

**43**

**MATSCIENCE REPORT 43**

**CONCEPTS IN MODERN MATHEMATICS-I**  
(ALGEBRA)

**BY**  
**K. R. UNNI**  
Member, Matscience

**NOTES BY**  
**G. N. KESHAVAMURTHY AND**  
**N. R. NANDAKUMAR**

**THE INSTITUTE OF MATHEMATICAL SCIENCES, MADRAS-20, (INDIA)**

MATSCIENCE REPORT 43

**THE INSTITUTE OF MATHEMATICAL SCIENCES**

MADRAS - 20 (India)

CONCEPTS IN MODERN MATHEMATICS-I  
(ALGEBRA)

By

K. R. Unni\*

Notes by

G. N. Keshavamurthy and N. R. Nandakumar

---

\* Member, The Institute of Mathematical Sciences, Madras-20 (India)



## I N T R O D U C T I O N

These notes are the outcome of a systematic course of lectures given at MATSCIENCE to the students of Mathematics Faculty. An attempt is being made at this institute to offer a graduate programme in Mathematics similar to the ones in American Universities. The entire series 'Concepts in Modern Mathematics' is aimed at introducing some basic concepts in today's Mathematics and may be generally classified under what "every student of Mathematics ought to be familiar with".

Being first of the series, this volume on algebra contains some well known theorems; for example, Sylow Theorems on Groups, Wedderburn's Theorems on Semi-simple algebra and the theorem that every module can be embedded in an injective module. As is the fashion, emphasis is laid on modules. Galois Theory and the notions of Category, Functor, etc. have been omitted for some reason or other.

In the preparation of these notes, I have drawn freely from standard books and from the lectures given by Professor Eben Matlis at Northwestern University in 1961-62 for which I wish to make due acknowledgement here.

K.R.U.

C O N T E N T S

CHAPTER 1. GROUPS. . . . .	1
1. Extracts from set theory . . . . .	1
2. Definition and examples of a group . . . . .	5
3. Subgroups and cosets . . . . .	9
4. Homomorphism . . . . .	14
5. Finite groups . . . . .	26
6. Sylow theorems . . . . .	31
7. Permutation groups . . . . .	36
8. Direct product . . . . .	45
9. Jordan Holder series . . . . .	49
10. Solvable groups . . . . .	53
CHAPTER 2. RINGS AND MODULES . . . . .	55
1. Rings . . . . .	55
2. Ideals . . . . .	57
3. Homomorphisms . . . . .	61
4. Principal ideal ring . . . . .	69
5. Modules . . . . .	73
6. Direct product and direct sum . . . . .	79
7. Free modules . . . . .	87
8. Simple and Semisimple modules . . . . .	102
9. Projective, Injective and Hereditary modules . . . . .	106

CHAPTER 3. VECTOR SPACES AND ALGEBRAS . . . . .	117
1. Vector spaces over a skew field . . . . .	117
2. Matrices . . . . .	122
3. Algebra and ideals . . . . .	129
4. Wedderburn's theorems . . . . .	130
CHAPTER 4. TENSOR PRODUCT AND COMPLEXES . . . . .	142
1. Tensor product . . . . .	142
2. Group of Homomorphisms . . . . .	152
3. Divisible and injective modules . . . . .	158
4. Complexes and resolutions . . . . .	166
5. Ext. and Tor. . . . .	173
CHAPTER 5. MULTILINEAR ALGEBRAS . . . . .	175
1. Tensor product . . . . .	175
2. Covariant and contravariant tensors . . . . .	178
3. Symmetry and skew symmetry . . . . .	181
REFERENCES . . . . .	185





## CHAPTER 1

### GROUPS

#### 1. Extracts From Set Theory

The concept of a set is fundamental in Mathematics. We shall not try to define a set and an element of the set, but take them as undefined terms. In what follows, capital letters will be used to denote sets and small letters will designate the elements. If  $A$  and  $B$  are two sets, then  $A$  is a subset of  $B$  if every element of  $A$  is also an element of  $B$ . Two sets are said to be equal if each is a subset of the other.  $A$  is a proper subset of  $B$ , if  $A$  is a subset of  $B$  and  $A$  is not equal to  $B$ . We write  $a \in A$  symbolically to mean that  $a$  is an element of  $A$  or  $a$  belongs to  $A$ . The contrary is expressed by  $a \notin A$  which means that  $a$  does not belong to  $A$ . If  $A$  is a subset of  $B$ , we usually write  $A \subset B$ . Symbolically  $A=B$  if  $A \subset B$  and  $B \subset A$ . The set  $A$  all of whose elements 'a' possess a property  $\phi(a)$  is denoted by  $A = \{a | \phi(a)\}$ . If  $A$  contains only a finite number of elements  $a_1, a_2, \dots, a_n$  we write  $A = \{a_1, a_2, \dots, a_n\}$ .

While dealing with algebraic operations on sets it is convenient to introduce the notation of empty set or void set denoted by  $\phi$ . The set  $\phi$  contains no elements and is a subset of every set. The union of two sets  $A$  and  $B$  is a

set  $C$  consisting of elements which belong to at least one of the sets  $A$  and  $B$ . We write  $C = A \cup B$ . The intersection of two sets  $A$  and  $B$  is a set  $D$  consisting of all the elements which belong to both  $A$  and  $B$ . We write this by  $D = A \cap B$ .

It is very easy to verify that the operations of union and intersection are both commutative and associative i.e.,

$$A \cup B = B \cup A, \quad A \cap B = B \cap A.$$

$$(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C)$$

By virtue of these relations, it is easy to define union and intersection of any finite number of sets.

Bearing these in mind, we define the concept of union and intersection of any number of sets as follows. Let  $\Lambda$  be a set called the index set. Let  $\{A_\lambda\}_{\lambda \in \Lambda}$  be a family of sets then we define

$$\bigcup_{\lambda \in \Lambda} A_\lambda = \{a \mid a \in A_\lambda \text{ for some } \lambda \in \Lambda\}$$

and

$$\bigcap_{\lambda \in \Lambda} A_\lambda = \{a \mid a \in A_\lambda \text{ for all } \lambda \in \Lambda\}$$

to be union and intersection respectively for the family

$$\{A_\lambda\}_{\lambda \in \Lambda}.$$

Two sets are said to be disjoint if their intersection is the empty set and a family of sets are said to be disjoint if every pair of sets in the family are disjoint.

The cartesian product  $A \times B$  of two sets  $A$  and  $B$  is the set of all ordered pairs  $(a,b)$  with  $a \in A, b \in B$ .

We write this as

$$A \times B = \{ (a,b) \mid a \in A, b \in B \}$$

Let  $A$  and  $B$  be two sets. A function (or mapping)  $f$  on  $A$  into  $B$  is a subset of the cartesian product  $A \times B$  such that for each  $a \in A$ , there exists one and only one pair  $(a,b) \in f$ . If  $(x,y)$  is a pair belonging to the function  $f$  we write  $y = f(x)$  and  $y$  is called the image of  $x$  under  $f$ . The set  $A$  is called the domain of  $f$ . The range of  $f$  is the set of all images under  $f$  of elements of  $A$ . We usually write  $f: A \rightarrow B$  i.e. mapping  $f$  of  $A$  into  $B$ .

The inverse image of an element  $b \in B$  is the set of all elements  $a \in A$  such that  $f(a) = b$ . If  $X \subset A$ , then  $f(X) = \{ f(x) \mid x \in X \}$  similarly if  $Y \subset B$ , then  $f^{-1}(Y) = \{ x \mid f(x) \in Y \}$ .

Let  $f: A \rightarrow B$  be a mapping. If  $f(a_1) = f(a_2)$  implies  $a_1 = a_2$  for all  $a_1, a_2 \in A$  then  $f$  is said to be one to one. If  $f(A) = B$  then  $f$  is said to be onto. A one to one mapping of  $A$  onto  $B$  is called a one to one correspondance between  $A$  and  $B$ .

A relation  $R$  between two sets  $A$  and  $B$ , is a subset of  $A \times B$  we will write  $a R b$  if  $(a,b) \in R$ . An equivalence relation on  $A$  is a relation  $R$  contained in  $A \times A$  such that

$$\text{i) } a R a$$

$$\text{ii) } a R a' \Rightarrow a' R a$$



$$\text{III) } a R a', a' R a'' \implies a R a''$$

We use  $\sim$  for an equivalence relation

A partition of a set  $A$  is a collection  $\{A_\lambda\}_{\lambda \in \Lambda}$  of disjoint subsets of  $A$  such that  $\bigcup_{\lambda \in \Lambda} A_\lambda = A$

THEOREM: Let  $A$  be a set and  $\sim$  an equivalence relation on  $A$ . Then there exists a unique partition on  $A$  such that two elements of  $A$  lie in the same subset of the partition iff they are equivalent. The subsets of the partition are called equivalence classes. Conversely given a partition of  $A$ , there exists an equivalence relation on  $A$  such that the equivalence classes are the same as the subsets of the partition.

PROOF: Let  $\sim$  be an equivalence relation. Let  $a \in A$  define  $E_a = \{x \in A \mid a \sim x\}$ . Clearly  $A = \bigcup_{a \in A} E_a$ . Suppose  $c \in E_a \cap E_b$  we show that  $E_a = E_b$ . For,  $a \in A$  let  $x \in E_a$  then  $x \sim a$ ,  $c \sim a \implies x \sim c$ .  $c \in E_b, \therefore b \sim c$ . Hence  $x \sim c, c \sim b \implies x \sim b$  and hence  $x \in E_b$ . Therefore  $E_a \subset E_b$ . Similarly  $E_b \subset E_a$  and hence  $E_a = E_b$ .

Conversely given a partition  $A = \bigcup_{\alpha} A_\alpha$ ,  $A_\alpha$  disjoint, define  $a \sim b$  if and only if  $a, b$  lie in the same  $A_\alpha$ .

Clearly  $\sim$  is an equivalence relation.



Let  $A$  be a set then a relation  $R$  on  $A$  is called a partial ordering of  $A$  if

$$i) \quad a R a, \quad \forall a \in A$$

$$ii) \quad a R b, \quad b R a \Rightarrow a = b$$

$$iii) \quad a R b, \quad b R c \Rightarrow a R c$$

We generally write  $a \leq b$  for  $a R b$ . A partial ordering is simply ordering: if  $a, b \in A \Rightarrow a \leq b$  or  $b \leq a$

Zorn's Lemma: Let  $A$  be a partially ordered set, if every simply ordered subset of  $A$  has an upper bound then  $A$  has a maximal element.

Well Ordering Principle: Every set can be well ordered. That is, every set can be endowed with a linear ordering such that with respect to that order every subset has a smallest element.

## 2. Definition and examples of a group

DEFINITION 1: A nonempty set  $G$  is called a group if there exists a binary operation  $\circ$  defined on  $G$  (a binary operation is a mapping of  $G \times G$  into  $G$ ) satisfying

$$(1) \quad (\text{associative law}) \quad a \circ (b \circ c) = (a \circ b) \circ c$$

for all  $a, b, c \in G$

(2) there exists an element  $e$  in  $G$  such that

$$e \circ a = a \quad \text{for all } a \in G$$

(3) for each  $a \in G$ , there exists  $a^{-1} \in G$  such that  $a^{-1} \circ a = e$ .

$G$  is said to be commutative or abelian if  $a \circ b = b \circ a$  for all  $a, b \in G$ .

Remark 1. Given  $a \in G$ , we have  $a \circ a^{-1} = e$  and  $a \circ e = a$ .

PROOF: By (3), we can choose  $b \in G$  such that  $b \circ a^{-1} = e$ . Then

$$a^{-1} = e \circ a^{-1} = (a^{-1} \circ a) \circ a^{-1} = a^{-1} \circ (a \circ a^{-1})$$

so that

$$\begin{aligned} e &= b \circ a^{-1} = b \circ (a^{-1} \circ (a \circ a^{-1})) = (b \circ a^{-1}) \circ (a \circ a^{-1}) \\ &= e \circ (a \circ a^{-1}) = a \circ a^{-1} \end{aligned}$$

Also  $a \circ e = a \circ (a^{-1} \circ a) = (a \circ a^{-1}) \circ a = e \circ a = a$ .

Remark 2.  $e$  and  $a^{-1}$  are unique.

$e$  is called the identity of  $G$  and  $a^{-1}$  is called the inverse of  $a$ .

#### Examples

1. Integers under the ordinary addition
2. Complex numbers under addition
3. Positive rational numbers under multiplication.
4. The set of all rotations of the planes about the origin under composition
5. Let  $n > 0$  be an integer. Let  $G = \{0, 1, 2, \dots, n-1\}$ . If  $a, b \in G$ , define  $a \circ b =$  residue with respect to  $n$  of  $a + b$
6. Let  $A$  be a set with  $n$  elements. A one to one mapping of  $A$  onto itself is called a permutation. Let  $S_n$  denote the set of

all permutations on  $A$ . If  $A = \{a_1, a_2, \dots, a_n\}$  and  $\sigma \in S_n$ , we also write

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix} \quad \text{where } \sigma(a_k) = a_{i_k}$$

If

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix} \quad \text{and } \tau = \begin{pmatrix} a_{i_1} & a_{i_2} & \dots & a_{i_n} \\ a_{j_1} & a_{j_2} & \dots & a_{j_n} \end{pmatrix}$$

We define

$$\begin{aligned} \tau \cdot \sigma &= \begin{pmatrix} a_{i_1} & a_{i_2} & \dots & a_{i_n} \\ a_{j_1} & a_{j_2} & \dots & a_{j_n} \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix} \\ &= \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{j_1} & a_{j_2} & \dots & a_{j_n} \end{pmatrix} \end{aligned}$$

Then  $S_n$  is a group with  $n!$  elements. Notice that  $S_n$  is not abelian.

All groups will be denoted multiplicatively.

**THEOREM 1:** Let  $G$  be a nonempty set with an associative binary operation. Then  $G$  is a group if and only if given  $a, b \in G$  there exist  $x, y \in G$  (unique) such that  $ax = b, ya = b$ .

**PROOF:** Suppose  $G$  is a group and let  $a, b \in G$ . Take  $x = a^{-1}b$  and  $y = ba^{-1}$ . If  $ax = ax'$ , then  $x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ax') = (a^{-1}a)x' = x'$ . Similarly if  $ya = y'a$  then  $y = y'$ .



Conversely, suppose  $x, y$  exists for any  $a, b \in G$  such that  $ax = b$  and  $ya = b$ . Take  $a \in G$ . Then there exists  $e_a \in G$  such that  $e_a a = e$ . If  $b \in G$ , we will show  $e_a b = b$  also. Now  $e_a b = e_a (ay) = (e_a a)y = ay = b$ . So  $e_a = e$ . There exists  $x \in G$  such that  $ax = e$ .

Thus  $G$  is a group.

Remark:  $(a^{-1})^{-1} = a$  and  $(ab)^{-1} = b^{-1} a^{-1}$ .

DEFINITION 2: A nonempty set with an associative binary operation is called a semigroup. A semigroup  $S$  satisfies the left cancellation law if  $ax = ax'$  for  $a, x, x' \in S$  implies  $x = x'$ . Similarly we can define right cancellation law.

THEOREM 2: If  $S$  is a finite semigroup with cancellation law, then  $S$  is a group.

PROOF: Let  $S = \{a_1, a_2, \dots, a_n\}$ . Choose  $a, b \in S$ . We assume without loss of generality  $a = a_1$ . Then the set  $\{a_1 a_1, a_1 a_2, \dots, a_1 a_n\}$  is all of  $S$ . There exists  $x = a_j$  for some  $j$  such that  $a_1 a_j = b$ . Similarly there exists  $y \in S$  such that  $y a_1 = b$ . By Theorem 1,  $S$  is a group.

### 3. Subgroups and Cosets

DEFINITION 3: Let  $G$  be a group. A subset  $H$  of  $G$  is called a subgroup of  $G$  if it is a group under the group operation of  $G$ .

Example: 1. For any group  $G$ ,  $G$  and  $e$  are subgroups of  $G$ .

2. The set of all multiples of a prime  $p$  is a subgroup of the additive group of integers.

THEOREM 3: Let  $G$  be a group and  $H$  a nonempty subset of  $G$ . Then the following are equivalent.

- (i)  $H$  is a subgroup of  $G$ .
- (ii) if  $a, b \in H$ , then  $ab \in H$  and  $a^{-1} \in H$ .
- (iii) if  $a, b \in H$ , then  $ab^{-1} \in H$ .

PROOF: i)  $\Leftrightarrow$  ii) follows from the definition of a subgroup.

i)  $\Rightarrow$  iii) Suppose  $H$  is a subgroup,  $b \in H$  implies  $b^{-1} \in H$ . If  $a, b \in H$ , then  $a, b^{-1} \in H$  and  $ab^{-1} \in H$ .

iii)  $\Rightarrow$  i) Suppose (iii) is satisfied  $a \in H$  implies  $a \cdot a^{-1} \in H$  that is  $e \in H$ .  $a, e \in H$  implies  $e \cdot a^{-1} \in H$  that is  $a^{-1} \in H$ .  $a, b \in H$  implies  $a, b^{-1} \in H$  which implies  $a \cdot (b^{-1})^{-1} \in H$ . That is  $ab \in H$ .

Hence  $H$  is a subgroup.

THEOREM 4: If  $H$  is a finite nonempty subset of a group  $G$ , then  $H$  is a subgroup of  $G$  if and only if  $a, b \in H$  implies  $ab \in H$ .

PROOF: Exercise.

DEFINITION 4: A nonempty subset of a group is called a complex. If  $S, T$  are complexes, we define

$$ST = \{st \mid s \in S, t \in T\}$$

and

$$S^{-1} = \{s^{-1} \mid s \in S\}$$

The subgroup generated by a complex  $S$  of a group  $G$  is the smallest subgroup of  $G$  containing  $S$ .

Exercise 1. Let  $\{H_\lambda\}_{\lambda \in \Lambda}$  be a collection of subgroups of a group  $G$ . Then

- 1)  $\bigcap_{\lambda \in \Lambda} H_\lambda$  is a subgroup of  $G$ .
- 2) if the collection is simply ordered, then

$$\bigcup_{\lambda \in \Lambda} H_\lambda \text{ is a subgroup of } G.$$

Exercise 2. Let  $S$  be a complex in a group  $G$ . Then the subgroup  $A(S)$  **generated** by  $S$  is the intersection of all subgroups of  $G$  containing  $S$  and

$$A(S) = \{s_1 \dots s_n \mid s_i \in S \text{ or } S^{-1}\}$$



that is, the set of all finite products of elements of  $S$  or  $S^{-1}$ .

DEFINITION 5: Let  $G$  be a group and  $H$  a subgroup of  $G$ . Let  $x \in G$ . Then  $xH = \{xh \mid h \in H\}$  is called a left coset of  $H$ . Similarly  $Hx$  is a right coset of  $H$ .

The cosets of a subgroup have the following properties.

THEOREM 5: Let  $G$  be a group and  $H$  a subgroup of  $G$ . Then

- (1)  $G = \bigcup_{x \in G} xH$
- (2)  $xH = yH$  if and only if  $y^{-1}x \in H$ ,  
 $x, y \in G$ .
- (3) two left cosets of  $H$  are either identical or disjoint
- (4) there exists a one to one correspondence between any two left cosets of  $H$ .
- (5) there exists a one to one correspondence between the collection of left cosets of  $H$  and the collection of right cosets of  $H$ .

PROOF: (1) For any  $x \in G$ ,  $x = xe \in xH$ .

(2) Suppose  $xH = yH$   $x, y \in G$ .

Then  $y = ye = xh$  for some  $h \in H$ . So that  $y^{-1}x = h^{-1} \in H$ .

Conversely, suppose  $y^{-1}x \in H$ . Then  $y^{-1}x = h$  for some  $h \in H$ . If  $h_1$  is any element of  $H$ , then  $xh_1 = yhh_1 = yh' \in yH$ ,  $h' = hh_1 \in H$ , so that  $xH \subset yH$ . Similarly if



$h_1$  is any element of  $H$ , then  $y h_1 = x h^{-1} h_1 \in x H$  since  $h^{-1} h_1 \in H$ , which implies  $y H \subset x H$ .

Hence  $y H = x H$

3) Suppose  $z \in x H \cap y H$ . Then  $z \in x H$  and  $z \in y H$ .  $z \in x H$  implies  $z = xh$  for some  $h \in H$  so that  $x^{-1}z = h \in H$ . Therefore  $zH = xH$ . Similarly  $z \in yH$  implies  $zH = yH$ . Hence  $xH = yH$ .

4) First notice that  $H = eH$  is a left coset of  $H$ . If  $x \in G$ , define a map  $xH \rightarrow H$  by  $xh \rightarrow h$ . Notice that this is a well defined onto function.

5) The correspondence is given by  $xH \rightarrow Hx^{-1}$  for  $x \in G$ . Suppose  $xH = yH$ . Then  $y^{-1}x \in H$ . Therefore  $y^{-1}x = h$  for some  $h \in H$ . Then  $x^{-1}(y^{-1})^{-1} = h^{-1} \in H$  so that  $Hx^{-1} = Hy^{-1}$ . Thus the above mapping is well defined. If  $z \in G$ , then  $z^{-1}H \rightarrow Hz$  so that it <sup>is</sup> onto. If  $Hx^{-1} = Hy^{-1}$ , then  $xH = yH$  by an argument similar to the above, so that the map is 1-1.

**THEOREM 6:** Let  $G$  be a group. Then

(a) if  $H$  is a subgroup of  $G$  there exists an equivalence relation  $\sim$  on  $G$  defined by  $x \sim y$  if and only if  $y^{-1}x \in H$ . The equivalence class of  $x$  is  $xH$  and if  $x \sim y$  then  $zx \sim zy$ .

(b) let  $\sim$  be an equivalence relation on  $G$  such that  $x \sim y$  implies  $zx \sim zy$ ,  $z \in G$ . Then there exists a subgroup  $H$  such that  $x \sim y$  if and only if  $y^{-1}x \in H$ .

PROOF: a)(i)  $e = x^{-1}x \in H \therefore x \sim x$ .

(ii) if  $x \sim y$ , then  $y^{-1}x \in H$  so that  $x^{-1}y = (y^{-1}x)^{-1} \in H$  which implies  $y \sim x$ .

(iii) if  $x \sim y$  and  $y \sim z$ , then  $y^{-1}x \in H$  and  $z^{-1}y \in H$  so that  $z^{-1}x = (z^{-1}y)(y^{-1}x) \in H$ . Therefore  $x \sim z$ . If  $y \sim x$ , then  $x^{-1}y \in H$  so that  $y \in xH$ . Conversely, if  $xh \in xH$ , then  $h^{-1}x^{-1}x = h^{-1} \in H$  so that  $xh \sim x$ .

Let  $z \in G$  and  $x \sim y$ . Then  $y^{-1}x = h \in H$  so that  $(zy)^{-1}(zx) = (y^{-1}z^{-1})(zx) = y^{-1}x = h \in H$ . That is  $zx \sim zy$ .

(b) Set  $H = \{x \in G \mid x \sim e\}$

Let  $x, y \in H$ . Then  $x \sim e, y \sim e$  so that  $x \sim y$  which implies  $y^{-1}x \sim y^{-1}y = e$  so that  $y^{-1}x \in H$ . Hence  $H$  is a subgroup of  $G$ . Now  $x \sim y$  if and only if  $e = x^{-1}x \sim x^{-1}y$  if and only if  $x^{-1}y \in H$  if and only if  $y^{-1}x = (x^{-1}y)^{-1} \in H$ .

DEFINITION 6: The number of left cosets of a subgroup  $H$  of  $G$  is called the index of  $H$  in  $G$  and is denoted by  $[G:H]$  and the number of elements in a group  $G$  is called the order of the group.

THEOREM 7: Let  $H$  and  $K$  be subgroups of a group  $G$ , such that  $K \subset H \subset G$ . Then

$$[G:K] = [G:H] [H:K]$$

PROOF: Let  $\{x_i H\}_{i \in I}$  be a complete system of left cosets of  $H$  such that  $G = \bigcup_{i \in I} x_i H$  and  $x_i H \neq x_j H$  if  $i \neq j$ .

Let  $\{y_j K\}_{j \in J}$  be a complete system of left cosets of  $K$  in  $H$ . We shall now prove that  $\{x_i y_j K\}_{(i,j) \in I \times J}$  is a complete system of left cosets of  $K$  in  $G$ . Let  $g \in G$ . Then  $g = x_i h$  for some  $h \in H$  and for some  $i \in I$ . Now  $h = y_j k$  for some  $j \in J$  and  $k \in K$ . Then  $g = x_i h = x_i y_j k \in x_i y_j K$ . Thus  $G = \bigcup_{i,j} x_i y_j K$ . To complete the proof, it is enough to show that  $x_i y_j K \neq x_m y_n K$  if  $i \neq m$ ,  $j \neq n$ . Suppose  $x_i y_j K = x_m y_n K$ . Then  $x_i y_j = x_m y_n k$  for some  $k \in K$  so that  $x_i = x_m y_n k y_j^{-1} \in H$  since  $y_n k y_j^{-1} \in H$ . Therefore  $x_i H = x_m H$ . Therefore  $i = m$ . Now  $y_j K = y_n K$ . Therefore  $j = n$ .

COROLLARY: (Lagrange). If  $H$  is a subgroup of a group  $G$ , then

$$[G:e] = [G:H] [H:e]$$

i.e., the order of a subgroup of a finite group divides the order of the group and so is the index.

#### 4. Homomorphism.

DEFINITION 7: Let  $G$  and  $G'$  be groups. A mapping  $f: G \rightarrow G'$  is called a homomorphism if

$$f(a.b) = f(a)f(b)$$



for all  $a, b \in G$ . A homomorphism is called a monomorphism if it is one to one and an epimorphism if it is onto. An isomorphism is a homomorphism which is one to one and onto.

Examples: 1. Let  $Z$  denote the additive group of integers and let  $Z/nZ$  denote integers (mod  $n$ ). Define

$$f : Z \longrightarrow Z/nZ$$

by

$$f(m) = \bar{m}$$

where  $\bar{m}$  denotes the unique element in  $Z/nZ$  determined by the residue  $m \pmod{n}$ .  $f$  is a homomorphism onto but not 1-1.

2. Define  $f: 2Z \rightarrow Z$  by  $f(2n) = 2n$ . Then  $f$  is a homomorphism which is one-to-one but not onto.

3. Define  $g: 2Z \rightarrow Z$  by  $g(2n) = n$ . Then  $g$  is an isomorphism.

THEOREM 8: Let  $G, G'$  be groups and  $f: G \rightarrow G'$  a homomorphism. Then

(a)  $f(e) = e'$  where  $e$  and  $e'$  are identities in  $G$  and  $G'$  respectively.

(b)  $[f(x)]^{-1} = f(x^{-1})$ ,  $x \in G$

(c)  $f(G)$  is a subgroup of  $G'$ .

PROOF: (a) follows from  $f(x) = f(ex) = f(e)f(x)$  for all  $x \in G$ .

(b)  $f(x)f(x^{-1}) = f(x.x^{-1}) = f(e) = e'$  so that  $(f(x))^{-1} = f(x^{-1})$ .

(c) Let  $x', y' \in f(G)$ . There exist  $x, y \in G$  such that  $f(x) = x'$ ,  $f(y) = y'$ . Now  $y'^{-1} x' = [f(y)]^{-1} f(x) = f(y^{-1}) f(x) = f(y^{-1} x) \in f(G)$  since  $y^{-1} x \in G$ . Hence  $f(G)$  is a subgroup of  $G'$ .

DEFINITION 8: A homomorphism of a group into itself is called an endomorphism. An isomorphism of a group onto itself is called an automorphism.

$\xi(G)$  and  $\alpha(G)$  will denote respectively the set of all endomorphisms and automorphisms of the group  $G$ .

Exercise 3. If  $f, g \in \alpha(G)$  (or  $\xi(G)$ ), define  $f.g$  by  $(fg)(x) = f(g(x))$  for all  $x \in G$ . Show that  $\alpha(G)$  is a group and  $\xi(G)$  is a semigroup.

We shall now consider a special kind of automorphisms called inner automorphisms. Let  $x$  be an element of a group  $G$ . Define

$$I_x : G \longrightarrow G$$

$$\text{by } I_x(g) = x g x^{-1} \text{ for } g \in G.$$

We now assert that  $I_x$  is an automorphism of  $G$ . To this end, if  $g_1, g_2 \in G$ , we have

$$\begin{aligned} I_x(g_1 g_2) &= x (g_1 g_2) x^{-1} = (x g_1 x^{-1}) (x g_2 x^{-1}) \\ &= I_x(g_1) I_x(g_2) \end{aligned}$$

so that  $I_x$  is a homomorphism. It is clearly onto, since if  $y \in G$ , then  $I_x(x^{-1} y x) = y$ . Further  $x g_1 x^{-1} = x g_2 x^{-1}$  implies  $g_1 = g_2$  so that  $I_x$  is one-to-one. Thus  $I_x \in \alpha(G)$ .

If we consider the map

$$\varphi : G \longrightarrow \mathcal{O}(G)$$

defined by

$$\varphi(x) = I_x, \text{ we have}$$

$$\begin{aligned} I_{xy}(g) &= (xy) g (xy)^{-1} = x (y g y^{-1}) x^{-1} \\ &= I_x (y g y^{-1}) = I_x (I_y(g)) \\ &= (I_x \cdot I_y)(g) \quad \text{for all } g \in G \end{aligned}$$

so that

$$I_{xy} = I_x \cdot I_y \text{ i.e., } \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

Thus  $\varphi$  is a homomorphism and the image  $I(G)$  of  $G$  under  $\varphi$  is a subgroup of  $\mathcal{O}(G)$  called the group of inner automorphisms of  $G$  and each element  $I_x$  of  $G$  is called the conjugation by  $x$  and inner automorphism by  $x$ .

DEFINITION 9: Let  $G$  be a group and  $H$  a subgroup of  $G$ .  $H$  is called an invariant (or normal) subgroup of  $G$  if  $H$  is mapped into itself by every element of  $I(G)$ , that is  $x H x^{-1} \subset H$  for all  $x \in G$ .

Exercise 4. (1) The intersection of any family of normal subgroups is a normal subgroup.

(2) The union of a simply ordered chain of normal subgroups is normal.

(3) If  $H$  is a subgroup of a group  $G$ , then  $x H x^{-1} \subset H$  for all  $x \in G$  implies  $x H x^{-1} = H$ .



THEOREM 9: Let  $G$  be a group and  $H, K$  subgroups of  $G$ . Then  $HK$  is a subgroup if and only if  $HK=KH$ . If  $K$  is a normal subgroup of  $G$ , then  $HK$  is a subgroup of  $G$ . If  $H$  and  $K$  are both normal subgroups, then  $HK$  is also a normal subgroup.

PROOF: Suppose  $H$  and  $K$  are subgroups of a group  $G$ .

Suppose  $HK$  is a subgroup of  $G$ . Let  $k \in K, h \in H$  and consider the element  $kh \in KH$ . Now  $hk \in HK$ . Since  $HK$  is a subgroup  $(hk)(hk) \in HK$  so that there exist  $h_1 \in H, k_1 \in K$  such that  $(h.k)(h.k) = h_1 k_1$ . This implies  $kh = h^{-1}(h_1 k_1)k^{-1} = (h^{-1}h_1)(k_1 k^{-1}) = h_2 k_2 \in HK$ . Thus  $KH \subset HK$ . Similarly  $HK \subset KH$ .

$$\therefore HK = KH.$$

Conversely, suppose that  $HK=KH$  we will show that  $HK$  is a subgroup of  $G$ . Let  $x=hk$  and  $y=h_1 k_1$  be any two elements of  $HK$ . Enough to show  $xy^{-1} \in HK$ . Now

$$\begin{aligned} xy^{-1} &= (hk)(h_1 k_1)^{-1} = h(kk_1^{-1})h_1^{-1} \\ &= hk_2 h_1^{-1} \quad kk_1^{-1} = k_2 \in K. \\ &= hh_3 k_3 \quad \text{since } k_2 h_1^{-1} = h_3 k_3 \\ &= h_4 k_3 \in HK. \end{aligned}$$

Therefore  $HK$  is a subgroup.

If  $K$  is a normal subgroup of  $G$ , then  $xK=Kx$  for all  $x \in G$  and hence  $Kx=xK$  for all  $x \in H$ . Therefore



$HK = KH$  and so  $HK$  is a subgroup.

If  $H$  and  $K$  are normal subgroups of  $G$ ,  $HK$  is clearly a subgroup of  $G$ . Enough to show the normality. If  $x \in G$  and  $hk \in HK$ , then  $xhkx^{-1} = (xhx^{-1})(xkx^{-1}) \in HK$  since  $H$  and  $K$  are normal so that  $xHKx^{-1} \subset HK$ .

This completes the proof.

If  $K$  is a normal subgroup of a group  $G$ , we denote by  $G/K$  the collection of all left cosets of  $K$ . If  $x \in G$ , we let  $\bar{x} = xK$ . We make  $G/K$  a group by defining  $xK \cdot yK = xyK$ . Notice first that this is well defined. Suppose  $\bar{x} = \bar{x}'$  and  $\bar{y} = \bar{y}'$ . Then  $\overline{xy} = xyK = xK \cdot yK = x'K \cdot y'K = x'y'K = \overline{x'y'}$ . This multiplication is thus independent of the choice of representatives of the coset.  $\bar{e}$  is the identity in  $G/K$  and the inverse of  $\bar{x}$  is  $\bar{x}^{-1}$ .  $G/K$  is called the quotient group (or the factor group) of  $G$  modulo  $K$ .

Exercise 5. Give an example to show that  $G/K$  is not a group if  $K$  is not a normal subgroup.

DEFINITION 10: Let  $f : G \rightarrow G'$  be a homomorphism of  $G$  into  $G'$ . Kernel of  $f$  is defined by

$$\text{Ker } f = \{x \in G \mid f(x) = e'\}$$

where  $e'$  is the identity in  $G'$ .

$\text{Ker } f$  is a normal subgroup of  $G$ .

THEOREM 10: Let  $G$  be a group and  $K$  a normal subgroup of  $G$ . Then the map

$$\varphi : G \rightarrow G/K$$

defined by  $\varphi(x) = xK$ ,  $x \in G$  is an onto

homomorphism with  $\ker \varphi = K$ .  $\varphi$  is called a natural or canonical homomorphism.

PROOF: First we remark that the map is well defined since  $x=y$  implies  $xK = yK$ . If  $x, y \in G$ , then

$$\varphi(xy) = xyK = xK.yK = \varphi(x)\varphi(y)$$

so that  $\varphi$  is a homomorphism. It is clearly onto. We shall now show that  $K$  is the kernel of  $\varphi$ . To this end, suppose  $x \in K$ . Then  $\varphi(x) = xK = K$  so that  $x \in \ker \varphi$  and we have  $K \subset \ker \varphi$ . If  $x \in \ker \varphi$ , then  $xK = \varphi(x) = K$  so that  $x \in K$  and we have  $\ker \varphi \subset K$ .

$$K = \ker \varphi.$$

THEOREM 11: Let  $G, G'$  be groups and  $f:G \rightarrow G'$  a homomorphism with  $\ker f = K$ . Then there exists a unique homomorphism

$$\bar{f} : G/K \rightarrow G'$$

such that  $\bar{f}\varphi = f$  where

$$\varphi : G \rightarrow G/K$$

is the Canonical map i.e., the diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \varphi \searrow & & \nearrow \bar{f} \\ & G/K & \end{array}$$

commutes further if  $f$  is onto, then  $\bar{f}$  is an isomorphism.

PROOF: Define  $\bar{f} : G/K \longrightarrow G'$  by

$$f(xK) = f(x)$$

Then  $\bar{f}$  is a well defined homomorphism (check). If  $x \in G$ , then

$$\bar{f}\varphi(x) = \bar{f}(x \cdot K) = f(x)$$

Since this is true for all  $x \in G$ , we conclude that  $\bar{f}\varphi = f$ . To see that  $\bar{f}$  is unique, let

$$g : G/K \longrightarrow G'$$

such that  $g\varphi = f$ . Then  $g(xK) = g\varphi(x) = f(x) = \bar{f}\varphi(x) = \bar{f}(x \cdot K)$  for all  $xK \in G/K$  so that  $g = \bar{f}$ .

Suppose now that  $f$  is onto. If  $x' \in G'$ , there exists  $x \in G$  such that  $f(x) = x'$  so that  $\bar{f}(x \cdot K) = x'$  which implies that  $\bar{f}$  is onto also. Now, to complete the proof, it is enough to show  $\bar{f}$  is one-to-one. If  $\bar{f}(x \cdot K) = \bar{f}(y \cdot K)$  then  $f(x) = f(y)$  so that  $f(y^{-1}x) = e'$  where  $e'$  is the identity in  $G'$ . This means  $y^{-1}x \in K$  and then  $xK = yK$  and  $\bar{f}$  is one-to-one.

Notation: If  $G$  and  $G'$  are isomorphic, we write  $G \cong G'$ .

THEOREM 12: Let  $G$  be a group and  $H, K$  are normal subgroups of  $G$  such that  $K < H < G$ . Then

$$\frac{G/K}{H/K} \cong G/H$$

PROOF: Define  $f : \frac{G}{K} \longrightarrow \frac{G}{H}$  by

$$f(xK) = xH \quad x \in G.$$



If  $xK = yK$  then  $y^{-1}x \in K \subset H$  so that  $xH = yH$  so  $f$  is well defined. Now

$$f(xK \cdot yK) = f(xyK) = xyH = xH \cdot yH = f(xK) f(yK)$$

$f$  is a homomorphism. It is trivially onto. Let  $xK \in \ker f$ . Then  $f(xK) = xH = H$  so that  $x \in H$  and  $xK \in H/K$ . Therefore  $\ker f \subset H/K$ . If  $xK \in H/K$ ,  $x \in H$ , then  $f(xK) = xH = H$ . Therefore  $xK \in \ker f$ . Therefore  $H/K \subset \ker f$ .

Hence  $\ker f = H/K$ .

By Theorem 11,

$$\frac{G/K}{H/K} \cong G/H.$$

**THEOREM 13:** Let  $G$  be a group,  $H$  a subgroup of  $G$  and  $K$  a normal subgroup of  $G$ . Then

$$\frac{H}{H \cap K} \cong \frac{KH}{K}$$

**PROOF:** By Theorem 9,  $KH$  is a subgroup of  $G$ . Since  $K$  is normal in  $G$ ,  $K$  is normal in  $KH$  also. Consider the map

$$f : H \longrightarrow \frac{KH}{K} = \frac{HK}{K}$$

defined by

$$f(h) = hK \quad h \in H$$

Notice that an element in  $\frac{HK}{K}$  is of the form  $hkK = hK$  since  $k \in K$  implies  $kK = K$ . If  $h_1, h_2 \in H$ , then  $f(h_1 h_2) = h_1 h_2 K = h_1 K \cdot h_2 K = f(h_1) f(h_2)$ .  $f$  is therefore a homomorphism. It is clearly onto. To complete the proof, it is enough to show  $\ker f = H \cap K$ .

Clearly  $\ker f \subset H$ . If  $f(x) = K$ , then  $xK = K$  and  $x \in K$ . Therefore  $\ker f \subset K$ . Thus  $\ker f \subset H \cap K$ . Conversely, let  $x \in H \cap K$ . Then  $f(x) = xK = K$ . Therefore  $x \in \ker f$ . Hence  $H \cap K \subset \ker f$ .

THEOREM 14: Let  $H$  be a normal subgroup of a group  $G$ . If  $K$  is a normal subgroup of  $L$  and  $L$  is a subgroup of  $G$ , then

$$\frac{LH}{KH} \cong \frac{L}{K(L \cap H)}$$

PROOF: Since  $K$  is a normal subgroup of  $L$ , we have  $KL = LK = L$ . First we prove that  $KH$  is a normal subgroup of  $LH = LK \cdot H = L \cdot KH$ . By Theorem 9,  $KH = HK$ . Let  $x \in LH$ . Then  $x = lh$  where  $l \in L$  and  $h \in H$ . Now  $xKHx^{-1} = (lh)KH(lh)^{-1} = lhKhh^{-1}l^{-1} = lhKhl^{-1} = lhHkl^{-1} = lHkl^{-1} = (lh)l^{-1}(kl^{-1}) = HK = KH$ .

Now by Theorem 13,

$$\frac{LH}{KH} = \frac{L \cdot KH}{KH} \cong \frac{L}{KH \cap L}$$

The proof is completed, if we show that  $KH \cap L = K(L \cap H)$ . To this end, let  $x \in KH \cap L$ . Then  $x = kh$  where  $k \in K$  and  $h \in H$ . Then  $h = k^{-1}x \in KL = L$ . Thus  $h \in L \cap H$  which implies  $x = kh \in K \cdot (L \cap H)$ .

To prove the converse, let  $x \in K(L \cap H)$ . Then  $x = km$  where  $k \in K$  and  $m \in L \cap H$ . Then  $km \in KL = L$  and  $km \in KH$  so that  $x \in KH \cap L$ .

Exercise 6. Let  $f: G \rightarrow G'$  be a homomorphism of groups  $G$  and  $G'$ . Let  $H$  be a normal subgroup of  $G$  and  $H'$  a normal subgroup of  $G'$  such that  $f(H) \subset H'$ . Then if

$$\varphi: G \rightarrow G/H$$

and

$$\varphi': G' \rightarrow G'/H'$$

are the canonical maps, show that there exists a unique homomorphism

$$\bar{f}: G/H \rightarrow G'/H'$$

such that  $\bar{f}\varphi = \varphi'f$  i.e., the diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \varphi \downarrow & & \uparrow \varphi' \\ \frac{G}{H} & \xrightarrow{\bar{f}} & \frac{G'}{H'} \end{array}$$

commutes. If  $f$  is onto, so is  $\bar{f}$ . Further show that

$$\text{Ker } \bar{f} = \frac{f^{-1}(H')}{H}$$

Show also that if  $K$  is the kernel of  $f$  and  $M$  a subgroup of  $G$ , then  $f^{-1}f(M) = KM$ .

DEFINITION 11: Let  $G$  be a group. Then the center  $Z(G)$  is defined by

$$Z(G) = \{x \in G \mid yx = xy \text{ for all } y \in G\}.$$

THEOREM 15: Let  $G$  be a group. Then

(1)  $Z(G)$  is a normal subgroup of  $G$  and  $I(G)$  is a normal subgroup of  $\mathcal{O}(G)$

$$(2) G/Z(G) \cong I(G).$$

The proof is left as an exercise.



DEFINITION 12: Let  $S$  be a complex in  $G$ . Define

$$N(S) = \{x \in G \mid xSx^{-1} = S\}$$

Then  $N(S)$  is called the normalizer of  $S$ .

THEOREM 16:  $N(S)$  is a subgroup of  $G$ . Further if  $S$  is a subgroup of  $G$ , then  $N(S)$  is the largest subgroup of  $G$  containing  $S$  as a normal subgroup.

PROOF: Exercise.

DEFINITION 13: Let  $x$  and  $y$  be any two elements of a group  $G$ . The element  $xyx^{-1}y^{-1}$  is called the commutator of  $x$  and  $y$  in  $G$ . The subgroup  $[G, G]$  generated by all commutators in  $G$  is called the commutator subgroup of  $G$ .

The commutator subgroup has the following properties.

THEOREM 17: Let  $G$  be a group. Then

- (1)  $[G, G]$  is a normal subgroup of  $G$ .
- (2)  $G/[G, G]$  is abelian
- (3) If  $H$  is any normal subgroup of  $G$  such that  $G/H$  is abelian, then  $[G, G] \subset H$

PROOF: 1) Let  $k \in [G, G]$ . Now  $k$  is a product of a finite number of commutators  $k_1 k_2 \dots k_n$ . To prove that  $[G, G]$  is normal in  $G$ , we have to show that  $xkx^{-1} \in [G, G]$  for  $x \in G$ . Since  $xkx^{-1} = xk_1 k_2 \dots k_n x^{-1} = (xk_1 x^{-1})(xk_2 x^{-1}) \dots (xk_n x^{-1})$  the proof is completed if we can show that  $xkx^{-1}$  is commutator whenever  $k$  is. Thus we may assume  $k$  is a



commutator.  $k = aba^{-1}b^{-1}$ .  $a, b \in G$ .

$$\begin{aligned} \text{Now } xkx^{-1} &= (xax^{-1})(xbx^{-1})(xa^{-1}x^{-1})(xb^{-1}x^{-1}) \\ &= (xax^{-1})(xbx^{-1})(xax^{-1})^{-1}(xbx^{-1})^{-1} \end{aligned}$$

which is again a commutator.

(2) Let  $x, y \in G$ . Then  $x^{-1}y^{-1}xy = x^{-1}y^{-1}(x^{-1})^{-1}(y^{-1})^{-1} = k \in [G, G]$  so that  $xy = yxk$ . Then

$$\begin{aligned} x [G, G] \cdot y [G, G] &= xy [G, G] = yxk [G, G] \\ &= yx [G, G] = y [G, G] \cdot x [G, G] \end{aligned}$$

Thus  $G/[G, G]$  is abelian.

(3) Let  $k \in [G, G]$ . There exist  $x, y \in G$  such that  $x^{-1}y^{-1}xy = k$ . Since  $G/H$  is abelian,  $xHyH = yH \cdot xH$  so that  $xyH = yxH$  which implies  $xy = yxh$  for some  $h$  in  $H$ . Thus  $k = x^{-1}y^{-1}xy = h \in H$ .

Therefore  $[G, G] \subset H$ .

## 5. Finite groups

We recall that a group which has only a finite number of elements is called a finite group, and the number of elements is the order of the group. We observed that in a finite group the order of a subgroup divides the order of the group.

We remark that if  $x$  is an arbitrary element of a group  $G$ , we can define  $x^n = \underbrace{x \cdot x \cdot \dots \cdot x}_{n \text{ times}}$  by means of associativity and it is easy to show that the usual laws of exponents hold viz.

$$x^m x^n = x^{m+n}$$

and

$$(x^m)^n = x^{mn}$$

for all integers  $m, n$  where  $x^0 = e$ , the identity in  $G$ .

DEFINITION 14: Let  $G$  be a group and  $g \in G$ . Then the subgroup generated by  $\{g\}$  is called the cyclic subgroup generated by  $g$  and consists of all elements of the form  $g^n$  where  $n \in \mathbb{Z}$  and we write  $\langle g \rangle$ . A group  $G$  is called cyclic if there exists  $g \in G$  such that  $G = \langle g \rangle$ .  $g$  is then called the generator of  $G$ .

Exercise 7. Let  $G$  be a cyclic group generated by  $g$ . If  $g^n \neq g^m$  for  $n \neq m$ , then  $\langle g \rangle$  is infinite. Otherwise there exists a positive integer  $k$  such that  $g^k = e$ , and  $G = \{e, g, g^2, \dots, g^{k-1}\}$  with exactly  $k$  elements where  $g^i \neq g^j$  for  $i \neq j$  and  $0 \leq i, j \leq k-1$ . Prove also that every subgroup of a cyclic group is cyclic.

DEFINITION 15: If  $g \in G$ , we define the order of  $g$  to be the smallest positive integer  $k$  such that  $g^k = e$ .

Notice that in a finite group the order of an element divides the order of the group.

THEOREM 18: A group  $G$  with more than one element has no proper subgroup different from  $e$  if and only if  $G$  is cyclic of prime order.

PROOF: Suppose  $G$  is cyclic with  $p$  elements, where  $p$  is a prime. Let  $g \in G$ ,  $g \neq e$ . The order of  $g$  divides the order of  $G$  which is  $p$  and the order of  $g$  is different from 1. So order of  $g = p$  and hence  $G = \langle g \rangle$ .



Conversely, suppose  $G$  has no proper subgroups  $\neq e$ . We shall show that  $G$  is cyclic of prime order. To this end, let  $g \in G$ ,  $g \neq e$ . Then  $\langle g \rangle \neq e$  and by hypothesis  $\langle g \rangle = G$ . Suppose  $g^n \neq g^m$  for  $n \neq m$ . Then  $\langle g^2 \rangle$  is a proper subgroup of  $G$  which is a contradiction. Hence  $G$  is of finite order  $k$ . Now suppose  $k = nm$  where  $n \neq 1$ ,  $m \neq 1$ . Let  $h = g^n$ . Then by hypothesis  $\langle h \rangle = \langle g \rangle = G$ . Since  $h^m = g^{nm} = e$ , we can take  $r$  such that  $0 < r \leq m-1$  and  $g = h^r = g^{nr}$ . Then

$$g^{nr-1} = e$$

from which it follows that  $nr-1 \geq k$  or  $nr \geq k+1$ . By taking  $r$  to be  $m-1$  (largest possible value) we get  $n(m-1) \geq k+1$  or  $k-n \geq k+1$  which is a contradiction. Hence  $k$  is a prime.

Remarks (1). Upto isomorphism there is only one infinite cyclic group. For if  $G = \langle a \rangle$ , then the map  $f: G \rightarrow \mathbb{Z}$  defined by  $f(a^n) = n$  is an isomorphism.

(2) Upto isomorphism there is only one cyclic group of order  $n$ , namely integers (mod  $n$ ).

THEOREM 19: (Cayley). Let  $G$  be a finite group of order  $n$ . Then  $G$  is isomorphic to a subgroup of  $S_n$ .

PROOF: Let  $G$  be a group of order  $n < \infty$ . Let  $g \in G$ . Define a mapping  $L_g: G \rightarrow G$  by  $L_g(x) = gx$  for all  $x \in G$ . Then  $L_g$  is a permutation of  $G$  considered as a set (Prove) and hence belongs to  $S_n$ . Now define

$$\varphi: G \rightarrow S_n$$

by

$$\varphi(g) = L_g$$



Suppose  $\varphi(g_1) = \varphi(g_2)$ . Then  $Lg_1 = Lg_2$  which means  $Lg_1(x) = Lg_2(x)$  for all  $x \in G$ . In particular  $Lg_1(e) = Lg_2(e)$  which gives  $g_1 = eg_1 = eg_2$ . Thus  $\varphi$  is one to one. Now we will show that  $\varphi$  is a homomorphism. To this end, let  $x \in G$ . Then, if  $g_1, g_2 \in G$ ,

$$\begin{aligned} Lg_1g_2(x) &= (g_1g_2)x = g_1(g_2x) = Lg_1(g_2x) \\ &= Lg_1(Lg_2(x)) = (Lg_1Lg_2)(x). \end{aligned}$$

Since  $x$  is arbitrary, we have  $Lg_1g_2 = Lg_1Lg_2$ . In other words  $\varphi$  is a homomorphism and the proposition is proved.

DEFINITION 16: Let  $G$  be a group and  $x, y \in G$ .

Define an equivalence relation on  $G$  by  $x \sim y$  if and only if there exists  $g \in G$  such that  $gxg^{-1} = y$ .

Clearly  $\sim$  is an equivalence relation (check). Let

$[x]$  denote the equivalence class of  $x$ . The elements of  $[x]$  are called conjugates of  $x$ .

THEOREM 20: Let  $G$  be a finite group and  $x \in G$ .

Then the number of elements in  $[x]$  is equal to the index of the normalizer of  $x$  in  $G$ .

PROOF: Define a map from  $[x]$  into the collection of left cosets of  $N(x)$  in  $G$  by

$$gxg^{-1} \longrightarrow gN(x)$$

If  $gxg^{-1} = hxh^{-1}$  then  $(h^{-1}g)x(h^{-1}g)^{-1} = x$  which implies  $h^{-1}g \in N(x)$  so that  $gN(x) = hN(x)$ . So the map is well defined.

It is clearly onto. Now suppose that  $gN(x) = hN(x)$ . Then

$h^{-1}g \in N(x)$  and so  $(h^{-1}g)x(h^{-1}g)^{-1} = x$  which is  $gxg^{-1} = hxh^{-1}$ .

Hence the map is one-to-one.

Remark:  $[x]$  consists of one element if and only if  $x \in Z(G)$ .

THEOREM 21: (class equation). Let  $G$  be a finite group. Then the number of elements of  $G =$  the number of elements of  $Z(G) + \sum h_i$  where  $h_i$  divides the order of the group.

PROOF: Exercise (use Theorem 20).

DEFINITION 17: If  $p$  is a prime, then a  $p$ -group is a group whose order is a power of  $p$ .

THEOREM 22: If  $G$  is a  $p$ -group, then  $Z(G) \neq e$ .

PROOF: Suppose  $Z(G) = e$ . By class equation

$$[G:e] = [Z(G):e] + \sum h_i \quad \text{where } h_i \mid [G:e]$$

and  $h_i \neq 1$ .

$$\text{Therefore } [G:e] = 1 + \sum h_i$$

Since  $[G:e]$  is a power of  $p$  and each  $h_i$  is a power of  $p$  we get a contradiction.

Exercise 8. Let  $G$  be a group and  $H$  a subgroup of  $G$  such that  $H \subset Z(G)$ . Show that if  $G/H$  is cyclic then  $G$  is abelian. Deduce that a group of order  $p^2$  where  $p$  is a prime is abelian (use class equation).



Exercise 9. Let  $H$  be a subgroup of a group  $G$  and  $S$  a complex of  $G$ . A complex  $T$  in  $G$  is said to be conjugate to  $S$  relative to  $H$  if there exists an element  $h \in H$  such that  $T = hSh^{-1}$ . Show that the number of distinct conjugates relative to  $H$  is equal to  $[H:N(S) \cap H]$  where  $N(S)$  is the normalizer of  $S$  in  $G$ .

Exercise 10. Let  $G$  be an abelian group of order  $n$  and  $p$  a prime dividing  $n$ . Prove that  $G$  has an element of order  $p$ .

## 6. Sylow Theorems.

DEFINITION 18: Let  $G$  be a group of order  $n$ . Let  $p$  be a prime such that  $n = p^{\alpha}m$  where  $m$  and  $p$  are prime to each other i.e.  $(m,p)=1$ . Then a subgroup of order  $p^{\alpha}$  is called a p-sylow subgroup of  $G$ .

THEOREM 23: (First Sylow theorem). Let  $G$  be a group of order  $n$ . Let  $p$  be a prime such that  $p$  divides  $n$ ,  $n = p^{\alpha}m$ ,  $(m,p)=1$ . Then  $G$  has a subgroup of order  $p^{\alpha}$ .

PROOF: By induction on  $n$ . When  $n=2$ , the theorem is trivial. Now assume the theorem for all groups of order  $< n$ . Now suppose  $G$  has order  $n$ . If  $G$  has a proper subgroup of order divisible by  $p^{\alpha}$ , there is nothing to prove. Hence assume the contrary. Then the index of every proper subgroup of  $G$  is divisible by  $p$ . By class equation,



$n = [Z(G):e] + \sum h_i$  where each  $h_i$  is the index of a proper subgroup of  $G$  and hence is divisible by  $p$ . Since  $n$  is divisible by  $p$ , so is  $[Z(G):e]$ . By exercise 10,  $Z(G)$  has a subgroup  $K$  of order  $p$ .  $K$  is normal in  $G$ . The order of  $G/K$  is less than  $n$  and is divisible by  $p^{\alpha-1}$ . Then, by induction hypothesis,  $G/K$  has a subgroup  $H/K$  of order  $p^{\alpha-1}$ . Where  $H \supset K$  is a subgroup of  $G$ . Thus the order of  $H$  is  $p^\alpha$ .

COROLLARY: If  $G$  is a group of order  $n$  and  $p$  is a prime dividing  $n$ , then  $G$  has an element of order  $p$ .

THEOREM 24: (Second Sylow Theorem). Let  $G$  be a group of order  $n$  and  $p$  a prime dividing  $n$ . Let  $P$  be a  $p$  sylow subgroup of  $G$  and  $S$  a  $p$ -subgroup of  $G$ . Then  $S \cap P = S \cap N(P)$ .

PROOF: Let  $S' = S \cap N(P)$ . Since  $P \subset N(P)$ , we have  $S \cap P \subset S \cap N(P)$ . Now  $S'P$  is a subgroup of  $N(P)$ . Since  $P$  is a normal in  $N(P)$ ,  $P$  is normal in  $S'P$  also. Then by Theorem 13,

$$\frac{S'}{S' \cap P} = \frac{S'P}{P}$$

Since  $S' \subset S$ ,  $S'$  is a  $p$ -group. Thus  $\frac{S'}{S' \cap P}$  has order a power of  $p$ . Therefore  $\frac{S'P}{P}$  has order a power of  $p$ . But  $P$  is a  $p$ -sylow subgroup. Hence  $\frac{S'P}{P}$  has order not divisible by  $p$ . Thus  $\frac{S'P}{P}$  has order 1. Therefore  $\frac{S'}{S' \cap P}$  has order 1. This means  $S' = S' \cap P$  or  $S' \subset P$ . Hence  $S' \subset P \cap S$ . Therefore  $P \cap S = N(P) \cap S$ .

THEOREM 25: (Third Sylow Theorem). Let  $G$  be a group of order  $n$  and  $p$  a prime dividing  $n$ . Then

- (1) If  $S$  is a  $p$ -subgroup of  $G$ , then  $S$  is contained in a  $p$ -sylow subgroup of  $G$ .
- (2) any two  $p$ -sylow subgroups are conjugates
- (3) if a  $p$ -sylow subgroup of  $G$  is normal in  $G$ , it is the only  $p$ -sylow subgroup of  $G$ .
- (4) the number of  $p$ -sylow subgroup of  $G$  is  $1 \pmod{p}$ .

PROOF: Let  $P$  be a  $p$ -sylow subgroup of  $G$ . Let  $\mathcal{C}$  be the set of all conjugates of  $P$  in  $G$ . Let  $S$  be a  $p$ -subgroup of  $G$ . Define an equivalence relation on  $\mathcal{C}$  in relation to  $S$  by  $x \sim y$  if there exists  $s \in S$  such that  $y = sxs^{-1}$  for  $x, y \in \mathcal{C}$ . Notice that if  $W$  is a subset of  $G$  conjugate to some  $x \in \mathcal{C}$  relative to  $S$ , then  $W \in \mathcal{C}$ . Let  $X_1, X_2, \dots, X_k$  be a full set of representatives in  $\mathcal{C}$  of the equivalence classes. We can assume  $X_1 = P$  also  $X_i = x_i P x_i^{-1}$  for some  $x_i \in G$ . The number of elements in the conjugate classes of  $X_i$  is equal to

$$[S : S \cap N(X_i)]$$

The number of elements in  $\mathcal{C} = [G : N(P)]$

$$\text{Then } [G : N(P)] = \sum_{i=1}^k [S : S \cap N(X_i)]$$

Since  $X_i$  is conjugate to  $P$ , it is also a  $p$ -sylow subgroup of  $G$ . Then by Second Sylow Theorem  $S \cap N(X_i) = S \cap P$

$$\text{Therefore } [G : N(P)] = \sum_{i=1}^k [S : S \cap X_i]$$

Now  $[G : N(P)]$  is prime to  $p$  and  $[S : S \cap X_i]$

is a power of  $p$ . Thus there exists an integer  $i$  such



that  $[S:S \cap X_i] = 1$ . That is  $S = S \cap X_i$  or  $S \subset X_i$ . If  $S$  is a  $p$ -sylow subgroup then  $S = X_i$  and there is only one index  $i$  such that  $[S:S \cap X_i] = 1$ . For if  $[S:S \cap X_j] = 1$  also, then  $S \subset X_i$  and  $S \subset X_j$  and so  $X_i = S = X_j$ . Since  $S, X_i, X_j$  are of the same number of elements,  $[G:N(P)] =$  number of conjugates of  $P =$  the number of  $p$ -sylow subgroups of  $G$ . It follows from the above that this number is  $1 \pmod{p}$ .

Remark. Let  $G$  be a group of order  $n < \infty$ .  $p, q$  distinct primes dividing  $n$ .  $P$  is a  $p$ -sylow subgroup of  $G$  and  $Q$  is a  $q$ -sylow subgroup of  $G$ . If  $x \in P \cap Q$ ,  $x^{p^\beta} = e$  and  $x^{q^\gamma} = e$ . There exist integers  $r, s$  such that  $rp^\beta + sq^\gamma = 1$ . Then  $x = x^{p^\beta r + q^\gamma s} = x^{p^\beta r} x^{q^\gamma s} = e$ .

LEMMA: Let  $G$  be a finite group and  $P$  a sylow subgroup of  $G$ . Let  $H$  be a subgroup of  $G$  such that  $N(P) \subset H \subset G$ . Then  $H = N(H)$ .

PROOF: Enough to show that  $N(H) \subset H$ . Let  $x \in N(H)$ . Then  $xHx^{-1} = H$ . Now  $P \subset H$  so that  $xPx^{-1} \subset xHx^{-1} = H$ . Now  $P$  and  $xPx^{-1}$  are  $p$ -sylow subgroups of  $H$ . Hence they are conjugates in  $H$ . Therefore, there exists  $h \in H$  such that  $P = hxPx^{-1}h^{-1}$ . Therefore  $hx \in N(P) \subset H$ . Hence  $x \in H$ .

THEOREM 26: Let  $G$  be a group of order  $n$  and  $p$  a prime dividing  $n$ .  $n = p^x m$ ,  $(m, p) = 1$ . Then for  $y \leq x$  there exists a subgroup of  $G$  of order  $p^y$  and if  $y < x$  and if  $H$  is any subgroup of  $G$  of order  $p^y$ , then there exists a subgroup  $K \supset H$ ,  $H$



normal in  $K$  and the order of  $K$  is  $p^{\alpha+1}$ .

PROOF: There exists a  $p$ -sylow subgroup of  $G$  and the theorem is true for  $G$  if and only if it is true for this subgroup. Hence we assume  $G$  is a group of order  $p^\alpha$ . Then the theorem makes two assertions.

(1) there exists a chain of subgroups  $G \supset G_1 \dots \supset G_n = e$  such that  $G_{i+1}$  is normal in  $G_i$  and  $G_i/G_{i+1}$  is cyclic of order  $p$ .

(2) if  $H$  is a subgroup of  $G$ , there exists a chain as above for which  $H$  is one of the  $G_i$ 's. These two assertions are equivalent to the theorem.

We prove by induction on  $\alpha$ . If  $\alpha=0$  theorem is trivial. Hence assume theorem is true for all  $p$ -groups of order  $< p^\alpha$ .

(1)  $Z(G) \neq e$  since  $G$  is a  $p$ -group.  $Z(G)$  has a subgroup of order  $p$  (Call it  $G_{n-1}$ ) and  $G/G_{n-1}$  is a group of order  $p^{\alpha-1}$ . Hence by induction hypothesis we have a chain

$$\frac{G}{G_{n-1}} \supset \frac{G_1}{G_{n-1}} \supset \dots \supset \frac{G_{n-1}}{G_{n-1}} \text{ such that}$$

$\frac{G_i}{G_{n-1}}$  is normal in  $G_i/G_{n-1}$  and the order of  $\frac{G_i/G_{n-1}}{G_{i+1}/G_{n-1}}$

is  $p$ . But then  $G_{i+1}$  is normal in  $G_i$ . Furthermore

$\frac{G_i/G_{n-1}}{G_{i+1}/G_{n-1}} \cong \frac{G_i}{G_{i+1}}$ . Hence  $G_i/G_{i+1}$  is of order  $p$  and

$G \supset G_1 \supset \dots \supset G_{n-1} \supset e$  is the desired chain.

(2)  $H \supset H_1 \supset H_2 \dots \supset H_m = e$ ,  $H_{i+1}$  is normal in  $H_i$  and  $H_i/H_{i+1}$  is of order  $p$  by (1). If  $H \neq N(H)$ , then

we can find a similar chain in  $\frac{N(H)}{H}$  and lift it to  $N(H)$  obtaining

$$N(H) \supset K_1 \supset K_2 \supset \dots \supset H \supset H_1 \supset \dots \supset H_m = e$$

We repeat with  $N(H)$  until we reach a subgroup  $M$  such that  $M=N(M)$  by the finiteness of  $G$ . Now assume  $M=N(M)$ . Then  $Z(G) \subset N(M)=M$ . The group  $G/Z(G)$  has smaller order than  $G$  and  $M/Z(G)$  is a subgroup. If  $M \neq G$ , then we can find

$\frac{N}{Z(G)} \subset \frac{M}{Z(G)}$  such that the latter is normal in the former.

Then  $M$  is normal in  $N$  and  $M \neq N$  and  $N \subset N(M)$ , contradiction.

Hence  $M=G$ .

COROLLARY: Let  $G$  be a group of order  $p^x$ .  $H$  is a subgroup of order  $p^{x-1}$ . Then  $H$  is normal in  $G$ . If  $K$  is any proper subgroup of  $G$ , then  $K$  is contained in a maximal normal proper subgroup of  $G$ .

## 7. Permutation Groups.

DEFINITION 19: Let  $S_n$  denote the group of permutations on  $\{1, 2, \dots, n\}$ . A cycle in  $S_n$  is a permutation  $\sigma$  having the following properties.

(1) there exists a subset  $A$  of  $\{1, 2, \dots, n\}$  such that  $\sigma(A) \subset A$ ,  $\sigma$  moves every element in  $A$  and leaves fixed every element not in  $A$ .

(2) if  $x, y \in A$ , then there exists an integer  $i$  such that  $y = \sigma^i(x)$  and  $\sigma(A) = A$ .

If  $\sigma$  is a cycle, we denote the movable set by  $A_\sigma$ .

Notation:  $(i_1, i_2, \dots, i_k)$  denotes the cycle which sends  $i_1 \rightarrow i_2 \rightarrow i_3, \dots, i_{k-1} \rightarrow i_k$  and  $i_k \rightarrow i_1$ .

Two cycles  $\sigma$  and  $t$  are said to be disjoint if  $A_\sigma \cap A_t = \emptyset$ .

Remark: Disjoint cycles always commute.

THEOREM 27: Let  $\sigma$  be a cycle of order  $k$  and  $x \in A_\sigma$ . Then

$$(x, \sigma(x), \sigma^2(x), \dots, \sigma^{k-1}(x)) = \sigma$$

Conversely, if  $t = (x_1, x_2, \dots, x_k)$ , then  $t$  is a cycle of order  $k$ .

PROOF: Let  $\sigma$  be a cycle of order  $k$  and let  $x \in A_\sigma$  we shall show that

$$A_\sigma = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{k-1}(x)\}$$

If  $y \in A_\sigma$ , then by (2), there exists  $i$  such that  $y = \sigma^i(x)$ . Since  $i = jk + r$  where  $0 \leq r < k$ , we have  $\sigma^i = \sigma^{jk+r} = (\sigma^k)^j \cdot \sigma^r = \sigma^r$  so that  $y = \sigma^r(x)$ . Now we have to show that if  $y = \sigma^i(x)$ ,  $0 \leq i < k$ ,  $\sigma(y) \neq y$ . To this end, suppose  $\sigma^i(x) = \sigma^{i+1}(x)$  for some  $i < k$ . Let  $z \in \{1, 2, \dots, n\}$ . If  $z \notin A_\sigma$ , then  $\sigma^i(z) = z$ . If  $z \in A_\sigma$ , then  $z = \sigma^j(x)$  for some  $j$ .

Then

$$\begin{aligned} \sigma^i(z) &= \sigma^i(\sigma^j(x)) = \sigma^{i+j}(x) = \sigma^j(\sigma^i(x)) \\ &= \sigma^j(\sigma^{i+1}(x)) = \sigma^{i+1}(\sigma^j(x)) = \sigma^{i+1}(z) \end{aligned}$$

Therefore  $\sigma(z) = z$ .

Hence  $\sigma = I$ . contradiction.



Thus if  $y \in \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$ , then  $\sigma(y) \neq y$  so that  $y \in A_\sigma$ .

Let  $t = (x_1, x_2, \dots, x_k)$ . To show that  $t$  is a cycle of order  $k$ . Take  $x_2 = t(x_1)$ ,  $x_3 = t(x_2) = t^2(x_1)$ , .....

$$x_k = t(x_{k-1}) = t^{k-1}(x_1).$$

**THEOREM 28:** Every permutation can be uniquely (upto ordering) as a product of disjoint cycles.

**PROOF:** Let  $X = \{1, 2, \dots, n\}$  and  $t \in S_n$ . Define an equivalence relation  $\sim$  on  $X$  by  $x \sim y$  if and only if  $y = \sigma^j(x)$  for some integer  $j$ .  $\sim$  is an equivalence relation (Prove).

Let  $A_1, A_2, \dots, A_k$  be the equivalence classes of this relation. For given  $i$ ,  $0 \leq i \leq k$  define  $t_i$  by

$$t_i(x) = \begin{cases} t(x) & \text{for } x \in A_i \\ x & \text{for } x \notin A_i \end{cases}$$

Now if  $x \in A_i$ , then  $t(x)$  belongs to the same equivalence class as  $x$  which is  $A_i$ . Thus  $t(A_i) = A_i$ . Since  $A_i$  is finite and  $t$  is 1-1,  $t(A_i) = A_i$ . Now we show that  $t_i \in X$ . Suppose  $t_i(x) = t_i(y)$ .

Case (i). If  $x \in A_i$ , then  $x \sim t(x) = t_i(x) = t_i(y) \in A_i$ . If  $y \notin A_i$  then  $t_i(y) = y \notin A_i$  which is a contradiction. Thus  $y \in A_i$ . Then  $t_i(y) = t_i(x)$  gives  $t(y) = t(x)$ . Since  $t$  is one to one  $x = y$ .

Case (ii). If  $x \notin A_i$ , then  $t_i(y) = t_i(x) = x \notin A_i$ . If  $y \in A_i$ , then  $t_i(y) = t(y) \sim y$ . Therefore  $x = t_i(y) \in A_i$  contradiction. Hence  $y \notin A_i$ . Then  $x = t_i(y) = y$ .

Hence  $t_i$  is one to one. It is clearly onto. In

fact  $t_i$  is a cycle and  $A_{t_i} = A_i$ .

1) If  $x \notin A_i$ , then  $t_i(x) = x$ .

2) If  $x, y \in A_i$ , then there exists  $j$  such that  $y = t_i^j(x)$ . This is true on  $A_i$ , since  $t_i$  is the restriction of  $t$ .

3) Suppose  $t_i \neq I$ . Let  $x \in A_i$ . If  $t_i(x) = x$ ,  $t_i(y) = y$  for all  $y \in A_i$ . Then  $t_i = I$  which is a contradiction. Thus  $t_i(x) \neq x$ . Hence  $t_i$  is a cycle.

$$\text{Now } t = \prod_{i=1}^k t_i$$

Clearly  $t_i$ 's are disjoint. Let  $x \in X$ . Then  $x \in A_j$  for some  $j$ . Then

$$\left( \prod_{i=1}^k t_i \right) (x) = \left( \prod_{i \neq j} t_i \right) (t_j(x)) = t_j(x) = t(x)$$

It remains to show that this representation is unique apart from the order of the factors. Suppose

$$\prod_{i=1}^k t_i = \prod_{j=1}^m \sigma_j$$

Where  $\sigma_j \neq I$ ,  $t_i \neq I$  and  $\{t_i\}$  are disjoint cycles,  $\{\sigma_j\}$  are disjoint cycles. We show that

$t_i = \sigma_j$  for some  $j$ . Choose  $x \in A_i$ . Then

$$t_i(x) = \prod_{i=1}^k t_i(x) = t(x) = \sigma_j(x) \text{ for some } j.$$

Then

$$t_i^l(x) = \sigma_j^l(x) \text{ for all integers } l.$$

$$\text{Therefore } t_i = \sigma_j$$

Similarly each  $\sigma_j$  is a  $t_i$ .

Remark. If  $t = \prod_{i=1}^k t_i$  where  $t_i$ 's are disjoint cycles, then the order of  $t$  is the l.c.m. of the orders of  $t_i$ .

DEFINITION 20: A transposition is a cycle of length two i.e., a cycle of the form  $(x,y)$ .

Remark. Every permutation can be expressed as a product of transpositions. In fact

$$(x_1, x_2, \dots, x_k) = (x_1, x_2) (x_2, x_3) \dots (x_{k-1}, x_k)$$

DEFINITION 21: Set  $\text{Sgn} : S_n \rightarrow \{-1, 1\}$  by

$$\text{Sgn}(\sigma) = \prod_{\substack{i < j \\ i, j \in \{1, \dots, n\}}} \frac{\sigma(i) - \sigma(j)}{i - j}, \sigma \in S_n$$

$\sigma$  is odd if  $\text{Sgn}(\sigma) = -1$  and even if  $\text{Sgn}(\sigma) = 1$ .

$\text{Ker Sgn} = A_n =$  set of all even permutations in  $S_n$ .

Remark.1.  $\text{Sgn}(\sigma t) = \text{Sgn}(\sigma) \cdot \text{Sgn}(t)$ .

Remark.2.  $A_n$  is a normal subgroup of  $S_n$ . For, if  $\sigma = (1,2)$ , then  $\text{Sgn}(\sigma) = -1$  so that  $\text{Sgn}$  is onto  $\{1, -1\}$ .

Thus  $\frac{S_n}{A_n} \cong \{1, -1\}$ .  $A_n$  has thus index 2 and hence normal in  $S_n$ . Further order of  $A_n = \frac{n!}{2}$ .

Remark 3. If  $t$  is a transposition, then  $\text{Sgn}(t) = -1$ . This follows from the fact that

$t = (k,m) = (k,k+1)(k+1,k+2) \dots (m-1,m) (m-1,m-2) \dots (k+1,k)$   
which a product of an odd number of adjacent transpositions and  $\text{Sgn}(i,i+1) = -1$ .

Remark 4. If  $\sigma = (x_1, x_2, \dots, x_k)$  then  $\text{Sgn}(\sigma) = \pm 1$  according as  $k$  is odd or even, for  $(x_1, x_2, \dots, x_k) = (x_1, x_2) \cdot (x_2, x_3) \dots (x_{k-1}, x_k)$ .

Remark 5.  $A_n$  is generated by three-cycles. In fact every element of  $A_n$  can be expressed as a product of



three-cycles. Let  $\sigma \in A_n$ . Then  $\sigma$  is a product of transpositions and the number of terms must be even. Thus it is sufficient to prove that a product of two transpositions is either a three-cycle or a product of three-cycles. Consider  $(x_1, x_2)(x_3, x_4)$ .

(i) if  $(x_1, x_2)$  and  $(x_3, x_4)$  are disjoint, then

$$(x_1, x_2)(x_3, x_4) = (x_1, x_2, x_3)(x_2, x_3, x_4).$$

(ii) if  $x_2 = x_3$ ,  $x_4 \neq x_1$ , then  $(x_1, x_2) \cdot (x_3, x_4) = (x_1, x_2, x_4)$

(iii) if  $x_1 = x_3$ ,  $x_4 = x_1$ , then  $(x_1, x_2)^2 = I$ .

Remark 6.  $S_n$  is generated by  $(1, 2), (1, 3), \dots, (1, n)$ .

PROOF: Every element of  $S_n$  is a product of transpositions. Hence it is enough to show that every transposition can be written as a product of the above. We have seen that every transposition is a product of adjacent transpositions. Hence it is enough to prove for the transposition  $(i, i+1)$ .

$$(i, i+1) = (1, 2)(1, 3) \dots (1, i) \cdot (1, i+1) \cdot (1, i) \dots (1, 2)$$

THEOREM 29: If  $t \in S_n$ , then

$$t(x_1, x_2, \dots, x_k)t^{-1} = (tx_1, tx_2, \dots, tx_k).$$

PROOF: We shall prove that  $t(x_1, x_2, \dots, x_k) = (tx_1 \dots tx_k)t$ . Let  $x_i \in \{x_1, \dots, x_k\}$ . Then

$$t(x_1, x_2, \dots, x_k)(x_i) = \begin{cases} t(x_{i+1}) & i < k \\ t(x_1) & i = k \end{cases}$$

$$\text{and } (tx_1, tx_2, \dots, tx_k)t(x_i) = \begin{cases} t(x_{i+1}) & \text{if } i < k \\ t(x_1) & i = k \end{cases}$$

Suppose  $x \notin \{x_1, x_2, \dots, x_k\}$ . Then

$$t(x_1, x_2, \dots, x_k)(x) = t(x)$$

and  $(tx_1, tx_2, \dots, tx_k)t(x) = t(x)$  for if  $t(x) = t(x_1)$

then  $x = x_1$  which is a contradiction.

Exercise 11. Prove the following

- $S_n$  is generated by  $(1, 2)$  and  $(1, 2, \dots, n-1)$
- $A_n$  is generated by  $(1, 2, 2), (1, 2, 4), \dots, (1, 2, n)$
- $A_n$  is generated by 2 elements
  - by  $(1, 2, 3)$  and  $(1, 2, \dots, n)$  if  $n$  is odd
  - by  $(1, 2, 3)$  and  $(2, 3, \dots, n)$  if  $n$  is even.

THEOREM 30: If  $H$  is a normal subgroup of  $A_n$   
for  $n \geq 2$  and if  $H$  contains a three-cycle then  
 $H = A_n$ .

PROOF: When  $n=3$ ,  $H$  contains a three-cycle and its square and hence all three cycles. So  $H \supset A_n$  since  $A_n$  is given by three-cycles. Now suppose  $n > 3$ . We have  $(x_1, x_2, x_3) \in H$ . If  $x_1 \neq 1$ , we have

$$(x_1, 1, x_2)(x_1, x_2, x_3)(x_1, 1, x_2)^{-1} = (1, x_1, x_3) \in H.$$

If  $x_1$  or  $x_3 \neq 2$ , we have

$$(x_1, 2, x_3)(1, x_1, x_3)(x_1, 2, x_3)^{-1} = (1, 2, x_1) \in H.$$

If  $k \neq x_1, 1, 2$ , then we get

$$(2, k, x_1)(1, 2, x_1)(2, k, x_1)^{-1} = (1, k, 2) \in H$$

Now  $(1, k, 2) \in H \implies (1, 2, k) \in H$ .

But  $A_n$  is generated by  $\{(1, 2, k)\}$ . Hence  $H = A_n$ .

DEFINITION 22: A group  $G$  is said to be simple if  $G$  has no normal subgroup different from  $G$  and  $e$ .

THEOREM 31:  $A_n$  is a simple group if  $n \geq 5$ .

PROOF: Let  $H$  be a normal subgroup of  $A_n$ ,  $H \neq e$ . Let  $t$  be any element of  $H$  which is not the identity and which moves the smallest number of elements in  $\{1, 2, \dots, n\}$ .  $t$  moves more than two elements, since transpositions are odd.  $t$  moves more than three elements, since, otherwise,  $t$  is a three-cycle and  $H = A_n$  by Theorem 30. Thus  $t$  moves at least four elements.

Case (i).  $t$  is a product of disjoint cycles.

(a) If  $t$  is a product of two disjoint two cycles after renumbering, we can write  $t = (1, 2)(3, 4)$ . Let  $\sigma = (3, 4, 5)$ . Then  $t_1 = \sigma t \sigma^{-1} \in H$  and  $t^{-1} t_1 \in H$ . Now  $t_1 = (1, 2)(4, 5)$  and  $t^{-1} t_1 = (1, 2)(3, 4)(1, 2)(4, 5) = (3, 4, 5)$ .

Hence  $H = A_n$  contradiction.

(b)  $t = (1, 2)(3, 4)(5, 6)$  take  $\sigma = (3, 4, 5)$ . Then  $t_1 = \sigma t \sigma^{-1} \in H$  and  $t^{-1} t_1 \in H$ . Now  $t_1 = (1, 2)(4, 5)(3, 6)$  and  $t^{-1} t_1 = (3, 4)(5, 6) \in H$ . This moves fewer elements than  $t$ . Contradiction.

Case (2). If we write  $t$  as a product of disjoint cycles, there is one cycle of length  $\geq 3$ .

Note  $t$  must move at least 5 elements. If  $t$  moves only four elements, it is either a four-cycle which is odd



or a product of two two-cycles which we are assuming does not happen. Thus  $t=(1,2,3,\dots)$ . There exists  $x \in X$  such that  $x$  and  $t(x) \notin \{1,2,3\}$  and  $t(x) \neq x$ . Take a movable  $z \notin \{1,2,3\}$ . If  $t(z) \in \{1,2,3\}$  then  $t(z)=1$  and there exists a movable  $x$  such that  $x \notin \{1,2,3\}$  and for this  $x$ , we have a  $t(x)=y \notin \{1,2,3\}$  and  $y \neq x$ . Let  $x=4$  and  $y=t(x)=5$ . Let  $\sigma=(3,4,5)$   $t_1 = \sigma t \sigma^{-1} \in H$   $t_1=(1,2,4,\dots)$ . Therefore  $t_1 \neq t$ .  $t^{-1}t_1 \in H$  and  $t^{-1}t_1 \neq I$ . We assert that  $t^{-1}t_1$  moves fewer elements than  $t$ . First we notice that  $t^{-1}t_1(1)=1$ ,  $t(1) \neq 1$ . Let  $k > 5$ .

(i) Suppose  $t(k) > 5$ . Then

$$t^{-1}t_1(k) = t^{-1}\sigma t \sigma^{-1}(k) = t^{-1}\sigma t(k) = t^{-1}t(k) = k.$$

$t(k)=5$  does not happen since  $t(4)=5$ .

(ii) Suppose  $t(k) < 5$ .

In either case  $k$  is moved by  $t$ . Thus  $t^{-1}t_1$  moves fewer elements than  $t$ . For  $t$  moves  $1,2,3,4,5$  while  $t^{-1}t_1$  moves at most four of these since  $t^{-1}t_1(1)=1$  and for  $k > 5$ , if  $k$  is moved by  $t^{-1}t_1$  then  $t(k)$  is 1 or 4 so  $k$  is moved by  $t$ .

COROLLARY: If  $n \geq 4$ , then  $A_n$  is the only non-trivial normal subgroup of  $S_n$ .

PROOF: For  $n=1,2$ , theorem is trivial. For  $n=3$  or  $>4$ ,  $A_n$  is simple. Let  $H \neq e$  be normal subgroup of  $S_n$  and  $H \neq S_n$ . Then  $H \cap A_n$  is a normal subgroup of  $A_n$ . Hence  $H \cap A_n = A_n$  or  $e$ . If  $H \cap A_n = A_n$  then  $A_n \subseteq H$ . Since  $A_n$  has

index 2 and  $H \neq S_n$ ,  $A_n = H$ .

Suppose  $H \cap A_n = e$ . Now  $HA_n$  is a subgroup of  $S_n$ . Since  $H \subset HA_n$ , we have  $A_n \subsetneq HA_n \subset S_n$  we could conclude again that  $HA_n = S_n$ . Then

$$H \cong \frac{H}{H \cap A_n} \cong \frac{HA_n}{A_n} = \frac{S_n}{A_n}$$

Since  $A_n$  is of index 2,  $H$  is of order 2. This  $H$  is cyclic of order 2, generated by  $t$ . This  $t$  is a product of odd number of two-cycles since  $H \cap A_n = e$   $t = (1,2) \dots$ . Let  $\sigma = (1,2,3)$ . If  $t$  does not move 3,  $\sigma t \sigma^{-1} = (2,3) \dots \notin H \neq e$ . But  $\sigma t \sigma^{-1} = t$  since  $H$  is cyclic of order 2. Therefore  $t$  moves 3. Then  $t = (1,2)(3,4)$ ,  $\sigma t \sigma^{-1} = (2,3)(1,4)$ . But  $\sigma t \sigma^{-1} \neq t$  and yet  $\sigma t \sigma^{-1} \in H$  and so  $\sigma t \sigma^{-1} = t$ . Contradiction.

## 8. Direct Product

DEFINITION 23: Let  $G$  be a group and  $H, K$  subgroups of  $G$ . Then  $G$  is the direct sum (product) of  $H$  and  $K$  if

- (a)  $H$  and  $K$  are normal in  $G$
- (b)  $H \cap K = e$
- (c)  $G = HK$ .

THEOREM 32: A group  $G$  is a direct sum of two subgroups  $H$  and  $K$  if and only if

- (1)  $H$  and  $K$  commute elementwise i.e.,  $hk = kh$  for all  $h \in H, k \in K$ .
- (2) every element of  $G$  can be uniquely expressed as  $hk, h \in H, k \in K$ .



PROOF: Suppose  $G$  is a direct sum of  $H$  and  $K$ .  
 Let  $h \in H, k \in K$ . Then  $kh^{-1}k^{-1} \in H$  and hence  $hkh^{-1}k^{-1} \in H$ .  
 Similarly  $hkh^{-1}k^{-1} \in K$ . Thus  $hkh^{-1}k^{-1} \in H \cap K$ . By (b),  
 $hkh^{-1}k^{-1} = e$  so that  $hk = kh$ . This is (1). To prove (2), since  
 $G = HK$ , every element of  $G$  can be expressed in the form  $hk$ ,  
 $h \in H, k \in K$ . Suppose  $h_1k_1 = h_2k_2$ . Then  $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = e$ .  
 Therefore  $h_1 = h_2$  and  $k_1 = k_2$ .

Conversely, suppose the theorem holds. We shall show  
 that  $G$  is the direct sum of  $H$  and  $K$ . By 2),  $G = HK$ . By  
 1),  $H$  and  $K$  are normal in  $HK = G$ . Let  $x \in H \cap K$ . Then  
 $x = xe \in HK$  and  $x = ex \in HK$ . By uniqueness, we get  $x = e$ .  $\therefore H \cap K = e$ .

Exercise 12. Let  $G, G'$  be groups. Consider the pro-  
 duct  $G \times G' = \{(g, g') \mid g \in G, g' \in G'\}$ . Defining  $(g, g')(g_1, g'_1) =$   
 $(gg_1, gg'_1)$  for  $(g, g'), (g_1, g'_1) \in G \times G'$  show  $G \times G'$  is a  
 group.  $G \times G'$  is called the direct product of  $G$  and  $G'$ .  
 If  $G_1 = \{(g, e') \mid g \in G\}$ ,  $G'_1 = \{(e, g') \mid g' \in G'\}$ , show that  
 $G_1 \cong G$  and  $G'_1 \cong G'$ . Show further that  $G \times G'$  is the direct  
 sum of  $G_1$  and  $G'_1$ .

Exercise 13. Let  $G$  be a group that is a direct sum  
 of two subgroups  $H$  and  $K$ . Then  $G \cong H \times K$  under the isomor-  
 phism that sends  $H \rightarrow H_1$  and  $K \rightarrow K_1$  where  $H_1 = \{(h, e) \mid h \in H\}$   
 and  $K_1 = \{(e, k) \mid k \in K\}$ .

DEFINITION 24: Let  $G$  be a group with subgroups  
 $H_1, H_2, \dots, H_n$ . Then we say that  $G$  is a direct  
 product of the subgroups  $H_i$  if



- 1) the  $H_i$ 's are normal in  $G$
- 2)  $H_i \cap H_1 \dots \dots \widehat{H_i} \dots \dots H_n = e$
- 3)  $G = H_1 \dots \dots H_n$ .

THEOREM 33: Let  $G$  be a group with subgroups  $H_1, \dots, H_n$ . Then  $G$  is a direct product of  $H_1 \dots H_n$  if and only if

- (i) the elements of  $H_i$  commute with elements of  $H_j$  for  $i \neq j$ .
- (ii) every element  $x \in G$  can be uniquely written as  $x = h_1 h_2 \dots h_n$ ,  $h_i \in H_i$ .

PROOF: Proof itself as an exercise.

Exercise 14. Show that if  $G_1, \dots, G_n$  are groups then  $G_1 \times G_2 \times \dots \times G_n$  is a group under the componentwise multiplication. If

$$G_i' = e_1 \times e_2 \times \dots \times e_{i-1} \times G_i \times e_{i+1} \times \dots \times e_n$$

then  $G_i' \cong G_i$  and  $G_1 \times G_2 \times \dots \times G_n$  is a direct product of the subgroups  $G_i'$ .

Exercise 15. Let  $G$  be a direct product of the subgroups  $H_1, H_2, \dots, H_n$ . Then

- (i)  $G \cong H_1 \times H_2 \times \dots \times H_n$  under the isomorphism

$$H_i \longrightarrow H_i' = e_1 \times \dots \times H_i \times \dots \times e_n$$

- (ii)  $\frac{G}{H_1 \dots H_i} \cong H_{i+1} \dots H_n$

THEOREM 34: Let  $G$  be a finite group. Then every proper subgroup of  $G$  is different from its normalizer if and only if  $G$  is the direct product

of its sylow subgroups.

PROCF: Suppose every proper subgroup of  $G$  is different from its normalizer. Let  $P$  be a sylow subgroup of  $G$ . Then  $N(P)=N(N(P))$ .  $\therefore N(P)=G$  i.e.,  $P$  is normal in  $G$ .

Let  $P_1, P_2, \dots, P_n$  be the sylow subgroups of  $G$ . Then  $P_i \cap P_j = e$  for  $i \neq j$ . Let  $x \in P_i, y \in P_j$   $xy x^{-1}y^{-1} \in P_i \cap P_j = e$ .  $\therefore xy = yx$ . Also  $P_1 \dots P_n$  is a subgroup of  $G$ .  $P_1 \dots P_n \cong P_1 \times \dots \times P_n$ .  $\therefore P_1 \dots P_n$  has the same number of elements as  $G$ .  $\therefore G = P_1 \dots P_n$  and  $G$  is the direct product.

Conversely, suppose  $G$  is the direct product of its sylow subgroups. Let  $H \subset G$ . Let  $x \in H$ . Then  $x = x_1 x_2 \dots x_n$ , where  $x_i \in P_i, m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ . Let  $k = p_2^{\alpha_2} \dots p_n^{\alpha_n}$ . Then  $(p_1^{\alpha_1}, k) = 1$ . Therefore there exist integers  $s, r$  such that

$$sp_1^{\alpha_1} + rk = 1.$$

Then

$$x^k = x_1^k \dots x_n^k \text{ and } x_1 = x_1^{kr} x_1^{sp_1^{\alpha_1}} = x_1^{rk} \in H.$$

Thus every component of  $x$  is in  $H$ . Let  $H_i = H \cap P_i$ .  $H_i$  is a normal subgroup of  $P_i$ . Then

$$H = H_1 \times H_2 \times \dots \times H_n.$$

Since  $H$  is a proper subgroup, there exists  $H_i \neq P_i$ .

Therefore  $H_i \neq N(H_i)$  in  $P_i$ . Therefore

$$H \subset (H_1 \times H_2 \times \dots \times N(H_i) \times \dots \times H_n) \subset N(H)$$

$$\therefore H \neq N(H).$$

9. Jordan Holder Series.

DEFINITION 25: Let  $G$  be a group. A subinvariant series  $\Sigma$  for  $G$  is a chain of subgroups

$$G = G_0 \supset G_1 \supset \dots \supset G_n = e$$

such that  $G_{i+1}$  is normal in  $G_i$ . If each  $G_i$  is normal in  $G$ , then  $\Sigma$  is called a normal series.

A subinvariant series  $\Sigma$  is called a Jordan Holder Series if each  $G_i / G_{i+1}$  is a simple group. Two subinvariant series

$$\Sigma : G = G_0 \supset G_1 \supset \dots \supset G_n = e$$

and

$$\Sigma' : G = G'_0 \supset G'_1 \supset \dots \supset G'_m = e$$

are said to be isomorphic if  $n=m$  and if there exists a permutation  $\sigma$  of the integers  $1, 2, \dots, n$  such that

$$\frac{G_{\sigma(i)}}{G_{\sigma(i)+1}} \cong \frac{G'_i}{G'_{i+1}}$$

Remark: Two groups can have isomorphic JH-series without being isomorphic.

DEFINITION 26: Let  $\Sigma, \Sigma'$  be subinvariant series for  $G$ .  $\Sigma'$  is said to be a refinement of  $\Sigma$  if every  $G_i$  is a  $G'_j$  for some  $j$ .  $\Sigma'$  is a proper refinement of  $\Sigma$  if there exists a  $G'_j$  which is not a  $G_i$ . A subinvariant series is said to be proper if  $G_i / G_{i+1} \neq e$  for all  $i$ .



THEOREM 35: Let  $\Sigma$  be a proper subinvariant series for the group  $G$ . Then  $\Sigma$  is a J.H series if and only if  $\Sigma$  has no proper refinements.

PROOF: Let  $\Sigma: G = G_0 \supset G_1 \supset \dots \supset G_n = e$

Suppose  $\Sigma$  has no proper refinement. If  $G_i/G_{i+1}$  is not simple then it has a proper normal subgroup  $H/G_{i+1}$ . Then

$$G = G_0 \supset G_1 \supset \dots \supset G_i \supset H \supset G_{i+1} \supset \dots \supset G_n = e$$

is a proper refinement. Contradiction.

2) Suppose  $\Sigma$  is a JH series. If  $\Sigma$  has a proper refinement, there exists an index  $i$  and a subgroup  $H$  of  $G$  such that  $G_i \supset H \supset G_{i+1}$  and  $H$  is normal in  $G_i$ . Then  $H/G_{i+1}$  is a proper normal subgroup of  $G/G_{i+1}$ , which is a contradiction to the simplicity.

THEOREM 36: Let  $G$  be a group. Suppose

$$\Sigma_1: G = G_0 \supset G_1 \supset \dots \supset G_n = e$$

and

$$\Sigma_2: G = H_0 \supset H_1 \supset \dots \supset H_m = e$$

are two subinvariant series for  $G$ . Then  $\Sigma_1, \Sigma_2$  have isomorphic refinements.

PROOF: Define  $G_{i,j} = G_{i+1} (G_i \cap H_j)$

$$\text{and } H_{j,i} = H_{j+1} (H_j \cap G_i)$$

1)  $G_{i,j+1}$  is a normal subgroup of  $G_{i,j}$  and

$H_{j,i+1}$  is a normal subgroup of  $H_{j,i}$ . (Prove).

Define  $\Sigma'_1 =$  the chain  $\{G_{i,j}\}$  ordered lexicographically

and  $\Sigma'_2 =$  the chain  $\{H_{j,i}\}$  ordered lexicographically.

2) Then  $\Sigma'_1$  is a refinement of  $\Sigma_1$ , and  $\Sigma'_2$  is a refinement of  $\Sigma_2$ . Further

$$G_{i,0} = G_{i+1} (G_i \cap H_0) = G_{i+1} G_i = G_i$$

$$\text{and } G_{i,m} = G_{i+1} (G_i \cap H_m) = G_{i+1} e = G_{i+1} = G_{i+1,0}$$

$\therefore$  Similarly  $H_{0,j} = H_j$  etc.

3)  $\Sigma'_1$  and  $\Sigma'_2$  have the same number of terms viz.  $nm+1$ .

4) Let  $L = G_{i+1}$ ,  $K = G_i \cap H_j$ ,  $M = G_i \cap H_{j+1}$ . Then  $M \subset K$  and  $M$  is normal in  $K$ . Then  $ML \subset KL$  and  $ML$  is normal in  $KL$ . Also

$$\frac{KL}{ML} \cong \frac{K}{M(L \cap K)}$$

Now

$$KL = G_{i+1} (G_i \cap H_j) = G_{i,j}$$

$$ML = G_{i+1} (G_i \cap H_{j+1}) = G_{i,j+1}$$

$\therefore G_{i,j+1}$  is normal in  $G_{i,j}$

$$\begin{aligned} \frac{G_{i,j}}{G_{i,j+1}} &\cong \frac{G_i \cap H_j}{(G_i \cap H_{j+1}) (G_{i+1} \cap G_i \cap H_j)} \\ &= \frac{G_i \cap H_j}{(G_i \cap H_{j+1}) (G_{i+1} \cap H_j)} \end{aligned}$$

Similarly

$$\frac{H_{j,i}}{H_{j,i+1}} \cong \frac{H_j \cap G_i}{(H_j \cap G_{i+1}) (H_{j+1} \cap G_i)}$$

This completes the proof.

THEOREM 37: Any two J.H. series for a group are isomorphic.

PROOF: If  $\Sigma_1, \Sigma_2$  are J.H. series, let  $\Sigma'_1, \Sigma'_2$  be isomorphic refinements.  $\Sigma'_1$  is obtained from  $\Sigma_1$  by repetitions. Similarly  $\Sigma'_2$  is obtained from  $\Sigma_2$  by repetitions. The number of repetitions in  $\Sigma'_1$  is equal to the number of zero factor groups in  $\Sigma'_1$  or  $\Sigma'_2$  = number of repetitions in  $\Sigma_2$ . Throwing away repetitions we preserve isomorphism, to reduce to  $\Sigma_1 \cong \Sigma_2$

COROLLARY 1: If a group G has a proper infinite subinvariant series it does not have a J.H. series.

COROLLARY 2: If an abelian group G has an element of infinite order, then G does not have a J.H. series.

COROLLARY 3: Let G be a finite direct product of simple subgroups. Then these subgroups are unique. This means if  $G = H_1 H_2 \dots H_n = K_1 K_2 \dots K_m$  are two direct product representations of G where  $H_i, K_j$  are simple, then  $m = n$  and there exists a permutation  $(1, \dots, n)$  such that  $H_i = K_{\sigma(i)}$

To prove this, one has only to note that

$$G = H_1 \dots H_n \supset H_1 \dots H_{n-1} \supset H_1 \dots H_{n-2} \supset \dots \\ \dots \supset H_1 \supset e$$

and

$$G = K_1 \dots K_m \supset K_1 \dots K_{m-1} \supset K_1 \dots K_{m-2} \supset \dots \supset K_1 \supset e$$



are two J.I. series with the corresponding factor groups  $H_i$ ,  $K_j$  are simple.

10. Solvable groups.

DEFINITION 27: A group  $G$  is said to be solvable if there exists a subinvariant series  $\{G_i\}$  such that the factor groups are abelian. That is

$$G \supset G_1 \supset \dots \supset G_n = e$$

where  $G_{i+1}$  is normal in  $G_i$  and  $G_i/G_{i+1}$  is abelian.

THEOREM 38: For  $n > 4$ ,  $S_n$  is not solvable.

PROOF: Exercise.

THEOREM 39 : Let  $H$  be a normal subgroup of a group  $G$ . Then  $G$  is solvable if and only if  $H$  and  $G/H$  are solvable.

PROOF: Suppose  $G$  is solvable. Then  $\Sigma$  and  $G \supset H \supset e$  have isomorphic refinements. Hence it is sufficient to show that a refinement of a series with abelian factors has abelian factors. Suppose  $H \supset K$  is normal and  $H/K$  is abelian. Further suppose  $H \supset L \supset K$  where  $K$  is normal in  $L$ ,  $L$  is normal in  $H$ . Now  $\frac{L}{K} \subset \frac{H}{K}$  implies  $\frac{L}{K}$  is abelian. Then

$$\frac{H}{L} = \frac{H/K}{L/K} \text{ is also abelian.}$$

Thus  $H$  is solvable. Then

$$G = G_0 \supset G_1 \supset \dots \supset H \supset H_1 \supset \dots \supset e$$

Then

$$\frac{G_i/H}{G_{i+1}/H} \cong \frac{G_i}{G_{i+1}} \quad \text{which is abelian}$$

Thus

$$\frac{G}{H} \supset \frac{G_1}{H} \supset \dots \supset \frac{H}{H} = \{e\} \text{ has abelian}$$

factors so that  $G/H$  is also solvable.

Conversely, suppose  $H$  and  $\frac{G}{H}$  are both solvable.

$$\text{Then } \frac{G}{H} \supset \frac{G_1}{H} \supset \dots \supset \frac{H}{H} = e \quad \text{and} \quad H \supset H_1 \supset \dots \supset e$$

These have abelian factors. Then

$G \supset G_1 \supset G_2 \supset \dots \supset H \supset H_1 \supset \dots \supset e$  is a sub-invariant series with abelian factors. This completes the proof.

**THEOREM 40:** The following are equivalent for a group  $G$ .

- 1)  $G$  is solvable
- 2)  $G$  has a normal series with abelian factors, that is,  $G = H_0 \supset H_1 \supset \dots \supset H_m \supset e$  where  $H_i$  is normal in  $G$  and  $H_i/H_{i+1}$  is abelian
- 3) there exists an integer  $t$  such that  $G^t = e$  where  $G' = [G, G]$ ,  $G^i = [G^{i-1}, G^{i-1}]$ .

PROOF: Exercise.

Exercise 14. Let  $G$  be a group with a J.H series. Show that  $G$  is solvable if and only if  $G$  has a normal series whose factor groups are cyclic of prime order.

## RINGS AND MODULES

1. Rings.

DEFINITION 1: A ring  $R$  is a nonempty set with two binary operations  $+$  and  $\cdot$  such that

1.  $R$  is an abelian group under  $+$
2.  $R$  is a semigroup under  $\cdot$ .
3. if  $a, b, c$  are any elements of  $R$ , then

$$a(b+c) = ab + ac$$

$$(a+b)c = ac + bc$$

The identity for the additive group is called the zeroelement of the ring and is denoted by  $0$ . It then follows that  $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in R$ . The identity for multiplication, if it exists is denoted by  $1$  and is called the identity of the ring. If  $R$  has  $1$ , we say that  $R$  is a ring with identity.  $R$  is said to be commutative if  $ab = ba$  for all  $a, b \in R$ .

Example 1: 1. The set of all integers  $Z$  is a commutative ring with  $1$  under the usual addition and multiplication.

2. If  $C[0,1]$  denotes the set of all continuous functions on  $[0,1]$ , defining addition and multiplication by

$$(f+g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

for all  $x \in [0,1]$ , where  $f, g \in C[0,1]$ , then  $C[0,1]$  is a commutative ring with  $1$ .



DEFINITION 2: Let  $R$  be a ring. An element  $a \neq 0$  of  $R$  is called a left zero divisor if there exists  $b \neq 0$ ,  $b \in R$  such that  $ab = 0$  and a right divisor of zero if  $ba = 0$ . A commutative ring with 1 is called an integral domain if it has no zero divisors. A skew-field (or division ring) is a ring in which the non-zero elements form a group under multiplication and a commutative skewfield is known as a field

Example: The set of all rational numbers under the usual addition and multiplication is a field.

THEOREM 1: A finite commutative ring without divisors of zero is a field

PROOF: Let  $R$  be a finite commutative ring with no zero divisors. This means that if  $a, b \in R$  and  $ab = 0$  then either  $a = 0$  or  $b = 0$ . Let  $D = \{x_1, x_2, \dots, x_n\}$  denote the nonzero elements of  $R$ . Then the hypothesis implies that  $D$  is a semi-group under multiplication satisfying cancellation laws and hence is a group by Theorem 2, chapter 1.

COROLLARY: If  $p$  is a prime number and  $\mathcal{I}_p$  is the ring of integers (mod  $p$ ), then  $\mathcal{I}_p$  is a field

2. Ideals.

DEFINITION 3: A subset  $A$  of a ring  $R$  is called a subring of  $R$  if  $a, b \in A$  implies  $a-b \in A$  and  $ab \in A$ . A subring  $I$  of  $R$  is called a left ideal of  $R$  if  $RI = \{rs \mid r \in R, s \in I\} \subset I$  and a right ideal of  $R$  if  $IR \subset I$ .  $I$  is a two-sided ideal if it is both a left ideal and a right ideal and is called an ideal of  $R$ .

Exercise 1: Show that the intersection of an arbitrary family of left ideals of  $R$  is a left ideal of  $R$  and the union of a simply ordered chain of left ideals of  $R$  is also a left ideal of  $R$ .

DEFINITION 4: Let  $S$  be a subset of a ring  $R$ . Then the left ideal  $I_S$  generated by  $S$  is the intersection of all left ideals of  $R$  containing  $S$ .

THEOREM 2: Let  $S$  be a subset of a ring  $R$ . Then the left ideal  $I_S$  generated by  $S$  is the set

$$I = \left\{ ns + \sum_{i=1}^f r_i s_i \mid n \in \mathbb{Z}, s, s_i \in S, r_i \in R \right\}$$

where  $f$  over the  $\Sigma$  indicates finite sum.

PROOF: Let  $\bar{I}_S$  denote the left ideal generated by  $S$ . clearly  $T \subset \bar{I}_S$ . To complete the proof, it is enough to show that  $T$  is a left ideal of  $R$ . It is clearly a subgroup of  $R$ . If  $r \in R$ , then  $r(\sum \gamma_i s_i) = \sum (r\gamma_i) s_i$  which is again an element of  $T$ . Thus  $T$  is a left ideal of  $R$ .

DEFINITION 5: A left ideal  $J$  of a ring  $R$  is called a maximal left ideal if (i)  $J \neq R$  and (ii)  $J \subset I$  where  $I$  is a left ideal of  $R$  such that  $I \neq R$  implies  $J = I$ . A left ideal  $I$  of  $R$  is said to be proper if  $I \neq R$ .

DEFINITION 6: An element  $a$  of a ring  $R$  is called a unit if it has a multiplicative inverse in  $R$ .

THEOREM 3: If  $R$  is a ring with 1 and  $I$  is a left ideal of  $R$  then  $I = R$  if it contains a unit.

PROOF: If  $a \in I$  is a unit, then  $a^{-1} \in R$  so that  $1 = a^{-1} \cdot a \in I$ . Now if  $r \in R$ , then  $r = r \cdot 1 \in I$  and hence  $R \subset I$ .

THEOREM 4: If  $R$  is a ring with 1, then every left ideal is contained in a maximal left ideal

PROOF: Let  $\mathcal{C}$  be the collection of all left ideals of  $R$  which contains the left ideal  $I$ . This collection is not empty since  $I \in \mathcal{C}$  and is partially ordered by inclusion. Now  $1$  remains outside every ideal and the union of all ideals which belong to a totally ordered set is again a left ideal. Thus by Zorn's lemma  $\mathcal{C}$  contains a maximal element.



Let  $I$  be an ideal of a ring  $R$ . Since  $I$  is a subgroup of the abelian group  $R$ , the quotient group  $R/I$  is also an abelian group. Each element of  $R/I$  is called a residue class modulo  $I$ . Now we define a multiplication in  $R/I$  by

$$(x+I)(y+I) = xy+I$$

Assuming for a moment, that this multiplication is well-defined, it is easy to verify that  $R/I$  is ring and is called the quotient ring. Further if  $R$  is commutative, so is  $R/I$ . If  $R$  has an identity, so does  $R/I$ .

Now to verify that this multiplication is well-defined, we choose arbitrary elements  $p, q$  in  $I$ . Then, by distributive laws it follows that

$$(x+p)(y+q) = xy + xq + py + pq \in xy + I$$

since  $I$  is an ideal. This proves that the multiplication is independent of the coset representation and our assertion is proved.

**THEOREM 5:** Let  $R$  be a commutative ring with 1.

Suppose  $I$  is an ideal of  $R$ . Then  $I$  is maximal if and only if  $R/I$  is a field.

PROOF: Suppose  $I$  is maximal in  $R$ . Then  $R/I$  has at least two elements. Let  $\bar{R} = R/I$ . We must show that if  $\bar{r}$  is a nonzero element in  $\bar{R}$ , then there exists  $\bar{s}$  such that  $\bar{r} \cdot \bar{s} = \bar{1}$ . Since  $\bar{r} \neq \bar{0}$   $r \notin I$ . Consider the ideal generated by  $r$  and  $I$  which we denote by  $(r, I)$ . Every element in  $(r, I)$  is of the form  $sr+n$  where  $s \in R$  and  $n \in I$ . Since  $I$  is maximal and  $I \subsetneq (r, I)$  we must have  $(r, I) = R$ . Since  $1 \in R$ , there exists  $s \in R$  so that we have the representation

$$1 = sr+n.$$

It then follows  $1-sr = n \in I$  so that  $1+I = sr+I = (s+I)(r+I)$ . Hence  $R/I$  is a field.

Conversely, suppose that  $R/I$  is a field. Assume  $I$  is not maximal. We shall arrive at a contradiction. Now there must exist an ideal  $M$  such that  $I \subset M \subset R$  and  $I \neq M$ ,  $M \neq R$ . Let  $a \in R$  and  $b \in M$ ,  $b \notin I$ . Since  $\bar{R}$  is a field, there exists  $c \in R$ , such that  $\bar{b} \bar{c} = \bar{a}$  which implies  $bc+I = a+I$ . Since  $b \notin I$ ,  $b+I \neq I$ . Since  $bc - a \in I \subset M$ , we have  $bc + M = a + M$ . But  $b \in M$ . Therefore  $bc+M = M$ . Hence  $a \in M$ . Thus  $M = R$ . This gives a contradiction. Hence  $I$  must be maximal.

DEFINITION 6: Let  $R$  be a ring and  $P$  an ideal of  $R$ .

$P$  is called a prime ideal if  $ab \in P$  implies  $a \in P$  or  $b \in P$ .

THEOREM 6: Let  $R$  be a commutative ring with 1 and let  $P$  be an ideal of  $R$ . Then  $R/P$  is an integral domain if and only if  $P$  is a prime ideal.

PROOF: Exercise.

It follows from Theorems 5 and 6 that in a commutative ring with 1 every maximal ideal is also a prime ideal.

### 3. Homomorphisms.

DEFINITION 7: Let  $R$  and  $R'$  be rings. A mapping  $f : R \rightarrow R'$  is called a homomorphism if

$$f(a+b) = f(a) + f(b)$$

and  $f(ab) = f(a) \cdot f(b)$

for all  $a, b \in R$ . The notions of epi-, mono, and isomorphisms are similarly defined. The kernel of  $f$  is defined by

$$\text{Ker } f = \{ r \in R \mid f(r) = 0 \}$$

THEOREM 7: Let  $R$  and  $R'$  be rings and  $f: R \rightarrow R'$  a homomorphism. Then

- 1)  $\text{Im}(f) = f(R)$  is a subring of  $R'$
- 2)  $\text{Ker } f = f^{-1}(0)$  is an ideal of  $R$

PROOF: Exercise.



Consider an ideal  $I$  of a ring  $R$ . Then there is a natural map (canonical map)

$$\phi : R \rightarrow R/I$$

defined by  $\phi(r) = r+I$   $r \in R$ .

$\phi$  is clearly an epimorphism of the abelian group of  $R$  onto the abelian group of  $R/I$ . With  $\text{Ker } \phi = I$ , we can say more. In fact, if  $r, s \in R$ , then

$$\phi(rs) = rs+I = (r+I) \cdot (s+I) = \phi(r) \phi(s)$$

which means that  $\phi$  is actually a ring homomorphism.

Exercise 2: Let  $R, R'$  be rings and  $f: R \rightarrow R'$  a homomorphism with  $\text{Ker } f = I$ . Then there exists a unique homomorphism

$$\tilde{f} : \frac{R}{I} \rightarrow R'$$

such that the diagram

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \phi \searrow & & \nearrow \tilde{f} \\ & \frac{R}{I} & \end{array}$$

commutes. That is  $\tilde{f}\phi = f$  where  $\phi : R \rightarrow R/I$  is the canonical map. If  $f$  is onto, then  $\tilde{f}$  is an isomorphism ( $\tilde{f}$  is called the induced map)

All isomorphism laws which we proved for groups also hold for rings.

DEFINITION 8: A ring  $R$  is said to be imbedded in a ring  $R'$  if there exists an isomorphism of  $R$  onto a subring of  $R'$ .

THEOREM 8: Every ring without identity can be imbedded in a ring with identity.

PROOF: Let  $R$  be a ring without identity and  $Z$  denote the ring of integers. Consider the product  $R \times Z = \{(r,m) \mid r \in R, m \in Z\}$ , We make  $R \times Z$  a ring by defining addition and multiplication by

$$(r,m) + (s,n) = (r+s, m+n)$$

$$(r,m) \cdot (s,n) = (rs + nr + ms, mn)$$

for  $r, s \in R$  and  $m, n \in Z$ . Then  $R \times Z$  is a ring with identity  $(0,1)$ . And  $R \times \{0\}$  is a subring of  $R \times Z$ . Now  $R$  and  $R \times \{0\}$  are naturally isomorphic via the isomorphism given by

$$R \rightarrow R \times \{0\}$$

i.e.,

$$r \rightarrow (r, 0)$$

The details are left for the reader.

DEFINITION 9: Let  $R$  be an integral domain. Then a quotient field of  $R$  is a pair  $(F, f)$  where  $F$  is a field and  $f: R \rightarrow F$  is a monomorphism such that for every monomorphism  $g: R \rightarrow D$ , where  $D$  is a division ring, there exists a unique homomorphism  $h: F \rightarrow D$  such that the diagram

$$\begin{array}{ccc}
 R & \xrightarrow{f} & F \\
 \searrow g & & \swarrow h \\
 & & D
 \end{array}$$

commutes.

THEOREM :9: Let  $R$  be an integral domain. Then there exists a field of quotients of  $R$ . Further if  $(F, f)$  and  $(F', f')$  are two fields of quotients of  $R$ , then there exists an isomorphism  $j: F \rightarrow F'$ , such that the diagram

$$\begin{array}{ccc}
 F & \xrightarrow{j} & F' \\
 \swarrow f & & \searrow f' \\
 & & R
 \end{array}$$

commutes.



PROOF: Let  $R^*$  denote the set of all nonzero elements of  $R$  and consider the Cartesian product  $R \times R^*$ . Then the elements of  $R \times R^*$  are of the form  $(x, y)$  where  $y \neq 0$ . Let us define an equivalence relation  $\sim$  in  $R \times R^*$  as follows: If  $(x_1, y_1)$  and  $(x_2, y_2)$  are any two elements in  $R \times R^*$ , we define

$$(x_1, y_1) \sim (x_2, y_2)$$

if and only if  $x_1 y_2 = x_2 y_1$ . Now we assert that  $\sim$  is an equivalence relation.

- 1)  $(x, y) \sim (x, y)$  is trivial.
- 2) if  $(x_1, y_1) \sim (x_2, y_2)$ , then  $x_1 y_2 = x_2 y_1$ , so that  $(x_2, y_2) \sim (x_1, y_1)$  also.
- 3) if  $(x_1, y_1) \sim (x_2, y_2)$  and  $(x_2, y_2) \sim (x_3, y_3)$ , we have  $x_1 y_2 = x_2 y_1$  and  $x_2 y_3 = x_3 y_2$  so that

$$x_1 y_2 y_3 = x_2 y_1 y_3 = y_1 (x_2 y_3) = y_1 x_3 y_2 = x_3 y_1 y_2.$$

Since  $y_2$  is not 0 and  $R$  has no divisors of zero, it follows that  $x_1 y_3 = x_3 y_1$ . Hence  $(x_1, y_1) \sim (x_3, y_3)$ .

Let  $F$  denote the set of all equivalence classes in  $R \times R^*$  of  $\sim$ . and the equivalence class which contains the elements  $(x, y)$  is denoted by  $\frac{x}{y}$  and is called the quotient

of  $x$  over  $y$ . If  $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in F$ , then the addition and multiplication are defined by

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} = \frac{x_1 y_2 + x_2 y_1}{y_1 y_2}$$

and

$$\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} = \frac{x_1 x_2}{y_1 y_2}$$

It is easy to verify that these are independent of the representatives of the equivalence classes and  $F$  is a commutative ring with identity. The zero element of  $F$  is the equivalence class consisting of the elements of the form  $(x, y)$  where  $x = 0$  and identity is the class consisting of all  $(x, y)$  such that  $x = y$ . It now remains to show that  $F$  is a field. To prove it is enough to show that every nonzero element of  $F$  is a unit. Let  $\frac{x}{y}$  be a nonzero element of  $F$ . Then  $x \neq 0$  and thus  $\frac{y}{x} \in F$ . From the commutativity and the definition of multiplication, it follows that

$$\frac{x}{y} \cdot \frac{y}{x} = \frac{xy}{xy} = 1$$

This completes the proof that  $F$  is a field.

Now the desired monomorphism  $f: R \rightarrow F$  is defined by

$$f(x) = \frac{x}{1} \in F, \quad x \in R$$

Now we shall show that  $(f, f)$  is a quotient field of  $R$ . To this end, let  $D$  be any skewfield and  $g: R \rightarrow D$  a monomorphism since  $g(y) \neq 0$  for  $y \neq 0$ , we are in a position to define a map

$$k: R \times R^* \rightarrow D$$

by

$$k(x, y) = [g(x)] [g(y)]^{-1} \quad (x, y) \in R \times R^*$$

one can verify that  $k$  is well-defined. Now  $h: f \rightarrow D$  is defined by

$$h\left(\frac{x}{y}\right) = k(x, y).$$

We assert that  $h$  is a homomorphism. Suppose  $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in F$ .

Then

$$\begin{aligned} h\left(\frac{x_1}{y_1} + \frac{x_2}{y_2}\right) &= h\left(\frac{x_1 y_2 + x_2 y_1}{y_1 y_2}\right) = g(x_1 y_2 + x_2 y_1) [g(y_1 y_2)]^{-1} \\ &= g(x_1) \cdot g(y_2) + g(x_2) g(y_1) [g(y_1)]^{-1} [g(y_2)]^{-1} \\ &= g(x_1) g(y_2)^{-1} + g(x_2) g(y_1)^{-1} \\ &= h\left(\frac{x_1}{y_2}\right) + h\left(\frac{x_2}{y_1}\right) \end{aligned}$$



and

$$\begin{aligned} h\left(\frac{x_1}{y_1} \cdot \frac{x_2}{y_2}\right) &= h\left(\frac{x_1 x_2}{y_1 y_2}\right) = g(x_1 x_2) \cdot g(y_1 y_2)^{-1} \\ &= g(x_1)g(x_2) g(y_1)^{-1}g(y_2)^{-1} \\ &= g(x_1)g(y_1)^{-1} g(x_2)g(y_2)^{-1} \\ &= h\left(\frac{x_1}{y_1}\right) \cdot h\left(\frac{x_2}{y_2}\right) \end{aligned}$$

Further if  $x \in R$ , then

$$hf(x) = h\left(\frac{x}{1}\right) = g(x) \cdot [g(1)]^{-1} = g(x)$$

and hence  $hf = g$ .

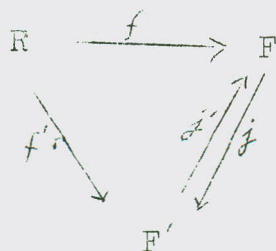
Now we shall show that  $h$  is unique. To this end let us suppose that  $h'$  be any homomorphism of  $F$  into  $D$  such that  $h'f = g$ .

If  $\frac{x}{y} \in F$ , then

$$h'\left(\frac{x}{y}\right) = g(x)g(y)^{-1} = h(x/y)$$

Hence  $h' = h$ .

To complete the proof, let us suppose that  $(F, f)$  and  $(F', f')$  are two fields of quotients of  $R$ . Consider the diagram



Since  $(F, f)$  is a field of quotients of  $R$ , there exists

$j' : F' \rightarrow F$  such that  $j' \cdot f' = f$ . Similarly there exists  $j : F \rightarrow F'$  such that  $jf = f'$ . Here  $j, j'$  are homomorphisms.

Now  $jj'f' = jf = f'$  and  $j'jf = j'f' = f$ . so that by the uniqueness of the maps.  $jj'$  is identity on  $F'$  and  $j'j$  is the identity on  $F$ . Thus  $j$  is an isomorphism.

#### 4. Principal ideal ring

DEFINITION 10: A ring  $R$  is called a principal ideal ring if

- 1)  $R$  is an integral domain
- and 2) every ideal of  $R$  is generated by a single element.

Example:  $\mathbb{Z}$  is a principal ideal ring.

PROOF: Let  $I$  be an ideal of  $\mathbb{Z}$ . Let  $a$  be the smallest positive integer such that  $a \in I$ . If  $b$  is any other element of  $I$ , there exist integers  $q$  and  $r$  such that

$$b = aq + r \text{ where } 0 \leq r < a.$$

Since  $I$  is an ideal,  $r = b - aq \in I$ .  $\therefore r = 0$ . Otherwise contradicts the choice of  $a$ . Hence every element  $b \in I$  is of the form  $a \cdot q$ . Hence  $I$  is generated by  $a$ .

DEFINITION 11: An integral domain  $R$  is called a euclidean ring if there exists a function  $\varphi$  which maps  $R - \{0\}$  into nonnegative integers such that if  $a$  and  $b$  any two nonzero elements of  $R$  there exists elements  $q, r \in R$  such that  $a = bq + r$  and either  $r = 0$  or  $\varphi(r) < \varphi(b)$ .

Example:  $\mathbb{Z}$  with  $\varphi =$  absolute value.

THEOREM 10: A euclidean ring is a principal ideal ring.

PROOF: Let  $I$  be an ideal of a euclidean ring  $R$ .  $I \neq 0$ . Let  $a \neq 0$  be an element of  $I$  such that  $\varphi(a)$  is minimum. Let  $b \in I$ . Then there exist  $q, r \in R$  such that  $b = aq + r$ . either  $r = 0$  or  $\varphi(r) < \varphi(a)$ . Now  $\varphi(r) < \varphi(a)$  contradicts the choice of  $a$ . So  $r = 0$  and  $b = qa \in Ra$ .

DEFINITION 12: An element  $p$  in a ring  $R$  is called a prime element if  $p = ab$  implies either  $a$  or  $b$  is a unit.

DEFINITION 13: Let  $a, b \in R$ . We say that  $d$  is a g.c.d. of  $a, b$  if

- (1)  $d$  divides  $a$  and  $b$  i.e.  $a = rd, b = sd, r, s \in R$ .
- (2) if  $c$  divides  $a$  and  $b$ , then  $c$  divides  $d$ .



$m$  is an l.c.m. of  $a$  and  $b$  if

- (1)  $a$  and  $b$  divide  $m$
- (2) if  $a$  and  $b$  divide  $n$ , then  $m$  divides  $n$

Notation:  $a \mid_r$  means  $a$  divides  $r$ .

THEOREM 11: Let  $R$  be a principal ideal ring. Any two elements  $a$  and  $b$  of  $R$  have a g.c.d. of the form  $ra+sb$  where  $r, s \in R$  and an l.c.m.

PROOF: The ideal  $(a, b)$  generated by a single element  $d$ . Then  $d = ra+sb$  for some  $r, s \in R$ . Now  $(a) \subset (d)$  which implies  $d \mid a$ . Similarly  $d \mid b$ . Now suppose  $c \mid a$  and  $c \mid b$ . Then  $(a) \subset (c)$  and  $(b) \subset (c)$ .  $\therefore (d) = (a, b) \subset (c)$ ,  $\therefore c \mid d$ .

Thus  $d$  is the g.c.d. of  $a$  and  $b$ .

Also  $(a) \cap (b)$  is generated by a single element  $m$ .

$(m) \subset (a)$   $\therefore a \mid m$ . Similarly  $b \mid m$ . Now suppose  $a \mid n$ ,  $b \mid n$ . Then  $(n) \subset (a) \cap (b) = (m)$ .

$\therefore m \mid n$

Hence  $m$  is an l.c.m.

Remark: g.c.d. and l.c.m., when they exist, are unique.

Exercise 3: Let  $R$  be an integral domain and  $a, b \in R$ . Then  $(a) = (b)$  if and only if  $a = ub$  where  $u$  is a unit.

DEFINITION 14: Let  $R$  be a principal ideal ring and  $a, b \in R$ .  $a, b$  are relatively prime if  $(a, b) = R$ , that is, there exist,  $r, s \in R$  such that  $1 = ra + sb$ . We write  $(a, b) = 1$ .

THEOREM 12: Let  $R$  be a principal ideal ring and  $a, b, c \in R$  such that  $(a, c) = 1$ . If  $a | bc$  then  $a | b$ .

PROOF: There exist  $r, s \in R$  such that  $1 = ra + sc$ . Then  $b = rab + sbc$  which implies  $a | b$ .

COROLLARY: If  $p \in R$  is a prime element and  $p | ab$  then then  $p | a$  or  $p | b$ .

Exercise 4: Let  $R$  be a principal ideal ring and  $I$  an ideal of  $R$  with generator  $x$ . Then  $I$  is a prime ideal if and only if  $x$  is a prime element

Exercise 5: Show that in a principal ideal ring every prime ideal is maximal.

DEFINITION 15: A ring  $R$  is said to satisfy ascending chain condition (A.C.C.) on ideals if every chain of ideals

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

reduces to equality at some stage.

DEFINITION 16: Let  $R$  be a commutative ring with 1.  $R$  satisfies maximal condition (M.C.) on ideals if every nonempty family of ideals of  $R$  has a maximal element.

DEFINITION 17: Let  $R$  be a commutative ring with 1.  $R$  is said to satisfy finite basis condition (F.B.C.) if every family of ideals of  $R$  is finitely generated.

THEOREM 13: Let  $R$  be a commutative ring with 1. The following conditions on ideals are equivalent.

- 1) A.C.C.
- 2) M.C.
- 3) F.B.C.

PROOF: 1)  $\implies$  2). Assume (1). Let  $\mathcal{C}$  be the collection of ideals of  $R$ . Choose  $I_1 \in \mathcal{C}$ . If  $I_1$  is not maximal in  $\mathcal{C}$ , there exists  $I_2 \in \mathcal{C}$  such that  $I_1 \subset I_2$ . Inductively we choose a chain of ideals

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

By A.C.C. we must reach a maximal element.

2)  $\implies$  3). Assume (2). Let  $I$  be an ideal of  $R$ . Let  $\mathcal{C}$  be the collection of all finitely generated ideals of  $R$  contained in  $I$ . Then  $\mathcal{C}$  has a maximal element. Say  $J$ . Now  $J$  is generated by a finite number of elements say  $x_1, x_2, \dots, x_n$ .



Suppose  $J \neq I$ . Take  $x \in I - J$ . Then if  $J_1 = (J, x)$ , then  $J_1$  is generated by  $x_1, \dots, x_n$  and  $x$ . Since  $J_1$  is contained in  $I$  it contradicts the maximality of  $J$ .

3)  $\implies$  1). Assume 3). Let

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

be an ascending chain of ideals. Let  $I = \bigcup I_j$ . Then  $I$  is generated by a finite number of elements,  $x_1, x_2, \dots, x_k$ .

There exists an integer  $N$  such that  $x_1, x_2, \dots, x_k \in I_N$  and then  $I \subset I_N$ . This implies

$$I_N = I_{N+1} = \dots$$

DEFINITION 13: A commutative ring with 1 which satisfies any one and all the conditions of Theorem 13. is called a Noetherian ring.

Example: A principal ideal ring is Noetherian.

THEOREM 14: In a principal ideal ring every element different from zero can be expressed as a product of primes. This factorization is unique apart from the unit factors and the order of the factors.

PROOF: Let  $\mathcal{E}$  be the collection of ideals generated by elements which are not products of primes. Suppose  $\mathcal{E} \neq \varnothing$ . Choose 'a' such that (a) is maximal in the collection  $\mathcal{E}$ . 'a' is not a unit  $\therefore a = b \cdot c$  where b and c are not units. Then  $(a) \subset (b)$  and  $(a) \subset (c)$ . Therefore  $(b) \notin \mathcal{E}, (c) \notin \mathcal{E}$ . Thus b and c are products of primes. Then  $a = bc$  is again a product of primes. We have a contradiction  $\therefore \mathcal{E} = \varnothing$ .

Now suppose  $p_1 p_2 \dots p_n = q_1 \dots q_m$  where p's and q's are primes. Now  $p_1$  must divide some  $q_j$ . Since  $X$  is commutative, we assume that  $p_1 | q_1$ . Then  $q_1 = u_1 \cdot p_1$  where  $u_1 \in R$ . Since  $R$  has no divisors of zero, it follows from  $p_1 p_2 \dots p_n = u_1 p_1 q_2 \dots q_m$  that  $p_2 \dots p_n = u_1 q_2 \dots q_m$  since p's and q's are primes  $u_1$  is a unit. Repeating the argument we notice that  $m \leq n$  and  $q_i = u_i p_i, i = 1, 2, \dots, m$  and

$$1 = u_1 u_2 \dots u_m q_{m+1} \dots q_n.$$

where  $u_i$ 's are units. Since q's are not units, we must have  $m = n$ . This completes the proof.

5. Modules.

All rings under consideration will be assumed to have 1.

DEFINITION 19: Let  $R$  be a ring. A nonempty set  $M$  is called a left  $R$ -module (a left module over  $R$ ) if

- (1)  $M$  is an abelian group under  $+$ .
- (2) there exists a map  $\mathcal{F} : R \times M \rightarrow M$  written

$$\mathcal{F}(r, m) = rm \text{ satisfying.}$$

$$r(m_1 + m_2) = rm_1 + rm_2, \quad r \in R, \quad m_1, m_2 \in M$$

$$(r+s)m = rm + sm, \quad r, s \in R, \quad m \in M$$

$$r(sm) = (rs)m, \quad r, s \in R, \quad m \in M$$

$$1 \cdot m = m, \quad 1 \in R$$

A right  $R$ -module is defined similarly. The mapping  $\mathcal{F}$  is called the module multiplication of  $M$  by  $R$ .

Examples: 1:1. a ring  $R$  can be thought of as a module over itself.

2. an (additive) abelian group is a module over the ring of integers  $\mathbb{Z}$ .

Let  $M$  and  $T$  be left  $R$  modules. Suppose  $f: M \rightarrow T$  is a mapping of  $M$  into  $T$ . Then  $f$  is called a linear map (or an  $R$ -homomorphism) if  $f$  is a homomorphism of the additive group of  $M$  into the additive group of  $T$  such that

$$f(rm) = rf(m), \quad r \in R, \quad m \in M.$$



The notions of epi-, mono- and isomorphisms are defined with their obvious meaning.

Let  $M$  be a left  $R$ -module and  $N$  a subset of  $M$ .  $N$  is called a submodule of  $M$  if

- (1)  $N$  is a subgroup of the additive group of  $M$ .
- (2)  $r \in R, n \in N$  imply  $rn \in N$ .

Notice that when  $R$  is considered as a left  $R$ -module each submodule is a left ideal of  $R$ .

If  $N$  is a submodule of a left  $R$ -module  $M$ , we can form the factor module  $M/N$ , the cosets of  $N$  in  $M$ .  $M/N$  is a group. The module multiplication is defined by

$$r(m+N) = rm+N \quad r \in R, m \in M.$$

If  $m' \in N$ , it follows that

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

so that this multiplication is well defined. The map

$$\varphi : M \rightarrow M/N$$

given by  $\varphi(m) = m+N$  is a linear map which is called the canonical map.

DEFINITION 20: Let  $M$  and  $T$  be left  $R$  modules and  $f: M \rightarrow T$  an  $R$ -homomorphism. Then we define

$$\begin{aligned} \text{Ker } f &= \{ m \in M \mid f(m) = 0 \} \\ \text{Im } f &= \{ t \in T \mid \text{there exists } m \in M \text{ such that } f(m) = t \}. \end{aligned}$$

$\text{Ker} f$  and  $\text{Im} f$  are submodules of  $M$  and  $T$  respectively.  
We also define

$$\text{Coker } f = T/\text{Im} f$$

$$\text{Co-im} f = M/\text{Ker} f$$

**THEOREM 15:** Let  $f: M \rightarrow N$  be an epimorphism where  $M$  and  $N$  are left  $R$ -modules. Then the induced map

$$f^* : \frac{M}{\text{Ker} f} \rightarrow N$$

is an isomorphism and  $\text{Coim} f \cong \text{Im} f$ .

**PROOF:** Exercise.

**Exercise 6:** Show that the intersection of an arbitrary family of submodules of a left  $R$ -module  $M$  is again a submodule of  $M$ . Defining the submodule  $M$  generated by a set  $S$  in  $M$  to be the intersection of all submodules containing  $S$ , show that

$$M_S = \left\{ \sum r_i s_i \mid s_i \in S, r_i \in R \right\}$$

**DEFINITION 21:** A sequence of left  $R$  modules and maps

$$\cdots \rightarrow A_n \xrightarrow{f_n} A_{n-1} \xrightarrow{f_{n-1}} A_{n-2} \rightarrow \cdots$$

is said to be exact if  $\text{Im} f_n = \text{Ker} f_{n-1}$  for all  $n$ .

Examples: 1. Let  $N$  be submodule of the left  $R$ -module  $M$ . Let  $i : N \rightarrow M$  to be injection i.e.  $i(n) = n$  and  $\varphi : M \rightarrow M/N$  to be the canonical map. Then

$$0 \rightarrow N \xrightarrow{i} M \xrightarrow{\varphi} M/N \rightarrow 0$$

is exact.

2. Let  $f : M \rightarrow N$  be a homomorphism of  $R$ -modules. Then

$$0 \rightarrow \text{Ker } f \xrightarrow{i} M \xrightarrow{f} N \rightarrow \text{Coker } f \rightarrow 0$$

is exact

Exercise 7: Show that if  $0 \rightarrow A' \xrightarrow{f} A \xrightarrow{g} A'' \rightarrow 0$  is exact, then  $A' \cong f(A')$  and  $A'' \cong A/f(A')$

## 6. Direct product and direct sum

DEFINITION 22: Let  $M$  be a left  $R$ -module and  $\{N_\alpha\}$

a family of submodules of  $M$ . Then  $M$  is the direct sum of the  $N_\alpha$ 's if every element  $x \in M$  can be written uniquely as a finite sum

$$x = x_{\alpha_1} + x_{\alpha_2} + \dots + x_{\alpha_n}, \quad x_{\alpha_i} \in N_{\alpha_i}$$

THEOREM 16: Let  $M$  be a left  $R$ -module and  $\{N_\alpha\}$  a family of submodules of  $M$ . Then  $M$  is the direct sum of the  $N_\alpha$ 's if and only if

(1) if  $N_1, N_2, \dots, N_n$  is any finite subfamily of  $\{N_\alpha\}$ , then

$$N_1 \cap (N_1 + N_2 + \dots + \widehat{N_1} + \dots + N_n) = 0$$

(2)  $M = \Sigma N_\alpha$ , the submodule generated by  $\{N_\alpha\}$



PROOF: Suppose  $M$  is the direct sum of the  $N_{\alpha}$ 's.

Clearly  $M = \sum N_{\alpha}$ . This proves (2). Now suppose

$N_i \cap (N_1 + \dots + \widehat{N_i} + \dots + N_n) \neq \emptyset$ . Let

$x_{\alpha_i} \in N_{\alpha_i} \cap (N_1 + \dots + \widehat{N_i} + \dots + N_n)$ . Then there exist elements  $x_{\alpha_j} \in N_{\alpha_j}$ , such that

$$x_{\alpha_i} = x_{\alpha_1} + \dots + x_{\alpha_{i-1}} + 0 + x_{\alpha_{i+1}} + \dots + x_{\alpha_n}$$

and  $x_{\alpha_i} = 0 + \dots + 0 + x_{\alpha_i} + 0 + \dots + 0$

Thus we have two different representations from  $x_{\alpha_i}$  contradiction

Conversely, suppose (1) and (2) are satisfied. Now if  $i \neq j$ , then

$$N_i \cap N_j \subset N_i \cap (N_1 + \dots + \widehat{N_i} + \dots + N_j + \dots + N_n) = 0$$

Let  $x \in N_{\alpha}$ . If  $x = x_{\alpha_1} + \dots + x_{\alpha_n}$  and  $x = y_{\alpha_1} + \dots + y_{\alpha_n}$

are two representations for  $x$ , then

$$\begin{aligned} x_{\alpha_i} - y_{\alpha_i} &= y_{\alpha_1} - x_{\alpha_1} + \dots + y_{\alpha_{i-1}} - x_{\alpha_{i-1}} + y_{\alpha_{i+1}} - x_{\alpha_{i+1}} + \\ &\quad \dots - x_{\alpha_{i+1}} + \dots + y_{\alpha_n} - x_{\alpha_n} \end{aligned}$$

Since  $N_i \cap N_j = 0$  for  $i \neq j$ , we have  $x_{\alpha_i} = y_{\alpha_i}$ .

Hence the representation is unique and the sum is direct.

Notation: Let  $A$  be an  $R$ -module. Let  $S$  be a subset of  $R$  and  $T$  a subset of  $A$ . Then we set

$$ST = \left\{ \sum s_i t_i \mid s_i \in S, t_i \in T \right\}$$

DEFINITION 23: Let  $\{M_\alpha\}_{\alpha \in \mathcal{A}}$  be a family of left  $R$ -modules. Then the cartesian product  $\prod_\alpha M_\alpha$  is the set  $\left\{ f \mid f: \mathcal{A} \rightarrow \bigcup_\alpha M_\alpha \text{ such that } f(\alpha) \in M_\alpha \right\}$ . Then  $\prod_\alpha M_\alpha$  becomes a left  $R$ -module when addition and module multiplication are defined by

$$(f+g)(\alpha) = f(\alpha) + g(\alpha)$$

$$(rf)(\alpha) = r \cdot f(\alpha) \quad r \in R, \alpha \in \mathcal{A}$$

where  $f, g \in \prod_\alpha M_\alpha$ .  $\prod_\alpha M_\alpha$  is called the direct product of the  $M_\alpha$ 's. Let  $\sum_\alpha \oplus M_\alpha$  denote the subset of  $\prod_\alpha M_\alpha$  consisting of those functions  $f$  such that there exists a finite set of indices  $\alpha_1, \dots, \alpha_n$  such that  $f(\beta) = 0$  for  $\beta \neq \alpha_i, i = 1, 2, \dots, n$ . Then  $\sum_\alpha \oplus M_\alpha$  is a submodule of  $\prod_\alpha M_\alpha$  and is called the direct sum of the  $M_\alpha$ 's.

For each  $x_\alpha \in M_\alpha$ , we have a map  $f_\alpha: \mathcal{A} \rightarrow \bigcup_\alpha M_\alpha$  defined by  $f_\alpha(\alpha) = x_\alpha$  and  $f_\alpha(\beta) = 0$  for  $\beta \neq \alpha$ . Then for each  $\alpha$ , we have maps

$$j_\alpha: M_\alpha \longrightarrow \prod_\alpha M_\alpha$$

$$\text{and } p_\alpha: \prod_\alpha M_\alpha \longrightarrow M_\alpha$$

defined by

$$j_\alpha(x_\alpha) = f_\alpha, \quad x_\alpha \in M_\alpha$$

$$\text{and } p_\alpha(f) = f(\alpha)$$

Now  $p_\alpha j_\alpha(x_\alpha) = p_\alpha(f_\alpha) = f_\alpha(\alpha) = x_\alpha$  for all  $x_\alpha \in M_\alpha$

and  $p_\beta j_\beta(x_\beta) = p_\beta(f_\beta) = f_\beta(\alpha) = 0$  for all  $x_\beta \in M_\beta$

Thus we have

$$M_\alpha \xrightarrow{j_\alpha} \prod_\alpha M_\alpha \xrightarrow{p_\beta} M_\beta$$

where  $p_\beta p_\alpha = \delta_{\beta\alpha}$

Now  $\text{Im}(j_\alpha) \subset \sum_\alpha \oplus M_\alpha$ . Further if  $p_\alpha | \sum_\alpha \oplus M_\alpha$  is also denoted by  $p_\alpha$ , we have

$$M_\alpha \xrightarrow{j_\alpha} \sum_\alpha \oplus M_\alpha \xrightarrow{p_\beta} M_\beta$$

DEFINITION:24 Let  $M$  be a left  $R$ -module. A family of maps  $M_\alpha \xrightarrow{h_\alpha} M \xrightarrow{k_\beta} M_\beta$  is called a direct family if  $k_\beta h_\alpha = \delta_{\beta\alpha}$



THEOREM 17: Let  $M$  be a left  $R$ -module and  $\{M_\alpha\}_{\alpha \in \mathcal{A}}$  a family of left  $R$ -modules. Then  $M \cong \prod_{\alpha} M_\alpha$  if and only if there exists a family of maps  $h_\alpha: M \rightarrow M_\alpha$  such that

(1)  $h_\alpha(a) = h_\alpha(a')$  for all  $\alpha$  implies  $a = a'$

(2) Given any left  $R$ -module  $N$  and a family of maps  $k_\alpha: N \rightarrow M_\alpha$  there exists a map  $k: N \rightarrow \prod_{\alpha} M_\alpha$  such that the diagram

$$\begin{array}{ccc}
 M & \xrightarrow{h_\alpha} & M_\alpha \\
 & \swarrow k_\alpha & \nearrow k'_\alpha \\
 & N &
 \end{array}$$

commutes for each  $\alpha$ .

PROOF:  $\Rightarrow$  Suppose  $k_\alpha: N \rightarrow M_\alpha$  are given consider the diagram

$$\begin{array}{ccc}
 \prod_{\alpha} M_\alpha & \xrightarrow{p_\alpha} & M_\alpha \\
 & \swarrow k & \nearrow k_\alpha \\
 & N &
 \end{array}$$

define  $k : N \rightarrow \prod_{\alpha} M_{\alpha}$  as follows. For each  $b \in N$ ,  $k_{\alpha}(b) \in M_{\alpha}$ .

Now let  $f \in \prod_{\alpha} M_{\alpha}$  such that  $f(\alpha) = k_{\alpha}(b)$ . Now define

$$k(b) = f.$$

Then

$$p_{\alpha}k(b) = p_{\alpha}(f) = f(\alpha) = k_{\alpha}(b)$$

Then  $k$  is an  $R$ -homomorphism and the diagram commutes.

Consider the diagram.

$$\begin{array}{ccc} \prod_{\alpha} M_{\alpha} & \xrightarrow{f_{\alpha}} & M_{\alpha} \\ \swarrow h & & \searrow h_{\alpha} \\ & & M \end{array}$$

$\nearrow k$

By the above, there exists  $h : M \rightarrow \prod_{\alpha} M_{\alpha}$  such that  $p_{\alpha}h = h_{\alpha}$ .

By definition there exists  $k : \prod_{\alpha} M_{\alpha} \rightarrow M$  such that  $h_{\alpha}k = p_{\alpha}$ .

If  $f \in \prod_{\alpha} M_{\alpha}$ , then  $hk(f) \in \prod_{\alpha} M_{\alpha}$ .

$$\text{Now } p_{\alpha}hk(f) = h_{\alpha}k(f) = p_{\alpha}(f)$$

$$hk(f) = f \quad fg = 1 \text{ on } \prod_{\alpha} M_{\alpha}$$

For each  $m \in M$ ,  $kh(m) \in M$ . Then

$$h_{\alpha}kh(m) = p_{\alpha}h(m) = h_{\alpha}(m), \text{ for all } \alpha$$

$$kh(m) = m \text{ which implies } kh = 1 \text{ on } M.$$

$$h : M \rightarrow \prod_{\alpha} M_{\alpha} \text{ is an isomorphism}$$

THEOREM 18: Given a family of left R-modules

$\{M_\alpha\}_{\alpha \in I}$  and a left R-module  $M$ . Then  $M$  is isomorphic to  $\sum_{\alpha} (+)M_\alpha$  if and only if there exists a family of maps  $h_\alpha: M_\alpha \rightarrow M$  such that

1) every element of  $M$  can be written in the form

$\sum_{\alpha} h_\alpha(x_\alpha)$  (finite sum) where  $x_\alpha \in M_\alpha$

2) if  $N$  is any left R-module with family  $k_\alpha: M_\alpha \rightarrow N$

then there exists  $k: M \rightarrow N$  such that the diagram

$$\begin{array}{ccc}
 M & \xleftarrow{h_\alpha} & M_\alpha \\
 & \searrow k & \downarrow k_\alpha \\
 & & N
 \end{array}$$

commutes for all  $\alpha$ .

PROOF: (1) Let  $M = \sum_{\alpha} (+)M_\alpha$ . Define

$$h_\alpha: M_\alpha \rightarrow \sum_{\alpha} (+)M_\alpha$$

$$\text{by } h_\alpha(x_\alpha) = f_\alpha$$

Clearly every element of  $M$  can be written in the form  $\sum h_\alpha(x_\alpha)$ , finite sum. Suppose there exist  $k_\alpha: M_\alpha \rightarrow N$ . Define

$k: M \rightarrow N$  as follows.



If  $x \in M$ , then  $x = \sum h_\alpha(x_\alpha)$  uniquely.

Let  $k(x) = \sum k_\alpha(x_\alpha) \in N$ .  $k$  is easily seen to be a homomorphism and  $kh(x_\alpha) = k_\alpha(x_\alpha)$  for all  $x_\alpha \in M_\alpha$  and the diagram commutes

(2) Suppose  $M$  has the properties (1) and (2)



Let  $x \in \sum_\alpha (+) M_\alpha$ . Then

$$x = \sum i_\alpha(x_\alpha)$$

$$\begin{aligned} kh(x) &= kh(\sum i_\alpha(x_\alpha)) = \sum kh \cdot i_\alpha(x_\alpha) = \sum kh_\alpha(x_\alpha) \\ &= \sum i_\alpha(x_\alpha) = x \end{aligned}$$

$$kh = 1 \text{ on } \sum (+) M_\alpha$$

Let  $x \in M$ . Then  $x = \sum h_\alpha(x_\alpha)$  so that

$$hk(x) = \sum hk h_\alpha(x_\alpha) = \sum h i_\alpha(x_\alpha) = \sum h_\alpha(x_\alpha) = x$$

$$hk = 1 \text{ on } M$$

$h$  is an isomorphism.

**THEOREM: 19:** Let  $\{M_\alpha\}_{\alpha \in \sigma}$  be a family of left R-modules and  $M$  a left R-module. Suppose there exists a direct family of maps

$$M_\alpha \xrightarrow{j_\alpha} M \xrightarrow{h_\beta} M$$

such that  $h_\beta j_\alpha = \delta_{\beta\alpha}$ . Then

1)  $M \cong \prod_{\alpha} M_{\alpha}$  if and only if for any  $f \in \prod_{\alpha} M_{\alpha}$  there exists a unique element  $x \in M$  such that  $p_{\alpha}(x) = f(\alpha)$  for all  $\alpha$

2)  $M \cong \sum_{\alpha} (\oplus) M_{\alpha}$  if and only if any element  $x \in M$  can be written in the form

$$x = \sum_{\alpha} r_{\alpha} (x_{\alpha}) \quad (\text{finite sum})$$

PROOF: Exercise.

## 7. Free Modules.

DEFINITION 25: Let  $M$  be a left  $R$ -module. A subset  $\{x_{\alpha}\}$  of elements of  $M$  is called free if any finite relation of the form

$$\sum_{i=1}^n r_i x_{\alpha_i} = 0 \quad r_i \in R$$

implies  $r_i = 0$  for  $i = 1, 2, \dots, n$ . A left  $R$ -module  $M$  is called a free  $R$ -module if it has a free generating set. A left  $R$ -module  $M$  is called cyclic if there exists  $x \in M$  such that  $M = R_x$ .

Exercise 8: Let  $F = \sum_{\alpha} \oplus F_{\alpha}$  where each  $F_{\alpha}$  is a cyclic  $R$ -module isomorphic to  $R$ . Show that  $F$  is a free  $R$ -module with basis  $\{f_{\alpha}\}$  where  $f_{\alpha} : R \rightarrow \bigcup_{\alpha} F_{\alpha}$  such that  $f_{\alpha}(\alpha) = x_{\alpha}$  and  $f_{\alpha}(\beta) = 0$  for  $\beta \neq \alpha$  and such that  $x_{\alpha}$  is a generator of  $F_{\alpha}$ .

Exercise 9: Let  $M$  be left  $R$  module which is free suppose  $\{x_\alpha\}_{\alpha \in \mathcal{A}}$  be a free basis for  $M$ . For each  $\alpha$ , let  $R_\alpha$  be a cyclic  $R$ -module isomorphic to  $R$  with generator  $y_\alpha$ . Let  $F = \Sigma \bigoplus R_\alpha$ . Show that  $M \cong F$  under an isomorphism which maps  $x_\alpha$  into  $y_\alpha$ .

THEOREM 20:  $R \times$  is free if and only if there exists  
 $g: R_x \rightarrow R$  such that  $g(x) = 1$  and  $g$  is an isomorphism.

PROOF: Suppose  $g: R_x \rightarrow R$  is an isomorphism and  $g(x) = 1$ . Let  $r \in R$  such that  $rx = 0$ . Then  $0 = g(rx) = rg(x) = r$ . So  $x$  is a free generator of  $R_x$ .

Conversely, suppose  $R_x$  is free. Define  $g: R_x \rightarrow R$  by  $g(rx) = r$ .  $g$  is well-defined for if  $rx = r's$ , then  $(r-r')x=0$ , which implies  $r = r'$ . Further  $g(r_1x+r_2x) = g(r_1+r_2)x = r_1+r_2 = g(r_1x)+g(r_2x)$  and  $g(srx) = sr = s.g(rx)$ . It is clearly onto. If  $0 = g(rx) = r$ , then  $rx = 0$ .

THEOREM 21: Let  $F$  be a free  $R$ -module with free basis  
 $\{x_\alpha\}$  . Let  $M$  be an  $R$ -module and

$$g : x_\alpha \longrightarrow M.$$

is any map. Then  $g$  can be extended uniquely to an  
 $R$ -homomorphism.

$$f : F \rightarrow M.$$



PROOF: Let  $x \in F$ . Then  $x = \sum_{\alpha} x_{\alpha}$ . Define  $f(x) = \sum_{\alpha} g(x_{\alpha})$ . Since the above representation for  $x$  in terms of  $x_{\alpha}$ 's is unique,  $f$  is well-defined. Check that  $f$  is a homomorphism clearly  $f(x_{\alpha}) = g(x_{\alpha})$

THEOREM 22: Let  $M$  be a left  $R$ -module. Then there exists a free  $R$ -module  $F$  and an epimorphism  $f: F \rightarrow M$

PROOF: Let  $\{y_{\alpha}\}_{\alpha \in \sigma}$  be a basis of  $M$ . Let  $F$  be the free module on the generators  $\{x_{\alpha}\}_{\alpha \in \sigma}$ . Define  $g(x_{\alpha}) = y_{\alpha}$ .  $g$  extends to  $f: F \rightarrow M$ . Clearly onto  $M$ .

Exercise 10: Consider the diagram

$$\begin{array}{ccccc} & & A & & \\ & & \downarrow f & & \\ B & \xrightarrow{g} & C & \longrightarrow & 0 \end{array}$$

where the bottom row is exact. Show that if  $A$  is free, there exists  $h: A \rightarrow B$  such that  $gh = f$ .

THEOREM 23: Let  $R$  be an integral domain.  $F$  is a free  $R$ -module with a free basis of  $n$  elements. Then every free basis of  $F$  has  $n$  elements.

PROOF: Let  $Q$  be the field of quotients of  $R$ . Let  $V$  be an  $n$  dimensional vector space over  $Q$  with basis  $v_1, v_2, \dots, v_n$ . Let  $\{x_1, x_2, \dots, x_n\}$  be any given free basis of  $F$ . Define  $f: F \rightarrow V$  by  $f(x_i) = v_i$ . This is an  $R$ -homomorphism  $f$  is 1-1. For, if  $0 = f(\sum r_i x_i) = \sum r_i f(x_i) = \sum r_i v_i$  then  $r_i = 0$  for all  $i$ .  
 $\therefore \sum r_i x_i = 0$

Let  $\{y_\alpha\}_{\alpha \in \Lambda}$  be any free subset of  $F$ . We will prove that the number of elements in  $\Lambda \leq n$ . It is sufficient to prove that  $\{\mu_\alpha\}$  is linearly independent in  $V$ , where  $\mu_\alpha = f(y_\alpha)$ . Suppose  $\sum q_\alpha \mu_\alpha = 0$  for some finite subset of the  $\mu_\alpha$ 's where  $q_\alpha \in Q$ . Then  $q_\alpha = \frac{r_\alpha}{s_\alpha}$  where  $r_\alpha, s_\alpha \in R$ . Without loss of generality we can choose  $s_\alpha = s_1$  for all  $\alpha$ . Then  $\sum r_\alpha \mu_\alpha = 0$ . Then  $f(\sum r_\alpha y_\alpha) = \sum r_\alpha f(y_\alpha) = \sum r_\alpha \mu_\alpha = 0$ . Since  $f$  is 1-1,  $\sum r_\alpha y_\alpha = 0$ . But  $y_\alpha$ 's are free  $\therefore r_\alpha = 0$  and  $\{\mu_\alpha\}$  are linearly independent. This completes the proof.

**LEMMA:** Let  $M, N$  be left  $R$ -modules. Suppose that we have

$$N \xrightarrow{j} M \xrightarrow{p} N \quad \text{where } j$$

and  $p$  are homomorphisms such that  $pj = 1$ . Then  $j$  is a monomorphism and  $p$  is an epimorphism. Further  
 $M \cong \text{Im } j \oplus \ker p \cong N \oplus \ker p$ .

PROOF: Suppose  $j(x) = 0$ . Then  $x = pj(x) = p(0) = 0$

$\therefore j$  is 1-1

Let  $y \in N$ , then  $p(j(y)) = y, \therefore p$  is onto. Let  $x \in \text{Im } j \cap \text{Ker } p$ . Then  $x = j(y), y \in N$  and  $p(x) = 0$ .

$$\therefore y = pj(y) = p(x) = 0 \quad x = j(y) = 0$$

$$\text{Im } j \cap \text{Ker } p = 0.$$

To show  $\text{Im } j + \text{Ker } p = M$ .

Let  $x \in M$ . Then  $x = jp(x) + (x - jp(x))$ . Now  $jp(x) \in \text{Im } j$  and  $p(x - jp(x)) = p(x) - pj(x) = p(x) - p(x) = 0$ .  $x - jp(x) \in \text{Ker } p$ .

Hence  $M = \text{Im } j \oplus \text{Ker } p$ .

THEOREM: 24: Let  $R$  be a principal ideal ring and  $F$  a free left  $R$ -module of dimension  $n$  ( $\dim F = \text{no. of elements of free basis}$ ). Let  $F' \neq 0$  be a submodule of  $F$ . Then  $F'$  is free and  $\dim F' \leq n$

PROOF: By induction on  $n$ .

Let  $n = 1$ .  $F = Rx$  where  $x \in F$ . There exists  $f: Rx \rightarrow R$  such that  $f(x) = 1$  and  $f$  is an isomorphism.  $f(F') \cong F'$ . Now  $f(F')$  is an ideal of  $R$ .  $\therefore f(F') = Ra, a \in R$ .  $Ra$  is free on generator  $a$ .  $\therefore F' = Rax$  is free.



Assume that the theorem is true for  $\dim < n$  and let  $\dim F = n$ .  
 Let  $x_1, x_2, \dots, x_n$  be a free basis of  $F$ . Suppose  $x \in F'$ ,  $x \neq 0$ .  
 Then

$$x = r_1 x_1 + \dots + r_n x_n \text{ for some } r_i \neq 0$$

Without loss of generality, we assume  $r_n \neq 0$ . (Otherwise we have only to remember the indices) Define

$$f_n : F \rightarrow R$$

as follows. If  $y = s_1 x_1 + \dots + s_n x_n$ , then  $f_n(y) = s_n$ .

Then  $f_n(F') = Ra \subset R$ . Take  $x \in F'$  such that  $f_n(x) = a$ . Let  $y \in F'$ .

Then  $f_n(y) = ra$  for some  $r \in R$ . Then

$$y = s_1 x_1 + \dots + s_{n-1} x_{n-1} + r a x_n$$

Define

$$g: F' \rightarrow Rx \text{ by}$$

$$g(y) = \frac{f_n(y)}{a} x$$

and

$$h: Rx \rightarrow F' \text{ by } h(sx) = sx$$

Then

$$Rx \xrightarrow{h} F' \xrightarrow{g} Rx \text{ where}$$

$$gh(sx) = g(sx) = \frac{f_n(sx)}{a} x = \frac{sf_n(x)}{a} x = sx$$

so that  $gh = 1$ .

$$f' = Rx \oplus \text{Ker } g.$$

We assert that  $\text{Ker } g \subset R^{\lambda_1} \oplus \dots \oplus R^{\lambda_{n-1}}$ . If  $0 = g(y)$   
 $= \frac{f_n(y)}{a} x$ , then  $f_n(y) = 0$

$$y \in R^{\lambda_1} \oplus R^{\lambda_2} \oplus \dots \oplus R^{\lambda_{n-1}}$$

By induction,  $\text{Ker } g = F''$  is free on  $\leq n-1$  generators

$$\therefore F' = R_x \oplus F''$$

is free on  $\leq n$  generators.

Let  $\text{Hom}_R(F, R)$  denote the set of all maps of  $F$  into  $R$ . Then  $\text{Hom}_R(F, R)$  is a left  $R$ -module. For if  $f, g \in \text{Hom}_R(F, R)$ , we set

$$(f+g)(x) = f(x) + g(x)$$

$$(rf)(x) = r \cdot f(x) \quad r \in R, x \in F.$$

THEOREM 25: Let  $R$  be a principal ideal ring. Let  $F$   
be a free left  $R$ -module of dimension  $n$  and  $F' \neq 0$   
a submodule of  $F$ . Then there exists a free basis  
 $y_1, y_2, \dots, y_n$  of  $F$  and elements  $a_1, a_2, \dots, a_n$  of  $R$   
such that

$$(a_1) \supset (a_2) \supset \dots \supset (a_n)$$

and the nonzero elements of

$$\{a_1 y_1, a_2 y_2, \dots, a_n y_n\}$$

form a free basis of  $F'$ .

PROOF: By induction on  $n$ .

Let  $n = 1$ . Let  $R[x] = F$ . Then there exists  $f: R[x] \rightarrow R$  such that  $f(x) = 1$  and  $f$  is an isomorphism  $f(F') = R$ .  $ax$  is a free generator of  $F'$ .

Now assume theorem is true for  $\dim < n$ . Let  $\dim F = n$ . Now for each  $g \in \text{Hom}_R(F, R)$   $g(F')$  is an ideal of  $R$ . Choose  $f \in \text{Hom}_R(F, R)$  such that  $f(F') = R_a$  is maximal in the collection of these ideals. There exists  $x' \in F'$  such that  $f(x') = a$ .

First we notice that if  $g \in \text{Hom}_R(F, R)$  then  $g(x') \in Ra$  i.e.  $a | g(x')$ . To prove this, suppose  $b = g(x')$ . Let  $d = \text{g.c.d.}(a, b)$ . Then

$$d = ra + sb \quad \text{for some } r, s \in R.$$

Define

$$f^* \in \text{Hom}_R(F, R) \text{ by } f^* = rf + sg$$

Then  $f^*(x') = rf(x') + sg(x') = ra + sb = d$

$$(a) \subset (d) \quad \therefore f(F') = (a) \subset (d) = f^*(F')$$

By maximality, we have  $(a) = (d)$

$$b \in (d) = (a)$$

Let  $x_1, x_2, \dots, x_n$  be a free basis of  $F$ . Define  $f_i \in \text{Hom}_R(F, R)$  by

$$f_i(x_j) = \delta_{ij}$$



Now  $x' = \sum_{i=1}^n r_i x_i$ ,  $\dots$ ,  $f_i(x') = r_i = s_i a$

Let  $y_1 = s_1 x_1 + \dots + s_n x_n$ . Then  $ay_1 = x'$ .

Define  $\varphi : F \rightarrow Ry_1$  by  $\varphi(x) = f(x) y_1$ . and  $j : Ry_1 \rightarrow F$  by  $j(ry_1) = ry_1$

Then we have

$$Ry_1 \xrightarrow{j} F \xrightarrow{\varphi} Ry_1$$

where

$$\varphi j(ry_1) = \varphi(ry_1) = f(ry_1) y_1 = r f(y_1) y_1 = ry_1$$

since  $f(y_1) = 1$   $\varphi j = 1$ .

Then  $F = Ry_1 \oplus \text{Ker } \varphi$

If  $\varphi' = \varphi|_{F'}$  and  $j' : Rx' \rightarrow F'$  the inclusion then

$$Rx' \xrightarrow{j'} F' \xrightarrow{\varphi'} Rx'$$

where  $\varphi' j' = 1$

$$F' = Rx' (+) \text{Ker } \varphi'$$

But  $\text{Ker } \varphi = \text{Ker } \varphi' \cap F'$   $F' = Rx' + \text{Ker } \varphi'$

$\text{Ker } \varphi'$  is a free R-module and  $\dim \text{Ker } \varphi' = n-1$ . There exists a basis  $Y_2, Y_3, \dots, Y_n$  of  $\text{Ker } \varphi'$  and elements  $a_2, a_3, \dots, a_n$  of R such that  $(a_2) \supset (a_3) \supset \dots \supset (a_n)$  and the non-zero elements of  $a_2 Y_2, \dots, a_n Y_n$  form a free basis of  $\text{Ker } \varphi' \cap F'$ . Therefore

$y_1, y_2 \dots y_n$  are a free basis of  $F$  and the non-zero elements of  $a_1 y_1, \dots, a_n y_n$  form a basis of  $F'$ . To complete the proof it only remains to show that  $(a_1) \supset (a_2)$

Let  $g_i \in \text{Hom}_R(F, R)$  be defined by  $g_i(y_j) = \delta_{ij}$ . Then  $g_1 = f$ . For  $f(y_1) = 1$  as we have already proved. For  $y_i, i > 1$ , we have  $0 = \varphi(y_i) = f(y_i) y_1 \therefore f(y_i) = 0$ .

Let  $d = \text{g.c.d.}(a_1, a_2)$ . Then

$$d = ra_1 + sa_2 \text{ where } r, s \in R.$$

Define  $f^{**} \in \text{Hom}_R(F, R)$  by

$$f^{**} = rf + sg_2$$

Then

$$\begin{aligned} f^{**}(a_1 y_1 + a_2 y_2) &= a_1 f^{**}(y_1) + a_2 f^{**}(y_2) \\ &= a_1 r + a_2 s = d. \end{aligned} \quad f(F') = (a_1) \subset (d) = (f^{**}(F'))$$

By maximality  $(a_1) = (d)$  and

$$(a_2) \subset (a_1) = (a)$$

DEFINITION 26: Let  $M$  be a left  $R$ -module. Let  $S$  be a subset of  $M$ . Then the annihilator of  $S$  is defined by

$$\text{Ann}_R(S) = \{r \in R \mid rS = 0\}$$

Let  $R$  be a principal ideal ring and  $M$  a left  $R$ -module. Suppose  $x \in M$  and  $I = \text{ann}_R(x)$ .

Define

$$\varphi: R \rightarrow R_x \text{ by } \varphi(1) = x$$

Clearly  $\varphi$  is onto and  $\text{Ker } \varphi = \text{ann}_R(x)$

$$\frac{R}{I} \cong R_x.$$

**THEOREM 26:** Let  $A$  be a left  $R$ -module and  $A = A_1 \oplus A_2 \oplus \dots \oplus A_n$ . Where  $A_i$  is a submodule of  $A$ . Let  $A_i'$  be a submodule of  $A_i$  and  $A' = A_1' \oplus A_2' \oplus \dots \oplus A_n'$ . Then

$$\frac{A}{A'} \cong \frac{A_1}{A_1'} \oplus \frac{A_2}{A_2'} \oplus \dots \oplus \frac{A_n}{A_n'}$$

**PROOF:** Exercise.

**THEOREM 27:** (Fundamental Theorem). Let  $M$  be a finitely generated module over a principal ideal ring  $R$ . Then

$$M = M_1 \oplus M_2 \oplus \dots \oplus M_n$$

where each  $M_i = Rx_i$ , cyclic with generator  $x_i$ . and if  $I_i = \text{ann}_R(x_i)$  then  $I_1 \supset I_2 \supset \dots \supset I_n$  and this is unique.



PROOF: Let  $m_1, m_2, \dots, m_k$  be a finitely generating set for  $M$ . Choose a free module with basis  $x_1, \dots, x_k$ . Map  $F$  onto  $M$  by

$$x_i \xrightarrow{\varphi} m_i$$

Let  $F' = \text{Ker } \varphi$ . Then  $\frac{F}{F'} \cong M$ . By Theorem 25, there exists a basis  $y_1, y_2, \dots, y_k$  of  $F$  and elements  $a_1, \dots, a_k$  of  $R$  such that the nonzero elements of  $a_1 y_1, a_2 y_2, \dots, a_k y_k$  are a free basis of  $F'$  ( $a_1$ )  $\supset$  ( $a_2$ )  $\supset$   $\dots$   $\supset$  ( $a_k$ ).

Then

$$\begin{aligned} \frac{F}{F'} &\cong \frac{Ry_1 \oplus Ry_2 \oplus \dots \oplus Ry_k}{Ra_1 y_1 \oplus Ra_2 y_2 \oplus \dots \oplus Ra_k y_k} \\ &\cong \frac{Ry_1}{Ra_1 y_1} \oplus \frac{Ry_2}{Ra_2 y_2} \oplus \dots \oplus \frac{Ry_k}{Ra_k y_k} \end{aligned}$$

Further  $\frac{Ry_i}{Ra_i y_i} \cong Rx_i$  and  $I_i = \text{ann}_R(x_i) \neq (q_i)$

DEFINITION 27: Let  $M$  be a left module over an integral domain  $R$ . Let  $x \in M$ . We say that  $x$  is a torsion element if there exists  $r \neq 0$ ,  $r \in R$  such that  $rx = 0$ .

Exercise 10: Let  $M_T$  denote the set of all torsion elements of  $M$ . Then  $M_T$  is a submodule of  $M$  and  $M/M_T$  is torsion free.

$M$  is called a torsion module if  $M = M_T$

Example: Every finite abelian group is a torsion group.

Exercise 11: Show that a direct sum of any family of torsion modules is a torsion module.

DEFINITION 28: Let  $R$  be a principal ideal ring.

Suppose  $M$  is a left  $R$  module and  $p$  a prime element of  $R$ . Then the  $p$ -primary component  $M_p$  of  $M$  is defined by

$$M_p = \{ x \in M \mid \text{there exists } p^n \text{ such that } p^n x = 0 \}$$

Clearly  $M_p$  is a submodule of  $M$ .

THEOREM 28: Let  $R$  be a principal ideal ring and  $M$  a torsion  $R$  module. Then  $M$  is a direct sum of its  $p$ -primary components.

PROOF: Let  $x \in M$ ,  $x \neq 0$ . There exists  $r \neq 0$  such that  $rx = 0$ . Let  $r = p_1^{\alpha_1} \dots p_n^{\alpha_n}$  where  $p_i$ 's are primes and this representation is unique. Let  $r_i = r/p_i^{\alpha_i}$ . Then the ideal  $(r_1, r_2, \dots, r_n) = R$ . Therefore there exists  $s_i \in R$  such that  $1 = r_1 s_1 + r_2 s_2 + \dots + r_n s_n$ .

Hence  $x = r_1 s_1 x + \dots + r_n s_n x$ .

Now  $p_i^{\alpha_i} (r_i s_i x) = s_i r x = 0 \quad r_i s_i x \in M_{p_i}$

$$M = \sum M_{p_i}$$

Suppose  $x = x_1 + \dots + x_n = 0$ , where  $x_i \in M_{p_i}$ ,  $p_i \neq p_j$  for  $i \neq j$ . Suppose  $p_i^{\alpha_i} x_i = 0$

Let  $q_i = p_i^{\alpha_i} p_2^{\alpha_2} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_n^{\alpha_n}$  Then  $(q_i, p_i^{\alpha_i}) = 1$

$$\therefore 1 = r q_i + s p_i^{\alpha_i} \quad \text{for } r, s \in R.$$

Now  $r q_i x_1 + r q_i x_2 + \dots + r q_i x_n = 0$

Now  $r q_i x_j = 0$  for all  $j \neq i$   $r q_i x_i = 0$ .

But  $r q_i = 1 - s p_i^{\alpha_i}$

$$0 = r q_i x_i = (1 - s p_i^{\alpha_i}) x_i = x_i - s p_i^{\alpha_i} x_i = x_i$$

$$M = \Sigma \bigoplus M_{p_i}$$

THEOREM 29: Let  $M$  be a finitely generated module over a principal ideal ring. Then  $M = F \oplus \Lambda_1 \oplus \dots \oplus \Lambda_n$  where  $F$  is a free module and each  $\Lambda_i$  is cyclic of prime order for various primes.

$$\Lambda_i = R / p_i^{\alpha_i} R$$

PROOF: By the fundamental theorem

$$M = B_1 \oplus B_2 \oplus \dots \oplus B_q$$

where  $B_i$  is cyclic and

$$\text{ann}(B_1) \supset \text{ann}(B_2) \supset \dots \supset \text{ann}(B_q)$$



Let  $k$  be the smallest integer such that  $\text{ann}(B_{k+1}) = 0$ . Let  $B_{k+1} \oplus B_{k+2} \oplus \dots \oplus B_q = F$ . Then  $F$  is free.

Let  $T = B_1 \oplus B_2 \oplus \dots \oplus B_k$ . Then  $\text{ann}(B_q)T = 0$   
 $\therefore T \subset M_T$

Conversely suppose  $x \in M_T$ . Then  $x = y+z$ , where  $y \in T$ ,  $z \in F$ . There exists  $r \neq 0$  such that  $rx = 0$   $ry+rz = 0 \therefore ry = 0$  and  $rz = 0$  since  $M = T \oplus F$ . But a free  $R$ -module is torsion free  $z = 0$  so  $x = y \in T$ .

$$T = M_T$$

$$M = M_T \oplus F.$$

Now  $M_T = M_{p_1} \oplus \dots \oplus M_{p_n}$  where  $M_{p_i}$  are  $p_i$  primary components.  $M_{p_i}$  is a direct sum of cycles. Each cycle is of order a power of  $p_i$ .

Exercise 12: Let  $M$  be a left module over a principal ideal ring  $R$ . Let  $x, y \in M$ . Let  $(a) = \text{ann}(x)$ ,  $(b) = \text{ann}(y)$ . Suppose  $\text{gcd}(a, b) = 1$ . Then  $Rx + Ry = Rx \oplus Ry$  and is cyclic with generator  $x+y$ .

Exercise 13: (Chinese Remainder Theorem). Let  $R$  be a principal ideal ring. Let  $r_1, r_2, \dots, r_n \in R$  such that  $(r_i, r_j) = 1$  for  $i \neq j$ . Let  $a_1, a_2, \dots, a_n$  be  $n$  elements of  $R$ . The simultaneous congruences

$$x \equiv a_1 \pmod{r_1}$$

$$x \equiv a_2 \pmod{r_2}$$

$$x \equiv a_n \pmod{r_n}$$

have unique solution mod  $(r_1, \dots, r_n)$

8. Simple and Semi-simple Modules

DEFINITION 29: A left  $R$ -module  $M$  is simple if  $0$  and  $M$  are the only submodules of  $M$ .

THEOREM 30: A left  $R$ -module  $M$  is simple if and only if  $M = Rx$  for any  $x \in M$  such that  $x \neq 0$ .

PROOF: Suppose  $M$  is a simple left  $R$ -module. If  $x \neq 0$  is an element of  $M$ , then  $Rx$  is a submodule of  $M$ . Since  $M$  is simple,  $Rx = M$  or  $Rx = 0$ . Now  $1 \in R$  implies  $1 \cdot x \neq 0$  and thus  $Rx \neq 0$ . Hence  $M = Rx$ .

To prove the converse, let  $N$  be a submodule of  $M$ . There exists  $x \in N$  such that  $x \neq 0$ . Then  $Rx \subset N$  and  $M = Rx$  by hypothesis.  $\therefore M \subset N$ . Hence  $N = M$  and  $M$  is simple.

THEOREM 31: A left  $R$ -module  $M$  is simple if and only if there exists a maximal ideal  $I \subset R$  such that  $M \cong R/I$ .

PROOF: Suppose  $M$  is simple and  $m \in M$ ,  $m \neq 0$ . Then  $Rm = M$  by Theorem 30. Let  $I = \{r \in R \mid rm = 0\}$ . Then  $I$  is an ideal of  $R$ . Let  $J$  be an ideal of  $R$  such that  $I \subset J \subset R$ . There exists  $s \in J$ ,  $s \notin I$ , such that  $sm \neq 0$ . Then since  $M$  is simple  $Rsm = M = Rm$ . Therefore there exists  $t \in R$  such that  $tsm = m$ . That is  $(ts-1)m = 0$ . Hence  $ts-1 \in I \subset J$ . This implies

$-1 \in J$  and  $J = R$ . Hence  $I$  is maximal. Define  $f: R \rightarrow M$  by  $f(r) = rm$ . Then  $\text{Ker } f = I$  and  $f$  is onto.  $\therefore R/I \cong M$ .

Conversely, suppose  $I$  is maximal. Then  $R/I$  is a field by Theorem 6 and contains no proper ideal. Considering  $R/I$  as a module over  $R$ ,  $R/I$  has no proper submodules. Since  $R/I \cong M$ ,  $M$  has no proper submodules and hence  $M$  is simple.

DEFINITION 30: A left  $R$ -module  $M$  is semi-simple if there exists a family  $\{M_\alpha\}_{\alpha \in \mathcal{A}}$  of simple  $R$ -modules such that

$$M = \sum_{\alpha \in \mathcal{A}} \oplus M_\alpha$$

DEFINITION 31: Let  $M$  be a left  $R$ -module and  $N$  a submodule of  $M$ . Then  $N$  is called a direct summand if there exists a submodule  $L$  such that  $M = N \oplus L$ .

THEOREM 32: Let  $M$  be a left  $R$ -module. Then  $M$  is semi simple if and only if every submodule of  $M$  is a direct summand

PROOF: Suppose  $M$  is semisimple. Let  $N$  be a submodule of  $M$ . By definition, there exists  $\{M_\alpha\}_{\alpha \in \mathcal{A}}$  such that  $M = \sum_{\alpha \in \mathcal{A}} \oplus M_\alpha$ . Let  $\mathcal{A}'$  be a subset of  $\mathcal{A}$ . Define

$$M' = \sum_{\alpha \in \mathcal{A}'} \oplus M_\alpha$$



Then  $M'$  is a submodule of  $M$ . By Zorn's lemma there exists a maximal subset  $\alpha'$  of  $\alpha$  such that  $N \cap M' = 0$ . We assert that  $M = N \oplus M'$ . Let  $T = N \oplus M'$ . Now  $M_\alpha \cap T = 0$  or  $M_\alpha$  since  $M_\alpha$ 's are simple. Suppose  $M_\alpha \cap T = 0$ . Then  $N \cap M'' = 0$  where  $M'' = \sum_{\beta \in \alpha' \cup \alpha} M_\beta$  which contradicts the maximality of  $\alpha'$ . Hence  $M_\alpha \cap T = M_\alpha$  for all  $\alpha$ .

$$M_\alpha \subset T \text{ for all } \alpha. \therefore M \subset T$$

$$\text{Thus } T = M$$

We shall now prove the converse.

1) Suppose  $N$  is a submodule of  $M$ . Let  $L$  be a submodule of  $N$ . Then  $L$  is a direct summand of  $N$ .  $L$  is a submodule of  $M$ .

$$M = L \oplus D$$

Let  $N_1 = N \cap D$ . We assert that  $N = L \oplus N_1$ .

Now  $N_1 \cap L \subset D \cap L = 0$  and  $L \oplus N_1 \subset N$ . Let  $n \in N$ . Then  $n = l + d$  where  $l \in L, d \in D$ . Since  $L \subset N, n - l \in N$ . Hence  $d \in L \cap N = N_1$ . Hence  $n \in L \oplus N_1$  and so  $N \subset L \oplus N_1$ .

(2) Let  $N$  be a submodule of  $M$ . Then  $N$  contains a simple submodule.

Let  $n \neq 0 \in N$ . By Zorn's lemma we can find a maximal submodule  $L$  of  $N$  such that  $n \notin L$ . By (1),  $N = L \oplus D$ . We now claim  $D$  is simple. Suppose not. Let  $E$  be a submodule of  $D, E \neq 0$ . Suppose  $E \neq D$ . By (1),  $D = E \oplus F$  where  $F \neq 0$ .

Suppose

$$n \in (L \oplus E) \cap (L \oplus F)$$

Then  $n = \ell_1 + e = \ell_2 + f$  for some  $\ell_1, \ell_2 \in L$ ,  $e \in E$  and  $f \in F$ .

Since  $N = L \oplus E \oplus F$ , it follows that  $e = f = 0$  since  $E \cap F = 0$ ,  $e = f = 0$ .  $n = \ell_1 \in L$  contradiction. Hence  $n \notin L \oplus E$  or  $n \notin L \oplus F$ . In either case, we get a contradiction to the maximality of  $L$ .  $\therefore D$  is simple

(3) Let  $\mathcal{C}$  be the collection of all submodules of  $M$  which are direct sums of simple modules. By Zorn's lemma, there exists a maximal element  $N$  in  $\mathcal{C}$ . Suppose  $N \neq M$ . By (1),  $M = N \oplus L$  where  $N$  is semisimple. By (2),  $L$  contains a simple submodule  $D$ . Then  $N \oplus D$  is semisimple and  $N \oplus D \supset N$  but  $N \oplus D \neq N$ . This contradicts the maximality of  $N$ . Hence  $N = M$  and  $M$  is semisimple

This completes the proof.

COROLLARY: 1.  $M$  is semisimple if and only if every nonzero submodule of  $M$  is semisimple.

PROOF: Let  $M$  be semisimple and  $N$  a submodule of  $M$ . Let  $L$  be a submodule of  $N$ . Then  $L$  is a direct summand of  $N$ . Hence  $N$  is semisimple. Conversely if every submodule of  $M$  is semisimple, then  $M$  is itself a submodule and hence semi-simple.

COROLLARY 2: Suppose  $M = \sum_{\lambda \in \Lambda} \oplus M_{\lambda}$ . Then  
M is semisimple if and only if every  $M_{\lambda}$  is semisimple

PROOF: If M is semisimple, each  $M_{\lambda}$  is a submodule of M. By corollary 1,  $M_{\lambda}$  is semisimple.

If  $M_{\lambda}$  is semisimple, each  $M_{\lambda}$  is a direct sum of simple modules and so M is a direct sum of simple modules. Hence M is semisimple.

Exercise 14: Prove or disprove. Let M be a left R-module and N a submodule of M. Then M is semisimple if and only if N and  $M/N$  are semisimple.

### 9. Projective, Injective and Hereditary Modules

DEFINITION 32: A left R-module P is called projective if given any diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow f & & \\ B & \xrightarrow{g} & C & \longrightarrow & 0 \end{array}$$

With bottom row exact, there exists  $h: P \rightarrow B$  such that  $gh = f$ .



Exercise 15: Show that every free module is projective.

DEFINITION 32: An exact sequence of the form

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

is called a short exact sequence.

THEOREM 33: Let  $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$  be exact. Then the following are equivalent:

- (1) there exists  $s : C \rightarrow B$  such that  $ps = 1$
- (2) there exists  $h : B \rightarrow A$  such that  $hi = 1$
- (3)  $\text{Im } i$  is a direct summand
- (4) There exists a direct family  $(i, h), (s, p)$  such that  $ih + sp = 1$ , where  $i, p$  as above

PROOF:  $1) \implies 3)$ . To prove  $B = \text{Im } i + \text{Im } s$ . Let  $x \in \text{Im } i \cap \text{Im } s = \text{Ker } p \cap \text{Im } s$ .

Then  $p(x) = 0$  and  $x = s(y) \quad y \in C$

$$0 = p(x) = p(s(y)) = (ps)(y) = y. \therefore x = s(y) = 0$$

If  $x \in B$ , then  $x = sp(x) + (x - (sp)(x))$

$$sp(x) \in \text{Im } s \quad \text{and}$$

$$p(x - sp(x)) = p(x) - psp(x) = p(x) - p(x) = 0$$

$$x - sp(x) \in \text{Ker } p$$

$$\text{Hence } B = \text{Im } i \oplus \text{Im } s = \text{Ker } p \oplus \text{Im } s$$

3)  $\implies$  2) Suppose  $B = \text{Im } i \oplus D$ .

Define  $h: B \rightarrow A$  as follows. Let  $x \in B$ . Then  $x = i(a) + d$  where  $a \in A$ ,  $d \in D$ . Set  $h(x) = a$ . Then  $h$  is a homomorphism and  $h i(a) = a$  for all  $a \in A$ .

2)  $\implies$  4). By an argument similar to the one used to prove 1)  $\implies$  3), we can show that

$$B = \text{Im } i \oplus \text{Ker } h$$

Then if  $x \in B$ , then  $x = u + v$  where  $u \in \text{Im } i$  and  $v \in \text{Ker } h$ .

Define  $s: C \rightarrow B$  as follows. Let  $y \in C$   $y = p(x)$  where  $x \in B$ .

Then  $x = u + v$  with  $u \in \text{Im } i$  and  $v \in \text{Ker } h$ . Set

$s(y) = u'$ . Now  $s$  is well defined. Suppose  $p(x) = y$ ,  $x' = u' + v'$ .

Then  $p(x - x') = 0$  which means  $p(u - u' + v - v') = 0$ .

Since  $u, u' \in \text{Im } i = \text{Ker } p$  by hypothesis,  $p(u - u') = 0$ .

Hence  $p(v - v') = 0$ . Then  $v - v' \in \text{Im } i$ . Since

the sequence is exact  $i$  is 1-1. Hence  $v - v' = 0$ . This

proves that  $s$  is well-defined. Then  $s$  is a homomorphism (check).

Now  $(ps)(y) = p(v) = p(u+v) = p(x) = y$   $\therefore ps = 1$ .

If  $x \in B$ ,  $(ih + sp)(x) = ih(x) + sp(x) = ih(u+v) + sp(u+v)$

$= ih(u) + v = u+v$  for  $u = ia$ ,  $(ih)u = (ihi)a = i(a) = a$ .

This proves (4)

4)  $\implies$  1) is trivial.

DEFINITION 34: The sequence is said to split if any one of the conditions of the above theorem is satisfied.

THEOREM 34: Let  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  be exact. If the sequence splits, then  $B \cong A \oplus C$ . Conversely if  $B \cong A \oplus C$  there exists an exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

which splits.

PROOF: Suppose the sequence

$$0 \rightarrow A \xrightarrow{i} B \xrightarrow{s} C \rightarrow 0$$

splits. Then by Theorem 33,

$$B = \text{Im } i \oplus \text{Im } s$$

Since  $i$  and  $s$  are monomorphisms  $B = A \oplus C$ .

Conversely, suppose  $B = A \oplus C$ .

Define  $i : A \rightarrow B$  by  $i(a) = a + 0$ ,  $a \in A$ . Define  $p : B \rightarrow C$  by  $p(y) = c$  where  $y = a + c$  with  $a \in A$ ,  $c \in C$ . Then  $i$  is a monomorphism and  $p$  is an epimorphism. Further  $\text{Ker } p = \text{Im } i$  and the sequence is exact. The sequence splits because  $A = \text{Im } i$  is a direct summand of  $B$ .



THEOREM 35: Let  $0 \rightarrow A \xrightarrow{i} B \xrightarrow{f} C \rightarrow 0$   
 be a short exact sequence with  $C$  projective. Then the  
sequence splits

PROOF: Now consider the diagram

$$\begin{array}{ccccc}
 & & C & & \\
 & & \downarrow \text{identity} & & \\
 B & \xrightarrow{f} & C & \longrightarrow & 0
 \end{array}$$

where the bottom row is exact. Since  $C$  is projective, there exists  $s : C \rightarrow B$  such that  $ps = 1$ . Hence the sequence splits.

Remark: Let  $A$  be a finitely generated abelian group (An abelian group is a  $\mathbb{Z}$  module) Let  $T$  denote the torsion submodule of  $A$ . Then

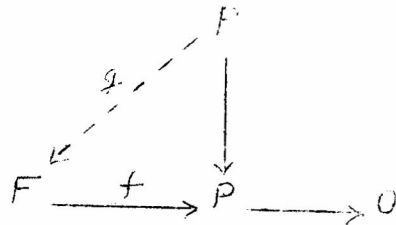
$$0 \rightarrow T \rightarrow A \rightarrow A/T \rightarrow 0$$

$A/T$  is torsion free. By the fundamental theorem,  $A/T$  is a direct sum of cyclic subgroups. A cyclic torsion free group is isomorphic to  $\mathbb{Z}$ .  $A/T$  is free and therefore projective. The exact sequence splits.

Hence  $A = T \oplus A/T$

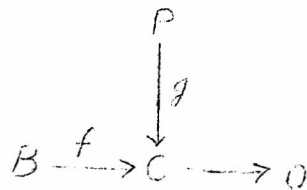
THEOREM 36: A left R module is projective if and only if it is a direct summand of free module.

PROOF: Suppose  $P$  is projective. By Theorem 22, there exists a free module  $F$  such that  $F \xrightarrow{f} P \rightarrow 0$  is exact. There exists  $g: P \rightarrow F$  such that  $fg = 1$ .

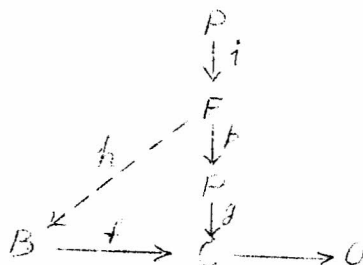


Hence  $0 \rightarrow \text{Ker } f \rightarrow F \xrightarrow{f} P \rightarrow 0$  splits. and therefore  $F = P \oplus \text{Ker } f$ .

Conversely, suppose  $P$  is a direct summand of a free module  $F$ . This means there exists  $P \xrightarrow{i} F \xrightarrow{f} P$  such that  $fi = 1$ . Now we shall show that  $P$  is projective. To



be any given diagram with bottom row exact. We can embed this diagram in



There exists  $h : F \longrightarrow B$  such that  $fh = gp$ . Let  $h_1 = h_i$   
Then

$$fh_1 = f(h_i) = (fh)i = (gp)i = g(pi) = g$$

Thus  $P$  is projective.

Exercise 16: Show that a left  $R$ -module  $P$  is projective if and only if every exact sequence of the form  
 $0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$  splits.

THEOREM 37: Let  $\{ \Lambda_\alpha \}_{\alpha \in \mathcal{A}}$  be a family of left  $R$ -modules. Then  $\sum_{\alpha} \oplus \Lambda_\alpha$  is projective if and only if each  $\Lambda_\alpha$  is projective.

PROOF: Exercise.

DEFINITION:35: A left  $R$ -module  $Q$  is injective if given any diagram of the form

$$\begin{array}{ccc} 0 & \longrightarrow & C \xrightarrow{i} B \\ & & \downarrow f \\ & & Q \end{array}$$

there exists  $g : B \longrightarrow Q$  such that  $gi = f$ .

The concept of injectiveness is 'dual' to projectiveness.



Exercise 17: Let  $Q$  be the field of quotients of an integral domain  $R$ . Show that

- 1)  $Q$  is divisible that is given  $x \in Q$  and any  $r \in R$   $r \neq 0$ , there exists  $y \in Q$  such that  $x = ry$ .
- 2)  $Q$  is injective.

DEFINITION 36: A left  $R$ -module is said to be hereditary if every submodule is projective and a ring  $R$  is hereditary if it is hereditary as a module over itself.

THEOREM 38: Let  $\{A_i\}_{i \in I}$  be a family of modules where  $I$  is a well ordered set. Let  $B$  be a submodule of the direct sum  $\sum_{i \in I} A_i$  such that there exists a subfamily of submodules  $\{B_i\}_{i \in I}$  of  $B$  such that

$$B \cap \sum_{i \geq j} \bigoplus A_i = \sum_{i \geq j} \bigoplus B_i \text{ for } j \in I. \text{ Then } B = \sum \bigoplus B_i.$$

PROOF: It is enough to show that  $\{B_i\}_{i \in I}$  generates  $B$ . Let  $b \in B$ . Then there exists  $j \in I$  such that

$$b \in \sum_{i \geq j} \bigoplus A_i \cap B = \sum_{i \geq j} \bigoplus B_i \subseteq \sum_{i \in I} B_i$$

For  $j \in I$ , let

$$S_j = \sum_{i \neq j} B_i. \text{ Then } S_j \cap B_j = 0.$$

For, let  $b_j \in S_j \cap B_j$ . Then

$$b_j = b_{i_1} + \dots + b_{i_n} \quad \text{where } b_{i_k} \in B_{i_k}$$

$$i_k \neq j, \quad i_1 < i_2 < \dots < i_n$$

$$0 = -b_j + b_{i_1} + \dots + b_{i_n}$$

Set  $r = \max(i_n, j)$ . Then R.H.S.  $\in \sum_{i \leq r} B_i = \sum_{i \leq r} \oplus B_i$   
 each  $b_{i_k} = 0$ . Hence  $b_j = 0$  and  $B = \sum_{i \in I} \oplus B_i$

THEOREM 39: Let  $\{A_i\}_{i \in I}$  be a family of hereditary left R-modules. Let  $A = \sum_{i \in I} \oplus A_i$  and  $B$  a submodule of  $A$ . Then  $B$  is isomorphic to a direct sum of submodules of  $A_i$ .

PROOF: Well order  $I$  with first element  $1$ . The idea of the proof here is to obtain the  $B_i$ 's satisfying conditions of Theorem 38. We shall inductively define for each  $i \in I$ , a submodule  $B_i$  of  $B$  such that

$$(1) \quad B \cap \sum_{i \leq j} \oplus A_i = \sum_{i \leq j} \oplus B_i$$

and (2)  $B_i$  is isomorphic to a submodule of  $A_i$ . To this end, we proceed as follows:

$$\text{Let } B_1 = B \cap A_1$$

Let  $j \geq 1$  and suppose  $B_i$  has already been obtained for all  $i < j$ .

Define  $p_j : B \bigcap_{i \leq j} \Sigma \oplus A_i \longrightarrow \Lambda_j$  by, restriction of projection of onto  $\Lambda_j$ . Then  $\text{Ker } p_j = B \bigcap_{i < j} \Sigma \oplus A_i$  and we have an exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & (B \bigcap_{i < j} \Sigma \oplus A_i) & \longrightarrow & B \bigcap_{i \leq j} \Sigma \oplus A_i & \longrightarrow & \\ & & \downarrow & & & & \\ & & \text{Imp}_j & \longrightarrow & 0 & & \end{array}$$

Since  $\text{Imp}_j \subset A_j$  and  $\Lambda_j$  is hereditary,  $\text{Imp}_j$  is projective and the sequence splits. Thus there exists

$$s_j : \text{Imp}_j \longrightarrow B \bigcap_{i \leq j} \Sigma \oplus A_j$$

such that  $p_j s_j = 1$ . Let  $B_j = \text{Im } s_j$ . Then  $B_j \cong \text{Imp}_j$

which is a submodule of  $\Lambda_j$  and  $B \bigcap_{i \leq j} \Sigma \oplus A_i$

$$= \left[ B \bigcap_{i < j} \Sigma \oplus A_j \right] \oplus \Lambda_j$$

Apply Theorem 38 to

$$B \bigcap_{i < j} \Sigma \oplus A_i \subset \Sigma \bigoplus_{i < j} A_i$$

and for any  $i_0 < j$ , we have

$$B \bigcap_{i \leq i_0} \Sigma \oplus A_i = \Sigma_{i \leq i_0} \oplus B_1 \text{ by induction.}$$

By Theorem 38,

$$\begin{aligned} B \bigcap_{i \leq j} \Sigma \oplus A_i &= \Sigma_{i < j} \oplus B_1 \oplus B_j = \\ &= \Sigma_{i \leq j} \oplus B_j \end{aligned}$$



COROLLARY 1: A direct sum of hereditary left R-modules is hereditary.

COROLLARY 2: Let R be a hereditary ring. Let P be any submodule of a free R-module F. Then P is projective and is isomorphic to a direct sum of left ideals.

COROLLARY 3: Let R be a left hereditary ring. An R-module P is projective if and only if it is a submodule of a free R-module.

COROLLARY 4: A ring R is left hereditary if and only if every projective R-module is hereditary.

## VECTOR SPACES AND ALGEBRAS

1. Vector spaces over a skew field.

DEFINITION 1: Let  $D$  be a skew field. A left (right) module over  $D$  is called a left (right) vector space. The submodules of the vector space  $V$  are called subspaces.

$D$  itself is a left vector space over  $D$ . Notice when  $D=F$ , a field, we get the ordinary vector spaces.

DEFINITION 2: Let  $V$  be a vector space over  $D$ . Then the elements  $x_1, x_2, \dots, x_n \in V$  are said to be linearly independent if  $d_1 x_1 + \dots + d_n x_n = 0$ ,  $d_i \in D$ ,  $i=1, 2, \dots, n$  implies  $d_i = 0$ .  $x_1, x_2, \dots, x_n$  are said to form a basis for  $V$  if they generate  $V$  and are linearly independent. This means that if  $x \in V$ , then

$$x = d_1 x_1 + \dots + d_n x_n \quad d_i \in D$$

uniquely.

DEFINITION 3: The number of elements in a basis for the vector space  $V$  is called the dimension of  $V$ .

This definition makes sense only when all the bases have the same number of elements. Actually it is the case.

However we deal with only finite dimensional vector spaces which means that there exists an integer  $n$  such that every  $n+k$  ( $k \geq 1$ ) vectors are linearly dependent.

THEOREM 1: Let  $V$  be a finite dimensional vector space over  $D$ . If  $V$  has a basis with  $n$  elements then any  $n+1$  vectors in  $V$  are linearly dependent.

PROOF: By induction on  $n$ . Let  $e_1, e_2, \dots, e_n$  be a basis and let  $x_1, x_2, \dots, x_n, x_{n+1}$  be  $n+1$  vectors in  $V$ . When  $n=1$ , we have  $x_1 = d_1 e_1$  and  $x_2 = d_2 e_1$  where  $d_1, d_2 \in D$ . If  $x_1 \neq 0$ , then  $x_2 = d_2 e_1 = d_2 d_1^{-1} x_1$ . Thus the result is true for  $n=1$ . Now assume the theorem for spaces that have basis of  $n-1$  vectors. Suppose the vectors  $x_1, x_2, \dots, x_n, x_{n+1}$  are linearly independent. Then we also have the representations

$$x_j = d_{j1} e_1 + d_{j2} e_2 + \dots + d_{jn} e_n \quad j=1, 2, \dots, n+1$$

in terms of  $e_1, e_2, \dots, e_n$ . Assume  $x_1 \neq 0$ . Then without loss of generality  $d_{1n} \neq 0$ . Set  $y_1 = x_1$ ,  $y_j = x_j - d_{jn} d_{1n}^{-1} x_1$ , for  $j > 1$  and the set of vectors  $y_1, y_2, \dots, y_{n+1}$  is a linearly independent set. Therefore the  $n$  vectors  $y_2, y_3, \dots, y_{n+1}$  are linearly independent and belong to  $V_1$ , the subspace generated by  $e_1, e_2, \dots, e_{n-1}$ . Now  $e_1, \dots, e_{n-1}$  form a basis for  $V_1$ , the vectors  $y_2, \dots, y_{n+1}$  which are  $n$  in number are linearly dependent by the inductive hypothesis and gives a contradiction.



THEOREM 2: Let  $V$  be a finite dimensional vector space over  $D$ . If  $V$  has a basis with  $n$  elements, then every other basis also has  $n$  elements.

PROOF: Let  $\{e_1, e_2, \dots, e_n\}$  be a basis for  $V$ . Let  $\{f_1, f_2, \dots, f_n\}$  be any other basis for  $V$ . Now by Theorem 1, every  $n+1$  vectors are linearly dependent. Therefore  $m \leq n$ . Similarly  $n \leq m$ . Hence  $n=m$ .

DEFINITION 4: Let  $V_1, V_2$  be left vector spaces over  $D$ . A linear transformation

$$T: V_1 \longrightarrow V_2$$

is a  $D$ -homomorphism i.e.,

$$T(d_1x_1 + d_2x_2) = d_1T(x_1) + d_2T(x_2)$$

where  $d_1, d_2 \in D$  and  $x_1, x_2 \in V$ .

A linear functional  $f: V \longrightarrow D$  where  $V$  is a left vector space over  $D$ , is a linear transformation of  $V$  into  $D$ , considered as a left vector space. The set of all linear functionals on  $V$  is denoted by  $V^*$  or  $\text{Hom}_D(V, D)$ .  $V^*$  is called the dual space of  $V$ .

THEOREM 3: If  $V$  is a left (right) vector space over  $D$ , then  $V^*$  is a right (left) vector space over  $D$ .

PROOF: Suppose  $V$  is a left vector space. We will show that a module multiplication can be defined so that  $V^*$  is a right vector space. Let  $f_1, f_2 \in V^*$ . Define

$f_1+f_2$  by  $(f_1+f_2)(x) = f_1(x)+f_2(x)$ ,  $x \in V$ .

If  $d \in D$ , we define  $fd$  by

$$(fd)(x) = f(x)d$$

We first show that  $fd \in V^*$ . Now  $(fd)(x_1+x_2) = f(x_1+x_2)d$   
 $= (fd)(x_1)+(fd)(x_2)$ .

and if  $d' \in D$ , then

$$\begin{aligned} (fd)(d'x) &= f(d'x)d = (d'f(x))d \\ &= d'.f(x).d = d'(fd)(x) \end{aligned}$$

This proves  $fd \in V^*$ . To complete the proof, we have to show that  $fd_1d_2 = (fd_1)d_2$ . This follows from

$$(fd_1d_2)(x) = f(x).d_1d_2 = ((fd_1)x)d_2 = ((fd_1)d_2)(x)$$

for all  $x \in V$ .

**THEOREM 4:** Let  $V$  be a left vector space over a division ring  $D$  such that  $\dim V = n < \infty$ .  
Then  $\dim V^* = n$ .

**PROOF:** Let  $x_1, x_2, \dots, x_n$  be a basis for  $V$ . Define  $f_i \in V^*$  by  $f_i(x_j) = \delta_{ij}$ . Then  $f_1, \dots, f_n$  form a basis for  $V^*$ .

**THEOREM 5:** If  $\dim V < \infty$ , then  $V \cong V^{**}$ .

**PROOF:** Let  $x \in V$ . Define  $x^{**} \in V^{**}$  by  $x^{**}(f) = f(x)$  for all  $f \in V^*$ . Define a linear transformation  $V \rightarrow V^{**}$  by  $x \rightarrow x^{**}$ . This is 1-1. We have to show that the Kernel of this map is 0. Suppose  $x^{**} = 0$ .

Then  $f(x)=0$  for all  $f \in V^*$ . If  $x \neq 0$ , we can find a basis with  $x$  as an element. Then there exists  $g \in V^*$  such that  $g(x)=1$  and  $g(y)=0$  where  $y$  belongs to this basis and  $y \neq x$ . Contradiction. Hence  $x=0$ . Now  $\dim V^{**} = \dim V^* = \dim V$ . Thus the map is onto also.

DEFINITION 5: Let  $V$  be a left vector space and  $W$  a right vector space over  $D$ . A bilinear function  $F$  from  $V \times W$  into  $D$  is a mapping  $F: V \times W \rightarrow D$  such that

$$F(x_1 + x_2, y) = F(x_1, y) + F(x_2, y)$$

$$F(x, y_1 + y_2) = F(x, y_1) + F(x, y_2)$$

$$F(dx, y) = dF(x, y)$$

and  $F(x, yd) = F(x, y)d$

where  $x_1, x_2, x \in V, y_1, y_2, y \in W, d \in D$ .  $F$  is said to be nondegenerate if  $F(x, y) = 0$  for all  $y \in W$  implies  $x = 0$  and  $F(x, y) = 0$  for all  $x \in V$  implies  $y = 0$ . A similar definition holds when  $V$  is a right vector space and  $W$  is a left vector space over  $D$ .

THEOREM 6: Let  $V$  be a finite dimensional left vector space and  $W$  a finite dimensional right vector space over a division ring  $D$ . Then  $V$  and  $W$  are duals of each other if and only if there exists a nondegenerate bilinear form  $F: V \times W \rightarrow D$ .



PROOF: Suppose  $W=V^*$ . Define  $F:V \times W \rightarrow D$  by  $F(x,f)=f(x)$ ,  $x \in V$ ,  $f \in V^*=W$ .  $F$  is obviously bilinear. If  $F(x,f)=0$  for all  $x \in V$ , fixed  $f$ , then  $f=0$  since  $f$  is a homomorphism on  $V$ . If  $F(x,f)=0$  for all  $f$ , fixed  $x$ , then  $x=0$  since  $0=f(x)=x^{**}(f)$  for all  $f$  which implies  $x^{**}=0$  and hence  $x=0$ . Thus  $F$  is nondegenerate.

Conversely, suppose  $F:V \times W \rightarrow D$  is a nondegenerate bilinear function. If  $y \in W$ , define  $f_y \in V^*$  by  $f_y(x)=F(x,y)$ . Now we have to show  $f_y$  is really an element of  $V^*$  and this is immediate since  $F$  is linear in  $x$ . Now the linearity of  $F$  in  $y$  means that  $f_{y_1+y_2}=f_{y_1}+f_{y_2}$  and  $f_{y_1d}=(f_{y_1})d$ . Thus the mapping  $W \rightarrow V^*$  given by  $y \rightarrow f_y$  is a linear transformation over  $D$ . If  $f_y=0$ , then  $F(x,y)=0$  for all  $x$ . Then by the nondegeneracy of  $F$ ,  $y=0$ . Therefore the mapping  $W \rightarrow V^*$  given above is actually a monomorphism and hence  $\dim W \leq \dim V^* = \dim V$ . In exactly the same way,  $\dim V \leq \dim W^* = \dim W$ . Hence  $\dim V^* = \dim W$  and the map  $W \rightarrow V^*$  is an isomorphism. Similarly  $V$  and  $W^*$  are also isomorphic.

## 2. Matrices.

DEFINITION 6: Let  $I$  and  $J$  be sets. A mapping  $A$  defined on  $I \times J$  is called a matrix of type  $(I,J)$ . A matrix of type  $(I,I)$  is called a square matrix.  $A$  is called a row matrix or a column

matrix according as  $I = \{1\}$  or  $J = \{1\}$ . If  $I = 1, 2, \dots, m$  and  $J = 1, 2, \dots, n$ . Where  $m$  and  $n$  are positive integers,  $A$  is called an  $m \times n$  matrix or matrix of type  $(m, n)$ . An  $n \times n$  matrix is called a square matrix of degree  $n$ .

If  $A(i, j) = a_{ij}$  for  $(i, j) \in I \times J$ , the matrix itself is denoted by  $(a_{ij})$ .

Suppose  $\{A_{ij}\}_{(i,j) \in I \times J}$  be a

family of sets indexed by  $I \times J$ . If  $\mathcal{O}$  denotes the set of matrices  $(a_{ij})$  such that  $a_{ij} \in A_{ij}$ , then

$$\mathcal{O} = \prod_{(i,j) \in I \times J} A_{ij}$$

Then it follows that if  $A_{ij}$  is an additive group or a left  $R$ -module for each  $(i, j)$  so is  $\mathcal{O}$ . Notice that the addition and module multiplication are given by

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$

$$r(a_{ij}) = (ra_{ij})$$

Let  $M$  and  $N$  be two left  $R$  modules. Suppose  $\{M_i\}_{i \in I}$  be a family of submodules of  $M$  and  $N_j$  a family of submodules of  $N$  such that  $M = \sum_{i \in I} \oplus M_i$  and  $N = \sum_{j \in J} \oplus N_j$ . If  $f: M \rightarrow N$  is a linear map, then we have

$$M_i \xrightarrow{f_i} M \xrightarrow{f} N \xrightarrow{p_j} N_j$$

where  $q_i$  is the injection and  $p_j$  is the projection. Then their composition  $f_{ij} = p_j f q_i$  is a linear map of  $M_i$  into  $N_j$ .

DEFINITION 7: The matrix  $F = (f_{ij})_{(j,i) \in (J \times I)}$  of type  $(J, I)$  is called the representative matrix of the map  $f$ .

THEOREM 7: Let  $f: M \rightarrow N$  be a linear map of the modules  $M$  and  $N$ . Then  $F = (f_{ij})_{(j,i) \in J \times I}$  is a representative matrix if and only if for each  $x \in M_i$  there exists only a finite number of indices  $(i, j)$  such that  $f_{ij}(x) \neq 0$ .

PROOF: Exercise.

Let  $M \xrightarrow{f} N \xrightarrow{g} T$  be modules and maps where  $M = \sum_{i \in I} \oplus M_i$ ,  $N = \sum_{j \in J} \oplus N_j$  and  $T = \sum_{k \in K} \oplus T_k$ . If  $F = (f_{ij})_{(j,i) \in I \times J}$  and  $G = (g_{jk})_{(k,j) \in K \times J}$  are the representative matrices of  $f$  and  $g$  respectively what is the representative matrix  $H = (h_{ik})_{(k,i) \in K \times I}$  of  $gf$ ?

Let  $x \in M_i$ . Then

$$h(x) = g(f(x)) = g\left(\sum_{j \in J} f_{ij}(x)\right) = \sum_{j \in J} g(f_{ij}(x))$$

Now  $f_{ij}(x) \in N_j$  so that  $g(f_{ij}(x)) = \sum_{k \in K} g_{jk}(f_{ij}(x))$

Hence

$$h_{ik}(x) = \sum_{j \in J} (g_{jk} f_{ij})(x)$$

If  $J$  is a finite set, we have

$$h_{ik} = \sum_{j \in J} g_{jk} f_{ij}$$



DEFINITION 8: If  $A=(a_{ij})$  is a matrix of type  $(I,J)$  and  $i \in I$ , then the mapping  $\rho:(1,j) \longrightarrow a_{ij}$  is called the row of index  $i$  of  $A$ . Similarly the mapping  $\gamma:(i,1) \longrightarrow a_{ij}$  is called the column of index  $j$  of  $A$ .

From now on we assume that the elements  $a_{ij}$  come from a ring  $R$ .

DEFINITION 9: The matrix  $(a_{ij})$  is said to be column finite if there are only a finite number of non zero elements  $a_{ij}$  in each column. Let  $B=(b_{kj})_{(k,j) \in K \times J}$  be any matrix of type  $(K,J)$  and  $A=(a_{ji})$  any column finite matrix of type  $(J,I)$ . If  $k \in K, i \in I$ , then the product  $\rho_k \gamma_i$ , where  $\rho_k$  is the row of index  $k$  of  $B$  and  $\gamma_i$  is the column of index  $i$  of  $A$ , is defined by

$$\rho_k \gamma_i = \sum_{j \in J} a_{ji} b_{kj}$$

The matrix  $(\rho_k \gamma_i)_{(k,i) \in K \times I}$  is called the product of the matrices  $B$  and  $A$  and is denoted by  $BA$ .

If  $M$  and  $N$  are free modules over a ring  $R$  with free bases  $\{x_i\}_{i \in I}$  and  $\{y_j\}_{j \in J}$  respectively, then  $f_{ij}: R \times_i \longrightarrow R \times_j$ , so that there exists  $a_{ij} \in R$  such that  $f_{ij}(x_i) = a_{ij} y_j$ . The matrix  $(a_{ij})_{(j,i) \in J \times I}$  is the representative matrix of  $f$  with respect to the bases  $\{x_i\}, \{y_j\}$ .

THEOREM 8: Let  $M, N, T$  be left modules over a ring  $R$  with free bases  $\{x_i\}_{i \in I}$ ,  $\{y_j\}_{j \in J}$  and  $\{z_k\}_{k \in K}$  respectively. Let  $M \xrightarrow{f} N \xrightarrow{g} T$ . Suppose  $A$  is the representative matrix of  $f$  with respect to the bases  $\{x_i\}$  and  $\{y_j\}$  and  $B$  the representative matrix of  $g$  with respect to the bases  $\{y_j\}$  and  $\{z_k\}$ . Then the representative matrix of  $gf$  with respect to the bases  $\{x_i\}$  and  $\{z_k\}$  is  $BA$ .

PROOF: Suppose  $F, G, H$  denote the representative matrices for  $f, g$  and  $gf$  respectively with respect to the bases. We then have

$$f_{ij}(x_i) = a_{ij}y_j, \quad g_{jk}(y_j) = b_{jk}z_k$$

where  $a_{ij}, b_{jk} \in R$ . Then, since  $(a_{ij})$  is row finite,

$$h_{ik}(x) = \sum_{j \in J} (g_{jk}f_{ij})(x)$$

so that

$$\begin{aligned} h_{ik}(x_i) &= \sum_{j \in J} (g_{jk}f_{ij})(x_i) = \sum_{j \in J} g_{jk}(f_{ij}(x_i)) \\ &= \sum_{j \in J} g_{jk}(a_{ij}y_j) = \sum_{j \in J} a_{ij}g_{jk}(y_j) \\ &= \sum_{j \in J} a_{ij}b_{jk}z_k \end{aligned}$$

Thus  $C = (c_{ik})_{(i,k) \in K \times I}$  is the representative matrix for  $gf$  with respect to the bases where

$$c_{ik} = \sum_{j \in J} a_{ij}b_{jk}$$

This completes the proof.

**DEFINITION 10:** The unit matrix of type  $(I, I)$  is the matrix  $(\delta_{ij})$  where  $\delta_{ij} = 1$  if  $i = j$  or  $0$  if  $i \neq j$ .

The set of all square matrices of type  $(I, I)$  is the set of all endomorphisms of the module  $R_I = \sum_{i \in I} \oplus R_i$ . Where each  $R_i \cong R$  and the unit matrix is the representative matrix for the identity automorphism:

**DEFINITION 11:** A linear map  $f: V \rightarrow W$  where  $V$  and  $W$  are vector spaces is of finite rank if  $f(V)$  is finite dimensional and then the rank of  $f$  is defined to be the dimension of  $f(V)$ . A matrix  $A$  of type  $(I, J)$ , being the representative matrix of a map  $\varphi: R_J \rightarrow R_I$ , is of finite rank if  $\varphi$  is of finite rank. Then the rank of  $A$  is defined to be the rank of  $\varphi$ .

**THEOREM 9:** Let  $M$  and  $N$  be free modules with free basis  $\{x_j\}_{j \in J}$  and  $\{y_i\}_{i \in I}$  and  $f: M \rightarrow N$  a linear map. Then  $f$  is of finite rank if and only if  $A$  is of finite rank where  $A$  is the representative matrix of  $f$ . Further rank of  $f = \text{rank of } A$ .

**PROOF:** Exercise.



DEFINITION 12: Two column finite matrices  $A$  and  $B$  of type  $(I, J)$  are said to be equivalent if there exist invertible column finite square matrices  $P$  of type  $(I, I)$  and  $Q$  of type  $(J, J)$  such that  $B = PAQ$  (invertible element in a ring is the same as a unit)

Exercise 1. Show that the set of all column finite square matrices of type  $(I, I)$  is a ring with identity.

Exercise 2. Show that two equivalent matrices have the same rank.

DEFINITION 13: Let  $A$  be a matrix of type  $(I, J)$ . If  $I_1 \subset I$  and  $J_1 \subset J$ , then the restriction of  $A$  to  $I_1 \times J_1$  is a matrix of type  $(I_1, J_1)$  extracted from  $A$ .

Suppose  $I = \{1, 2, \dots, m\}$ ,  $J = \{1, 2, \dots, n\}$  where  $m$  and  $n$  are positive integers. Select integers

$$1 \leq m_1 < m_2 < \dots < m_p < m$$

and

$$1 \leq n_1 < n_2 < \dots < n_q < n$$

and set  $m_{p+1} = m+1$ ,  $n_{q+1} = n+1$ . If  $1 \leq s \leq p$  and  $1 \leq t \leq q$ , let

$$I_s = \{m_s, m_s+1, \dots, m_{s+1}-1\}$$

and

$$J_t = \{n_t, n_t+1, \dots, n_{t+1}-1\}$$

Suppose  $A_{st} = (a'_{\lambda, \mu})$  ( $1 \leq \lambda \leq m_{s+1} - m_s$  and  $1 \leq \mu \leq n_{t+1} - n_t$ ) be given matrix of type  $(m_{s+1} - m_s, n_{t+1} - n_t)$ . If we set

$$a_{ij} = a'_{i-m_s+1, j-n_t+1} \quad i \in I_s, j \in J_t$$

we get the matrix of type  $(I_s, J_t)$  exacted from  $A$ . A matrix  $A=(a_{ij})$  of type  $(m,n)$  is then denoted by

$$A = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1q} \\ A_{21} & A_{22} & \dots & A_{2q} \\ \dots & \dots & \dots & \dots \\ A_{p1} & A_{p2} & \dots & A_{pq} \end{bmatrix}$$

THEOREM 10: Let  $A$  be a matrix of type  $(m,n)$  and of rank  $r$  with elements in a division ring. Then  $A$  is equivalent to the matrix

$$\begin{bmatrix} E_r & O_{r,n-r} \\ O_{m-r,r} & O_{m-r,n-r} \end{bmatrix}$$

where  $E_r$  is the unit matrix of degree  $r$  and  $O_{s,t}$  represents the zero matrix of type  $(s,t)$ .

PROOF: Exercise.

### 3. Algebra and ideals

DEFINITION 14: Let  $R$  be a commutative ring with

1. An algebra  $A$  over  $R$  is a module over  $R$  which is also a ring together with the mixed multiplications.

$$(\lambda x)y = x(\lambda y) = \lambda(xy) \text{ for all } x,y \in A, \lambda \in R$$

Example:1. Let  $V$  be a vector space over a field. Define  $xy=0$  for all  $x,y \in V$ . Then  $V$  is an algebra.

2. If  $V$  is a vector space over a field  $K$ , then  $\text{Hom}_K(V, V)$  is an algebra over  $K$ .

3. The set of all  $n \times n$  matrices over  $K$ .
4. Let  $A$  be a ring with 1 and let  $R$  be a subring of  $A$  containing 1 such that every element  $x \in R$  commutes with every element  $y \in A$ . Then  $A$  is an algebra over  $R$ .
5. Every commutative ring with 1 is an algebra over every subring containing 1.

DEFINITION 15: Let  $A$  be an algebra over  $R$ . A subalgebra  $B$  of  $A$  is a submodule of  $A$  which is itself an algebra over  $R$  relative to the multiplication of  $A$ .

Example: Every ideal of a commutative ring  $R$  with 1 is a subalgebra of  $R$  when considered as an algebra over itself.

DEFINITION 16: A left ideal  $I$  of an algebra  $A$  over  $R$  is a subalgebra of  $A$  such that  $AI \subseteq I$  and a right ideal if  $IA \subseteq I$ . If  $I$  is a two sided ideal of an algebra  $A$ , then  $A/I$  is also an algebra over  $R$  called the quotient algebra of  $A$  over its ideal  $I$ .

From now on, we consider only algebras over a field  $K$ .

Notation: Let  $S, T$  be nonempty subsets of  $A$ .

$$ST = \left\{ \sum s_i t_i \mid s_i \in S, t_i \in T \right\}$$

If  $I$  is a left ideal and  $J$  is a right ideal of an algebra



$A$ , then  $I:J$  is a two sided ideal of  $A$ . Thus  $A^2$  is a two sided ideal of  $A$ .

DEFINITION 17: Let  $S$  be a nonempty subset of an algebra  $A$ . Then the left annihilator  $J$  of  $S$  is defined by

$$J = \{x \in A \mid xS = 0\}$$

DEFINITION 18: The center of an algebra  $A$  is the set  $\{x \in A \mid xy = yx \text{ for all } y \in A\}$ .

Exercise 3. Let  $S$  be a nonempty subset of an algebra  $A$ . If  $J$  is the left annihilator of  $S$ , show that  $J$  is a left ideal of  $A$ . Further if  $S$  is a left ideal of  $A$ , this  $J$  is a two sided ideal of  $A$ .

Exercise 4. The center of  $A$  is a subalgebra.

Exercise 5. The intersection of an arbitrary family of subalgebras is again a subalgebra.

DEFINITION 19: An algebra  $A$  is called a division algebra if  $A$  has  $1$  and every nonzero element has a left inverse.

Exercise 6. Let  $A$  be an algebra with  $1$ . Show that  $A$  is a division algebra if and only if  $A$  has no left ideals other than  $0$  and  $A$ .

DEFINITION 19:  $A$  is a simple algebra if  $A^2 \neq 0$  and  $A$  has no two-sided ideals other than  $0$  and  $A$ . A similar definition holds for simple rings.

THEOREM 11: A simple algebra is a simple ring.

PROOF: Let  $A$  be a simple algebra. Let  $I \neq 0$  be a two sided ring ideal of  $A$ . We shall show that  $I=A$ .

$$\text{Let } B = \left\{ \sum_{i=1}^n \lambda_i x_i \mid x_i \in I, \lambda_i \in K \right\}$$

Then  $B$  is a two-sided ideal of  $A$ . To prove  $I^2 \subset I$ . We assert that  $A=A^2=ABI$ . Let  $y \in A$ .  $b = \sum \lambda_i x_i \in B$ . Then  $yb = y \left( \sum \lambda_i x_i \right) = \sum (\lambda_i y) (x_i) \in I$ .

Hence  $ABI \subset I$ . Therefore  $I=A$ .

THEOREM 12: Let  $A$  be the set of  $n \times n$  matrices over a division algebra (ring)  $D$ . Then  $A$  is a simple algebra (ring).

PROOF: Let  $e_{ij}$  be the matrix with 1 at the  $(i,j)^{\text{th}}$  spot and 0 else where

$$\text{Then } e_{11} + e_{22} + \dots + e_{nn} = I \in A$$

Let  $I \neq 0$  be a two-sided ideal of  $A$ . Let  $x \in I$ ,  $x \neq 0$ . Then  $e_{ij}$ 's generate  $A$  over  $D$ . Then  $x = \dots + \alpha e_{ij} + \dots$  where  $\alpha \neq 0$  and  $\alpha \in D$ .

Then  $\alpha^{-1} e_{ki} x e_{jk} = e_{kk} \in I$ . This implies  $1 = e_{11} + \dots + e_{nn} \in I$  also. Hence  $I=A$ .

THEOREM 13: Let  $I$  be a minimal two sided ideal in a ring (algebra)  $A$ . Suppose  $I^2 \neq 0$ . Then  $I$  is a simple ring (algebra).

PROOF: Exercise.

DEFINITION 20: Let  $x \in A$  where  $A$  is a ring.  $x$  is said to be nilpotent if there exists  $n > 0$  such that  $x^n = 0$ .  $x$  is said to be idempotent if  $x \neq 0$  and  $x^2 = x$ .

Exercise 7. Let  $A$  be a ring. If every nilpotent element of  $A$  is in the center of  $A$ , then every idempotent element is in the center of  $A$ .

Exercise 8. Let  $A$  be a ring with  $1$ . Let  $x$  be a nilpotent element of  $A$ . Prove that  $1+x$  has two sided inverse in  $A$ .

Let  $A$  be a ring and  $I$  and  $J$  are two sided ideals of  $A$  such that  $I \cap J = 0$  and  $I+J=A$ . Then  $A$  is the direct sum of  $I$  and  $J$ . Also every element of  $A$  can be uniquely expressed as  $x+y$  where  $x \in I, y \in J$ . If  $A=I \oplus J$ , then  $IJ=0$ . For, if  $x \in I, y \in J$ , then  $xy \in I \cap J = 0$ .

Now suppose  $A$  has  $1$  and  $A=I+J$ . Then  $1=e+f$   $e \in I, f \in J$ . Further  $ef=fe=0$  so that  $e^2=e$  and  $f^2=f$ . This means that  $e$  and  $f$  are orthogonal idempotents.

Let  $x \in I$ . Then  $x=xe+xf=xe$  and  $x=ex+fx=ex$ . Therefore  $e$  is the identity for  $I$ . Similarly  $f$  is the identity for  $J$ . We now assert that  $I=eA=eA$ . Now  $I \subseteq eA$  since  $x \in I$



implies  $x = xe \in Ae$ . But  $e \in I$ .  $\therefore Ae \subset I$ . Also  $J = Af = fA$ .

Thus  $A = Ae \oplus Af$ .

THEOREM 14: Let  $A$  be a ring and  $I$  a two-sided ideal with identity. Then  $I$  is a direct summand of  $A$ .

PROOF: Let  $e$  be the identity of  $I$ . Let  $J$  be the right annihilator of  $e$ . That is

$$J = \{ x \in A \mid ex = 0 \} .$$

Then  $J$  is a right ideal of  $A$ . Now let  $x \in A$ . Then  $ex = 0$  if and only if  $xe = 0$ . Suppose  $ex = 0$ . Now  $xe \in I$  and  $e$  is the identity for  $I$ . Therefore  $xe = e(xe) = (ex)e = 0$ . Conversely if  $xe = 0$ , then  $exe \in I$  and  $ex = (ex)e = e(xe) = 0$ . Thus  $J$  is also a left annihilator of  $e$ . Hence  $J$  is a two sided ideal. Let  $x \in I \cap J$ . If  $x \in I$ , then  $xe = x$ . If  $x \in J$ , then  $xe = 0$ . Hence  $I \cap J = 0$ .

Now let  $a \in A$ . Then  $a = ae + (a - ae)$ . Now  $ae \in I$ . Since  $((a - ae)e = ae - ae = 0, a - ae \in J$ .  $\therefore A = I + J$ .

This completes the proof.

DEFINITION 21: Let  $I$  be a left ideal of a ring  $A$ . Then  $A$  is said to be nilpotent if there exists an  $n > 0$  such that  $I^n = 0$ .

THEOREM 15: Let  $A$  be a ring. Then every nilpotent ideal of  $A$  is contained in a nilpotent two sided ideal of  $A$ .

PROOF: Let  $I$  be a left ideal of  $A$  and  $I^n = 0$ . Let  $J = IA + I$ . Then  $I \subset J$ . We assert that  $J$  is a two sided ideal.  $J$  is clearly a left ideal. Now we show that  $J$  is a right ideal also. Let  $x \in J$ . Then  $x$  has the representation

$$x = \sum y_i a_i + y$$

where  $y_i, y \in I$  and  $a_i \in A$ . Let  $b$  be any element of  $A$ . Then  $xb \in IA \subset IA + I = J$ . Thus  $J$  is a two sided ideal. Now we claim  $J^n = 0$ . Let  $x_1, \dots, x_n$  and  $y_1, \dots, y_n \in I$  and  $a_1, a_2, \dots, a_n \in A$ . It is enough to show that

$$(x_1 a_1 + y_1) \cdot (x_2 a_2 + y_2) \cdots (x_n a_n + y_n) = 0$$

and follows immediately from the expansion.

THEOREM 16: Let  $I$  be a minimal left ideal of a ring (algebra)  $A$ . Then either  $I^2 = 0$  or  $I = Ae$  where  $e$  is an idempotent.

PROOF: Suppose  $I^2 \neq 0$ . Then  $I^2 \subset I$  and  $I^2$  is a left ideal. Therefore  $I^2 = I$ . Further  $I^2 \neq 0$  implies there exists  $a \neq 0, a \in I$  such that  $Ia \neq 0$ . Then  $Ia \subset I$  and  $Ia$  is a left ideal. Hence  $Ia = I$ . Therefore there exists  $e \in I$  such that  $ea = a$ . Now  $e^2 a = ea$  or  $(e^2 - e)a = 0$ . Let  $J = \{x \in I \mid xa = 0\}$ . Then  $J$  is a left ideal of  $A$ .  $\therefore J \subset I$ . Hence  $J = 0$  or  $J = I$ . If  $J = I$ , then  $Ia = 0$  which is a contradiction. This means that  $J = 0$  and  $e$  is an idempotent. Again,  $Ae \neq 0$  and  $Ae \subset I$ .  $\therefore Ae = I$ .

THEOREM 17: Let  $e$  be an idempotent of a ring (algebra)  $A$  such that  $Ae$  is a minimal left ideal. Then  $eAe$  is a division ring (algebra).

PROOF: We first remark that if  $R$  is a ring with  $1$  such that every element  $\neq 0$  has a left inverse, then  $R$  is a division ring. Now  $eAe$  is a ring with  $e$  as the identity. Let  $ea \in Ae$ ,  $ea \neq 0$ . Then  $Aea \neq 0$  and  $Aea \subset Ae$ . Therefore  $Aea = Ae$ . Hence  $eAe \cdot ea = eAe$ . There exists therefore  $b \in Ae$  such that  $eba = e$ .

This completes the proof.

#### 4. Wedderburn's theorems

THEOREM 18: Let  $A$  be a finite dimensional algebra over a field  $K$ . Then  $A$  is isomorphic to the algebra of  $n \times n$  matrices over a division ring.

PROOF: Since  $A$  is finite dimensional,  $A$  has a minimal left ideal  $I \neq 0$ . If  $I^2 = 0$  then  $I$  is contained in a nilpotent two sided ideal  $J$ . Since  $A$  is simple  $J = A$ . Then  $A^2 = 0$  contradiction. Thus  $I^2 \neq 0$ . Hence  $I = Ae$  where  $e$  is an idempotent. Then  $eAe$  is a division ring. We identify  $K$  with  $Ke \subset eAe$ .  $Ae$  is therefore a finite dimensional right vector space over  $eAe$ .  $xe(ea) = (xea)e \in Ae$ . Similarly  $eA$  is a finite dimensional left vector space over  $eAe$ . We now assert that  $Ae$  and  $eA$  are duals of each other.

Define

$$F: eA \times Ae \longrightarrow eAe \quad \text{by}$$

$$F(ex, ye) = exye$$

$F$  is clearly bilinear. Thus we have to show that  $F$  is nondegenerate. Suppose  $F(ex, Ae) = 0$ . Then  $exAe = 0$  which implies  $exAeA = 0$ . Now  $AeA$  is a two sided ideal in  $A$ . Now  $e \notin AeA$  and  $e \neq 0$ . Therefore  $AeA = A$ . Hence  $exA = 0$ .

Now suppose  $J = \{z \in A \mid zA = 0\}$ . Then  $J$  is a two sided ideal of  $A$ . If  $J = A$ , then  $A^2 = 0$  which is a contradiction.  $\therefore J = 0$  and  $ex = 0$ . Similarly if  $F(eA, ye) = 0$  then  $ye = 0$ . Thus  $F$  is a nondegenerate bilinear form and our assertion is proved.

For each  $a \in A$ , let  $L_a: Ae \longrightarrow Ae$  by  $L_a(xe) = axe$ . Then

$$L_a(x_1e + x_2e) = a(x_1e + x_2e) = ax_1e + ax_2e$$

$$= L_a(x_1e) + L_a(x_2e)$$

and  $L_a(xe \cdot ebe) = axe \cdot ebe = (L_a(xe)) \cdot ebe$ . Thus  $L_a$  is a linear transformation of  $Ae$  over  $eAe$ . Further  $L_{a_1 + a_2}(xe) = (a_1 + a_2)(xe) = a_1xe + a_2xe = L_{a_1}(xe) + L_{a_2}(xe) = (L_{a_1} + L_{a_2})(xe)$  for all  $xe \in Ae$  which implies that  $L_{a_1 + a_2} = L_{a_1} + L_{a_2}$ .

Let  $L = \text{Hom}_{eAe}(Ae, Ae)$ . Then  $L$  is the set of  $n \times n$  matrices over  $eAe$ . We shall now show that  $A$  and  $L$  are isomorphic. To this end, we define a map  $\varphi: A \longrightarrow L$  by  $\varphi(a) = L_a$  for  $a \in A$  and show that  $\varphi$  is an algebra isomorphism. We need to check a few things here for  $\varphi$ . Let



$$a, a_1, a_2 \in A.$$

$$\begin{aligned} \varphi(a_1+a_2)(xe) &= L_{a_1+a_2}(xe) = (a_1+a_2)(xe) \\ &= L_{a_1}(xe) + L_{a_2}(xe) \\ &= \varphi(a_1)(xe) + \varphi(a_2)(xe) \\ &= (\varphi(a_1) + \varphi(a_2))(xe) \quad \text{for all } xe \in Ae \end{aligned}$$

Thus  $\varphi(a_1+a_2) = \varphi(a_1) + \varphi(a_2)$ .

Also  $\varphi(ebe \cdot a)(xe) = L_{ebe \cdot a}(xe) = ebe \cdot axe$  and  $(ebe\varphi(a))(xe) = (ebe \cdot L_a)(xe) = ebe \cdot axe$  so that  $\varphi(ebe \cdot a)(xe) = ebe \cdot \varphi(a) \cdot xe$  for all  $xe \in Ae$  which implies  $\varphi(ebe \cdot a) = ebe\varphi(a)$ . This shows that  $\varphi$  is a linear mapping of the left vector space over  $eAe$ .

Now we show it is an algebra homomorphism. It follows immediately since  $\varphi(a_1 \cdot a_2)(xe) = L_{a_1 a_2}(xe) = a_1 a_2(xe)$  and  $(\varphi(a_1)\varphi(a_2))(xe) = \varphi(a_1)(a_2 xe) = a_1 a_2(xe)$  so that  $\varphi(a_1 a_2)(xe) = \varphi(a_1)\varphi(a_2)xe$  for all  $xe \in Ae$ .

Now suppose  $\varphi(a) = 0$ . Then  $axe = 0$  for all  $x \in A$ . Therefore  $aAe = 0$  which implies  $aAeA = 0$ . By an argument already used, it follows that  $a = 0$  which proves that  $\varphi$  is one-to-one.

To complete the proof, it remains to show that  $\varphi$  is onto also. To this end, we choose a basis  $x_1e, x_2e, \dots, x_n e$  of  $Ae$  over  $eAe$ . Suppose  $xe$  is an arbitrary element of  $Ae$ . Let  $T_1$  be a linear mapping such that  $T(x_1e) = xe$  and  $T_1(x_j e) = 0$  for  $j \neq 1$ . Since any linear mapping  $Ae \rightarrow Ae$  is a linear combination of the  $T_1$ 's, if we can show that there exists  $a_1 \in A$  such that  $\varphi(a_1) = T_1$ , we would have established that  $\varphi$  is onto. This we do as follows. Since  $eA$  is the

dual space of  $Ae$ , there exists  $ey \in eA$  such that  $ey \cdot x_1 \cdot e = e$  and  $eyx_j e = 0$  for  $j \neq 1$ . Set  $a = xey$ . Then  $\varphi(a)(x_1 e) = ax_1 e = xey \cdot x_1 e = xe(yx_1 e) = xe$  and  $\varphi(a)(x_j e) = ax_j e = xeyx_j e = 0$ . Hence  $\varphi(a) = T_1$  and the proof is completed.

Remark. Let  $A$  be a finite dimensional algebra over a field  $K$ . Then the following are equivalent

- 1)  $A$  has no nonzero nilpotent left ideal
- 2)  $A$  has no nonzero nilpotent right ideal
- 3)  $A$  has no nonzero nilpotent two sided ideal

DEFINITION 22: A finite dimensional algebra over a field  $K$  is semi simple if  $A$  is a direct sum of simple algebras.

THEOREM 19: Let  $A$  be a finite dimensional algebra over a field  $K$ . Then  $A$  is semi simple if and only if  $A$  has no nonzero nilpotent two sided ideals.

PROOF: Suppose  $A$  is semi simple. Then  $A = A_1 \oplus A_2 \oplus \dots \oplus A_n$  where  $A_1$  is a simple algebra. Suppose  $I$  is a two sided ideal of  $A$ . Then  $I = I_1 \oplus I_2 \oplus \dots \oplus I_n$  where  $I_1$  is a two sided ideal of  $A_1$ . Since  $A_1$  is simple,  $I_1 = 0$  or  $A_1$ . Now  $I^2 = I_1^2 \oplus \dots \oplus I_n^2$ . Since  $0^2 = 0$  and  $A_1^2 = A_1$  it follows that  $I^2 = I_1 \oplus I_2 \oplus \dots \oplus I_n = I$  and  $I^n = I$ . Therefore  $I^n \neq 0$  for any  $n$  and  $I$  is not nilpotent.

Conversely, suppose  $A$  has no nilpotent two sided ideal. We show that  $A$  is semi simple. Let  $I \neq 0$  be a

minimal two sided ideal of  $A$ . Then  $I^2 \neq 0$  by hypothesis. Then  $I$  is a simple algebra. By Theorem 18,  $I$  consists of  $n \times n$  matrices over a division ring. Hence  $I$  has an identity.  $I$  is therefore a direct summand. That is  $A = I \oplus J$ . Then  $J$  has no nilpotent two sided ideals. To complete the proof we appeal to mathematical induction.

Remark. A finite dimensional semi simple algebra has an identity. Every simple algebra is also a semi simple algebra.

THEOREM 20: Let  $A$  be a finite dimensional algebra over a field  $K$ . Then there exists in  $A$  a unique two sided ideal  $J$  such that

(1)  $J$  is nilpotent

(2)  $J$  contains any nilpotent left or right ideal

(3)  $A/J$  is semi simple.

$J$  is called the Jacobson Radical of  $A$ .

PROOF: Suppose  $J \subset A$  is a nilpotent two sided ideal of maximum dimension and let  $I$  be any two sided nilpotent ideal. Suppose  $J^n = I^m = 0$ . Then

$$(J+I)^{m+n-1} = 0 \quad (\text{Prove})$$

Therefore  $J+I$  is nilpotent and  $J \subset J+I$ . By the maximality,  $J = J+I$  and hence  $I \subset J$ . Thus  $J$  contains every nilpotent

ideal of  $A$ . This proves (1) and (2). Now we shall prove (3).

Let  $I$  be a two sided ideal of  $A/J$ . Then  $I=L/J$  where  $L$  is a two sided ideal of  $A$ . Then it follows that  $I^n = \frac{L^n+J}{J}$ . Suppose  $I^m=0$ . Then  $\frac{L^m+J}{J}=0$  which means  $L^m+J=J$  and hence  $L^m \subset J$ . Since  $J$  is nilpotent there exists  $n$  such that  $J^n=0$ . This would imply  $L^{mn}=0$  and  $L$  is nilpotent. Hence  $L \subset J$  so that  $I=L/J=0$ .

This completes the proof.



## TENSOR PRODUCT, AND COMPLEXES

1. Tensor Product:

DEFINITION 1: Let  $R$  be a ring. Let  $A$  be a right  $R$ -module and  $B$  a left  $R$ -module. Let  $F$  be the free abelian group generated by  $A \times B$  i.e.  $F$  consists of all finite formal sums of the form

$$\sum n_i (a_i, b_i)$$

where  $n_i$  is an integer,  $a_i \in A$  and  $b_i \in B$ . Let  $S$  be the subgroup of  $F$  generated by elements of the form

$$(i) \quad (a_1 + a_2, b) - (a_1, b) - (a_2, b)$$

$$(ii) \quad (a, b_1 + b_2) - (a, b_1) - (a, b_2)$$

$$(iii) \quad (ar, b) - (a, rb) \quad r \in R$$

Then the tensor product  $A \otimes_R B$  of  $A$  and  $B$  is defined by

$$A \otimes_R B = F/S \quad (\text{abelian group})$$

We write  $A \otimes B$  instead of  $A \otimes_R B$  as there will be no confusion.

THEOREM 1: There exists a bilinear map  $f$

$f : A \times B \longrightarrow A \otimes B$  such that  $f(A \times B)$  generates  
 $A \otimes B$

PROOF: Define  $f(a,b) = (a,b) + S \in A \otimes B$ . Then  $f$  does  
the job.

Notation: The element  $(a,b) + S$  is denoted by  $a \otimes b$ .  
Then we have the following properties:

$$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$$

$$a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$$

$$ar \otimes b = a \otimes rb$$

$$a \otimes 0 = 0 \otimes b = 0$$

THEOREM 2: If  $G$  is an abelian group and

$h : A \times B \longrightarrow G$  is a bilinear map, there exists a  
unique  $\tilde{h} : A \otimes B \longrightarrow G$  where  $\tilde{h}$  is a  $\mathbb{Z}$ -homomor-  
phism such that the diagram

$$\begin{array}{ccc} A \times B & \xrightarrow{h} & G \\ & \searrow f & \nearrow \tilde{h} \\ & & A \otimes B \end{array}$$

commutes.

PROOF: Let  $F$  and  $S$  be as in Definition 1. Consider

$$h_1 : F \longrightarrow G$$

defined by  $h_1(a, b) = h(a, b)$ . Then  $h_1$  is bilinear and  $S \subset \text{Ker } h_1$ . Then  $h_1$  induces a map  $\tilde{h}$  on the quotient group  $A \otimes B$  such that  $\tilde{h}(a \otimes b) = h(a, b)$ . Now  $\tilde{h}f(a, b) = \tilde{h}(a \otimes b) = h(a, b)$ .

If we have  $g : A \otimes B \longrightarrow G$  such that  $gf = h$  also, then  $g(a \otimes b) = gf(a, b) = h(a, b) = \tilde{h}(a \otimes b)$ . Since the elements  $a \otimes b$  generate  $A \otimes B$ , and  $g, \tilde{h}$  agree on these generators, we have  $g = \tilde{h}$ .

THEOREM 3: Let  $(C, g)$  be a pair such that  $C$  is an abelian group and  $g : A \times B \longrightarrow C$  a bilinear map such that  $g(A \times B)$  generates  $C$ . Suppose for any abelian group  $G$  and a bilinear map  $h : A \times B \longrightarrow G$  there exists a homomorphism  $\tilde{h} : C \longrightarrow G$  such that  $\tilde{h}g = h$ . Then there exists a unique isomorphism.

$$\varphi : A \otimes B \longrightarrow C$$

such that  $\varphi f = g$

PROOF: Consider the commutative diagrams

$$\begin{array}{ccc} A \times B & & \\ f \downarrow & \searrow g & \\ A \otimes B & \xrightarrow{\varphi} & C \end{array}$$

$$\begin{array}{ccc} A \times B & & \\ g \downarrow & \searrow f & \\ C & \xrightarrow{\tilde{f}} & A \otimes B \end{array}$$

Now

$$\varphi \tilde{f}(g(a,b)) = \varphi(\tilde{f}g(a,b)) = \varphi f(a,b) = g(a,b)$$

Thus  $\varphi \tilde{f}$  is the identity on the generators of  $C$ . Similarly  $\tilde{f} \varphi$  is the identity on the generators of  $A \otimes B$ . Hence  $\varphi$  is an isomorphism.

Remark: Let  $G$  be an abelian group. In order to define a homomorphism  $\varphi : A \otimes B \longrightarrow G$ , it is necessary and sufficient to define  $\varphi$  to be a bilinear map on the generators.

Let  $A \xrightarrow{f} A'$  (right  $R$ -modules) and  $B \xrightarrow{g} B'$  (left  $R$ -modules). Then  $f$  and  $g$  induce a homomorphism

$$f \otimes g : A \otimes B \longrightarrow A' \otimes B'$$

where

$$(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$$

It follows immediately that if  $f : A \longrightarrow A$  and  $g : B \longrightarrow B$  are identity maps, then  $f \otimes g : A \otimes B \longrightarrow A \otimes B$  is also the identity map.

THEOREM 4: If  $A \xrightarrow{f} B \xrightarrow{g} C$  (right  $R$ -modules)  
and  $D \xrightarrow{h} E \xrightarrow{k} F$  (left  $R$ -modules)

then the diagram

$$\begin{array}{ccc} A \otimes D & \xrightarrow{gf \otimes kh} & C \otimes F \\ & \searrow f \otimes h & \nearrow g \otimes k \\ & B \otimes E & \end{array}$$



commutes.

PROOF: Check all the maps in the diagram are bilinear and apply the remark to show homomorphism. To prove the commutativity of the diagram, let  $a \in A, d \in D$ . Then

$$\begin{aligned} [(g \otimes k)(f \otimes h)](a \otimes b) &= (g \otimes k) [(f \otimes h)(a \otimes b)] \\ &= (g \otimes k)(f(a) \otimes h(b)) \\ &= gh(a) \otimes kh(b) = (gf \otimes kh)(a \otimes b) \end{aligned}$$

Thus  $(g \otimes k)(f \otimes h) = gf \otimes kh$  on the generators. This will imply that the diagram commutes.

COROLLARY: Suppose  $B$  is a left  $R$ -module and  $A,$   
 $\{A_k\}_{k \in K}$  are right  $R$ -modules. If  $(i_k, p_k)$  is a  
direct family for  $A$  and  $\{A_k\}_{k \in K}$

$$A_k \xleftarrow{i_k} A \xrightarrow{p_j} A_j \quad p_j i_k = \delta_{jk}$$

then  $(i_k \otimes 1, p_j \otimes 1)$  is a direct family for  $A \otimes B$   
and  $\{A_k \otimes B\}$

$$A_k \otimes B \xrightarrow{i_k \otimes 1} A \otimes B \xrightarrow{p_j \otimes 1} A_j \otimes B$$

THEOREM 5: (i) Let  $\{A_k\}_{k \in K}$  be a family of right R-modules and B a left R-module. Then

$$(\sum \oplus A_k) \otimes B \cong \sum \oplus (A \otimes B)$$

(ii) If  $\{B_k\}_{k \in K}$  is a family of left R-modules and A is a right R-module, then

$$A \otimes (\sum \oplus B_k) \cong \sum \oplus (A \otimes B_k)$$

PROOF: Exercise.

THEOREM 6: Let  $A', A, A''$  be right R-modules and  $B', B, B''$  be left R-modules such that the sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & A' & \xrightarrow{i} & A & \xrightarrow{p} & A'' \longrightarrow 0 \\ 0 & \longrightarrow & B' & \xrightarrow{j} & B & \xrightarrow{q} & B'' \longrightarrow 0 \end{array}$$

are exact, then we have a sequence

$$A' \otimes B' \xrightarrow{i \otimes j} A \otimes B \xrightarrow{p \otimes q} A'' \otimes B'' \longrightarrow 0$$

such that

- (i)  $p \otimes q$  is an epimorphism
- (ii)  $\text{Ker } p \otimes q$  is generated by elements of the form  
 $a \otimes b$  where  $a \in \text{Ker } p$  or  $b \in \text{Ker } q$ .

PROOF: Let  $C$  be the submodule generated by  $a \otimes b$  where  $a \in \text{Ker } p$  or  $b \in \text{Ker } q$ . Let  $a \otimes b$  be a generator of  $C$ . Then  $(p \otimes q)(a \otimes b) = p(a) \otimes q(b) = 0$ . Thus  $C \subset \text{Ker } p \otimes q$ . Then we have an induced homomorphism

$$\overline{p \otimes q} : \frac{A \otimes B}{C} \longrightarrow A'' \otimes B''$$

We shall now show that  $\overline{p \otimes q}$  is actually an isomorphism which will complete the proof. To this end, we define

$$\varphi : A'' \otimes B'' \longrightarrow \frac{A \otimes B}{C}$$

by  $\varphi(a'' \otimes b'') = a \otimes b + c$  where  $p(a) = a'', q(b) = b''$ . First we verify that  $\varphi$  is well-defined. If  $p(a_1) = a''$  and  $q(b_1) = b''$  also, then  $a - a_1 \in \text{Ker } p$  and  $b - b_1 \in \text{Ker } q$ . Then  $a \otimes b - a_1 \otimes b_1 = a \otimes b - a_1 \otimes b + a_1 \otimes b - a_1 \otimes b_1 = (a - a_1) \otimes b + a_1 \otimes (b - b_1)$ . Since  $a - a_1 \in \text{Ker } p$  and  $b - b_1 \in \text{Ker } q$ , we have  $a \otimes b - a_1 \otimes b_1 \in C$ .  $\varphi$  is easily seen to be bilinear and hence can be extended to a homomorphism on  $A'' \otimes B''$ . Now

$$\begin{aligned} \overline{p \otimes q} \cdot h(a'' \otimes b'') &= \overline{p \otimes q}(a \otimes b + c) = p(a) \otimes q(b) \\ &= a'' \otimes b'' \end{aligned}$$

Thus  $\overline{p \otimes q} \cdot h = 1$  on generators of  $A'' \otimes B''$  and hence on  $A'' \otimes B''$

Further:

$$h \cdot \overline{p \otimes q}(a \otimes b + c) = h(p(a) \otimes q(b)) = a \otimes b + c$$

Thus  $h \cdot \overline{p \otimes q} = 1$  on  $\frac{A \otimes B}{C}$  also.

This completes the proof.

COROLLARY 1: If B is a left R-module and

$$0 \longrightarrow A' \xrightarrow{i} A \xrightarrow{p} A'' \longrightarrow 0$$

is an exact sequence of right R-modules then

$$A' \otimes B \xrightarrow{i \otimes 1} A \otimes B \xrightarrow{p \otimes 1} A'' \otimes B \longrightarrow 0$$

is exact.

COROLLARY 2: If B is a right R-module and

$$0 \longrightarrow A' \xrightarrow{i} A \xrightarrow{p} A'' \longrightarrow 0$$

is an exact sequence of left R-modules, then

$$B \otimes A' \xrightarrow{1 \otimes i} B \otimes A \xrightarrow{1 \otimes p} B \otimes A'' \longrightarrow 0$$

is exact.

THEOREM 7: If A is a left R-module then  $R \otimes A \cong A$

PROOF: Define  $\varphi: R \otimes A \longrightarrow A$  by  $\varphi(r \otimes a) = ra$  and  $\psi: A \longrightarrow R \otimes A$  by  $\psi(a) = 1 \otimes a$  check that  $\varphi\psi = 1$  on  $A$  and  $\psi\varphi = 1$  on  $R \otimes A$ .

THEOREM 8: Let I be a right ideal of R and A a left R-module. Then  $R/I \otimes A \cong A/IA$ .

PROOF: Now  $0 \longrightarrow I \xrightarrow{i} R \xrightarrow{p} R/I \longrightarrow 0$

is exact. Hence

$$I \otimes A \xrightarrow{i \otimes 1} R \otimes A \xrightarrow{p \otimes 1} \frac{R}{I} \otimes A \longrightarrow 0$$

is also exact.



Now consider the diagram

$$\begin{array}{ccccccc}
 I \otimes A & \xrightarrow{i \otimes 1} & R \otimes A & \xrightarrow{p \otimes 1} & \frac{R}{I} \otimes A & \longrightarrow & 0 \\
 \downarrow \varphi_1 & & \downarrow \varphi & & \downarrow f & & \\
 0 & \longrightarrow & IA & \xrightarrow{j} & A & \xrightarrow{q} & \frac{A}{IA} \longrightarrow 0
 \end{array}$$

Define  $\varphi_1: I \otimes A \longrightarrow IA$  by  $\varphi_1(x \otimes a) = xa$   
 $\varphi: R \otimes A \longrightarrow A$  by  $\varphi(r \otimes a) = ra$

where  $x \in I$ ,  $r \in R$  and  $a \in A$ . Then  $j \varphi_1 = \varphi(i \otimes 1)$

Now define  $f: \frac{R}{I} \otimes A \longrightarrow A/IA$  as follows:

Let  $r \in R$ ,  $a \in A$ . Set

$$f((r+I) \otimes a) = ra + IA$$

Check that  $f$  is well defined and bilinear. Thus induces a homomorphism  $f: \frac{R}{I} \otimes A \longrightarrow A/IA$ . If  $a \in A$ , then  $a + IA = f((1+I)a)$  so that  $f$  is onto. We have to show that  $f$  is 1-1. Suppose  $f(z) = 0$  where  $z \in \frac{R}{I} \otimes A$ . Now  $z = (p \otimes 1)\omega$  for some  $\omega \in R \otimes A$ . Now  $q \varphi(\omega) = f(p \otimes 1)\omega = f(z) = 0$ . Hence  $\varphi(\omega) \in \text{Ker } q = \text{Im } j$ . Therefore  $\varphi(\omega) = j(x)$  for some  $x \in IA$ .  $\varphi_1$  being onto, there exists  $y \in I \otimes A$  such that  $\varphi_1(y) = x$ . Then  $\varphi(i \otimes 1)(y) = j \varphi_1(y) = j(x) = \varphi(\omega)$ . Since  $\varphi$  is 1-1,  $(i \otimes 1)(y) = \omega$ . Then  $z = (p \otimes 1)\omega = (p \otimes 1)(i \otimes 1)(y) = (pi \otimes 1)y = 0$ . Hence  $f$  is 1-1 also.

Exercise 1: Let  $B$  be a left  $R$ -module and

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$$

is a split exact sequence of right  $R$ -modules show that

$$0 \longrightarrow A' \otimes B \longrightarrow A \otimes B \longrightarrow A'' \otimes B \longrightarrow 0$$

is exact and splits.

Exercise 2: Show that if  $F$  is a free right  $R$ -module and  $0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$  is an exact sequence of left  $R$ -modules, then

$$0 \longrightarrow A' \otimes F \longrightarrow A \otimes F \longrightarrow A'' \otimes F \longrightarrow 0$$

is exact.

Exercise 3: Let  $P$  be a projective right  $R$ -module and  $0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$  is an exact sequence of left  $R$ -modules. Then

$$0 \longrightarrow A' \otimes P \longrightarrow A \otimes P \longrightarrow A'' \otimes P \longrightarrow 0$$

is exact.

2. Group of Homomorphisms

DEFINITION 2: Let  $A, B$  be left  $R$ -modules. Define

$\text{Hom}_R(A, B)$  to be the set of all  $R$ -homomorphisms of  $A$  into  $B$ .

In the following we will write  $\text{Hom}(A, B)$  instead of  $\text{Hom}_R(A, B)$ , the underlying ring being understood.

$\text{Hom}(A, B)$  is an abelian group when addition is defined by  $(f+g)(x) = f(x)+g(x)$  for all  $x \in A$ , where  $f, g \in \text{Hom}(A, B)$ . If we take multiplication as composition  $\text{Hom}(A, B)$  becomes a ring with identity.

Suppose  $A, B, C, D$  are left  $R$ -modules and

$$f : A \longrightarrow B$$

$$g : D \longrightarrow C$$

are  $R$ -homomorphisms. Then there exists a homomorphism  $\text{Hom}(f, g)$  of the abelian groups

$$\text{Hom}(f, g) : \text{Hom}(B, D) \longrightarrow \text{Hom}(A, C)$$

defined as follows:

Let  $h \in \text{Hom}(B, D)$ . Set  $\text{Hom}(f, g)h = ghf$ .

It is easy to check that  $\text{Hom}(f, g)$  is a homomorphism.

It follows immediately that if  $f : A \longrightarrow A$  and  $g : B \longrightarrow B$  are identity maps then

$\text{Hom}(f, g) : \text{Hom}(A, B) \longrightarrow \text{Hom}(A, B)$  is also the identity map.

THEOREM 9: If A, B, C, D are left R-modules and  
 $B \xrightarrow{g} C \xrightarrow{h} D$  are homomorphisms, then the diagrams

$$\begin{array}{ccc} \text{Hom}(A, B) & \xrightarrow{\text{Hom}(1, hg)} & \text{Hom}(A, D) \\ & \searrow \text{Hom}(1, g) & \nearrow \text{Hom}(1, h) \\ & & \text{Hom}(A, C) \end{array}$$

and

$$\begin{array}{ccc} \text{Hom}(D, A) & \xrightarrow{\text{Hom}(gh, 1)} & \text{Hom}(B, A) \\ & \searrow \text{Hom}(h, 1) & \nearrow \text{Hom}(g, 1) \\ & & \text{Hom}(C, A) \end{array}$$

are commutative.

PROOF: We prove the first part. The second one is similar. Let  $\varphi \in \text{Hom}(A, B)$ . Then

$$\text{Hom}(1, hg) \varphi = hg \varphi$$

now

$$\begin{aligned} [\text{Hom}(1, h) \text{Hom}(1, g)] \varphi &= \text{Hom}(1, h)(\text{Hom}(1, g) \varphi) \\ &= \text{Hom}(1, h)g \varphi = h(g \varphi) \\ &= hg \varphi \end{aligned}$$



THEOREM 10: If  $A, B, C$  are left  $R$ -modules and  $f, g \in \text{Hom}(A, B)$ , then

$$\text{Hom}(f+g, l) = \text{Hom}(f, l) + \text{Hom}(g, l)$$

and

$$\text{Hom}(l, f+g) = \text{Hom}(l, f) + \text{Hom}(l, g)$$

PROOF: Let  $\varphi \in \text{Hom}(B, C)$  and  $x \in A$ . Then

$$\begin{aligned} (\text{Hom}(f+g, l) \varphi)(x) &= \varphi(f+g)(x) = \varphi f(x) + \varphi g(x) \\ &= \text{Hom}(f, l) \varphi(x) + \text{Hom}(g, l) \varphi(x) \\ &= (\text{Hom}(f, l) \varphi + \text{Hom}(g, l) \varphi)(x) \end{aligned}$$

for all  $x \in A$ . Then

$$\text{Hom}(f+g, l) \varphi = \text{Hom}(f, l) \varphi + \text{Hom}(g, l) \varphi$$

$\varphi$  being arbitrary the result follows.

Exercise: Let  $A$  and  $B$  be left  $R$ -modules and

$\{B_k\}_{k \in K}$  a family of left  $R$ -modules. If  $(i_k, p_k)$  is a direct family for  $B$  and  $\{B_k\}_{k \in K}$ , show that  $(\text{Hom}(1, i_k), \text{Hom}(1, p_k))$  is a direct family for  $\text{Hom}(A, B)$  and  $\{\text{Hom}(A, B_k)\}$  and that  $(\text{Hom}(p_k, l), \text{Hom}(i_k, l))$  is a direct family for  $\text{Hom}(B, A)$  and  $\{\text{Hom}(B_k, A)\}$

Exercise. If  $A$  and  $\{B_k\}_{k \in K}$  are left  $R$ -modules  
then

$$\text{Hom}(\sum \oplus B_k, A) \cong \prod_{k \in K} \text{Hom}(B_k, A)$$

THEOREM 11. Let  $A, B, C, D$  be left  $R$ -modules. If the sequences

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

is exact, then

$$(1) 0 \longrightarrow \text{Hom}(D, A) \xrightarrow{\text{Hom}(1, i)} \text{Hom}(D, B) \xrightarrow{\text{Hom}(1, p)} \text{Hom}(D, C)$$

and

$$(2) 0 \longrightarrow \text{Hom}(C, D) \xrightarrow{\text{Hom}(p, 1)} \text{Hom}(B, D) \xrightarrow{\text{Hom}(i, 1)} \text{Hom}(A, D)$$

are exact.

Notation:  $\text{Hom}(1, f) = f_*$ ,  $\text{Hom}(f, 1) = f^*$

PROOF: We will prove (1) only. The proof of (2) is similar.

$$\text{Now } i_* = \text{Hom}(1, p) \text{Hom}(1, i) = \text{Hom}(1, pi) = \text{Hom}(1, 0) = 0$$

$$\text{Hence } \text{Im } i_* \subset \text{Ker } p_*$$

Next, we show that  $i_*$  is 1-1. To this end, let  $f \in \text{Hom}(D, A)$  such that  $i_*(f) = 0$ . By definition

$i_*(f) = \text{Hom}(1, i)f = if$ . Thus  $if = 0$ . Now if  $d \in D$ , then  $f(d) \in A$  and  $if(d) = 0$  so that  $f(d) \in \text{Ker } i$ . Since  $i$  is 1-1,  $f(d) = 0$ . Thus  $f(d) = 0$  for all  $d \in D$  which implies that  $f = 0$ .

Hence  $i_*$  is one to one.

To complete the proof, it remains to show that  $\text{Ker } p_* \subset i_*$ . Suppose  $f \in \text{Hom}(D, B)$  such that  $pf = p_*(f) = 0$ . We must find a  $g \in \text{Hom}(D, A)$  such that  $i_*(g) = f$ . Let  $d \in D$   $f(d) \in B$ . Then  $pf(d) = 0$ . Thus  $f(d) \in \text{Ker } p = \text{Im } i$ . Since  $i$  is 1-1, there exists a unique  $a \in A$  such that  $i(a) = f(d)$ . Define  $g(d) = a$ . Then  $g$  is a homomorphism. Also  $ig(d) = i(a) = f(d)$  for all  $d \in D$ . Hence  $ig = f$  or  $i_*(g) = f$ .

**THEOREM 12:** Let  $I$  be a left ideal of  $R$  and  $B$  a left  $R$ -module. Then

$$\text{Hom}(R/I, B) \cong \text{ann}_I(B)$$

**PROOF:** We recall that  $\text{ann}_I(B) = \{x \in B \mid rx = 0 \text{ for all } r \in I\}$ . Define  $\varphi: \text{Hom}(R/I, B) \rightarrow \text{ann}_I(B)$  as follows. Let  $f \in \text{Hom}(R/I, B)$ . Set  $\varphi(f) = f(1+I) \in B$ .

Now if  $f_1, f_2 \in \text{Hom}(R/I, B)$ , we have

$$\begin{aligned} \varphi(f_1 + f_2) &= (f_1 + f_2)(1+I) = f_1(1+I) + f_2(1+I) \\ &= \varphi(f_1) + \varphi(f_2) \end{aligned}$$

Now suppose  $\varphi(f) = \varphi(g)$ . Then  $f(1+I) = g(1+I)$ . Then  $f(\lambda + I) = f(\lambda(1+I)) = \lambda f(1+I) = \lambda g(1+I) = g(\lambda + I)$  which implies  $f = g$ .

Thus we have established that  $\varphi$  is a monomorphism of the abelian groups.

If  $\mu \in I$ , then  $\mu f(1+I) = f(\mu+I) = f(0+I) = 0$  so that  $f(1+I) \in \text{ann}_I(B)$ . This proves that  $\varphi$  maps into  $\text{ann}_I(B)$ . It remains to show that  $\varphi$  is onto. To see this, let  $x \in \text{ann}_I(B)$ . We define  $f(r+I) = rx$ ,  $f: R/I \longrightarrow B$ . Then  $f$  is a well defined  $R$ -homomorphism. Now  $\varphi(f) = f(1+I) = x$ .

This completes the proof.

COROLLARY: For every left  $R$ -module  $B$ .

$$\text{Hom}(R, B) \cong B$$

Exercise. Let  $A, B, C, D$ , be left  $R$ -modules. If

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

is exact and splits, so are

$$(1) 0 \longrightarrow \text{Hom}(C, D) \xrightarrow{p^*} \text{Hom}(B, D) \xrightarrow{i^*} \text{Hom}(A, D) \longrightarrow 0$$

and

$$(2) 0 \longrightarrow \text{Hom}(D, A) \xrightarrow{i_*} \text{Hom}(D, B) \xrightarrow{p_*} \text{Hom}(D, C) \longrightarrow 0$$

THEOREM 13: (1) A left  $R$ -module  $P$  is projective if and only if for every exact sequence

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

the sequence

$$0 \longrightarrow \text{Hom}(P, A) \xrightarrow{i_*} \text{Hom}(P, B) \xrightarrow{p_*} \text{Hom}(P, C) \longrightarrow 0$$

is exact.

(2) A left  $R$ -module is injective if and only if for every exact sequence

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$



the sequence

$$0 \longrightarrow \text{Hom}(C, Q) \xrightarrow{p^*} \text{Hom}(B, Q) \xrightarrow{i^*} \text{Hom}(A, Q) \longrightarrow 0$$

is exact

PROOF: We prove only (2). Enough to show  $Q$  is injective if and only if  $i^*$  is onto.

(i) Suppose  $Q$  is injective. Let  $f \in \text{Hom}(A, Q)$

Then we have

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B \\ & & \downarrow f & \swarrow & \\ & & Q & & \end{array}$$

where the top row is exact. Then, by definition there exists  $g : B \longrightarrow Q$  such that  $gi = f$ . Then  $f = gi = i^*(g)$  and  $i^*$  is onto.

(ii) Suppose  $i^*$  is onto. Then there exists  $g : B \longrightarrow Q$  such that  $i^*(g) = f$ . That is  $gi = f$  and  $Q$  is injective.

### 3. Divisible and Injective modules

We are going to show that every left module over a ring can be embedded in an injective module.

If  $R$  is commutative ring, and  $M$  is a left  $R$ -module, we can make  $M$  into a right module by putting  $mr = rm$  where  $m \in M$ ,  $r \in R$  and conversely. Thus all the modules over a commutative ring  $R$  are two sided.

Now if  $R$  is a commutative ring  $A \otimes B$  and  $\text{Hom}(A, B)$  can be given the structure of  $R$ -modules by defining

$$r(a \otimes b) = ar \otimes b = a \otimes rb$$

and for each  $f \in \text{Hom}(A, B)$ ,

$$(rf)(x) = r \cdot f(x) \quad r \in R, x \in A.$$

DEFINITION 3: Let  $R, S$  be two rings. If  $A$  is a left  $R$ -module and right  $S$ -module  $A$  is called a two sided module written  ${}_R A_S$  and define

$$r(as) = (ra)s \quad \text{for all } r \in R, a \in A, s \in S.$$

If  $A$  is a left  $R$ -module and a left  $S$ -module,  $A$  is called a  $R$ - $S$  bimodule, written  ${}_{R-S} A$  and define

$$s(ra) = r(sa) \quad r \in R, s \in S, a \in A.$$

Remarks: 1. If  ${}_{R-S} A, {}_R B$  are given, then  $\text{Hom}_R(A, B)$  is a right  $S$ -module under the definition

$$(fs)(a) = f(sa) \quad \text{for } f \in \text{Hom}_R(A, B) \quad a \in A, s \in S.$$

2. Given  $({}_R A, {}_R B)$ , then  $\text{Hom}_R(A, B)$  is a left  $S$ -module with the definition

$$(sf)(a) = f(as)$$

$a \in A, s \in S, f \in \text{Hom}_R(A, B).$

3. If  ${}_R A$  and  ${}_{R-S} B$  are given, then  $\text{Hom}_R(A, B)$  is a left  $S$ -module. Let

$$(sf)(a) = sf(a)$$

4. If  ${}_R A$  and  ${}_{R-S} B$  are given, then  $\text{Hom}_R(A, B)$  is a right  $S$ -module. Define

$$(fs)(a) = (f(a))s$$

5. Given  $({}_R A, {}_{R-S} B)$  then  $A \otimes_R B$  is a right  $S$ -module. Define

$$(a \otimes b)s = as \otimes b$$

6. Given  $({}_S A, {}_{R-S} B)$ ,  $A \otimes_R B$  is a left  $S$ -module. Define

$$s(a \otimes b) = sa \otimes b.$$

7. Given  $({}_R A, {}_{R-S} B)$ ,  $A \otimes_R B$  is a left  $S$ -module. Set

$$s(a \otimes b) = a \otimes sb$$

8. Given  $({}_R A, {}_{R-S} B)$ , then  $A \otimes_R B$  is a right  $S$ -module. Define

$$(a \otimes b)s = a \otimes bs$$

Then we have the following isomorphism laws.

THEOREM 14: (1) If  $R$  is a commutative ring and  $A, B$  are  $R$ -modules, then

$$A \otimes B \cong B \otimes A$$

(2) Let  $A_R, R^B, S^C$  be given. Then

$$A \otimes_R (B \otimes_S C) \cong (A \otimes_R B) \otimes_S C$$

(3) Let  $R^A, S^B, S^C$  be given. Then

$$\text{Hom}_S(B \otimes_R A, C) \cong \text{Hom}_R(A, \text{Hom}_S(B, C))$$

The proof is straight forward and hence omitted.

THEOREM 15: (Baer) A left  $R$ -module  $Q$  is injective if and only if every homomorphism  $g: I \rightarrow Q$  where  $I$  is a left ideal of  $R$  can be extended to a homomorphism  $f: R \rightarrow Q$

PROOF: If  $Q$  is injective, then the property follows from the definition.

Now suppose  $Q$  has the property stated in the theorem. We want to show  $Q$  is injective. Consider the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B \\ & & \downarrow h & & \\ & & Q & & \end{array}$$



Suppose  $A$  is a submodule of  $B$ . Let  $\mathcal{E}$  be the collection of all pairs  $(C, h_C)$  where  $C$  is a submodule of  $B$  containing  $A$  and  $h_C: C \rightarrow Q$  is a homomorphism extending  $h$ . We now introduce a partial ordering in  $\mathcal{E}$  by insisting that  $(C_1, h_{C_1}) < (C_2, h_{C_2})$  if  $C_1 \subset C_2$  and  $h_{C_2}$  is an extension of  $h_{C_1}$ . Let  $\alpha$  be a simply ordered chain in  $\mathcal{E}$ . Let  $D = \bigcup_{C \in \alpha} C$ . Define  $k: D \rightarrow Q$  by  $k(x) = h_C(x)$  when  $x \in C$ . Notice this is well defined since every  $x$  in  $D$  belongs to some  $C$  in  $\alpha$ . Then  $(D, k) \in \mathcal{E}$  and  $(C, h_C) < (D, k)$ . The application of Zorn's lemma gives a maximal element  $(E, p)$ . We assert  $E = B$ . Suppose  $E \neq B$ . Pick any element  $x_0 \in B$ ,  $x_0 \notin E$ . Let  $G = E + Rx_0$ . If  $I = \{r \in R \mid rx_0 \in E\}$ , then  $I$  is a left ideal of  $R$ . Define  $g: I \rightarrow Q$  by  $g(r) = p(rx_0)$ ,  $r \in I$ . Then  $g$  is a homomorphism. By assumption  $g$  extends to  $f: R \rightarrow Q$ . Now define  $q: G \rightarrow Q$  by

$$q(e+rx_0) = p(e)+f(r) \quad e \in E, r \in R.$$

Then  $q$  is a well defined homomorphism and extends  $p$ . By the maximality of  $(E, p)$ , this gives a contradiction. Hence  $E = B$ .

**DEFINITION 4:** A left  $R$ -module  $D$  is said to be divisible if  $x \in D$ ,  $r \in R$ ,  $r \neq 0$ , there exists  $y \in D$  such that  $ry = x$ .

THEOREM 16: If  $R$  is a ring with no zero divisors, every injective left  $R$ -module is divisible.

PROOF: Let  $Q$  be an injective left  $R$ -module. Let  $x \in Q$ ,  $x \neq 0$  and  $r \in R$ . We must show that there exists  $y \in Q$  such that  $ry = x$ . Define  $f: Rr \longrightarrow Q$  by  $f(sr) = sx$ . This is well defined since  $R$  has no divisors of zero. It is easy to verify that  $f$  is an  $R$ -homomorphism. By Baer's theorem, there exists  $g: R \longrightarrow Q$  extending  $f$ . Set  $y = g(1)$ . Then  $ry = rg(1) = g(r) = f(r) = x$ .

THEOREM 17: If  $R$  is a ring in which every left ideal is generated by a single element, then every divisible left  $R$ -module is injective.

PROOF: Let  $I$  be a left ideal of  $R$  and  $Q$  a divisible left module over  $R$ . Suppose  $f: I \longrightarrow Q$  is an  $R$ -homomorphism. Now  $I = Rr$  for some  $r \in R$ . Let  $x = f(r) \neq 0$ . Since  $Q$  is divisible, there exists  $y \in R$  such that  $ry = x$ . Define  $g: R \longrightarrow Q$  by  $g(1) = y$ . Then  $sr \in I$  and  $g(sr) = srg(1) = sry = sx = f(sx)$ . Hence  $g$  extends  $f$  and  $Q$  is injective.

THEOREM 18: If  $R$  is a principal ideal ring, then every  $R$ -module can be embedded in an injective  $R$ -module.

PROOF: Let  $A$  be an  $R$ -module. Then there exists a free module  $F$  and a submodule  $F'$  such that  $A \cong \frac{F}{F'}$ . Let  $Q$  be the quotient field of  $R$ . Then  $Q$  is divisible. We have an exact sequence

$$0 \longrightarrow R \longrightarrow Q \longrightarrow Q/R \longrightarrow 0$$

which gives an exact sequence.

$$0 \longrightarrow R \otimes F \longrightarrow Q \otimes F \longrightarrow Q/R \otimes F \longrightarrow 0$$

(see Exercise 2.) Now  $R \otimes F \cong F$ ,  $F' \subset F \subset Q \otimes F$ .  $Q \otimes F$  is a divisible  $R$ -module. The homomorphic image of a divisible module is also divisible (Prove).  $\frac{Q \otimes F}{F'}$  is also divisible. Then by Theorem 17,  $\frac{Q \otimes F}{F'}$  is injective.

This completes the proof.

**THEOREM 19:** Every left module  $A$  over a ring  $R$  can be embedded in an injective module  $C$

PROOF: Considering  $A$  as an abelian group there exists an injective (i.e. divisible) abelian group  $D$  containing  $A$ . (Note that we consider abelian groups as  $Z$  modules, where  $Z$  denotes integers). Let  $C = \text{Hom}_Z(R, D)$ . We assert that  $C$  satisfies our requirement. First we notice that  $C$  is  $R$ - $Z$  right module. We use the fact  $R$  is a right  $R$ -module to make  $C$  a left  $R$ -module by defining

$$(rf)(s) = f(sr) \quad r, s \in R.$$

Now we have to show that  $C$  is injective and  $A$  can be imbedded in  $C$ .

Now the sequence

$$0 \longrightarrow \text{Hom}_{\mathbb{Z}}(R, A) \longrightarrow \text{Hom}_{\mathbb{Z}}(R, D)$$

is exact and since these Hom's are both  $R$ -modules, this sequence is an exact sequence of  $R$ -modules. Further  $A \cong \text{Hom}_{\mathbb{Z}}(R, A)$  since  $A \subset D$ , every  $R$ -homomorphism is a fortiori a  $\mathbb{Z}$ -homomorphism. Hence  $\text{Hom}_R(R, A)$  is an abelian subgroup of  $\text{Hom}_{\mathbb{Z}}(R, A)$ . Now we shall make  $\text{Hom}_R(R, A)$  a left  $R$ -module. To do this, let  $f \in \text{Hom}_R(R, A)$  and  $r \in R$ . We have to show  $rf \in \text{Hom}_R(R, A)$ . But  $rf(s) = f(sr) \in A$  and

$$(rf)(s_1 s_2) = f(s_1 s_2 r) = s_1 f(s_2 r) = s_1 (rf)(s_2)$$

Thus  $rf$  is an  $R$ -homomorphism. Hence  $\text{Hom}_R(R, A)$  is an  $R$ -submodule of  $C$ .

To complete the proof, we have yet to show that  $C$  is injective.

Let  $0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$  be an exact sequence of left  $R$ -modules.

Now from Theorem 14, we have

$$\begin{aligned} \text{Hom}_R(X, \text{Hom}_{\mathbb{Z}}(R, D)) &\cong \text{Hom}_{\mathbb{Z}}(R \otimes_R X, D) \\ &\cong \text{Hom}_{\mathbb{Z}}(X, D) \end{aligned}$$

for the  $R$ -module  $X$ .



Now we have a commutative diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \text{Hom}_R(B'', \text{Hom}_Z(R, D)) & \longrightarrow & \text{Hom}_R(B, \text{Hom}_Z(R, D)) & \longrightarrow & \text{Hom}_R(B', \text{Hom}_Z(R, D)) \longrightarrow \dots \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Hom}_R(B'', D) & \longrightarrow & \text{Hom}_R(B, D) & \longrightarrow & \text{Hom}_R(B', D) \longrightarrow 0
 \end{array}$$

in which the vertical maps are isomorphisms and the bottom row is exact since  $D$  is injective. Chasing around the diagram, we get the top row is also exact and obtain an exact sequence

$$0 \longrightarrow \text{Hom}_R(B'', C) \longrightarrow \text{Hom}_R(B, C) \longrightarrow \text{Hom}_R(B', C) \longrightarrow 0$$

Thus  $C$  is injective by Theorem 13.

#### 4. Complexes and Resolutions

DEFINITION 5: A left complex over a ring  $R$  is a pair  $(C, d)$  where  $C$  is a left  $R$ -module and  $d: C \rightarrow C$  is an  $R$ -homomorphism such that  $d^2 = 0$ .

Let  $B = \text{Im } d$  and  $Z = \text{Ker } d$ . Then  $B \subseteq Z$ . Elements of  $B$  are called boundaries and the elements of  $Z$  are called cycles. Then  $H = Z/B$  is called the Homology Module.

DEFINITION 6: Let  $(C, d), (C', d')$  be complexes.

An  $R$ -homomorphism

$$f: C \longrightarrow C'$$

is called admissible or a complex map if  $d'f = fd$  and we write

$$f: (C, d) \longrightarrow (C', d')$$

Given  $f: (C, d) \longrightarrow (C', d')$  a complex map, we obtain an induced map

$$f_*: H \longrightarrow H'$$

defined by

$$f_*(z+B) = f(z)+B'$$

This is possible since  $f(z) \subset z'$  and  $f(B) \subset B'$

It has the following properties

(1) If  $f: (C, d) \longrightarrow (C', d')$  is the identity so is  $f_*$

(2) if  $f, g: (C, d) \longrightarrow (C', d')$  then  $(f+g)_* = f_*+g_*$

(3) If  $f: (C, d) \longrightarrow (C', d')$ ,

$g: (C', d') \longrightarrow (C'', d'')$  then

$$(gf)_* = g_*f_*$$

DEFINITION 7: Given  $f, g: (C, d) \longrightarrow (C', d')$ , we say that  $f, g$  are homotopic if there exists an  $R$ -homomorphism

$$D: C \longrightarrow C'$$

such that  $d'D + Dd = f - g$

THEOREM 20: If  $f, g: (C, d) \longrightarrow (C', d')$  are homotopic then  $f_* = g_*$

PROOF: There exists  $D: C \longrightarrow C'$  such that  $d'D + Dd = f - g$ . Then  $f = d'D + Dd + g$ . so that

$$\begin{aligned} f_*(z+B) &= f(z)+B' = (d'D + Dd + g)(z)+B' \\ &= d'D(z) + Dd(z) + g(z) + B' \end{aligned}$$

for  $z \in Z$ .

Now  $d(z) = 0$   $d'D(z) \in B'$ .

Hence  $f_*(z+B) = g(z)+B' = g_*(z+B)$

Suppose we are given an exact sequence of complexes

$$0 \longrightarrow (C', d') \xrightarrow{i} (C, d) \xrightarrow{p} (C'', d'') \longrightarrow 0$$

which means that  $i$  and  $p$  are complex maps and the sequence

$$0 \longrightarrow C' \longrightarrow C'' \longrightarrow 0 \text{ is exact.}$$

We are now going to introduce a map

$$\partial: H(C'') \longrightarrow H(C')$$

Let  $\bar{z}'' \in H(C'')$ . There exists  $z'' \in Z''$  such that  
 $\bar{z}'' = z'' + B''$ . There exists  $c \in C$  such that  $p(c) = z''$   
 Now  $p(dc) = (pd)(c) = d''(pc) = d''z'' = 0$

$$\therefore d(c) \in \text{Ker } \nu = \text{Im } i$$

Then  $d(c) = i(z')$ , where  $z' \in C$

$$\text{Now } i(d'(z')) = (id')(z') = (di)(z') = d(d(c)) = 0$$

$$\therefore d'z' = 0, \text{ since } i \text{ is 1-1. Hence } z' \in Z'$$

Define  $\partial(z'' + B'') = z' + B'$ . We shall now show that  $\partial$  is independent of the choice of representatives.

Suppose  $p(c') = z''$  also

Then  $p(c - c') = 0$  or  $c - c' = i(x)$ ,  $x \in C'$

$$d(c - c') = dc - dc' = iz' - iz'_1 = i(z' - z'_1)$$

$$dix = id'x, d'x = z' - z'_1$$

$$\therefore z' + B' = z'_1 + B'$$

Thus independent of the choice of  $c$  in  $C$ .

If  $p(c+y) = z'' + b''$ ,  $z'' \neq d''c''$ ,  $c'' \in C''$ . Take  $y \in C$  such that  $p(y) = c''$ . Then  $p(d(y)) = d''(p(y)) = d''c''$ . Then

$$d(c+dy) = dc + d^2y = dc = iz'$$

$$\partial(z'' + d''c'' + B'') = z' + B'$$

$\partial$  is independent of the choice of  $z''$ .

$\partial$  is an  $R$ -homomorphism.



DEFINITION 8:  $\partial$  is called the connecting homomorphism  
(or Bockstein operator)

THEOREM 21: Let

$$0 \longrightarrow (A', d') \xrightarrow{i} (A, d) \xrightarrow{p} (A'', d'') \longrightarrow 0$$

be an exact sequence of complexes. Then we have an  
exact sequence

$$\partial \longrightarrow H(A') \xrightarrow{i_*} H(A) \xrightarrow{p_*} H(A'') \xrightarrow{\partial} H(A') \longrightarrow$$

PROOF: Omitted.

DEFINITION 9: Let  $\{M_i\}$  be a family of submodules of  
an R-module M. This family is called a grading of M  
if  $M = \sum_{i \in \mathbb{Z}} \oplus M_i$  ( $z$  denotes integers) and M is called  
a graded module.

A submodule  $M'$  of M is called homogeneous if  
 $M' = \sum \oplus (M' \cap M_i)$ . The family  $\{M' \cap M_i\}$   
is called the induced grading of M and  $M'$  is graded.  
Then  $M/M'$  carries a canonical grading, for then

$$\frac{M}{M'} \cong \sum \oplus \frac{M_i}{M \cap M_i}$$

DEFINITION 10: Let  $M = \sum \oplus M_i$ ,  $N = \sum \oplus N_i$  be two graded  $R$ -modules. An  $R$ -homomorphism  $f: M \rightarrow N$  is said to be homogeneous of degree  $j$  if  $f(M_i) \subset N_{i+j}$

Given  $(X, d)$ ,  $X = \sum \oplus X_i$  and  $d$  of homogeneous of degree  $-1$ , we obtain

$$\longrightarrow X_n \xrightarrow{d_n} X_{n-1} \xrightarrow{d_{n-1}} X_{n-2} \longrightarrow$$

where  $d_n = d|_{X_n}$  and  $d_{n-1}d_n = 0$  and conversely.

Set  $X = \sum \oplus X_i$ ,  $d = \sum d_i$ ,  $Z_i(X) = \text{Ker } d_i$  and  $B_i(X) = \text{Im } d_{i+1}$

$$H_i(X) = \frac{Z_i(X)}{B_i(X)}$$

Then  $Z = \sum \oplus Z_i(X)$ ,  $B = \sum \oplus B_i(X)$  and

$$H = \sum \oplus H_i(X)$$

DEFINITION 11:  $(X, d_i)$  is called a left complex if

$X_i = 0$  for  $i < 0$ . Then

$$\longrightarrow X_n \xrightarrow{d_n} X_{n-1} \longrightarrow \dots \longrightarrow X_1 \longrightarrow X_0 \longrightarrow 0$$

and  $(X_i, d_i)$  is called a right complex if

$X_i = 0$  for  $i > 0$ . Then we write  $X^{-i} = X_i$ ,  
 $d^{-i} = d_i$

$$0 \longrightarrow X^1 \xrightarrow{d^1} X^2 \longrightarrow$$

DEFINITION 12: A complex  $(X_i, d_i)_{i \in \mathbb{Z}}$  is called projective (injective) if  $X_i$  is a projective (injective) module for all  $i$ , and it is said to be cyclic if  $H_1(X) = 0$  for all  $i$ .

DEFINITION 13: Given a left complex  $(X_i, d_i)$  the pair  $(A, \epsilon)$  where  $A$  is a left  $R$ -module and  $\epsilon: X_0 \rightarrow A$  is an epimorphism is called an augmentation of the complex if  $\text{Im } d_1 = \text{Ker } \epsilon$ . Given a right complex  $(X^i, d^i)$  the pair  $(A, \epsilon)$  is called an augmentation if  $A$  is a left  $R$ -module and  $\epsilon: A \rightarrow X^0$  is a monomorphism such that  $\text{Im } \epsilon = \text{Ker } d^0$ .

DEFINITION 14: Given the left  $R$ -module  $A$ , the complex  $(X_i, d_i)$  is called a projective resolution of  $A$  if  $(X_i, d_i)$  is a projective complex,  $H_i(X) = 0$  for all  $i > 0$  and if there exists an augmentation  $(A, \epsilon)$ .  $(X^i, d^i)$  is an injective resolution of  $A$  if  $(X^i, d^i)$  is an injective right complex such that  $H^i(X) = 0$  for  $i > 0$  and there exists an augmentation  $(A, \epsilon)$ .

THEOREM 22: Let  $A$  be a left  $R$ -module. Then  $A$  has a projective resolution.

PROOF: There exists a projective module  $X_0$  and an epimorphism  $\epsilon: X_0 \rightarrow A$ . Let  $Y_0 = \text{Ker } \epsilon$ . There exists a projective module  $X_1$  and epimorphism  $\alpha_1: X_1 \rightarrow Y_0$ . Let  $d_1$  denote the composition,  $X_1 \rightarrow Y_0 \rightarrow X_0$ . Complete the proof by induction.

THEOREM 23: Let  $A$  be a left  $R$ -module, then  $A$  has an injective resolution.

PROOF: Exercise.

### 5. Ext and Tor

DEFINITION 15: Let  $A, C$  be left  $R$ -modules. Consider a projective resolution  $(P, d)$  of  $A$ .

$$\rightarrow P_n \xrightarrow{d_n} P_{n-1} \rightarrow \cdots \rightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \rightarrow 0$$

Consider the sequence

$$0 \rightarrow \text{Hom}(P_0, C) \xrightarrow{\text{Hom}(d_1, 1)} \text{Hom}(P_1, C) \xrightarrow{\text{Hom}(d_2, 1)} \text{Hom}(P_2, C) \rightarrow \cdots$$

is no longer exact. But it is a complex since

$$\text{Hom}(d_{i+1}, 1) \text{Hom}(d_i, 1) = \text{Hom}(d_{i+1} d_i, 1) = 0$$

Denoting it by  $(\text{Hom}(P, C), \text{Hom}(d, 1))$

We define

$$\text{Ext}^n(A, C) = H^n(\text{Hom}(P, C))$$



DEFINITION 16: Suppose  $A$  is a right  $R$ -module and  $C$  is a left  $R$ -module. Let

$$\longrightarrow P_n \xrightarrow{d_n} P_{n-1} \longrightarrow \dots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \longrightarrow 0$$

be a projective resolution of  $A$ . Then

$$\longrightarrow P_n \otimes C \xrightarrow{d_n \otimes 1} P_{n-1} \otimes C \longrightarrow \dots \longrightarrow P_2 \otimes C \xrightarrow{d_2 \otimes 1} P_1 \otimes C \xrightarrow{d_1 \otimes 1} P_0 \otimes C \longrightarrow 0$$

is no longer exact. But it is a complex. Denoting this by  $(P \otimes C, d \otimes 1)$ , we define

$$\text{Tor}_n(A, C) = H_n(P \otimes C)$$

We shall just content with this definition of  $\text{Ext}$  and  $\text{Tor}$ . In fact they are independent of the projective resolution but we shall not prove it.

## MULTILINEAR ALGEBRA

1. Tensor Product

All the vector spaces considered in this Chapter are over a field  $F$ .

If  $U, V, W$  are vector spaces, a map  $f: V \times W \rightarrow U$  is bilinear if

$$f(\alpha_1 x_1 + \alpha_2 x_2, y) = \alpha_1 f(x_1, y) + \alpha_2 f(x_2, y)$$

$$f(x, \beta_1 y_1 + \beta_2 y_2) = \beta_1 f(x, y_1) + \beta_2 f(x, y_2)$$

where  $\alpha_1, \alpha_2, \beta_1, \beta_2 \in F$ ,  $x_1, x_2 \in V$ ,  $y_1, y_2 \in W$ . Similarly we define a multilinear map  $V_1 \times V_2 \times \dots \times V_n \rightarrow U$ .

The concept of tensor product has already been introduced in Chapter 4. However we will recall the definition for vector spaces.

Let  $V \circ W$  denote the linear space which consists of all formal sums

$$\sum \alpha_{xy}(x, y) \quad \alpha_{xy} \in F, \quad \alpha_{xy} = 0$$

except for a finite number of the pairs  $(x, y)$  where  $x \in V$ ,  $y \in W$ . Let  $S$  be the linear subspace of  $V \circ W$  generated by all elements of the form

$$(\alpha_1 x_1 + \alpha_2 x_2, \beta_1 y_1 + \beta_2 y_2) - \sum_{i,j=1}^2 \alpha_i \beta_j (x_i y_j)$$

Now  $V \times W$  is embedded in  $V \circ W$  with  $l.(x,y)=(x,y)$ . The tensor product is defined by

$$V \otimes W = \frac{V \circ W}{S}$$

Then we have

THEOREM 1: Let  $h: V \times W \rightarrow V \otimes W$  be the restriction of projection. Then

(1)  $h$  is bilinear

(2)  $h(V \times W)$  spans  $V \otimes W$

(3) If  $U$  is any vector space and

$f: V \times W \rightarrow U$  is any bilinear map there exists  $g: V \otimes W \rightarrow U$  such that  $f=gh$ .

THEOREM 2: If  $L(V,W;U)$  denotes the space of all bilinear maps  $V \times W \rightarrow U$  and  $L(V \otimes W, U)$  denotes the space of all linear maps  $V \otimes W \rightarrow U$  then  $L(V,W; U) \cong L(V \otimes W, U)$

As a consequence we have  $(V \otimes W)^* \cong L(V,W;F)$

THEOREM 3: If  $\dim V=m$ ,  $\dim W=n$ , then  $\dim V \otimes W=mn$

PROOF: Let  $e_1, \dots, e_m$  be a basis for  $V$  and  $f_1, \dots, f_n$  be a basis for  $W$ . Then it follows that

$$h\left(\sum_{i=1}^m \alpha_i e_i, \sum_{j=1}^n \beta_j f_j\right) = \sum_{i,j} \alpha_i \beta_j h(e_i, f_j)$$

Hence any element  $h(x,y)$  is a linear combination of  $h(e_i, f_j)$  which are  $mn$  in number. Since  $h(V \times W)$  spans

$V \otimes W$ ,  $\dim V \otimes W \leq mn$ .

Consider the bilinear maps

$$\varphi_{ij} : V \times W \rightarrow F$$

defined by

$$\varphi_{ij}(e_k, f_l) = \delta_{ik} \delta_{jl}$$

These maps are linearly independent in  $L(V, W; F)$ . Hence the vector space  $L(V, W; F)$  (and hence  $(V \otimes W)^*$ ) is of  $\dim \geq mn$ .

Thus we have proved that  $V \otimes W$  is of dimension  $mn$  and  $\{e_i \otimes f_j\}$  form a basis for  $V \otimes W$  where  $h(x, y) = x \otimes y$ .

**THEOREM 4:** If  $\dim V = m$  and  $\dim W = n$  and if there exists a bilinear map  $\varphi : V \times W \rightarrow U$  such that  $(V \times W)$  spans  $U$  and if  $\dim U = mn$ , then  $U \cong V \otimes W$ .

The following are also true

- (1)  $(V \otimes W)^* \cong V^* \otimes W^*$
- (2) space of endomorphisms of  $V$  is isomorphic to  $V \otimes V^*$
- (3)  $V \otimes W \cong W \otimes V$
- (4)  $V \otimes (W \otimes U) \cong (V \otimes W) \otimes U$

Analogously we have the following theorem.

**THEOREM 5:** To the Cartesian product  $V_1 \times V_2 \times \dots \times V_n$  of vector spaces, there exists a pair  $(V_1 \otimes V_2 \otimes \dots \otimes V_n, h)$  consisting of a vector space  $V_1 \otimes V_2 \otimes \dots \otimes V_n$  and a multilinear map  $h : V_1 \times V_2 \times \dots \times V_n \rightarrow V_1 \otimes V_2 \otimes \dots \otimes V_n$  such that to any multilinear



map  $f: V_1 \times V_2 \times \dots \times V_n \longrightarrow U$ , there exists a linear  
map  $g: V_1 \otimes \dots \otimes V_n \longrightarrow U$  such that  $f = gh$ . The  
space  $V_1 \otimes \dots \otimes V_n$  is determined to within  
isomorphism by the condition that it is spanned  
by  $h(V_1 \times V_2 \times \dots \times V_n)$ . Moreover it is isomorphic  
to  $((V_1 \otimes V_2) \otimes V_3) \otimes \dots \otimes V_n$  etc.

## 2. Covariant and Contravariant tensors.

DEFINITION 1: Let  $V$  be a vector space and  $V^*$  its dual space. Consider  $V_1 \otimes V_2 \otimes \dots \otimes V_t$  where each  $V_i$  is either  $V$  or  $V^*$ . If  $r$  of these  $V_i$ 's are  $V$  and  $s$  of these  $V_i$ 's are  $V^*$  ( $r+s=t$ ), an element of  $V_1 \otimes V_2 \otimes \dots \otimes V_n$  is called a tensor of the type  $(r, s)$  (contravariant of degree  $r$  and covariant of degree  $s$ ). A tensor of the type  $(r, 0)$  is called a contravariant tensor of degree  $r$  and a tensor of the type  $(0, s)$  is called a covariant tensor of degree  $s$ . A tensor of degree 1 is called a vector.

Notation.  $V_s^r = \underbrace{V \otimes V \otimes \dots \otimes V}_r \otimes \underbrace{V^* \otimes V^* \otimes \dots \otimes V^*}_s$

Let  $V$  be a vector space of dimension  $n$ . Suppose  $e_1, e_2, \dots, e_n$  be a basis for  $V$  and  $f^1, f^2, \dots, f^n$  be the dual basis for  $V^*$  which means  $f^j(e_i) = \delta_{ij}$ . We also

Thus an element  $x \in V_s^r$ , we may write  $x^{i_1 \dots i_r}_{j_1 \dots j_s}$  instead of  $x^{i_1 \dots i_r}_{j_1 \dots j_s}$ .

DEFINITION 2: If  $x_1$  and  $x_2$  are two tensors of the same type, the sum  $x_1 + x_2$  is defined by

$$(x_1 + x_2)^{i_1 \dots i_r}_{j_1 \dots j_s} = (x_1)^{i_1 \dots i_r}_{j_1 \dots j_s} + (x_2)^{i_1 \dots i_r}_{j_1 \dots j_s}$$

and the product  $\alpha x$ ,  $\alpha \in F$ ,  $x \in V_s^r$  is defined by

$$(\alpha x)^{i_1 \dots i_r}_{j_1 \dots j_s} = \alpha \cdot x^{i_1 \dots i_r}_{j_1 \dots j_s}$$

If  $x_1 \in V_{s_1}^{r_1}$  and  $x_2 \in V_{s_2}^{r_2}$  the product  $x_1 \otimes x_2 \in V_{s_1+s_2}^{r_1+r_2}$ .

Thus if  $x_1$  has the components  $(x_1)^{i_1 \dots i_{r_1}}_{j_1 \dots j_{s_1}}$

and  $x_2$  has the components  $(x_2)^{k_1 \dots k_{r_2}}_{l_1 \dots l_{s_2}}$  the

components of  $x_1 \otimes x_2$  is defined by

$$\begin{aligned} x_1 \otimes x_2^{i_1 \dots i_{r_1} k_1 \dots k_{r_2}}_{j_1 \dots j_{s_1} l_1 \dots l_{s_2}} \\ = (x_1)^{i_1 \dots i_{r_1}}_{j_1 \dots j_{s_1}} (x_2)^{k_1 \dots k_{r_2}}_{l_1 \dots l_{s_2}} \end{aligned}$$

DEFINITION 3: Suppose  $V \times V \times \dots \times V \times V^* \times V^* \times \dots \times V^*$  is a cartesian product with  $r$  factors  $V$  and  $s$  factors  $V^*$ . If  $1 \leq p \leq r$ ,  $1 \leq q \leq s$ , each multilinear map

$$h_{pq}: V \times V \times \dots \times V \times V^* \times V^* \times \dots \times V^* \longrightarrow V_{s-1}^{r-1}$$

defined by

$$\begin{aligned} h_{pq}(x_1, \dots, x_r, \bar{y}_1, \dots, \bar{y}_s) \\ = \langle x_p, \bar{y}_q \rangle x_1 \otimes x_2 \otimes \dots \otimes x_{p-1} \otimes x_{p+1} \otimes \dots \otimes x_r \otimes \bar{y}_1 \otimes \dots \\ \dots \otimes \bar{y}_{q-1} \otimes \bar{y}_{q+1} \otimes \dots \otimes \bar{y}_s \end{aligned}$$

induces a linear map

$$C_{pq}: V_s^r \longrightarrow V_{s-1}^{r-1}$$

called a contraction.

If  $x \in V_s^r$  with components  $x^{i_1 \dots i_r}_{j_1 \dots j_s}$  then

the components of  $C_{pq}(x)$  are given by

$$\sum_k x^{i_1 \dots i_{p-1} k i_{p+1} \dots i_r}_{j_1 \dots j_{q-1} k j_{q+1} \dots j_s}$$

where the summation is with respect to the  $p^{\text{th}}$  upper index and  $q^{\text{th}}$  lower index.

### 3. Symmetry and Skew symmetry.

Let  $V$  be a vector space and we consider  $V^r = V_0^r$ .

If  $\sigma$  is a permutation on  $1, 2, \dots, r$ , then

$$\sigma: V^r \longrightarrow V^r$$

given by  $\sigma(x_1 \otimes \dots \otimes x_r) = x_{\sigma_1} \otimes \dots \otimes x_{\sigma_r}$

DEFINITION 4:  $x \in V^r$  is called symmetric if  $\sigma(x) = x$  and skew symmetric if  $\sigma(x) = (\text{sgn } \sigma)x$ .

DEFINITION 5: A linear map  $f: V^r \longrightarrow U$  where  $U$  is a vector space is said to be symmetric if  $f\sigma = f$  for all permutations  $\sigma$  and skew symmetric if  $f\sigma = (\text{sgn } \sigma)f$  for all  $\sigma$ .

If  $y$  is a contravariant tensor of degree  $r$ , we set

$$S_r(y) = \frac{1}{r!} \sum_{\sigma} \sigma(y) \quad \text{and} \quad A_r(y) = \frac{1}{r!} \sum_{\sigma} (\text{sgn } \sigma) \sigma(y)$$

Then  $S_r$  and  $A_r$  are respectively called symmetrization

and skew symmetrization.

THEOREM 6: For any  $y \in V^r$ ,  $S_r(y)$  is symmetric and  $A_r(y)$  is skew symmetric. Moreover  $S_r(y) = y$  if  $y$  is symmetric and  $A_r(y) = y$  if  $y$  is skew symmetric.

PROOF: If  $\tau$  is any permutation of  $1, 2, \dots, r$ , then

$$\begin{aligned} \tau S_r(y) &= \frac{1}{r!} \sum_{\sigma} \tau(\sigma(y)) = \frac{1}{r!} \sum_{\sigma} (\tau\sigma)(y) = S_r(y) \\ \text{and } \tau A_r(y) &= \frac{1}{r!} \sum_{\sigma} (\text{Sgn}\sigma) \tau\sigma(y) = \frac{\text{Sgn}\tau}{r!} \sum_{\sigma} (\text{Sgn}\tau\sigma) \tau\sigma(y) \\ &= \text{Sgn}\tau A_r(y) \end{aligned}$$

The second part is easy.

DEFINITION 6: Let  $\wedge^r(V) = V^r / \text{Ker } A_r$ . Then  $\wedge^r(V)$  is called the space exterior  $r$ -vectors over  $V$ . Its elements are called exterior vectors.

Since the image of  $A_r$  is the space of all skew symmetric contravariant tensors of degree  $r$ ,  $A_r$  induces an isomorphism between  $\wedge^r(V)$  and the space of skew symmetric  $r$ -vectors.

If  $\psi: V^r \longrightarrow \wedge^r(V)$  is the natural projection, we write

$$\psi(x_1 \otimes \dots \otimes x_r) = x_1 \wedge x_2 \wedge \dots \wedge x_r \quad \text{for any } x_1, \dots, x_r \in V.$$



THEOREM 7: A linear map  $f: V^r \rightarrow U$  where  $U$  is a vector space, is skew symmetric if and only if  $f(N^r) = 0$  where  $N^r = \text{Ker } A_r$ .

Consider  $\Lambda^r(V)$  and  $\Lambda^s(V)$ . The tensor product  $V^r \otimes V^s$  can be identified with  $V^{r+s}$ , so that we have the sequence

$$V^r \times V^s \xrightarrow{h} V^r \otimes V^s \xrightarrow{i} V^{r+s} \xrightarrow{\psi} \Lambda^{r+s}(V)$$

We now define

$$u_y: V^r \longrightarrow \Lambda^{r+s}(V)$$

by  $u_y(x) = u(x, y)$  for fixed  $y \in V^s$

and  $u_x: V^s \longrightarrow \Lambda^{r+s}(V)$

by  $u_x(y) = u(x, y)$  for fixed  $x \in V^r$

where  $u = \psi \circ i \circ h$ .

Then  $u$  induces a map  $\tilde{u}: \Lambda^r(V) \times \Lambda^s(V) \longrightarrow \Lambda^{r+s}(V)$ , defined by

$$\tilde{u}(\xi, \eta) = u(x, y), \quad \xi \in \Lambda^r(V), \quad \eta \in \Lambda^s(V)$$

where  $x, y$  are representatives in the classes  $\xi, \eta$  defined mod  $N^r, N^s$  respectively.

DEFINITION 7:  $\tilde{u}(\xi, \eta)$  is the exterior product of  $\xi, \eta$  we denote it by  $\xi \wedge \eta$ .

THEOREM 8: Exterior multiplication has the following properties

$$1) (e_1 \wedge e_2 \wedge \dots \wedge e_r) \wedge (f_1 \wedge \dots \wedge f_s) = e_1 \wedge e_2 \wedge \dots \wedge f_1 \wedge \dots \wedge f_s$$

$$2) x \wedge (\alpha_1 y_1 + \alpha_2 y_2) = \alpha_1 (x \wedge y_1) + \alpha_2 (x \wedge y_2)$$

$$3) (x \wedge y) \wedge z = x \wedge (y \wedge z)$$

$$4) x \wedge y = (-1)^{rs} y \wedge x.$$

Where  $\alpha_1, \alpha_2 \in F$ ,  $e_1, \dots, e_r, f_1, \dots, f_s$  are vectors  $x, x_1, x_2, y_1, y_2, z$  are exterior vectors,  $r = \text{deg of } x$ ,  $s = \text{deg of } y$ . We remark that

$$\text{for } r > n = \dim V, \wedge^r(V) = 0$$

DEFINITION 8: Consider the direct sum

$$\wedge(V) = \sum_{0 \leq r \leq n} \wedge^r(V)$$

$$\text{For } x = \sum_{0 \leq r \leq n} x^r, y = \sum_{0 \leq s \leq n} y^s, x^r \in \wedge^r(V), y^s \in \wedge^s(V)$$

define the product by

$$x \wedge y = \sum_{r,s} x^r \wedge y^s.$$

Then  $\wedge(V)$  becomes an algebra called exterior algebra or Grassman algebra of the vector space  $V$ .

THEOREM 9: The exterior algebra  $\wedge(V)$  of vector space  $V$  of dim  $n$  is of dim  $2^n$ . If  $e_1, \dots, e_n$  form a basis for  $V$ , a basis of  $\wedge(V)$  is given by 1 and the elements

$$e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_r}$$

$$i_1 < i_2 < \dots < i_r, \quad i_r = 1, 2, \dots, n, \quad r = 1, 2, \dots, n.$$

References

1. Barnes W.E. Introduction to Abstract Algebra,  
D.C. Heath and Co., Buston 1963.
2. Cartan H and Eilenberg S Homological Algebra,  
Princeton University Press, Princeton 1956.
3. Chevalley C. Fundamental Concepts of Algebra,  
Academic Press, New York, 1956.
4. Deskins W.E. Abstract Algebra,  
The Macmillan Co., New York, 1964.
5. Hall, M. Jr. The Theory of Groups,  
The Macmillan Co., New York, 1959.
6. Hu S.T. Elements of Modern Algebra,  
Holden-Day Inc., San Francisco, 1965.
7. Herstein I.N. Topics in Algebra,  
Blaisdell Publishing Co., New York, 1964.
8. Jacobson N. Lectures in Abstract Algebra,  
Vol.II, D. Van Nostrand Co., Princeton, 1952.
9. Northcott D.G. Ideal Theory,  
Cambridge University Press, Cambridge, 1953.
10. " An Introduction to Homological Algebra,  
Cambridge University Press, Cambridge, 1960.
11. Van der Waerden B.L. Modern Algebra,  
2 Vols., Frederick Ungar Publishing Co.,  
New York, 1949.
12. Zariski O and Samuel P. Commutative Algebra,  
Vol.I, D. Van Nostrand Co., Princeton, 1958.

.....

## Proceedings of Matscience Symposia

Edited By

ALLADI RAMAKRISHNAN

There are two scientific meetings conducted by the Institute one in winter, the Anniversary symposium in January, and the other, the Summer School in August. The proceedings of these winter and summer meetings are being published in a series entitled

### PROCEEDINGS OF THE MATSCIENCE SYMPOSIA

by the Plenum Press, New York, a division of the Consultants Bureau Enterprises Inc.

### List of Matscience Reports (1964-65)

<i>Report No.</i>	<i>Author</i>	<i>Title</i>
35	K. Symanzik	Lecture on a modified models of Euclidean Quantum Field Theory.
36	K. Venkatesan	Report on Recent Experimental Data (1964).
37	A. Fujii	Lectures on Fermi dynamics.
38	M. Gourdin	Mathematical introduction to unitary symmetries.
39	J. V. Narlikar	Theories of Gravitation.
40	K. Venkatesan	Report on recent experimental data (1965).
41	K. R. Unni	Introduction to Hilbert space.
42	L. Rosenfeld	Theory of nuclear reactions.
43	K. R. Unni	Concepts in Modern Mathematics-I (Algebra)
<i>Under preparation</i>		
	H. Ruegg	Relativistic generalization of $SU_6$