

$$\Longrightarrow \quad r' - r'' \quad \text{is in } I_i$$

$$(rr')m = r(r'm) \text{ is in } N_i \quad \Longrightarrow \quad rr' \text{ is in } I_i \, .$$

Hence, $I_1 \subset I_2 \subset \ldots$ is an ascending chain of left ideals in R such that for each i, $N_i = I_i m$. By hypothesis the chain of left ideals terminates. That is, there exists an integer k such that $I_h = I_{h+1}$ for all $h \geq k$

$\Longrightarrow$ $N_i = I_k m$ for all $i \geq k$

$\Longrightarrow$ the given chain of submodules of Rm also terminates.

A similar procedure is valid when R is Artinian.

CHAPTER IV - COMPOSITION SERIES

Given an R-Module M, then M is simple or irreducible if it has exactly two submodules — namely, itself and (0). A normal series in M is a descending finite chain of submodules

$$M = N_0 \supset N_1 \supset \ . \ . \ . \ \supset N_r = (0) \ ,$$

where the inclusions need not be proper. If all inclusions are proper, then the normal series is said to be without repetitions. A proper refinement of a given normal series is a normal series resulting from the insertion of additional terms in the given series. A composition series of M is a normal series without repetitions, every proper refinement of which has repetitions. The length of a normal series is the integer r as above.

Note that the ring of integers, when considered as a module over itself, has no composition series, while it does have normal series.

Theorem 1: (Jordan) If an R-module M has one composition series of length r, then

A) every composition series of M has length r

B) every normal series of M without repetitions can be refined to a composition series .

Proof: To demonstrate the first part, we proceed by induction on r. The case of $r = 0$ is trivial, since $M = (0)$.

Any module M with r = 1 is irreducible, having

$$M = M_0 \supset M_1 = (0)$$

as its only composition series.

Now suppose that, in every module having one composition series of length < r, each such series has the same length. Let M be a module having composition series

i. $$M = M_0 \supset M_1 \supset \ldots \supset M_r = (0).$$

Then M can have no composition series of length < r, for, by the induction hypotheses, all composition series of M would have the same length, contrary to our assumption. Thus, we must show that M can have no composition series of length > r. If

ii. $$M = M_0 \supset M_1' \supset M_2' \ldots \supset M_s = (0)$$

is a normal series without repetitions, it will suffice to prove that $s \leq r$. Three cases need be considered.

Case I: $M_1' = M_1$. Then

series i. ==> M_1 has a composition series of length (r - 1)

series ii. ==> M_1' has a normal series without repetitions of length (s - 1), and

the inductive hypothesis ==> $(s-1) \leq (r-1)$, or $s \leq r$.

Case II: $M_1' \subset M_1$. Then

$$M_1 \supset M_1' \supset M_2' \supset \ldots \supset M_s = (0)$$

is a normal series of M_1 without repetitions of length s. Again, the induction hypothesis implies $s \leq r-1$, or $s < r$.

Case III: $M_1' \not\subset M_1$. First note once again the implications in Case I. Now $M_1 \not\subset M_1'$, for i. is a composition series, so there are no submodules between M and M_1. But, since

$M_1' \not\subset M_1$, then $(M_1 + M_1')$ is a submodule of M containing properly both M_1 and M_1'

==> $$M_1 + M_1' = M .$$

Consider M/M_1, which is a simple module. By the second Isomorphism Theorem we have

$$M/M_1 = (M_1 + M_1')/M_1 \cong_R M_1'/(M_1 \cap M_1')$$

==> $M_1'/(M_1 \cap M_1')$ is simple

==> there exist no submodules of M between M_1' and $M_1 \cap M_1'$.

Now form the series

iii. $$M = M_1 + M_1' \supset M_1 \supset M_1 \cap M_1'$$

iv. $$M = M_1 + M_1' \supset M_1' \supset M_1 \cap M_1' .$$

Since M_1 has a composition series of length (r-1) and, from iii. $M_1 \cap M_1' \subset M_1$, then $M_1 \cap M_1'$ has a composition series of length at most (r-2). However, from iv. $M_1 \cap M_1' \subset M_1'$, and we know that there exist no submodules of M between these two

==> M_1' has a composition series of length at most (r-1).

Hence, by the induction hypothesis, every composition series of M_1' has length at most (r-1)

==> $$(s-1) \leq (r-1), \text{ or } s \leq r .$$

This completes the proof of part A) of the theorem.

In the course of the above proof we have shown that each normal series of M without repetitions has length at most equal to the length of a composition series of M, all of which have the same length. This suffices to demonstrate part B).

In light of the preceding theorem we say that an R-module M has <u>length r</u>, denoted $l(M) = r$, if the common length of its composition series is r. If M has no composition series, we say $l(M)$ is infinite.

Theorem 2: If N is a submodule of R-module M, then

$$l(M) = l(N) + l(M/N) .$$

Proof: Assume $l(N)$ and $l(M/N)$ to be finite, and let

i. $$N = N_0 \supset N_1 \supset \ . \ . \ . \supset N_r = (0)$$

be a composition series of N. It follows from the first Isomorphism Theorem that every submodule of M/N has the form L/N, where L is a submodule of M containing N. Hence, let

ii. $$M/N = L_0/N \supset L_1/N \supset . \ . \ . \supset L_s/N = (0)$$

be a composition series of M/N, so that

iii. $$M = L_0 \supset L_1 \supset . \ . \ . \supset L_s = N$$

is a series that cannot be properly refined.

Combining i. and iii. yields

iv. $$M = L_0 \supset . \ . \ \supset L_s = N = N_0 \supset N_1 \supset . \ . \supset N_r = (0)$$

which is a composition series of M of length (r+s). Thus

$$l(M) = r + s = l(N) + l(M/N) .$$

Remark: In case either $l(N)$ or $l(M/N)$ is infinite, a slight modification of the proof yields the same result. Namely, take series i. and ii. to be finite normal series without repetitions of N and M/N respectively. Then either r or s can be made arbitrarily large, so that iv. becomes a normal series of M without repetitions of arbitrarily large length.

<u>Theorem 3</u>: An R-module M has a composition series if and only if M is both Noetherian and Artinian.

<u>Proof</u>: The implication to the right is clear; for if M has a composition series of length r, then every strictly ascending or descending chain of submodules of M has at most (r+1) elements.

Conversely, let M satisfy both chain conditions. If M = (0), the conclusion is trivial. If M $\neq$ (0), form the set

$$\mathfrak{m}_0 = \{ N \mid N \subset M \text{ a proper submodule of } M \}.$$

Choose M_1 in $\mathfrak{m}_0$ to be maximal; that is, such that there exists no element of $\mathfrak{m}_0$ which contains M_1. The existence of such an element M_1 is guaranteed by the ascending chain condition. If $M_1 = (0)$, then $\mathfrak{m}_0 = (0)$ and

$$M = M_0 \supset M_1 = (0)$$

is a composition series of M of lenght one. If $M_1 \neq (0)$, repeat the process, choosing M_2 to be maximal of the set

$$\mathfrak{m}_1 = \{ N \mid N \subset M_1 \text{ a proper submodule of } M_1 \}.$$

Continuing this procedure yields a strictly descending chain

$$M = M_0 \supset M_1 \supset M_2 \supset \ldots$$

which, by choice of M_i, cannot be properly refined. However, since the descending chain condition holds in M, then this chain must terminate. Hence, for some integer k, we have $M_k = (0)$ and

$$M = M_0 \supset \ldots \supset M_k = (0)$$

is the desired composition series.

In order to state more simply the concluding theorem of this section, which gives a relationship between the composition series of a given module, we introduce addition- terminology and definitions.

If $$M = M_0 \supset M_1 \supset \ldots \supset M_r = (0)$$

is a normal series of M, then the quotient modules

$$M_0/M_1, \ldots, M_{r-1}/M_r$$

are normal differences of the series. In case the given series is a composition series, these modules are called composition differences. If N is an R-submodule of M, then

$$M = M_0 \supset M_1 \supset \ldots \supset M_k = N$$

is a composition series between M and N if there are no repetitions and every proper refinement has repetitions. (Here, a proper refinement of such a series is defined as before.) Finally, we say two composition series are equivalent if there exists a pairing of composition differences such that each pairing is an R-isomorphism.

Theorem 4: If an R-module M has a composition series, then any two composition series are equivalent.

Proof: Again, we proceed by induction on the length of M. The $r = o$ case is trivial. If $r = 1$, then M is simple, and any two composition series are identical, hence equivalent.

Assume the induction hypothesis for all modules of length $< r$. Let

i. $$M = M_0 \supset M_1 \supset \ldots \supset M_r = (0)$$ and

ii. $$M = M_0 \supset M_1' \supset \ldots \supset M_r' = (0)$$

be any two composition series of M. Two cases need be considered.

Case I: $M_1 = M_1'$. Then i. and ii. afford two composition series of M_1 of length (r-1)

==> by hypothesis that these two composition series are equivalent; that is,

$$M_1/M_2 \cong_R M_1'/M_2' , \ . \ . \ . \ . \ , M_{r-1}/M_r \cong_R M_{r-1}'/M_r' .$$

But, in addition, $M_0/M_1 = M_0/M_1'$

==> the series i. and ii. are equivalent.

Case II: $M_1 \neq M_1'$. From before, $M_1 + M_1'$ is a submodule of M containing properly both M_1 and M_1'

==> $$M = M_1 + M_1' .$$

Now M/M_1 and M/M_1' are simple, and

$$M/M_1 = (M_1 + M_1')/M_1 \cong_R M_1'/(M_1 \cap M_1')$$
$$M/M_1' = (M_1 + M_1')/M_1' \cong_R M_1/(M_1 \cap M_1')$$

==> modules $M_1'/(M_1 \cap M_1')$ and $M_1/(M_1 \cap M_1')$ are both simple

==> iii. $M = M_1 + M_1' \supset M_1 \supset M_1 \cap M_1'$ and

iv. $M = M_1 + M_1' \supset M_1' \supset M_1 \cap M_1'$

are both composition series between M and $M_1 \cap M_1'$

==> from the isomorphisms above that iii. and iv. are equivalent.

However, i. and iii. each afford composition series of M_1 of length (r-1)

==> by the induction hypothesis that these two are equivalent.

In addition, $M_0/M_1 = M/M_1 = (M_1 + M_1')/M_1$.

==> the composition series of M afforded by i. and iii. are equivalent.

Similarly, the composition series of M afforded by ii. and iv. are equivalent. But, iii. and iv. have been shown to be equivalent, hence i. and ii. are likewise.

CHAPTER V - DIRECT SUMS

Submodules $\{ N_\alpha \mid \alpha \text{ in index set } A \}$ of R-module M are <u>independent</u> if the intersection of any one submodule with the sum of the others contains only the zero element. Or, equivalently, these submodules are independent if and only if $\sum_{\alpha \text{ in } A} n_\alpha = 0$, where n_α is in N_α, implies that $n_\alpha = 0$ for all α in A. If, in addition to being independent, the submodules are such that

$$M = \sum_{\alpha \text{ in } A} N_\alpha$$

then we say M is the <u>direct sum</u> of the given submodules, and is denoted by

$$M = \bigoplus_{\alpha \text{ in } A} N_\alpha .$$

We shall be primarily concerned with finite direct sums.

<u>Theorem 1</u>: $M = \bigoplus_{i=1}^{r} N_i$ if and only if each m in M can be written uniquely as $m = n_1 + \ldots + n_r$, where n_i is in N_i for $i = 1, \ldots, r$.

<u>Proof</u>: M a direct sum as given

$\Longrightarrow$ $m = n_1 + \ldots + n_r$ for some n_i in N_i.

Suppose there exist n_i' in N_i such that $m = n_1' + \ldots + n_r'$.

Then $m - m = (n_1 - n_1') + \ldots + (n_r - n_r') = 0$ where $(n_i - n_i')$ in N_i

$\Longrightarrow$ $(n_i - n_i') = 0$, or $n_i = n_i'$ by the independence of the N_i.

Conversely, for each m in M $m = n_1 + \ldots + n_r$, n_i in N_i

$\Longrightarrow$ $M = N_1 + \ldots + N_r$.

Also, since 0 is in M, and this representation is unique,

then $$0 = n_1 + \ldots + n_r$$

$\Longrightarrow$ $n_i = 0$ for each i

$\Longrightarrow$ the N_i are independent.

The following theorem, the Modular Law for Direct Sums, has a proof similar to that of the Dedekind Modular Law, and hence only its statement will be given here.

<u>Theorem 2</u>: If K, L, N are submodules of an R-module M such that $L \subset K$, then

$$K \cap (L \oplus N) = L \oplus (K \cap N)$$

whenever either of these direct sums make sense.

<u>Theorem 3</u>: If $M = N_1 \oplus N_2$, then

A) $N_1 \cong_R M/N_2$ and $N_2 \cong_R M/N_1$

B) $l(M) = l(N_1) + l(N_2)$.

<u>Proof</u>:

A) Since M is the direct sum of N_1 and N_2, then $M = N_1 + N_2$ and $N_1 \cap N_2 = (0)$. By the second Isomorphism Theorem

$$(N_1 + N_2)/N_1 \cong_R N_2/(N_1 \cap N_2)$$

$\Longrightarrow$ $$M/N_1 \cong_R N_2$$

and similarly $$M/N_2 \cong_R N_1 .$$

B) By Theorem 2 (IV)

$$l(M) = l(N_1) + l(M/N_1) = l(N_1) + l(N_2) .$$

Remark: In the case $M = N_1 \oplus \ldots \oplus N_t$, this theorem may be generalized by induction to read

A) $N_i \cong_R M/(N_1 + \ldots + N_{i-1} + N_{i+1} + \ldots + N_t)$

B) $l(M) = l(N_1) + \ldots + l(N_t)$.

Theorem 4: If $N_1, \ldots, N_t$ and $N'_1, \ldots, N'_t$ are submodules of R-modules M and M' respectively such that

$$M = N_1 \oplus \ldots \oplus N_t \quad , \quad M' = N'_1 \oplus \ldots \oplus N'_t$$

and $N_i \cong_R N'_i$ for $i = 1, \ldots, t$,

then $M \cong_R M'$.

Proof: Let $f_i : N_i \longrightarrow N'_i$ be the given isomorphisms, and define $f: M \longrightarrow M'$ by $f(m) = f_1(n_1) + \ldots + f_t(n_t)$, where $m = n_1 + \ldots + n_t$ and n_i is in N_i. That f is an R-isomorphism follows from each f_i being such.

A) f is well-defined

If $m = m^*$ is in M, then

$m = n_1 + \ldots + n_t$ and $m^* = n_1^* + \ldots + n_t^*$; n_i, n_i^* in N_i

$\Longrightarrow$ $n_i = n_i^*$ for $i = 1, \ldots, t$ by the uniqueness of representation of elements of M

$\Longrightarrow$ $f(m) = f(m^*)$

B) f is an R-homomorphism

For any m and m* in M, and r in R

$$\begin{aligned} f(m + m^*) &= f[(n_1 + \ldots + n_t) + (n_1^* + \ldots + n_t^*)] \\ &= f[(n_1 + n_1^*) + \ldots + (n_t + n_t^*)] \\ &= f_1(n_1 + n_1^*) + \ldots + f_t(n_t + n_t^*) \\ &= f_1(n_1) + f_1(n_1^*) + \ldots + f_t(n_t) + f_t(n_t^*) \\ &= [f_1(n_1) + \ldots + f_t(n_t)] + [f_1(n_1^*) + \ldots + f_t(n_t^*)] \\ &= f(n_1 + \ldots + n_t) + f(n_1^* + \ldots + n_t^*) \\ &= f(m) + f(m^*) \end{aligned}$$

$$f(rm) = f[r(n_1 + \ldots + n_t)] = f(rn_1 + \ldots + rn_t)$$
$$= f_1(rn_1) + \ldots + f_t(rn_t) = rf_1(n_1) + \ldots + rf_t(n_t)$$
$$= r[f(n_1 + \ldots + n_t)] = rf(m)$$

C) f is one-to-one

Let m be in M such that $f(m) = 0$. Then $f_1(n_1) + \ldots + f_t(n_t) = 0$

$\Longrightarrow$ $f_i(n_i) = 0$ for each i by the independence of the N_i

$\Longrightarrow$ $n_i = 0$ since each f_i is one-to-one

$\Longrightarrow$ $m = n_1 + \ldots + n_t = 0$

$\Longrightarrow$ $\ker f = (0)$

D) f is onto

For any m' in M' there exist n_i' in N_i' such that

$$m' = n_1' + \ldots + n_t'$$

and since each f_i is onto, then for each n_i' in N_i' there exists an n_i in N_i such that $f_i(n_i) = n_i'$. Hence, by definition of f

$$m' = f_1(n_1) + \ldots + f_t(n_t) = f(m)$$

where $m = n_1 + \ldots + n_t$ in M.

<u>Theorem 5</u>: If M is an R-module such that $M = \bigoplus_{i=1}^{t} N_i$ and $L_1, \ldots, L_t$ are submodules of $N_1, \ldots, N_t$ respectively, then $L = L_1 + \ldots + L_t$ is a direct sum, and M/L is a direct sum of submodules R-isomorphic to

$$N_1/L_1, \ldots, N_t/L_t .$$

<u>Proof</u>: Since the N_i are independent and each $L_i \subset N_i$, then the L_i are independent and $L = L_1 \oplus \ldots \oplus L_t$.

Let $\varphi: M \longrightarrow M/L$ be the natural homomorphism. Then $M/L = \varphi(M) = \varphi(N_1 + \ldots + N_t)$ or $M/L = \varphi(N_1) + \ldots + \varphi(N_t)$.

We claim that this sum is direct, and that $\varphi(N_i) \cong_R N_i/L_i$.

For, suppose $\varphi(n_1)+ . . +\varphi(n_t) = 0$ where n_i is in N_i. Then, $\varphi(n_1 + . . + n_t) = 0$ where $n_1+ . . +n_t$ is in M

==> $n_1 + . . + n_t$ belongs to L . But 1 in L

==> $1 = 1_1 + . . + 1_t$ where 1_i is in L_i

==> n_i belongs to $L_i \subset L$ for each i

==> $\varphi(n_i) = 0$ for each i.

Thus, the $\varphi(N_i)$ are independent and

$$M/L = \varphi(N_1) \oplus . . \oplus \varphi(N_t) .$$

Also, by the Fundamental Theorem, $\varphi(N_i) \cong_R N_i/\ker\varphi$. But $\ker\varphi$ when restricted to N_i is exactly L_i, since $N_i \cap L = L_i$. Hence, the desired conclusion

$$\varphi(N_i) \cong_R N_i/L_i .$$

An R-module M is said to be <u>completely reducible</u> if for every submodule $N \subset M$ there exists a submodule $N' \subset M$ such that $M = N \oplus N'$. It is well known that every vector space over a field F is completely reducible F-module, whereas the ring of integers considered as a Z-module is not completely reducible.

<u>Theorem 6</u>: If N_1 and N_2 are both complements of a submodule N of an R-module M (that is, $M = N \oplus N_1 = N \oplus N_2$) such that $N_1 \subset N_2$, then $N_1 = N_2$.

<u>Proof</u>:

$$\begin{aligned} N_2 &= N_2 \cap (N_1 + N) \\ &= N_1 + (N_2 \cap N) \quad \text{by the Modular Law} \\ &= N_1 + (0) = N_1 . \end{aligned}$$

<u>Theorem 7</u>: If M is a completely reducible R-module, then

A) every submodule of M is completely reducible

B) M is Noetherian if and only if M is Artinian .

<u>Proof</u>:

A) Let N be an arbitrary submodule of M, $L \subset N$ an arbitrary submodule of N, and $L' \subset M$ such that $L \oplus L' = M$. Then

$$N = N \cap M = N \cap (L \oplus L') = L \oplus (N \cap L')$$

so that $(N \cap L')$ is the complement of L in N.

B) Assume that the A.C.C. holds in M, and let

$$M \supset N_1 \supset N_2 \supset \ldots$$

be a descending chain of submodules. We claim that if $L \subset K$ are submodules of M, then every complement of K is contained in a complement of L, and every complement of L contains a complement of K.

For the former, let K' be a complement of K in M and L' a complement of L in K. Then

$$M = K \oplus K' \qquad \text{and} \qquad K = L \oplus L'$$

$$\Longrightarrow \qquad M = L \oplus L' \oplus K'$$

$\Longrightarrow$ $K' \subset L' \oplus K'$, where $L' \oplus K'$ is a complement of L in M.

For the latter, let L' and K' be arbitrary complements of L in M and $K \cap L'$ in L' respectively. Then

$$M = L \oplus L' \qquad \text{and} \qquad L' = (K \cap L') \oplus K' .$$

Noting that $K' \subset L'$ we have

$$M = L \oplus L' = L \oplus (K \cap L') \oplus K' = L \oplus K' \oplus (L' \cap K)$$
$$= L \oplus L' \cap (K' \oplus K) = M \cap (K' \oplus K)$$

$\Longrightarrow$ $M = K' \oplus K$

$\Longrightarrow$ $K' \subset L'$, where K' is a complement of K in M.

Returning to the given descending chain, let N_1' be an arbitrary complement of N_1 in M. Choose complement N_2' of N_2 such that $N_1' \subset N_2'$, and complement N_3' of N_3 such that $N_2' \subset N_3'$, etc. Then we have an ascending chain

$$(0) \subset N_1' \subset N_2' \subset \ . \ . \ .$$

which by hypotheses terminates

==> for some t, $N_t' = M$ ==> $N_t = (0)$

==> the given descending chain terminates .

A similar proof is applicable when M satisfies the D.C.C.

Remark: It should be noted here that, in light of Theorem 3 (IV), any completely reducible R-module which satisfies either chain condition has a composition series and hence finite length.

<u>Theorem 8</u>: An R-module M is completely reducible and of finite length 1(M) if and only if M is the direct sum of 1(M) simple submodules of M, each unique to R-isomorphism.

<u>Proof</u>: Let M be completely reducible and 1(M) = t, so that both chain conditions hold in M. Let N be an arbitrary submodule of M and $N' \subset M$ such that $N \oplus N' = M$. We claim that every submodule of M is the direct sum of a finite number of simple submodules. For, suppose the contrary, letting $\mathcal{X}$ be the set of all submodules of M such that each element of this set is not a direct sum of simple submodules of M. Since the D.C.C. holds for $\mathcal{X}$, choose a minimal K* in $\mathcal{X}$. That is, K* contains no other element of $\mathcal{X}$. Since

$K^* \neq (0)$ and is not simple, there exists an $L \subset K^*$ such that $(0) \subset L \subset K^*$. Now M completely reducible

$\Longrightarrow$ K^* completely reducible

$\Longrightarrow$ there exists an $L' \subset K^*$ such that $L \oplus L' = K^*$.

But $L, L' \subset K^*$ and K^* minimal in $\mathcal{K}$ $\Longrightarrow$ L, L' not in $\mathcal{K}$

$\Longrightarrow$ both L and L' are direct sums of simple submodules of M, and $K^* = L \oplus L'$

$\Longrightarrow$ K^* is likewise. Contradiction; hence, $M = N \oplus N'$ is the direct sum of a finite number of simple submodules of M, say

$$M = N_1 \oplus \ldots \oplus N_s .$$

In this case, the normal series

$$M = N_1 \oplus \ldots \oplus N_s \supset N_2 \oplus \ldots \oplus N_s \supset \ldots \supset N_{s-1} \oplus N_s \supset N_s \supset (0)$$

is a composition series, so $l(M) = t$ implies $s = t$.

Also, in this series

$$(N_k \oplus \ldots \oplus N_t)/(N_{k+1} \oplus \ldots \oplus N_t) \cong_R N_k$$

for $k = 1, \ldots, t$, where these composition differences are uniquely determined up to R-isomorphism by Theorem 4 (IV).

Conversely, suppose M is the direct sum of t simple submodules $N_1, \ldots, N_t$. Then $l(N_i) = 1$ for $i = 1, \ldots, t$ and, by Theorem 3 (V),

$$l(M) = l(N_1) + \ldots + l(N_t) = t .$$

To exhibit the complete reducibility of M, let N be an arbitrary proper submodule of M. Then choose N_{i_1} to be the first element of the set

$$N_1, N_2, \ldots, N_t$$

which is not contained in N. Clearly, since $N \neq M$, there must exist such an N_{i_1}. Now, N_{i_1} being simple $\Longrightarrow$ $N \cap N_{i_1} = (0)$ $\Longrightarrow$ $N + N_{i_1}$ is a direct sum.

If $M = N \oplus N_{i_1}$, then we have exhibited a complement of N. If not, let N_{i_2} be the first element of the same set which is not contained in $N \oplus N_{i_1}$. Then, as before, $(N \oplus N_{i_1}) + N_{i_2}$ is a direct sum.

Repeating this procedure, which must terminate in at most t steps, we finally arrive at

$$M = N \oplus N_{i_1} \oplus \cdots \oplus N_{i_s} \quad \text{where} \quad 1 \leq s \leq t.$$

An R-module M is <u>indecomposable</u> if it is not the direct sum of two proper submodules. For example, the ring of integers is indecomposable when considered as a module over itself. Any non-trivial module which is both completely reducible and indecomposable is necessarily simple.

<u>Theorem 9</u>: Every Artinian R-module M is the direct sum of a finite number of indecomposable submodules.

<u>Proof</u>: It sufficed to prove that every submodule of M, of which M is one, is the direct sum of a finite number of indecomposable submodules of M.

So, proceeding as in the foregoing proof, suppose the contrary, letting $\mathcal{X}$ be the set of all those submodules of M which are not the direct sum of a finite number of indecomposable submodules of M. Choosing K* minimal in $\mathcal{X}$, then $K^* \neq (0)$ since (0) is not in $\mathcal{X}$. (Note that, as defined,

(0) is indecomposable.) Also, K* not being the direct sum of indecomposable submodules, and $K^* = K^* + (0)$

$\Longrightarrow$ K* is not indecomposable

$\Longrightarrow$ $K^* = L \oplus L'$ for some $L, L' \subset K^*$.

But the minimality of K* $\Longrightarrow$ L, L' are not in $\mathcal{K}$

$\Longrightarrow$ L, L' are direct sums of indecomposable submodules

$\Longrightarrow$ K* is likewise. Q.E.D.

<u>Theorem 10</u>: If $M_1, \ldots, M_t$ are R-modules, then there exists an R-module M, uniquely determined to R-isomorphism, such that

$$M = M_1' \oplus \ldots \oplus M_t'$$

where $M_i \cong_R M_i'$ for $i = 1, \ldots, t$.

<u>Proof</u>: Define an R-module (M, +) by

$$M = \{ (m_1, \ldots, m_t) \mid m_i \text{ in } M_i \}$$

$$(m_1, \ldots, m_t) + (m_1^*, \ldots, m_t^*) = (m_1 + m_1^*, \ldots, m_t + m_t^*)$$

$$r(m_1, \ldots, m_t) = (rm_1, \ldots, rm_t) .$$

Let submodules M_i' be given by

$$M_i' = \{ (0, \ldots, m_i, \ldots, 0) \mid m_i \text{ in } M_i \} .$$

Then, certainly

$$M = M_1' \oplus \ldots \oplus M_t'$$

and $f: M_i \longrightarrow M_i'$ defined by

$$f(m_i) = (0, \ldots, m_i, \ldots, 0)$$

is an R-isomorphism.

That M is unique to R-isomorphism follows from Theorem 4 (V).

CHAPTER VI - TENSOR PRODUCTS

For the sake of generality we shall now consider left and right R-modules, denoted ${}_RN$ and M_R respectively. Two definitions precede the first theorem.

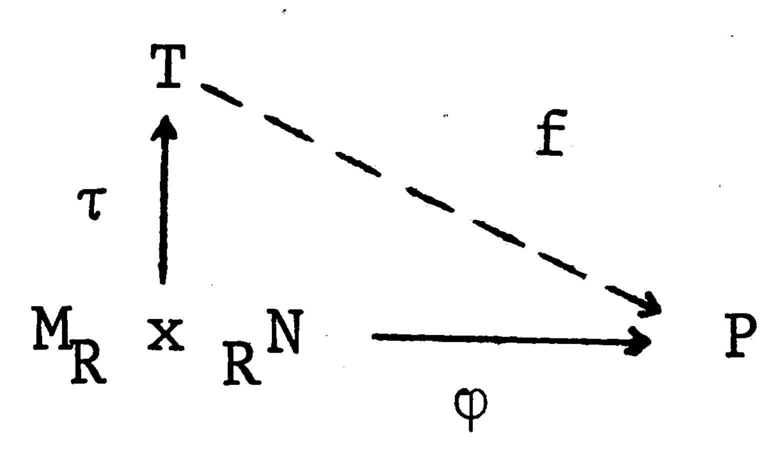
If P is a Z-module (that is, an additive abelian group) and M_R, ${}_RN$ are R-modules, then a map $\varphi: M_R \times {}_RN \longrightarrow P$ is called *R-bilinear* if for all m, m' in M_R, n, n' in ${}_RN$, and r in R

$$\varphi(m + m', n) = \varphi(m, n) + \varphi(m', n)$$

$$\varphi(m, n + n') = \varphi(m, n) + \varphi(m, n')$$

$$\varphi(mr, n) = \varphi(m, rn) ,$$

where $M_R \times {}_RN$ is the familiar Cartesian product of sets. If P, T are Z-modules and $\tau: M_R \times {}_RN \longrightarrow T$ is an R-bilinear map, then an R-bilinear map $\varphi: M_R \times {}_RN \longrightarrow P$ can be *factored through τ* (or, if no confusion can occur, *through T*) if there exists a homomorphism $f: T \longrightarrow P$ such that $f(\tau(m, n)) = \varphi(m, n)$ for all m in M_R and n in ${}_RN$. That is, if there exists an f such that



commutes.

<u>Theorem 1</u>: Given M_R, $_RN$ as before, then there exists a unique Z-module T and a corresponding R-bilinear map

$$\tau: M \times N \longrightarrow T$$

such that

A) any element of T can be written in the form

$$\sum \tau(m_i, n_i) \qquad \text{where } m_i \text{ is in } M_R, \text{ and } n_i \text{ in } {}_RN$$

B) every R-bilinear map $\varphi: M \times N \longrightarrow P$ into any Z-module P can be factored through T.

<u>Proof</u>: If X is a set, by the free abelian group F on X we mean the set of all integral-valued functions on X which are zero except at a finite number of elements of X. That is,

$$F = \{ f: X \longrightarrow Z \mid f(x) \neq 0 \text{ for only finitely many } x \text{ in } X \}.$$

Defining the operation

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$

for all f_1, f_2 in F, then (F, +) becomes an abelian group. In light of this definition it is natural to represent each element of F by a finite formal sum

$$\sum_{x_i \text{ in } X} f(x_i)\, x_i$$

where only finitely many of the integral coefficients $f(x_i)$ are non-zero. Hence, we may alternately represent F by

$$F = \left\{ \sum_{x \text{ in } X} k_x\, x \;\middle|\; k_x \text{ in } Z,\ x \text{ in } X, \text{ sum finite} \right\}.$$

Now, let F be the free abelian group on M x N (that is,

$$F = \left\{ \sum_{(m,n) \text{ in } M \times N} k_{m,n}(m,n) \;\middle|\; k_{m,n} \text{ in } Z;\ m \text{ in } M,\ n \text{ in } N; \text{ sum finite} \right\})$$

and let H be the subgroup of F generated by all elements of the forms

$$(m + m', n) - (m, n) - (m', n)$$

i. $$(m, n + n') - (m, n) - (m, n')$$

$$(mr, n) - (m, rn) .$$

Define $T = F/H$ and map $\tau: M \times N \longrightarrow T$ by

$$\tau(m, n) = (m, n) + H .$$

Then certainly T is a Z-module, and it is easily verified that τ is R-bilinear. Note that by construction the elements of T are equivalence classes, and for any m and m', n and n', r in M, N, R respectively, the elements given in i. all belong to the same equivalence class, namely H.

Since a general element of T is a finite sum of the form

$$\sum k_g(m, n) \quad + \quad H$$

it follows that every element can be written as

$$\sum \tau(m_i, n_i)$$

where the m_i are in M and n_i in N. As for the uniqueness of T, suppose there exist a Z-module T' and an R-bilinear map τ' such that any element of T' can be written in the corresponding form. Then, defining Z-homomorphisms

$f: T' \longrightarrow T$ and $g: T \longrightarrow T'$

by $f(\tau'(m, n)) = \tau(m, n)$ and

$g(\tau(m, n)) = \tau'(m, n)$ we see that

$gf = 1_{T'}$, the identity on T'

and $fg = 1_T$, the identity on T .

Thus, T is uniquely determined up to Z-isomorphism.

Given an R-bilinear map $\varphi: M \times N \longrightarrow P$ we may define a Z-homomorphism $f: T \longrightarrow P$ by

$$f((m, n) + H) = \varphi(m, n) .$$

Then $f(\tau(m, n)) = \varphi(m, n)$ for all m in M, n in N and φ can be factored through T. Moreover, for a given φ the Z-homomorphism f as defined is unique since, for an arbitrary element of T,

$$f(\sum \tau(m, n)) = \sum f\tau(m, n) = \sum \varphi(m, n). \qquad \text{Q.E.D.}$$

The Z-module T constructed above is called the <u>tensor product</u> of the R-modules M_R and $_RN$ and is usually written as $T = M \otimes_R N$. The element $\tau(m, n)$ in T is denoted by $m \otimes n$. As a consequence of this theorem we state the Universal Mapping Property of tensor products:

A unique Z-homomorphism $f: M \otimes_R N \longrightarrow G$ is completely determined if $\varphi: M \times N \longrightarrow G$ is prescribed for all m in M and n in N in such a way that φ is R-bilinear in M and N.

This formulation illuminates the correspondence between bilinear and linear maps which is of importance in the study of homological algebra. Before proceeding with the next theorem, several observations will be made.

Given R-modules M_R, M'_R, $_RN$, $_RN'$ and R-homomorphisms

$$f: M \longrightarrow M' \quad \text{and} \quad g: N \longrightarrow N'$$

then it is easily verified that the map $\varphi: M \times N \longrightarrow M' \otimes N'$

defined by $\varphi(m, n) = f(m) \otimes g(n)$ is R-bilinear. Moreover, there exists a unique Z-homomorphism

$$f \otimes g : M \otimes N \longrightarrow M' \otimes N'$$

such that

$$\begin{array}{ccc} M \times N & \xrightarrow{f \times g} & M' \times N' \\ \tau \downarrow & \searrow^{\varphi} & \downarrow \tau' \\ M \otimes N & \xrightarrow{f \otimes g} & M' \otimes N' \end{array}$$

commutes: namely, the Z-homomorphism

$$(f \otimes g)\left(\sum m_i \otimes n_i\right) = \sum f(m_i) \otimes g(n_i) .$$

If, in addition, we are given R-homomorphisms

$$f' : M' \longrightarrow M'' \quad \text{and} \quad g' : N' \longrightarrow N''$$

then again there exists a unique Z-homomorphism

$$(f' \otimes g')(f \otimes g) : M \otimes N \longrightarrow M'' \otimes N''$$

such that

$$\begin{array}{ccc} M \times N & \xrightarrow{(f' \times g')(f \times g)} & M'' \times N'' \\ \tau \downarrow & & \downarrow \tau' \\ M \otimes N & \xrightarrow{(f' \otimes g')(f \otimes g)} & M'' \otimes N'' \end{array}$$

commutes. This map is defined by

$$(f' \otimes g')(f \otimes g)(m \otimes n) = (f'f(m) \otimes g'g(n)) .$$

Given an R-module ${}_RN$ and a PR-bimodule ${}_PM_R$, where $p(mr) = (pm)r$ for all p in P, m in M and r in R; then $M \otimes_R N$ becomes a left P-module. Also, if we consider R to be a bimodule ${}_RR_R$, then

$$R \otimes_R N \cong_R N .$$

(The proof lies in demonstrating that the map $f : R \otimes_R N \longrightarrow N$

given by $f(r \otimes n) = rn$ is an R-isomorphism.)

Similarly, for M_R

$$M \otimes_R R \cong_R M,$$

as right R-modules.

We now pose a question. Given M_R and $_RN$, does submodule $M'_R \subset M_R$ imply that $M' \otimes_R N \subset M \otimes_R N$? Or, equivalently, does exact sequence

$$0 \longrightarrow M' \longrightarrow M$$

$$\Longrightarrow \quad 0 \longrightarrow M' \otimes_R N \longrightarrow M \otimes_R N \quad \text{also exact?}$$

(Recall that a sequence of module R-homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \longrightarrow \cdots$$

is <u>exact</u> if kernel φ_i = image φ_{i-1} for all i.)

The answer is no. By counterexample, let

$$M' = Z \subset Q = M$$

where Q is the additive group of rationals, and $N = Z_2$.

By a preceding remark $Z \otimes_Z Z_2 \cong_Z Z_2$, whereas

$$Q \otimes_Z Z_2 = (0) ;$$

since, for any q in Q and k in Z_2

$$\begin{aligned}(q \otimes k) &= 2(1/2\, q) \otimes k = (1/2\, q) \otimes (2k) \\ &= (1/2\, q) \otimes 0 = (1/2\, q) \otimes (0 \cdot 0) \\ &= (1/2\, q)0 \otimes 0 = 0 \otimes 0 .\end{aligned}$$

However, the analogous statement about right exact sequences is valid.

<u>Theorem 2</u>: If

$$E_1: \quad M' \xrightarrow{f'} M \xrightarrow{f''} M'' \longrightarrow 0$$

is an exact sequence of right R-modules, then for any left

R-module N

$$M'\otimes_R N \xrightarrow{f'\otimes 1_N} M\otimes_R N \xrightarrow{f''\otimes 1_N} M''\otimes_R N \longrightarrow 0$$

is also exact.

<u>Proof</u>: The fact that image $f'' = M''$

$\Longrightarrow$ for any $m''\otimes n$ in $M''\otimes N$ there exists at least one m in M such that $f''(m) = m''$, so that

$$(f''\otimes 1_N)(m\otimes n) = f''(m)\otimes 1_N(n) = m''\otimes n$$

$\Longrightarrow$ image $f''\otimes 1_N = M''\otimes N$.

It remains to show that image $f'\otimes 1_N$ = kernel $f''\otimes 1_N$.

By the exactness of E_1, for any $(m'\otimes n)$ in $M'\otimes N$

$$(f''\otimes 1_N)(f'\otimes 1_N)(m\otimes n) = (f''f'(m))\otimes(1_N 1_N(n)) = 0\otimes n$$
$$= 0\cdot 0\otimes n = 0\otimes 0\cdot n = 0\otimes 0$$

$\Longrightarrow$ image $f'\otimes 1_N \subset$ kernel $f''\otimes 1_N$.

Denoting the left and right sides of this inclusion by I and K respectively, then $f'\otimes 1_N$ induces a Z-homomorphism

$$u: M\otimes N/I \longrightarrow M''\otimes N$$

defined by $u(m\otimes n + I) = f''(m)\otimes n$. We already know that

$$M\otimes N/K \cong_R M''\otimes N$$

and $I \subset K$, so the equality of I and K follows if we demonstrate u to be an isomorphism. This shall be done by constructing an inverse.

Define $\varphi: M''\times N \longrightarrow M\otimes N/I$ by $\varphi(m'', n) = m\otimes n + I$, the coset of $m\otimes n$ in $M\otimes N/I$, where m is in M and $f''(m) = m''$. There is at least one such m by the exactness of E_1. Suppose m, m^* are in M such that $m \neq m^*$ and $f''(m) = f''(m^*)$. Then

$f''(m - m^*) = 0 \implies m - m^*$ belongs to $\ker f'' = \operatorname{im} f'$

$\implies$ there exists an m' in M' such that $f'(m') = m - m^*$.

Hence, $m = m^* + f'(m')$ and

$$
\begin{aligned}
m \otimes n + I &= [m^* + f'(m')] \otimes n + I \\
&= (m^* \otimes n) + [f'(m') \otimes n] + I \\
&= (m^* \otimes n) + [(f' \otimes 1_N)(m' \otimes n)] + I \\
&= (m^* \otimes n) + I \qquad \text{since } I = \text{image } (f' \otimes 1_N)
\end{aligned}
$$

$\implies \varphi$ is independent of the choice of $f''^{-1}(m'')$ in M, and hence is well-defined.

Again the R-bilinearity of φ is easily checked. Thus, by the Universal Mapping Property there exists a Z-homomorphism

$$v: M'' \otimes N \longrightarrow M \otimes N/I$$

such that $\quad v(m'' \otimes n) = \varphi(m'', n) = m \otimes n + I$

for all m'' in M'' and n in N.

We have, then, Z-homomorphisms u and v such that

$uv(m'' \otimes n) = u(m \otimes n + I) = f''(m) \otimes n = m'' \otimes n$, and

$vu(m \otimes n + I) = v(f''(m) \otimes n) = v(m'' \otimes n) = m \otimes n + I$.

That is, $\quad uv = \text{identity on } M'' \otimes N$, and

$\quad vu = \text{identity on } M \otimes N/I$.

<u>Theorem 3</u>: The tensor product is distributive over a direct sum. That is, given right R-modules $\{ M_\alpha \mid \alpha \text{ in index set } A \}$ and left R-module ${}_R N$, then

$$\Big(\bigoplus_{\alpha \text{ in } A} M_\alpha \Big) \otimes_R N \cong_Z \bigoplus_{\alpha \text{ in } A} (M_\alpha \otimes_R N) .$$

<u>Proof</u>: Let $\Big\{ i_\beta : M_\beta \longrightarrow \bigoplus_{\alpha \text{ in } A} M_\alpha \;\Big|\; \beta \text{ in } A \Big\}$

be the projections associated with the given direct sum. That is, for any m_β in M_β

$$i_\beta(m_\beta) = (0, \ldots, m_\beta, \ldots, 0, \ldots)$$

where m_β is the βth coordinate and zeroes elsewhere. The proof rests in verifying that the map u defined by

$$u\left[\left(\sum_{\alpha \text{ in } A} i_\alpha(m_\alpha)\right) \otimes n\right] = \sum_{\alpha \text{ in } A} [(i_\alpha \otimes 1_N)(m_\alpha \otimes n)]$$

is a Z-isomorphism.

Theorem 4: If M, N are K-free modules over a commutative ring K with respective bases $\{ m_\alpha \mid \alpha \text{ in index set } A \}$ and $\{ n_\beta \mid \beta \text{ in index set } B \}$, then $M \otimes_K N$ is K-free with basis

$$\{ m_\alpha \otimes n_\beta \mid \alpha \text{ in } A, \beta \text{ in } B \} .$$

Proof: When K is commutative, then M and N are both K-bimodules, and for any k in K

$$m \otimes nk = m \otimes kn = mk \otimes n = km \otimes n ,$$

which we shall write as $k(m \otimes n)$ or $(m \otimes n)k$.

To say M and N are K-free with bases as given means both M and N are direct sums of copies of the ring. Thatis,

$$M \cong_K \bigoplus_{\alpha \text{ in } A} Km_\alpha \quad \text{where} \quad Km_\alpha \cong_K K \quad \text{for all } \alpha, \text{ and}$$

$$N \cong_K \bigoplus_{\beta \text{ in } B} Kn_\beta \quad \text{where} \quad Kn_\beta \cong_K K \quad \text{for all } \beta.$$

Hence,
$$M \otimes N \cong_K \left(\bigoplus_{\alpha \text{ in } A} Km_\alpha\right) \otimes_K N \cong_K \bigoplus_{\alpha \text{ in } A} (Km_\alpha \otimes N)$$

$$\cong_K \bigoplus_{\alpha \text{ in } A} \left[Km_\alpha \otimes_K \left(\bigoplus_{\beta \text{ in } B} Kn_\beta\right)\right]$$

$$\cong_K \bigoplus_{\alpha,\beta} (Km_\alpha \otimes_K Kn_\beta)$$

But each $Km_\alpha \otimes_K Kn_\beta \cong_K K \otimes_K Kn_\beta \cong_K Kn_\beta \cong_K K$,

so that $M \otimes_K N$ is a direct sum of copies of K. Moreover, we have that every element of $M \otimes_K N$ has the form

$$m \otimes n = \sum_{\alpha,\beta} k_\alpha m_\alpha \otimes k_\beta n_\beta = \sum_{\alpha,\beta} k_\alpha m_\alpha k_\beta \otimes n_\beta$$
$$= \sum_{\alpha,\beta} k_\alpha k_\beta m_\alpha \otimes n_\beta = \sum_{\alpha,\beta} k_{\alpha\beta}(m_\alpha \otimes n_\beta)$$

where k_α, k_β, $k_{\alpha\beta}$ are in K. Thus, the desired conclusion

$$M \otimes_K N = \bigoplus_{\alpha,\beta} K(m_\alpha \otimes n_\beta) .$$

In addition, we conclude that the dimension (or length) of the tensor product of K-free modules over a commutative ring equals the product of the dimensions of the factors.

<u>Theorem 5</u>: Associativity of the tensor product: Given rings R, S and modules M_R, ${}_R N_S$, and ${}_S P$, then

$$M \otimes_R (N \otimes_S P) \cong_Z (M \otimes_R N) \otimes_S P .$$

<u>Proof</u>: We first establish a Z-homomorphism

$$u: M \otimes (N \otimes P) \longrightarrow (M \otimes N) \otimes P .$$

Let m in M be fixed. Define $\varphi: N \times P \longrightarrow (M \otimes N) \otimes P$ by $\varphi(n, p) = (m \otimes n) \otimes p$ for all n in N and p in P.

Then
$$\varphi(n + n', p) = [m \otimes (n + n')] \otimes p$$
$$= (m \otimes n + m \otimes n') \otimes p$$
$$= (m \otimes n) \otimes p + (m \otimes n') \otimes p$$
$$= \varphi(n, p) + \varphi(n', p) ;$$

similarly $\varphi(n, p + p') = \varphi(n, p) + \varphi(n, p')$, and for any s in S

$$\varphi(ns, p) = (m \otimes ns) \otimes p = (m \otimes n)s \otimes p$$
$$= (m \otimes n) \otimes sp = \varphi(n, sp).$$

Therefore, φ is S-bilinear. By definition of the tensor product φ determines a Z-homomorphism

$$\psi_m: N \otimes_S P \longrightarrow (M \otimes_R N) \otimes_S P$$

such that $\psi_m(n \otimes p) = \varphi(n, p) = (m \otimes n) \otimes p$.

Also, for any r in R

$$\psi_m[r(n \otimes p)] = \psi_m(rn \otimes p) = (m \otimes rn) \otimes p = (mr \otimes n) \otimes p$$

so that $\psi_m[r(n \otimes p)] = (mr \otimes n) \otimes p.$

Now, define

$$\zeta: M \times (N \otimes P) \longrightarrow (M \otimes N) \otimes P$$

by $\zeta(m, x) = \psi_m(x)$ where x is in $N \otimes P$. Then for any m, m' in M; x, x' in $N \otimes P$; and r in R

$$\zeta(m, x + x') = \psi_m(x + x') = \psi_m(x) + \psi_m(x')$$
$$= \zeta(m, x) + \zeta(m, x')$$
$$\zeta(m + m', x) = \psi_{m+m'}(x) = [(m + m') \otimes n] \otimes p$$
$$= (m \otimes n) \otimes p + (m \otimes n') \otimes p$$
$$= \psi_m(x) + \psi_{m'}(x) = \zeta(m, x) + \zeta(m', x)$$
$$\zeta(mr, x) = \psi_{mr}(x) = (mr \otimes n) \otimes p = \psi_m[r(n \otimes p)]$$
$$= \psi_m(rx) = \zeta(m, rx)$$

where $x = n \otimes p$ in $N \otimes P$. Therefore, ζ is R-bilinear, and there exists a Z-homomorphism

$$u: M \otimes (N \otimes P) \longrightarrow (M \otimes N) \otimes P$$

such that

$$u[m \otimes (n \otimes p)] = \psi_m(n \otimes p) = (m \otimes n) \otimes p$$

for all m in M, n in N, and p in P.

In a similar manner one can construct a Z-homomorphism

$$v\colon (M \otimes N) \otimes P \longrightarrow M \otimes (N \otimes P)$$

which is the inverse of u.

To conclude this section we shall consider free modules of finite basis over a field F (that is, finite dimensional vector spaces) and develop the notion of a tensor as used in differential geometry.

If M is a free module of length n over a field F, then the <u>dual space</u> M* of M is the set of all linear maps

$$\varphi\colon M \longrightarrow F \quad ;$$

or, for all m_i in M and f_i in F

$$M^* = \left\{ \varphi\colon M \longrightarrow F \;\middle|\; \varphi(f_1 m_1 + f_2 m_2) = f_1 \varphi(m_1) + f_2 \varphi(m_2) \right\} .$$

It follows rather directly that M*, with defined operation

$$(\varphi_1 + \varphi_2)(m) = \varphi_1(m) + \varphi_2(m)$$

becomes a vector space over F. In fact, since any element of M* is completely determined by its action on the basis elements of M, then there exists a one-to-one operation-preserving correspondence between M* and the set of all n-tuples of F (the operations of addition and scalar multiplication on the n-tuples being component-wise). Hence, the dual space of any n-dimensional vector space is also n-dimensional.

Given M and M* as above, the tensor product over F

$$T = \underbrace{M \otimes \ldots \otimes M}_{(r \text{ times})} \otimes \underbrace{M^* \otimes \ldots \otimes M^*}_{(s \text{ times})}$$

is called a <u>tensor space on M</u> contravariant of rank r and covariant of rank s. Any element of T is called a <u>tensor</u>. Now, if $m_1, \ldots, m_n$ is a fixed basis of M, we may select a basis $m'_1, \ldots, m'_n$ of linear functions in M* such that

$$m'_i(m_j) = \delta_{ij} = \begin{cases} 1 & \text{for } i = j \\ 0 & \text{for } i \neq j \end{cases} .$$

Having chosen the bases as such, from Theorem 4 (VI) it follows that T is a K-free module of length or dimension n^{r+s} and with basis

$$\left\{ m_{i_1} \otimes \ldots \otimes m_{i_r} \otimes m'_{j_1} \otimes \ldots \otimes m'_{j_s} \;\middle|\; i_k, j_k = 1, \ldots, n \right\} .$$

Therefore, any tensor t in T may be uniquely expressed in the form

$$t = \sum_{i_k, j_k}^{n} \left(\xi^{i_1, \ldots, i_r}_{j_1, \ldots, j_s} \right) m_{i_1} \otimes \ldots \otimes m_{i_r} \otimes m'_{j_1} \otimes \ldots \otimes m'_{j_s}$$

where the n^{r+s} coordinates ξ of t are elements of F.

BIBLIOGRAPHY

Bass, Hyman, Lecture notes on homological algebra, N.S.F. Summer Institute, University of Oregon, 1962.

Curtis, Charles, Lecture notes on group representations, N.S.F. Summer Institute, University of Oregon, 1962.

Halmos, Paul R., Finite Dimensional Vector Spaces, D. Van Nostrand Co., Princeton, N.J., 1958.

Jacobson, Nathan, Lectures in Abstract Algebra, Volume I (Basic Concepts), D. Van Nostrand Co., Princeton, N.J., 1951.

Jacobson, Nathan, Lectures in Abstract Algebra, Volume II (Linear Algebra), D. Van Nostrand Co., Princeton, N.J., 1953.

Northcott, D.G., An Introduction to Homological Algebra, Cambridge University Press, 1960.

Zariski, Oscar and Samuel, Pierre, Commutative Algebra, Volume I, D. Van Nostrand Co., Princeton, N.J., 1958.

VITA

James T. Sedlock was born on January 9, 1940, to Dr. and Mrs. John J. Sedlock in Philadelphia, Penna. He attended both La Salle College High School and La Salle College in Philadelphia, receiving a Bachelor of Arts in mathematics from the latter in June, 1961.

Presently, he is an N.D.E.A. fellow in mathematics studying at Lehigh University.