RINGS AND MODULES
(DM24)
(MSC-MATHS)

ACHARYA NAGARJUNA UNIVERSITY

CENTRE FOR DISTANCE EDUCATION

NAGARJUNA NAGAR,

GUNTUR

ANDHRA PRADESH

Lesson : 1 FUNDAMENTAL CONCEPTS OF ALGEBRA

1.0 Introduction : In this lesson we give a series of definitions to assure completeness and to fix our notations that we follow through out this book.

1.1 Definition : A system $(S,\cdot)$ where 'S' is a nonempty set and '$\cdot$' is a binary operation on 'S' is said to be a semigroup if

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c \text{ for all } a,b,c \text{ in } S$$

1.2 Definition : A system $(G,0,-,+)$ where G is a nonempty set, '0' is a zero-ry operation, '-' is a unary operation and '+' is a binary operation on G is said to be a group.

If (1) $(a+b)+c=a+(b+c)$ for all a,b,c in G.

(2) $a+0 = 0+a = a$ for all $a\in G$

(3) $a+(-a)=(-a)+a=0$ for all $a\in G$

1.3 Definition : A system $(R,0,-,+,\cdot)$ where R is a nonempty set, 0 and 1 are zero-ary operations, '$-$' is a unary operation and '+' and '$\cdot$' are binary operations on R is called a ring if

(1) $(R,0,-,+)$ is an abelion group.

(2) $(R,1,.)$ is a semigroup.

(3) $a.(b+c) = a.b + a.c$

$(a+b)\cdot c = a\cdot c+b\cdot c$ for all a,b,c in R

1.4 Definition : A ring $(R,0,1,-,+,\cdot)$ is said to be a division ring if $0\neq 1$ and for every $a\neq 0$, there exists an element $b\in R$, such that $ab=1=ba$.

1.5 Definition : A cummutative division ring is called a field.

1.6 Definition : A class of systems sharing a given set of operations and satisfying a given set of identities is called an equationally defined class.

1.7 Examples : The class of all groups is an equationally defined class, similarly the class of all semigroups, the class of all rings, the class of all cummutative rings are all equiationally defined classes. But the class of all division rings is not an equationally defined class.

1.8 Definition : A system $(S,\leq)$ where S is a nonempty set and '$\leq$' is abinary relation on S is called an ordered set if the binary relation '$\leq$' is reflexive, antisymmetric and transitive.

1.9 Definiion : An ordered set $(S,\leq)$ is called a simply ordered set if for any two elements a and b of S, either $a\leq b$ or $b\leq a$.

1.10 Definition : Let $(S,\leq)$ be an ordered set and $A\subseteq S$. Then

(a) An element $x\in S$ is called a lower bound of A if $x\leq a$ for all $x\in A$.

(b) An element $y\in S$ is called an upper bound of A if $a\leq y$ for all $a\in A$.

(c) An element $x_0 \in S$ is called the greatest lower bound of A if x_0 is a lower bound of A and for any lower bound x of A, $x_0\leq x$. The least upper bound of A is denoted by lub A.

1.11 Definition : An ordered set $(S,\leq)$ is said to be a semilattice if for any two elements a and b of S, the set $\{a,b\}$ has greatest lower bound in S. It is denote by $a\wedge b$ In other words.

1.12 Definition : A system $(S, \leq, \wedge)$ is said to be a semilattice if, $(S,\leq)$ is an ordered set and '$\wedge$' is a binary operation on S such that for any $a,b\in S$, $a\wedge b = g\ell b\{a,b\}$.

1.13 Remark : Let a and b be any two elements of an ordered set $(S,\leq)$. Then an element $x\in S$ is the $g\ell b\{a,b\}$ if and only if for any $c\in S$, $c\leq x$ implies and is implied by $c\leq a$ and $c\leq b$.

Proof : Suppose $x=g\ell b\{a,b\}$. Let c be any element of S. Assume that $c\leq x$. Since $x\leq a$ and $x\leq b$ we have $c\leq a$ and $c\leq b$. Now assume that $c\leq a$ and $c\leq b$, which implies c is a lower bound of $\{a,b\}$. Since $x=g\ell b\{a,b\}$ we have $c\leq x$. Thus $c\leq x$ implies and implied by $c\leq a$ and $c\leq b$.

Conversely suppose that for any $c\in S$, $c\leq x$ implies and is implied by $c\leq a$ and $c\leq b$.

Since $x\leq x$, we have $x\leq a$ and $x\leq b$ $\Rightarrow x$ is a lower bound of $\{a,b\}$. Suppose y is any lower bound of $\{a,b\}$ $\Rightarrow$ $y\leq a$ and $y\leq b$, which implies $y\leq x$. Therefore x is the greatest lower bound of $\{a,b\}$.

1.14 Remark : Any simply ordered set is a semilattice.

Proof : Suppose $(S,\leq)$ is a simply ordered set. Let $a,b\in S$. Since S is simply ordered set, we have either $a\leq b$ or $b\leq a$.

If $a\leq b$, then $a=g\ell b\{a,b\}$. If $b\leq a$ then $b=g\ell b\{a,b\}$. Thus any two elements of S have $g\ell b$. Hence S is a semilattice.

1.15 Remark : If $(S,\leq,\wedge)$ is a semilattice, then for any $a,b\in S$, $a\wedge b$ is unique.

Proof : Suppose $x=a\wedge b=y$. Since x is a lower bound of a and b, we have $x\leq a$ and $x\leq b$. Since y is the $g\ell b\{a,b\}$ we have $x\leq y$. Similarly $y\leq x$. Hence $x=y$ Therefore $a\wedge b$ is a unique element.

1.16 Example : Let N be the set of all natural numbers. For any $a,b\in N$, we define $a\leq b$ if and only if a divides b. Then $(N,\leq)$ is an ordered set which is not a simply ordered set but a semilattice Further for any $a,b\in N$, $a\wedge b=\gcd\{a,b\}$.

1.17 Example : Let X be any nonempty set and let $\mathbb{P}(X)$ be the set of all subsets of x. For any $A,B\in\mathbb{P}(X)$, we define $A\leq B$ iff $A\subseteq B$. Then $\mathbb{P}(X)$ is an ordered set which is not a simply ordered set. For any $A,B\in\mathbb{P}(X)$, $g\ell b\{A,B\}=A\cap B$ which is the intersection of A and B. Thus $\mathbb{P}(X)$ is a semilattice.

1.18 Theorem : The class of all semilattices can be equationally defined as the class of all semigroups $(S,\wedge)$ satisfying the commutative law and idempotent law.

Proof : Suppose $(S,\leq,\wedge)$ is a semilattice. Then '$\wedge$' is a binary operation on S such that for any $a,b\in S$, $a\wedge b=g\ell b\{a,b\}$. Now we shall prove that for any $a,b\in S$, $a\wedge b=g\ell b\{a,b\}$. Let $x=a\wedge(b\wedge c)\Rightarrow x=g\ell b\{a,b\wedge c\}\Rightarrow x\leq a$ and $x\leq b\wedge c$. Since $b\wedge c=g\ell b\{b,c\}$, we have $b\wedge c\leq b$ and $b\wedge c\leq c\Rightarrow x\leq b$ and $x\leq c$. Thus x is a lower bound of $\{a,b,c\}$. Suppose x_0 is any lower bound of $\{a,b,c\}\Rightarrow x_0\leq a$, $x_0\leq b$ and $x_0\leq c\Rightarrow x_0\leq a$ and $x_0\leq b\wedge c\Rightarrow x_0\leq x$. Thus $x=g\ell b\{a,b,c\}$. Similarly it can be shown that $y=(a\wedge b)\wedge c=g\ell b\{a,b,c\}$. Therefore $x=y$, Thus for any $a,b,c\in S$, $a\wedge(b\wedge c)=(a\wedge b)\wedge c$. Hence $(S,\wedge)$ is a semigroup. Further for $a,b\in S$,

$a \wedge b = g\ell b\{a,b\} = g\ell b\{b,a\} = b \wedge a$ and for any $a \in S$, $a \wedge a = g\ell a\{a\} = a$. Thus $(S,\wedge)$ is a semilattice satisfying commutative and idempotent laws.

Conversely suppose that $(S,\wedge)$ is a semigroup satisfying commutative and idempotent laws.

For any $a,b \in S$, we define $a \leq b$ if and only if $a \wedge b = a$. Since for any $a \in S$, $a \wedge a = a$ we have $a \leq a$ for any $a \in S$. Therefore '$\leq$' is reflexive. Suppose $a \leq b$ and $b \leq a \Rightarrow a \wedge b = a$ and $b \wedge a = b$. But $a \wedge b = b \wedge a \Rightarrow a = b$. Therefore '$\leq$' is antisymmetric. Suppose $a \leq b$ and $b \leq c \Rightarrow$ $a \wedge b = a$ and $b \wedge c = b$. Now $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$. Therefore $a \leq c \Rightarrow$ '$\leq$' is transitive. Hence $(S,\leq)$ is an ordered set. Now we show that for any $a,b \in S$, $a \wedge b = g\ell b\{a,b\}$.

Suppose $x \leq a \wedge b$. Since $(a \wedge b) \wedge b = a \wedge (b \wedge b) = a \wedge b$ we have $a \wedge b \leq b$. Since $(a \wedge b) \wedge a = a \wedge (b \wedge a) = a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b$, we have $a \wedge b \leq a \Rightarrow x \leq a$ and $x \leq b$. Conversely suppose that $x \leq a$ and $x \leq b$.

Now $x \wedge (a \wedge b) = (x \wedge a) \wedge b = x \wedge b = x \Rightarrow x \leq a \wedge b$. Thus we have $x \leq a \wedge b$ if and only if $x \leq a$ and $x \leq b$. Therefore $a \wedge b = \text{glb}\{a,b\}$. Hence $(S,\leq,\wedge)$ is a semilattice. Thus the class of all semilattices is equal to the class of all semigroups satisfying commutative and idempotent laws. Hence the class of all semilattices is equationally defined as the class of semigroups satisfying the commutative and idempotent laws.

1.19 Definition : A system $(S,\leq,\wedge,\vee)$ where $(S,\leq)$ is an ordered set and $\wedge$ and $\vee$ are two binary operations on S such that for any $a,b \in S$, $a \wedge b = g\ell b\{a,b\}$ and $a \vee b = \text{lub}\{a,b\}$ is called a lattice.

1.20 Remark : Every simply ordered set $(S,\leq)$ is a lattice.

Proof : Let $(S,\leq)$ be a simply ordered set. Let $a,b \in S$, Since S is simply ordered set, we have either $a \leq b$ or $b \leq a$ If $a \leq b$, then $a \wedge b = a$ and $a \vee b = b$. If $b \leq a$ then $a \wedge b = b$ and $a \vee b = a$. Thus for any two elements a,b in S, $a \wedge b$ and $a \vee b$ exist. Therefore $(S,\leq,\wedge,\vee)$ is a lattice.

1.21 Remark : If $(S,\leq,\wedge,\vee)$ is a lattice and $a,b \in S$, then an element $x \in S$ is the $\text{lub}\{a,b\}$ if and only if for any $c \in S$, $x \leq c$ implies and implied by $a \leq c$ and $b \leq c$.

Proof : The proof is similar to the proof of the Remark 1.13.

1.22 Remark : If $(S, \leq)$ is an ordered set, then for any two elements a and b in S, $a=b$ if and only if for any $c \in S$, $c \leq a$ implies and implied by $c \leq b$. Equivolently for any $c \in S$, $a \leq c$ implies and implied by $b \leq c$.

1.23 Definition : A lattice $(S, \leq, \wedge, \vee)$ is said to be a lattice with 0 and 1 if there exists two distinguished elements 0 and 1 in S such that $0 \leq a \leq 1$ for all $a \in S$. The lattice with 0 and 1 is written as $(S, \leq, \wedge, \vee, 0, 1)$.

1.23 Definition : Suppose $(S, \leq, \wedge, \vee, 0, 1)$ is a lattice with 0 and 1 and let $a \in S$. An element $a' \in S$ is said to be a complement of a, if $a \wedge a' = 0$ and $a \vee a' = 1$. If every element of S has a complement, then S is called a complemented lattice. A complemented lattice is denoted by $(S, \leq, \wedge, \vee, ', 0, 1)$.

1.23 Definition : A lattice $(S, \leq, \wedge, \vee, 0, 1)$ is said to be a distributive lattice if for any $a, b, c \in S$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

1.24 Remark : If $(S, \leq, \wedge, \vee, ', 0, 1)$ is a complemented distributive lattice, then for any $a \in S$, the complement a' of a is unique.

Proof : Suppose $a \in S$ and suppose that a_1 and a_2 are complements of a in S. $\Rightarrow a \wedge a_1 = 0$ and $a \wedge a_2 = 0$ and $a \vee a_1 = 1 = a \vee a_2$.

$$\text{Now } a_1 = a_1 \wedge 1 \quad (\because a_1 \leq 1)$$

$$= a_1 \wedge (a \vee a_2)$$

$$= (a_1 \wedge a) \vee (a_1 \wedge a_2)$$

$$= 0 \vee (a_1 \wedge a_2)$$

$$= a_1 \wedge a_2 \qquad (0 \leq a_1 \wedge a_2)$$

$$\text{Also} \qquad a_2 = a_2 \wedge 1 = a_2 \wedge (a \vee a_1)$$

$$= (a_2 \wedge a) \vee (a_2 \vee a_1)$$

$$= 0 \vee (a_2 \wedge a_1)$$

$$=(a_2 \wedge a_1)$$

$$=a_1 \wedge a_2$$

Therefore $a_1 = a_2$. Hence the complement of a is unique.

1.25 Remark : If $(S, \leq, \wedge, \vee)$ is a distributive lattice, then for any $a,b,c \in S$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Proof : $(a \vee b) \wedge (a \vee c) = [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c]$

$$= a \vee [(a \wedge c) \vee (b \wedge c)]$$

$$= [a \vee (a \wedge c)] \vee (b \wedge c)$$

$$= a \vee (b \wedge c)$$

1.26 Definition : A ring R is said to be a Boolean ring if $a^2 = a$ for all $a \in R$.

1.27 Definition : A system $(S, 0, ', \wedge)$ where $(S, \wedge)$ is a semilattice and 0 is an element of S and "$'$" is a unary operation on S is called a Boolean algebra if for any $a, b \in S$, $a \wedge b' = 0$ if and only if $a \wedge b = a (a \leq b)$.

1.28 Theorem : If $(S, 0, ', \wedge)$ is a Boolean algebra, then for any element $a \in S$, $a'' = (a')' = a$

Proof : Since $a' \leq a'$ we have $a' \wedge a' = a' \Rightarrow a' \wedge (a')' = 0 \Rightarrow a' \wedge a'' = 0 \Rightarrow a'' \wedge a' = 0 \Rightarrow a'' \leq a$.

Similarly since $a'' \leq a''$ we have $a''' \leq a'$ and $a'''' \leq a'' \Rightarrow a'''' \wedge a' = 0 \Rightarrow a' \wedge (a''')' = 0 \Rightarrow a' \leq a'''$.

Therefore $a' = a'''$.

Since $a \leq a$ we have $a \wedge a' = 0 \Rightarrow a \wedge a''' = 0 \Rightarrow a \wedge (a'')' = 0 \Rightarrow a \leq a''$. Hence $a = a''$.

1.29 Theorem : A Boolean algebra becomes a complemented distributive lattice by defining $a \vee b = (a' \wedge b')$ and $1 = 0'$. Conversely any complemented distributive lattice is a Boolean algebra in which the above equations are provable identities.

Proof : Suppose $(S, 0, ', \wedge)$ is a Boolean algebra. For any $a, b \in S$, define $a \vee b = (a' \wedge b')'$ and $1 = 0'$. Now we show that $(S, 0, 1, ', \wedge, \vee)$ is a complemented distributive lattice. Clearly for any

$a, b \in S$, $a \wedge b$ and $a \vee b$ exist in S and $a \wedge b = g\ell b\{a,b\}$. Now we show that $a \vee b = \ell ub\{a,b\}$. Let c be any element of S. We have $a \vee b \leq c$

iff $(a' \wedge b')' \leq c$

iff $(a' \wedge b')' \wedge c' = 0$

iff $c' \leq a' \wedge b'$

iff $c' \leq a'$ and $c' \leq b'$

iff $c' \wedge a = 0$ and $c' \wedge b = 0$

iff $a \leq c$ and $b \leq c$

Therefore $a \vee b = \text{lub}\{a,b\}$. Hence $(S, \leq, \wedge, \vee)$ is a lattice. Now we show that for any a, b, c in S, $a \wedge (b \vee c) = (a \wedge b) \vee (b \wedge c)$.

Suppose x is any element of S. Then

$a \wedge (b \wedge c) \leq x$ iff $a \wedge (b \vee c) \wedge x' = 0$

iff $(a \wedge x') \wedge (b \vee c) = 0$

iff $(a \wedge x') \wedge (b' \wedge c')' = 0$

iff $(a \wedge x') \leq b' \wedge c'$

iff $a \wedge x' \leq b'$ and $a \wedge x' \leq c'$

iff $a \wedge x' \wedge b = 0$ and $a \wedge x' \wedge c = 0$

iff $a \wedge b \leq x$ and $a \wedge c \leq x$

iff $(a \wedge b) \vee (a \wedge c) \leq x$

Therefore $a \wedge (b \wedge c) = (a \wedge b) \vee (a \wedge c)$. Hence $(S, \leq, \wedge, \vee)$ is a distributive lattice. For any $a \in S$, since $a \leq a$, we have $a \wedge a' = 0$ and $a \vee a' = (a' \wedge a'')' = (a' \wedge a)' = 0' = 1$. Therefore a' is the complement of a. Hence $(S, \leq, 0, 1, ', \wedge, \vee)$ is a complemented distributive lattice. Conversely suppose that $(S, \leq, 0, 1, ', \wedge, \vee)$ is a complemented distributive lattice. Clearly $(S, \leq, \wedge)$ is a semilattice. First we prove that $(S, 0, ', \wedge)$ is a [illegible]ean algebra.

Let $a, b \in S$. Suppose $a \wedge b' = 0$.

Now $a = a \wedge 1 = a \wedge (b \vee b') = (a \wedge b) \vee (a \wedge b') = (a \wedge b) \vee 0 = a \wedge b$. Suppose $a \wedge b = a$. Now $a \wedge b' = (a \wedge b) \wedge b' = a \wedge (b \wedge b') = a \wedge 0 = 0$. Thus we have for any $a, b, \in S$, $a \wedge b' = 0$ if and

only if $a \wedge b = a$. Therefore $(S,0,',\wedge)$ is a Boolean algebra. Further we have to show that the identtities $a \vee b = (a' \wedge b')'$ and $0' = 1$ are valid in S. For any $a,b \in S$, $(a \vee b) \wedge (a' \wedge b')$
$= (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = 0 \vee 0 = 0$ and $(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = 1 \wedge 1 = 1$

Therefore $a \vee b$ is the complement of $a' \wedge b' \Rightarrow a \vee b = (a' \wedge b')'$. Since $0 \wedge 1 = 0$ and $0 \vee 1 = 1$. We have 1 is the complement of $0 \Rightarrow 0' = 1$. Hence the theorem.

1.30 Definition : An ordered set $(S,\leq)$ is said to be a semilattice if any two elements have least upper bound.

1.31 Definition : A system $(S,1,',\vee)$ is said to be Boolean algebra if $(S,\vee)$ is semilattice and for any $a,b \in S$, $a \vee b = a$ if and only if $a \vee b' = 1$.

1.32 Remark : If $(S,0,',\wedge)$ is a Boolean algebra then so is $(S,1,',\vee)$.

Proof : Suppose $(S,0,',\wedge)$ is a Boolean algebra $\Rightarrow (S,0,1,',\wedge,\vee)$ is a complemented distributive lattice where $0' = 1$ and for any $a,b \in S$, $a \vee b = (a' \wedge b')'$. Since for any $a,b \in S, a \vee b = \text{lub}\{a,b\}$, we have that $(S,\vee)$ is a semilattice. Now for any $a,b \in S$,

$$a \vee b' = 1 \quad \text{iff} \quad (a' \wedge b'')' = 1 \quad \text{iff} \quad (a' \wedge b'') = 0$$

$$\text{iff} \quad a' \wedge (b')' = 0 \quad \text{iff} \quad a' \wedge b' = a'$$

$$\text{iff} \quad (a' \wedge b')' = a \quad \text{iff} \quad a \vee b = a$$

Therefore $(S,1,',\vee)$ is a Boolean algebra.

1.33 Theorem : A Boolean algebra $(S,0,',\cdot)$ becomes a Boolean ring $(S,0,1,-,+,\cdot)$ by defining $1 = 0'$, $-a = a$, $a + b = ab' \vee ba'$ where $a \vee b = (a'b')'$. Conversely any Boolean ring can be regarded as a Boolean algebra with $a' = 1 - a$ and the above definitions of $1, -$ and $+$ then become provable identities.

Proof : Suppose $(S,0,',\cdot)$ is a Boolean algebra $\Rightarrow (S,\cdot)$ is a semilattice in which for any $a,b \in S$, $a.b = g\ell b\{a,b\}$ and for any $a,b \in S$ $a \cdot b' = 0$ iff $a \cdot b = a$.

Define $1 = 0'$ and $-a = a$ for any $a \in S$ and for any $a,b \in S$

$a \vee b = (a'b')'$ and $a+b = ab' \vee ba'$.

Now we shall prove that $(S,0,1,-,+,\cdot)$ is a Boolean ring.

Clearly '-' is a unary operation and '+' and '$\cdot$' are binary operations on S. Let $a,b,c \in S$.

We have $(a+b)+c = (ab' \vee a'b)+c$

$$=(ab' \vee a'b)c' \vee c(ab' \vee a'b)'$$

$$=ab'c \vee a'bc' \vee c\left[(ab')'(a'b)'\right]$$

$$=ab'c' \vee a'bc' \vee c\left[(a' \vee b)(b' \vee a)\right]$$

$$=ab'c' \vee a'b'c' \vee ca'b' \vee cbb' \vee ca'a \vee cba$$

$$= ab'c' \vee ba'c' \vee ca'b' \vee abc$$

Similarly $a+(b+c) = ab'c' \vee ba'c' \vee a'b' \vee abc$. Therefore $a+(b+c) = (a+b)+c$. Hence '+' is assosiative.

For any $a \in S$, $a+0 = a.0' \vee 0.a' = a.1 \vee 0 = a.1 = a$. Similarly $0+a=a$. Therefore '0' is the additive identity in S. For any $a \in S, a+(-a) = a+a = aa' \vee a'a = 0 \vee 0 = 0$. Therefore $-a$ is the additive inverse of a

Also for any $a,b \in S$, $a+b = ab' \vee ba' = ba' \vee ab' = b+a$. $\Rightarrow$ '+' is commutative. Hence $(S,0,-,+)$ is an abelion group. For any $a,b,c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (given in the Hypothesis). For any $a \in S, a \cdot 1 = a = 1 \cdot a$. Hence $(S,1,\cdot)$ is a semigroup with identity. Further for any $a,b,c \in S$ $a \cdot (b+c) = a \cdot (bc' \vee cb') = abc' \vee acb'$.

Also $a \cdot b + a \cdot c = ab(ac)' \vee ac(ab)'$

$$=ab(a' \vee c') \vee ac(a' \vee b')$$

$$=ab\,a' \vee abc' \vee aca' \vee acb'$$

$$=abc' \vee acb'$$

Therefore $a \cdot (b+c) = a \cdot b + a \cdot c$. Similarly it can be shown that $(a+b) \cdot c = a \cdot c + b \cdot c$.

Hence both the distributive laws hold good. Therefore $(S,0,1,-,+,\cdot)$ is a ring. Since $a\cdot a=a$ we have that it is a Boolean ring.

Conversely suppose that $(S,0,1,-,+,\cdot)$ is a Boolean ring. Clearly $(S,\cdot)$ is a semigroup satisfying the idempotent law and commutative law. Let $a,b\in S$.

Suppose $a.b'=0 \Rightarrow a(1-b)=0 \Rightarrow a-ab=0 \Rightarrow a=ab$. Conversely suppose that $a=ab \Rightarrow a-ab=0$ $\Rightarrow a(1-b)=0 \Rightarrow ab'=0$. Thus for any $a,b\in S$, $ab'=0$ if and only if $ab=a$. Therefore $(S,0,',\cdot)$ is a Boolean algebra.

Now $0'=1-0=1$. Since S is a Boolean ring we have $a+a=0$ for all $a\in S \Rightarrow -a=a$ for all $a\in S$.

For any $a,b\in S$, $ab'\vee ba'$

$$= a(1-b)\vee b(1-a)$$

$$= (a-ab)\vee(b-ba)$$

$$= \left[(a-ab)'(b-ba)'\right]'$$

$$=\left[\left[1-(a-ab)\right]\left[1-(b-ba)\right]\right]'$$

$$=\left[(1-a+ab)(1-b+ba)\right]' = \left[(1+a+ab)(1+b+ba)\right]'$$

$$=1+(1+b+ba+a+ab+aba+ab+abb+ab\,ba)$$

$$=a+b$$

Hence $(S,0,',.)$ is a Boolean algebra where $a'=1-a$ for any $a\in S$ in which the identities $1=0'$, $-a=a$ and $a+b=ab'\vee ba'$ are provable.

1.34 Definition : An ordered set $(S,\leq)$ is said to be a complete lattice if every subset of S has both infimum and supreimum.

1.35 Remark : If $(S,\leq)$ is an ordered set in which every subset has infimum, then any subset of S has suprimum.

Proof : Suppose $(S,\leq)$ is an ordered set in which every subset has infimum. Let $T\subseteq S$. Let A be the set of all upper bounds of T. Let $t\in T$. Since A is the set of all upper bounds of T. we have

$t \leq a$ for all $a \in A \Rightarrow t$ is a lower bound of A. Thus every element of T is a lower bound of A. Since every subset of S has infimum, it follows that $Inf\ A$ exists in S say $a_0 \Rightarrow a_0$ is the greatest lower bound of $A \Rightarrow t \leq a_0\ \forall t \in T \Rightarrow a_0$ is an upper bound of T. Suppose b is any upper bound of $T \Rightarrow t \leq b \forall t \in T \Rightarrow b \in A \Rightarrow a_0 \leq b$. Thus a_0 is the last upper bound of T. i.e. $a_0 = Sup\,T$. Thus every subset of S has suprimum.

1.36 Definition : An ordered set $(S, \leq)$ is called a well ordered set if every non empty subset has a least element.

1.37 Remark : A well ordered set with greatest element is a complete lattice.

1.38 Definition : A Boolean algebra is said to be complete if it is a complete lattice.

1.39 Definition : Let $(S, \leq)$ be a complete lattice. By a closure operation on S we mean a mapping $a \mapsto a^c$ of S into it self such that $a \leq a^c, \left(a^c\right)^c \leq a^c$ and $a \leq b$ implies $a^c \leq b^c$ for all $a, b \in S$.

1.40 Definition : An element a of a complete lattice S with closure operation on it is said to be closed if $a^c \leq a$ i.e. $a^c = a$.

1.41 Example : Let G be any group, Then $\mathbb{P}(G)$, the power set of G is a complete lattice under set inclusion. For any subset A of G, let A^c be the smallest subgroup of G containing A. Then $A \mapsto A^c$ is a closure operation on $\mathbb{P}(G)$.

1.42 Theorem : Given a closure operation on a complete lattice; the inf of any set of closed elements is again closed. Hence the set of all closed elements form a complete lattice. Conversely any subset of a complete Lattice which is closed under the operation 'inf' can be obtained in this way.

Proof : Let S be any complete lattice with a closure operation. Let T be the set of all closed elements of S w.r.t. the closure operation. Let X be any subset of T. Since $X \subseteq S$ and S is complete, $\inf X$ exists. Let $a = \inf X$. Now we shall show that 'a' is also closed. For any $x \in X$, we have $a \leq x \Rightarrow a^c \leq x^c$. Since x is a closed element, we have $x^c = x \Rightarrow a^c \leq x \forall x \in X \Rightarrow a^c$ is a lower bund of $X \Rightarrow a^c \leq a$. But $a \leq a^c \Rightarrow a = a^c$. Therefore a is also closed and hence is in T. Thus for every subset A of T $\inf A$ exists in T. Hence T is a complete lattice.

Conversely suppose that T is any subset of S such that the infimum of every subset of T is in T. For any $a \in S$, define $a^c = \inf\{t \in T / a \leq t\}$. By definition, a is a lower bund of the set

$\{t \in T / a \le t\}$. Hence $a \le a^c$. For any $a \in S, \left(a^c\right)^c = \inf\left\{t \in T / a^c \le t\right\}$ and $a^c = \inf\{t \in T / a \le t\}$.

Since the infimum of any subset of T is in T, we have $a^c \in T \Rightarrow a^c \in \left\{t \in T / a^c \le t\right\} \Rightarrow \left(a^c\right)^c \le a^c$

For any $a, b \in S$ such that $a \le b$ we have $\{t \in T / b \le t\} \subseteq \{t \in T / a \le t\} \Rightarrow \inf\{t \in T / a \le t\}$ $\le \inf\{t \in T / b \le t\} \Rightarrow a^c \le b^c$.

Hence the operation $a \mapsto a^c$ of S in to itself is a closure operation. let a be any closed element $\Rightarrow a = a^c = \inf\{t \in T / a \le t\}$. Since $a^c \in T$ we have that $a \in T$. Thus T contains every closed element. Let $a \in T \Rightarrow a \in \{t \in T / a \le t\} \Rightarrow a^c \le a$. But $a \le a^c \Rightarrow a = a^c$. Hence a is closed. Thus T is precisely the set of all closed elements of S.

1.43 Problem : Show that in any Boolean ring R, for any $a \in R, a + a = 0$ and for any $a, b \in R, ab = ba$.

Proof : We know that in a Boolean ring R, $a^2 = a$ for all $a \in R$. Therefore $(a + a)^2 = a + a$

$\Rightarrow a^2 + a^2 + a^2 + a^2 = a + a \Rightarrow a + a + a + a = a + a \Rightarrow a + a = 0$

Also for any $a, b \in R$, $(a+b)(a+b) = a + b \Rightarrow a^2 + ab + ba + b^2 = a + b$

$\Rightarrow a + ab + ba + b = a + b \Rightarrow ab + ba = 0 \Rightarrow ab = ba$

1.44 Problem : If S is any lattice, then for any $a, b \in S$, $a \wedge (a \vee b) = a$ and $a \vee (a \wedge b) = a$.

Proof : Since $a \le a$ and $a \le a \vee b$, we have a is a lower bound of $\{a, a \vee b\}$.

$\Rightarrow a \le g\ell b\{a, a \vee b\}$ i.e. $a \le a \wedge (a \vee b)$

But $a \wedge (a \vee b) \le a \Rightarrow a = a \wedge (a \vee b)$

Also $a \vee (a \wedge b)$ is an upper bound of a and $a \wedge b \Rightarrow a \le a \vee (a \wedge b)$. Since $a \wedge b \le a$ and $a \le a$ we have that a is an upper bound of a and $a \wedge b \Rightarrow a \vee (a \wedge b) \le a$. Therefore $a = a \vee (a \wedge b)$.

Prof. G. Koteswara Rao
Department of Mathematics
Acharya Nagarjuna University

Lesson : 2 SUBRINGS, HOMOMORPHISMS, IDEALS

2.0 Introduction : In this lesson, the most important notions in ring theory namely ideals and homomorphisms are introduced and it is shown that there is a 1 - 1 correspondence between ideals and congruence relations of a rings.

2.1 Definition : Let $(R,0,1,-,+,\cdot)$ be a ring. A subset S of R is called a subring of R if S is closed under all the operations of R i.e., $O\in S, 1\in S$ for any $a\in S, -a\in S$ and for any $a,b\in S$, $ab\in S$, $a+b\in S$. In other words $(S,0,1,-,+,\cdot)$ is a ring.

2.2 Theorem : The subrings of a ring form a complete lattice under inclusion. The inf of any family of subrings is their intersection. The sup of a simply ordered family of subrings is their union.

Proof : Let Y be the class of all subrings of a ring R. For any $S,T\in Y$, we define $S\le T$ if and only if $S\subseteq T$. Clearly '$\le$' is an ordered relation on Y, so that $(Y,\le)$ is an ordered set. Let $\{S_\alpha\}$ be any family of elements of Y. Put $S=\bigcap S_\alpha$. Clearly S is a subring of R. (Since the intersection of any family of subrings is a subring). Also $S\subseteq S_\alpha\ \forall\alpha\Rightarrow S\le S_\alpha\ \forall\alpha$. Hence S is a lower bound of $\{S_\alpha\}$. Suppose T is a lowerbound of $\{S_\alpha\}\Rightarrow T\subseteq S_\alpha\ \forall\alpha\Rightarrow T\subseteq\bigcap S_\alpha=S\Rightarrow T\le S$.

Hence S is the greatest lowerbound of $\{S_\alpha\}\Rightarrow S=\inf\{S_\alpha\}$. Let $\{S_\alpha\}$ be a simply ordered family of elements of Y. Put $S=\bigcup S_\alpha$ since $0\in S_\alpha\ \forall\ \alpha$ and $1\in S_\alpha\ \forall\alpha$ we have $0\in S$ and $1\in S$. Suppose $a\in S\Rightarrow a\varepsilon S_\beta$ for some β. Since S_β is a subring, we have $-a\in S_\beta\ \Rightarrow -a\in S$. Let $a,b,\in S$. If a and b are in one S_β, then $a+b\in S_\beta$ and $a.b\in S_\beta\Rightarrow\ a+b\in S$ and $a\cdot b\in S$. Suppose $a\in S_\beta$ and $b\in S_\gamma$ for some β and γ. Since $\{S_\alpha\}$ is a simply orderedset, either $S_\beta\subseteq S_\gamma$ or $S_\gamma\ S\,S_\beta.\Rightarrow$ either both a and b are in S_β or in S_γ. $\Rightarrow$ either $a+b$ and ab are in S_β or in S_γ.

$\Rightarrow a+b$ and ab are in S.

Thus S is closed under all the operations $0,1,-,+$ and '.'. Hence S is a subring of R. Since $S=\bigcup S_\alpha$ we have $S_\alpha\subseteq S\,\forall\alpha\ \Rightarrow S_\alpha\le S\,\forall\alpha$.. Hence S is an upper bound of $\{S_\alpha\}$.

Suppose T is an upperbound of $\{S_\alpha\}\Rightarrow S_\alpha\le T\ \forall\ \alpha\Rightarrow S_\alpha\subseteq T\,\forall\alpha\ \Rightarrow\bigcup S_\alpha\subseteq T$. Hence $S\subseteq T\Rightarrow S\le T$.

$\therefore S$ is the least upper bound of $\{S_\alpha\}$. i.e., $S=Sup\{S_\alpha\}$.

2.3 Definition : Let R and S be rings. A mapping $\phi: R \to S$ is called a homomorphism, if ϕ preserves all the operations. i.e., $\phi(0)=0, \phi(1)=1, \phi(-a)=-\phi(a)$ $\phi(a+b)=\phi(a)+\phi(b)$ and $\phi(ab)=\phi(a)\phi(b)$ for all $a,b \in R$.

2.4 Definition : A homomorphism ϕ of R into S is called

(a) a monomorphism if ϕ is one - one.

(b) an epimorphism if ϕ is on to.

(c) an isomorphism if ϕ is both one-one and onto.

2.5 Definition : A homomorphism ϕ of R into itself is called an Endomorphism.

2.6 Definition : An isomorphism ϕ of R onto itself is called an automorphism.

2.7 Remark : If $\phi: R \to S$ and $\psi: S \to T$ are homomorphisms of rings then $\psi o \phi$ is a homomorphism from R in to T defined by $(\psi o \phi)(a) = \psi(\phi(a)) \; \forall \, a \in R$.

2.8 Theorem : Suppose $\phi: R \to S$ and $\psi: S \to T$ are homorphisms of rings.

(1) If ϕ and ψ are monomorphisms, then so is $\psi o \phi$

(2) If ϕ and ψ are epimorphisms, then so is $\psi o \phi$

(3) If $\psi \circ \phi$ is a monomorphism, then so is ϕ

(4) If $\psi \circ \phi$ is an epimorphism, then so is ψ

Proof : (1) Suppose $\psi o \phi(a) = \psi o \phi(b) \Rightarrow \psi(\phi(a)) = \psi(\phi(b))$

Since ψ is a monomorphism, $\phi(a)=\phi(b)$

Again since ϕ is a monomorphism. We have $a=b$. Hence $\psi o \phi$ is mono.

The proofs of (2), (3) and (4) are left as excercise.

2.9 Corollary : A homomorphism $\phi: R \to S$ is an isomorphism if and only if there exists a homomorphism $\psi: S \to R$ such that $\phi o \psi$ is an automorphism of S and $\psi o \phi$ is an automorphism of R.

Proof : Suppose $\phi: R \to S$ is an isomorphism. Define $\phi: S \to R$ as follows. Let $s \in S$. Since ϕ is onto there exist an element $r \in R \ni \phi(r) = s$. Since ϕ is one - one, this $r \in R$ is unique. Now define

$\psi(s)=r$. It can be verified that ψ is a homomorphism and ψ is also one-one and onto. Hence $\phi o \psi$ is a homomorphism of S on to S which is one - one and $\psi o \phi$ is a homomorphism of R on to R which is also one - one. Therefore $\phi o \psi$ is an automorphism of S and $\psi o \phi$ is an automorphism of R.

Conversly suppose that there exist a homorphism $\psi : S \to R$ such that $\phi o \psi$ is an automorphism of S and $\psi o \phi$ is an automorphism of R. Since $\phi o \psi$ is epi, we have ϕ is epi. Since $\psi o \phi$ is mono we have ϕ is mono. Hence ϕ is an isomorphism.

2.10 Definition : Let R and S be rings. A binary relation θ between R and S is called a homomorphic relation if $0\ \theta\ 0$, $1\ \theta\ 1$ and $r_1\ \theta\ s_1$ and $r_2\ \theta\ s_2$ implies $-r_1\ \theta\ -s_1$, $r_1+r_2\ \theta\ s_1+s_2$ and $r_1 r_2\ \theta\ s_1 s_2$.

2.11 Definition : A homomorphic relation from R into R is called a homomorphic relation on R.

2.12 Definition : A homomorphic relation θ on a ring R is called congruence relation if θ is an equivalence relation on R. i.e., θ is reflexive, symmetric, and transitive.

2.13 Theorem (Find Lay) : If θ is a reflexive homomorphic relation on a ring R, then θ is symmetric and transitive.

Proof : Let $a\ \theta\ b \Rightarrow -a\ \theta\ -b$

Now $a \theta a, -a \theta -b$ and $b \theta b$ together implies that $a-a+b\ \theta\ a-b+b \Rightarrow b \theta a$ $\therefore \theta$ is symmetric. Suppose $a \theta b$ and $b \theta c$. Since $b \theta b$, we have $-b\ \theta\ -b$. Now $a \theta b$, $-b \theta -b$ and $b\ \theta\ c$ together implies $a-b+b \theta\ b-b+c \Rightarrow a\ \theta\ c$. Hence θ is transitive.

2.14 Definition : Let θ be a congruence relation on a ring R. The set of all equivalence classes of R or cosets of R determined by the equivalence classes is denoted by R/θ. For any $r \in R$, the equivalence class containing r is denoted by θr which is equal to $\{r' \in R / r \theta r'\}$.

2.15 Theorem : If θ is a congruence relation on a ring R and R/θ is the class of all equivalence classes of R under the equivalence relation θ, then R/θ has the structure of a ring w.r.t. suitable operations.

Proof : For any $\theta a, \theta b$ in R/θ we define $-(\theta a)=\theta(-a)$ and $\theta a+\theta b=\theta(a+b)$ and $\theta a \cdot \theta b = \theta(ab)$.

First we shall prove that all the three operations are well defined.

Suppose $\theta a=\theta a'$ and $\theta b=\theta b'$.

$\Rightarrow a\ \theta\ a'$ and $b\theta b' \Rightarrow -a\theta -a'$. Hence $\theta(-a)=\theta(-a')$.

Also $a+b\ \theta\ a'+b'$ and $ab\theta a'b' \Rightarrow \theta(a+b)=\theta(a'+b')$ and $\theta(ab)=\theta(a'b')$. $\therefore$ All the three operations are well defined. Now we show that $\left(R/\theta, \theta 0, \theta 1, -, +, .\right)$ is a ring with $\theta 0$ as zero element and $\theta 1$ as the unity element.

For any $\theta a, \theta b, \theta c$ in R/θ,

$$\begin{aligned}\theta a+(\theta b+\theta c) = \theta a+\theta(b+c) &= \theta(a+(b+c)) \\ &= \theta((a+b)+c) \\ &= \theta(a+b)+\theta(c) \\ &=(\theta a+\theta b)+\theta c\end{aligned}$$

Hence + is associative.

For any $\theta a\in R/\theta$, $\theta a+\theta 0 = \theta(a+0) = \theta a= \theta 0+\theta a$

$\therefore \theta 0$ is the zero element of R/θ.

For any $\theta a\in R/\theta$, $\theta a+\theta(-a)=\theta 0 = \theta(-a)+\theta a$

$\therefore \theta(-a)$ is the additive inverse of θa.

For any $\theta a, \theta b\in R/\theta$, $\theta a+\theta b = \theta(a+b)=\theta(b+a)$

$$=\theta b+\theta a$$

Hence + is abelian in R/θ

Hence $\left(R/\theta, \theta 0, -, +\right)$ is an abelian group.

Similarly it can be prove that $\left(R/_{\theta},\theta 1,.\right)$ is a semi group with identity. Further, for any $\theta a,\theta b,\theta c$ in $R/_{\theta}$,

$$\theta a(\theta b+\theta c)=\theta a\ \theta b+\theta a\ \theta c \text{ and}$$

$$(\theta a+\theta b)\theta c=\theta a\ \theta c+\theta b\ \theta c$$

Hence two distributive laws hold good in $R/_{\theta}$.

Therefore $\left(R/_{\theta},\theta 0,\theta 1,-,+,.\right)$ is a ring.

2.16 Definition : Let R be a ring and let θ be a congruence relation on R so that $R/_{\theta}$ is a ring. Define $\pi : R\rightarrow R/_{\theta}$ by $\pi(r)=\theta r$ for any $r\in R$. Then π is a homomorphism which is on to. This π is called the canonical epimorphism of R on to $R/_{\theta}$.

2.17 Theorem : If $\phi : R\rightarrow S$ is a homomorphism, then there exists a congruence relation θ on R and an epimorphism $\pi : R\rightarrow R/_{\theta}$ and a monomorphism $K : R/_{\theta}\rightarrow S$ such that $\phi = Ko\pi$.

Proof : For any $r,r',\in R$ define $r\,\theta\, r'$ iff $\phi(r)=\phi(r')$ clearly $0\ \theta\ 0$ and $1\ \theta\ 1$.

Suppose $r\,\theta\, r' \Rightarrow \phi(r)=\phi(r')\Rightarrow -\phi(r)=-\phi(r')$

$$\Rightarrow \phi(-r)=\phi(-r')$$

$$\Rightarrow -r\ \theta\ -r'$$

Suppose $r_1\ \theta\ r_2$ and $r_1'\ \theta\ r_2' \Rightarrow \phi(r_1)=\phi(r_2)$ and $\phi(r_1')=\phi(r_2')$

$$\Rightarrow \phi(r_1+r_1')=\phi(r_1)+\phi(r_1')=\phi(r_2)+\phi(r_2')=\phi(r_2+r_2')$$

and $\quad \phi(r_1\ r_1')=\phi(r_1)\ \phi(r_1')=\phi(r_2)\ \phi(r_2')=\phi(r_2\ r_2')$

$$\Rightarrow r_1+r_1'\ \theta\ r_2+r_2' \text{ and } r_1\ r_1'\ \theta\ r_2\ r_2'$$

$\therefore\ \theta$ is a homomorphic relation on R.

For any $r \in R$, $\phi(r) = \phi(r) \Rightarrow r\theta r \ \forall \ r \in R$

Now $r\theta r' \Rightarrow \phi(r) = \phi(r') \Rightarrow \phi(r') = \phi(r) \Rightarrow r'\theta r$ for any $r, r' \in R$

$\therefore \theta$ is symmetric

Suppose $r\theta r'$ and $r'\theta r''$ $\Rightarrow \phi(r) = \phi(r')$ and $r\phi(r') = \phi(r'')$

$\Rightarrow \phi(r) = \phi(r'') \Rightarrow r \ \theta \ r''$.

$\therefore \theta$ is transitive. Hence θ is a congruence relation on R.

Let R/θ be the family of equivalence classes of R determined by θ and let $\pi: R \to R/\theta$ be the canonical epimorphism of R on to R/θ defined by $\pi(r) = \theta r$ for any $r \in R$.

Define $K: R/\theta \to S$ by $K(\theta r) = \phi(r)$ for any $\theta r \in R/\theta$.

Suppose $\theta r = \theta r' \Rightarrow r\theta r' \Rightarrow \phi(r) = \phi(r')$

Hence K is well defined.

Now $K(\theta 0) = \phi(0) = 0$

$K(\theta 1) = \phi(1) = 0$

$K(\theta r + \theta r') = K(\theta(r + r')) = \phi(r + r') = \phi(r) + \phi(r')$

$= K(\theta r) + K(\theta r')$

$K(\theta r. \theta r') = K(\theta(r r')) = \phi(r r') = \phi(r)\phi(r') = K(\theta r) \ K(\theta r')$

$\therefore$ K is a homomorphism of rings.

Suppose $K(\theta r) = K(\theta r')$ for some $\theta r, \theta r' \in R/\theta$.

$\Rightarrow \phi(r) = \phi(r') \Rightarrow r\theta r' \Rightarrow \theta r = \theta r'$. Hence K is a monomorphism.

For any $r \in R$, $K o \pi(r) = K(\pi(r)) = K(\theta r) = \phi(r)$

$\Rightarrow K o \pi = \phi$

2.18 Theorem : The congruence relations on a ring form a complete Lattice under inclusion. The infimum of any family of congruence relations is their intersection. The sup of a simply ordered family of congruence relations is their union.

Proof : Let S be the set of all congruence relations on a ring R. Every element of S is a subset of $R \times R$. Let $\theta_1, \theta_2 \in S$. We declare that $\theta_1 \le \theta_2$ iff $\theta_1 \subseteq \theta_2$ as subsets of $R \times R$. Now for any $\theta \in S$, Since $\theta \subseteq \theta$ we have $\theta \le \theta$. Hence '$\le$' is reflexive. Suppose $\theta_1 \le \theta_2$ and $\theta_2 \le \theta_1$, $\Rightarrow \theta_1 \subseteq \theta_2$ and $\theta_2 \subseteq \theta_1$.

$\Rightarrow \theta_1 = \theta_2$. $\therefore$ '$\le$' is antisymmetric.

Suppose $\theta_1 \le \theta_2$ and $\theta_2 \le \theta_3 \Rightarrow \theta_1 \subseteq \theta_2$ and $\theta_2 \subseteq \theta_3 \Rightarrow \theta_1 \subseteq \theta_3$

Hence $\theta_1 \le \theta_3$. Therefore '$\le$' is transitive.

Thus $(S, \le)$ is an ordered set.

Let $\{\theta_\alpha\}$ be any family of elements of S. Put $\theta = \bigcap \theta_\alpha$.

Clearly θ is a congruence relation on R and $\theta \le \theta_\alpha \ \forall \alpha$.

Hence θ is a lower bound of $\{\theta_\alpha\}$. If θ' is any other lower bound of $\{\theta_\alpha\} \Rightarrow \theta' \le \theta_\alpha \ \forall \alpha \Rightarrow \theta' \subseteq \theta_\alpha \ \forall \alpha \Rightarrow \theta' \subseteq \bigcap \theta_\alpha = \theta \Rightarrow \theta' \le \theta$

$\therefore \theta$ is the greatest lower bound of $\{\theta_\alpha\}$.

Hence infimum of any family of congruence relations is their intersection.

Now suppose that $\{\theta_\alpha\}$ is a simply ordered family of congruence relations on R. For any θ_β and θ_γ in $\{\theta_\alpha\}$, either $\theta_\beta \subseteq \theta_\gamma$ or $\theta_\gamma \subseteq \theta_\beta$. Hence it can be verified that $\theta = \bigcup \theta_\alpha$ is also a congruence relation on R. Clearly $\theta_\alpha \le \theta \ \forall \alpha \Rightarrow \theta$ is an upperbound of $\{\theta_\alpha\}$. If θ' is an upper bound of $\{\theta_\alpha\}$, we have $\theta_\alpha \le \theta' \ \forall \alpha \Rightarrow \theta_\alpha \subseteq \theta' \ \forall \alpha \Rightarrow \bigcup \theta_\alpha \subseteq \theta' \Rightarrow \theta \subseteq \theta' \Rightarrow \theta \le \theta'$. $\therefore$ θ is the last upper bound of $\{\theta_\alpha\}$. Thus the sup of a simply ordered family of congruence relations is their union.

2.19 Definition : If R is a ring, then an additive subgroup K of R is said to be an ideal of R if $ar \in K$ and $ra \in K$ for all $r \in R$ and $a \in K$.

2.20 Remark : The intersection of any family of ideals of a ring R is an ideal of R.

Proof : 1. Let $\{K_\alpha\}$ be any family of ideals of a ring R. Put $K = \cap K_\alpha$. Since the intersection of subgroups of a group is also a subgroup, it follows that K is also an additive subgroup of R. Let $a \in K$ and $r \in R \Rightarrow a \in K_\alpha \ \forall \alpha \Rightarrow ra \in K_\alpha$ and $ar \in K_\alpha \ \forall \alpha \Rightarrow ra \in K$ and $ar \in K$.

$\therefore$ K is ideal of R.

2.21 Definition : Suppose G is any additive abelian group and A and B are two subgroups. We define their sum $A+B$ as the set of all elements $a+b$ where $a \in A$ and $b \in B$. If $\{A_\alpha\}$ is a family of subgroups G, we define their sum $B = \sum A_\alpha$ as the set of all elements of the form $\sum a_\alpha$ where $a_\alpha \in A_\alpha \ \forall \alpha$ and all but a finite numer of a_α's are zero.

2.22 Remark : (1) If A and B are two subgroups of an additive abelian group G, then $A+B$ is also a subgroup of G. Further if $\{A_\alpha\}$ is a family of subgroups of G, then $\sum A_\alpha$ the sum of $\{A_\alpha\}$ is also a subgroup of G.

Proof : Since 0 = 0 + 0 $\in$ $A+B$, we have that $A+B$ is a non-empty subset of G. Let $a+b \in A+B$ and $c+d \in A+B \Rightarrow a, c \in A$ and $b, d \in B$. Now $(a+b)-(c+d) = (a-c)+(b-d) \in A+B$ $(\because a-c \in A$ and $b-d \in B)$.

$\therefore$ $A+B$ is a subgroup of G.

Since $0 \in \sum A_\alpha$, we have $\sum A_\alpha \neq \phi$. Let $a \in \sum A_\alpha$ and $b \in \sum A_\alpha$.

$\Rightarrow a = a_{\alpha_1} + \dots\dots + a_{\alpha_n}$ and $b = b_{\alpha_1} + \dots\dots + b_{\alpha_n}$. We may assume with out loss of generality that the components of a and b are same, by adding some zeroes if necessary.

Now $a - b = \left(a_{\alpha_1} - b_{\alpha_1}\right) + \left(a_{\alpha_2} - b_{\alpha_2}\right) + \dots\dots + \left(a_{\alpha_n} - b_{\alpha_n}\right)$.

Since $a_{\alpha_i} - b_{\alpha_i} \in A_{\alpha_i}$ for $i = 1, 2, \dots, n$; it follows that $a - b \in \sum A_\alpha$. Hence $\sum A_\alpha$ is a subgroup of G.

2.23 Result (2) : If $\{A_\alpha\}$ is a family of ideals of a ring R, then $\sum A_\alpha$ is also an ideal of R.

Proof : Clearly $\sum A_\alpha$ is an additive subgroup of R.

Let $a = a_{\alpha_1} + \dots\dots + a_{\alpha_n} \in \sum A_\alpha$ and $r \in R$. Now $ar = a_{\alpha_1} r + \dots\dots + a_{\alpha_n} r$ and $ra = ra_{\alpha_1} + \dots\dots + ra_{\alpha_n}$. Since each A_{α_i} is an ideal, we have $a_{\alpha_i} r \in A_{\alpha_i}$ and $r a_{\alpha_i} \in A_{\alpha_i} \ \forall i \Rightarrow ar \in \sum A_\alpha$ and $ra \in \sum A_\alpha$.

$\therefore \sum A_\alpha$ is an ideal of R.

2.24 Theroem : There is a one-to-one correspondence between the ideals K and the congruence relations θ of the ring R such that $r-r' \in K$ iff $r\,\theta\,r'$. Thus is an isomorphism between the lattice of ideals and the lattice of congruence relations.

Proof : Let $\mathcal{K}$ be the set of all ideals of the ring R and let $\mathcal{E}$ be the set of all congruence relations on R. We define $\phi : \mathcal{K} \to \mathcal{E}$ as follows. Let $k \in \mathcal{K}$. Define a binary relation θ_K on R by $a\theta b$ iff $a-b \in K$ for any $a, b \in R$.

Since $0 \in K$, $a-a \in K \;\; \forall a \in R \Rightarrow a\theta a \, \forall a \in R$. Hence θ is reflexive.

In particular $0\theta 0$ and $1\,\theta\,1$.

Suppose $a\theta b$ and $c\,\theta\,d \Rightarrow a-b \in K$ and $c-d \in K$.

Since K is an ideal of R. $(a-b)+(c-d) \in K \Rightarrow (a+c)-(b+d) \in K \Rightarrow (a+c)\theta(b+d)$.

Also $ac-bd = ac-ad+ad-bd = a(c-d)+(a-b)d$. Since $a-b \in K$ and $c-d \in K$, we have $a(c-d) \in K$ and $(a-b)d \in K$

$\Rightarrow ac-bd \in K \Rightarrow ac\;\theta\;bd$

Thus θ is a homomorphic relation which is reflexive and hence θ is a congruence relation on R. Denote this by θ_K.

Define $\phi(K) = \theta_K$. Clearly ϕ is well defined. Let K and J be two ideals of R.

$\ni \phi(K) = \phi(J) \Rightarrow \theta_K = \theta_J$.

Let $a \in K \Rightarrow a-0 \in K \Rightarrow a\theta_K 0 \Rightarrow a\theta_J 0 \Rightarrow a-0 \in J \Rightarrow a \in J$.

Thus $K \subseteq J$. Similarly $J \subseteq K$. Therefore $K = J$. Hence ϕ is 1 - 1. Let $\theta \in \mathcal{E}$ be an element, put $K = \{a \in S / a\theta 0\}$. It can be verified that K is an ideal of R and hence $k \in K$. Now $a\theta\, b$ iff $a-b\;\theta\; b-b$ iff $a-b\;\;\theta\;0$ iff $a-b \in K$. Hence $\theta = \theta_K$. Thus $\phi(K) = \theta$. Hence ϕ is onto. Thus ϕ is a one-to-one correspondence between $\mathcal{K}$ and $\mathcal{E}$. Let K and S be two elements of K. Now we show that $\theta_{K\cap S} = \theta_K \cap \theta_S$. Let $a, b \in R$. Now $a\theta_{K\cap S}\, b$ iff $a-b \in K \cap S$.

iff $a-b \in K$ and $a-b \in S$

iff $a\theta_K b$ and $a\theta_S\, b$.

$$\Rightarrow \theta_{K \cap S} = \theta_K \cap \theta_S \text{. Hence } \phi(K \cap S) = \phi(K) \cap \phi(S).$$

Further $\phi(K \vee S) = \phi(K+S) = \theta_{K+S}$.

Now we show that $\theta_{K+S} = \theta_K \vee \theta_S$.

Suppose $a\ \theta_K\ b \Rightarrow a-b \in K \Rightarrow a-b \in K+S \Rightarrow a\ \theta_{K+S}\ b$.

$\Rightarrow \theta_K \subseteq \theta_{K+S}$. Similarly $\theta_S \subseteq \theta_{K+S}$

$\therefore\ \theta_{K+S}$ is an upper bound of θ_K and θ_S. Let θ be any upper bound of θ_K and $\theta_S \Rightarrow$ $\theta_K \subseteq \theta$ and $\theta_S \subseteq \theta$

Suppose $a\theta_{K+S} b \Rightarrow a-b \in K+S \Rightarrow a-b = x+y$ for some $x \in K$ and $y \in S$.

$$\Rightarrow a-b-x = y \in S \text{ and } a-b-y = x \in K$$

$$\Rightarrow a-b\ \theta_S\ x \text{ and } a-b\ \theta_K\ y$$

$$\Rightarrow (a-b)+(a-b)\ \theta\ (x+y) \Rightarrow a-b\ \theta\ 0\ (\because a-b = x+y)$$

$$\Rightarrow a\ \theta\ b \Rightarrow \theta_{K+S} \subseteq \theta.$$

Thus θ_{K+S} is the least upper bound of θ_K and θ_S.

$\therefore \phi(K \vee S) = \theta_K \vee \theta_S = \phi(K) \vee \phi(S)$ Hence ϕ is a lattice homorphism. Since ϕ is a bijection it follows that ϕ is a lattice isomorphism.

2.25 : Definition : If there is an isomorphism between two rings R and S, we say that R and S are are isomorphic and write as $R \cong S$.

2.26 Remark : In a ring R, if θ and K are the corresponding congruence relation on R and ideal of R, then we write $R/\theta = R/K$.

2.27 Theorem : If ϕ is a homomorphism of a ring R into another ring S, then $\phi(R) \cong R / \phi^{-1}(0)$ where $\phi^{-1}(0) = \left\{ r \in R / \phi(r) = 0 \right\}$ which is the kernal of ϕ.

Proof : Since $\phi : R \to S$ is a homomorphism there exists a congruence relation θ on R and an epimorphism $\Pi : R \to R/_\theta$ and a monomorphism $K : R/_\theta \to S$ such that $\phi = K \circ \Pi$.

Now $\phi(R) = K O \Pi(R) = K\left(R/_\theta\right) \cong R/_\theta$ ($\because$ K is mono).

But the corresponding ideal of the congruence relation θ is given by $\theta 0$ and $\theta 0 = \{a \in R \,/\, a\theta 0\} = \{a \in R \,/\, \phi(a) = \phi(0) = 0\} = \phi^{-1}(0)$.

Hence $R/_\theta = R/_{\phi^{-1}(0)}$

2.28 Definition : A lattice $(S, \wedge, \vee)$ is said to be a modular lattice if a and b are any elements such that $a \le b$, then for any element $c \in S$, $(a \vee c) \wedge b = a \vee (c \wedge b)$.

2.29 Theorem : The set of all ideals in a ring R form a complete modular lattice under set inclusion. The inf of any family of ideals is their intersection. The sup of any family of ideals is their sum.

Proof : Let $\mathscr{I}$ be the set of all ideals of R. Clearly $\mathscr{I}$ is an ordered set underset inclusion. Let $\{A_\alpha\}$ be any family of ideals of R. Then $A = \bigcap A_\alpha$ is also an ideal of R and $A = \inf\{A_\alpha\}$. Thus $\mathscr{I}$ is a complete lattice. Let A and B be ideals such that $A \subseteq B$. Suppose C is any ideal. Now we shall prove that $(A \vee C) \wedge B = A \vee (C \wedge B)$. i.e., $(A + C) \cap B = A + (C \cap B)$. Let $x \in (A + C) \cap B \Rightarrow x \in a + c$ for some $a \in A$ and $c \in C$ and $x \in B$. Since $a \in A$, we have $a \in B$.

Now $x \in B$ and $a \in B \Rightarrow x - a = c \in B \Rightarrow c \in C \cap B$.

Hence $x = a + c \in A + (C \cap B)$

$(A + C) \cap B \subseteq A + (C \cap B)$. Similarly it can be verified that

$A + (C \cap B) \subseteq (A + C) \cap B \;\therefore\; A + (C \cap B) = (A + C) \cap B$.

Thus I is a modular lattice.

Let $\{B_\alpha\}$ be any family of ideals. Suppose $B = \sum B_\alpha$. Then clearly B is an ideal containing $B_\alpha \;\forall\; \alpha \Rightarrow B$ is an upper bound of $\{B_\alpha\}$. Let C be any upperbound of $\{B_\alpha\} \Rightarrow B_\alpha \subseteq C \;\forall\; \alpha$ $\Rightarrow \sum B_\alpha \subseteq C$. *i.e.,* $B \subseteq C \Rightarrow B \le C$.

Therefore B is the least upperbound of $\{B_\alpha\}$. Thus the sup. of any family of ideals is their sum.

2.30 Definition : If A and B are additive subgroups of a ring R, then we define AB as the set of all finite sums $\sum_{i=1}^{n} a_i b_i$ where $a_i \in A$ and $b_i \in B$. We define $(A \cdot\!\!\cdot B)$ (A over B) as the set $\{r \in R / rB \subseteq A\}$ and we define $(A \therefore B)$ (A under B) as the set $\{r \in R / Ar \subseteq B\}$ and for any $r \in R$ the set $rB = \{rb / b \in B\}$.

The sets $(A \cdot\!\!\cdot B)$ and $(A \therefore B)$ are called residual quotients.

2.31 Remark : If A and B are subgroups of a ring R, then AB, A∴B and A∵B are also subgroups of R.

2.32 Theorem : If A, B, C and $\{A_\alpha\}$ and $\{B_\alpha\}$ are all subgroups of R. Then the following are valied.

(1) $AB \subseteq C$ iff $A \subseteq C \cdot\!\!\cdot B$ iff $B \subseteq (A \therefore C)$

(2) $(A \cdot\!\!\cdot B) \cdot\!\!\cdot C = (A \cdot\!\!\cdot CB)$

(3) $(A \therefore B) \cdot\!\!\cdot C = A \therefore (B \cdot\!\!\cdot C)$

(4) $A \therefore (B \therefore C) = (BA) \therefore C$

(5) $(\sum A_\alpha) B = \sum (A_\alpha B)$

(6) $(\cap A_\alpha \cdot\!\!\cdot B) = \cap (A_\alpha \cdot\!\!\cdot B)$

(7) $(A \cdot\!\!\cdot \sum B_\alpha) = \cap (A \cdot\!\!\cdot B_\alpha)$

2.33 Result : If A, B are ideals of a ring R, then so are AB, ($A \cdot\!\!\cdot B$) and ($A \therefore B$). Moreover (1) $AR = A = RA$ (2) $(A \cdot\!\!\cdot R) = A = (R \therefore A)$. (3) $(A \cdot\!\!\cdot A) = R = (A \therefore A)$ (4) $AB \subseteq A \cap B$

Proof : (1) Since A is an ideal we have for any $a \in A$, $r \in R$, $ar \in A$. Every element of AR is the form $\sum_{i=1}^{n} a_i r_i$ where $a_i \in A$ and $r_i \in R$ and $n \in W$.

Since each $a_i r_i \in A$ we have $\sum_{i=1}^{n} a_i r_i \in A$. $\therefore AR \subseteq A$.

Since $I \in R$, we have for any $a \in A$, $a = a.1 \in AR \Rightarrow A \subseteq AR$.

Therefore $A = AR$. Similarly $A = RA$.

(2) Let $a \in A$, since A is an ideal, $aR \subseteq A \Rightarrow a \in (A.\cdot R)$

$\Rightarrow A \subseteq (A.\cdot R)$. Let $x \in (A.\cdot R) \Rightarrow x R \subseteq A \Rightarrow x.1 \in A \Rightarrow x \in A$

Therefore $(A.\cdot R) \subseteq A$

Then $A = (A.\cdot R)$ similarly $A = (R\cdot. A)$.

Prof. G. Koteswara Rao
Department of Mathematics
Acharya Nagarjuna University

3)

Lesson : 3 **MODULES, DIRECT PRODUCTS**

3.0 Introduction : In this lesson, another important algebric system namely module is introducec and the direct products are studied.

3.1 Definition : Let R be a ring. An additive abelian group A is said to be a right R - module denoted by A_R if there exists a mapping $(a,r)\mapsto ar$ from $A\times R$ into A satisfying.

(1) $a(r+s) = ar + as \quad \forall \quad a\in A,\ r,\ s\in R$

(2) $(a+b)r = ar+br \quad \forall \quad a,b\in A$ and $r\in R$

(3) $a(r\cdot s) = (ar)s \quad \forall \quad a\in A$ and $r,s\in R$

(4) $a.1 = a \quad \forall \quad a\in A$

3.2 Definition : An additive abelian group A is said to be a left R module if there is a mapping $(r,a)\mapsto ra$ from $R\times A\to A$ satisfying the corresponding above four identities.

3.3 Example :

1. Let A be an abelian group. Then A is a Z - module. Where for any $a\in A,\ n\in Z$,

   $an = a+a+......+a$ (n times) if n is positive and

   $an=-(a+a+....+a)$ ($-n$ times) if n is negative.

   $a0=0$

2. If R is a ring, then R itself an R - module.

3. Let A be any abelian group and Let F be the set of all endomorphisms of A. Let $\bar{0}$ be the zero endomorphism defined by $a\bar{0}=0$ for all $a\in A$. Let $\bar{1}$ be the identity endomorphism defined by $a\cdot\bar{1}=a$ for all $a\in A$. For all $f,g\in F$. Define $f+g$ and fg and $-f$ by

   $a(f+g)=af+ag$ and $a(f\,g)=((a)f)g$ and $a(-f) = -af$ for all $a\in A$. Then it can

be verified that $(F,\bar{0},\bar{1},-,+,.)$ is a ring. For any $a\in A$, $f\in F$, we define $af=(a)f$. This operation gives us that A is a right F-module A_F.

3.4 Theorem : Let $\Gamma : R \to F$ be a homomorphism of rings where R is a ring and F is the ring of endomorphisms of an additive abelian group A. For any $a \in A$ and $r \in R$, we define $ar = a(\Gamma(r))$. Then A is a right R - module. Further every right R-module may be obtained in this way.

Proof : Let $a, b \in A$ and $r, s \in R$.

Now $(a+b)r = (a+b)(\Gamma r) = a(\Gamma r) + b(\Gamma r)$ $\quad (\because \Gamma r$ is an endomorphism)

$$= ar + br$$

$$a(r+s) = a\Gamma(r+s)$$

$$= a(\Gamma(r) + \Gamma(s)) \qquad \text{(By the definition of addition of maps)}$$

$$= a\,\Gamma(r) + a\,\Gamma(s)$$

$$= ar + as$$

$$a(r.s) = a\Gamma(r\,s) = a(\Gamma r)\,\Gamma(s) \qquad (\because \Gamma \text{ is a homomorphism})$$

$$= ((a)\Gamma r)\Gamma(s) \text{ (composition of maps)}$$

$$= (ar)\Gamma(s) = (ar)s$$

$$a.1 = a.\Gamma(1) = a.I = a \qquad (\because \Gamma \text{ is homo, } \Gamma(1) = I)$$

Hence A is a right R - module.

Conversly Let A_R be any right R - module. Let F be the set of all endomorphism of the additive abelian group We know that F is a ring Define $\Gamma : R \to F$ by $\Gamma(r)$ as the endomorphism on A given by $(a)\Gamma(r) = ar$ for any $a \in A$. It can be verified that Γ is a ring homomorphism and the R - module structure is determined by Γ since $ar = (a)\Gamma(r)$.

3.4 Remark : Suppose A_R is a right R - module. Every $r \in R$ can be seen as a unary operation on A given by $a \mapsto ar$ satisfying $(a+b)r = ar + br$ for any $a, b \in A$. Thus the R - module A_R is regarded as a system $(A, 0, -, +, R)$ where $(A, 0, -, +)$ is an abelian group and each element r of R is a unary operation on A satisfying

$(a+b)r = ar+br$ for all $a,b \in A$.

3.5 Definition : Let A_R be a right R - module. An additive subgroup B of A is called a submodule of A_R if B_R is an R - module.

3.6 Definition : Let A_R and B_R be two right modules. A mapping $\phi: A \to B$ is said to be a module homomorphism if $\phi(0)=0$, $\phi(x+y)=\phi(x)+\phi(y)$ $\phi(-x)=-\phi(x)$ and $\phi(xr) = \phi(x)r$ for all $r \in R$, $x, y \in A$. i.e. ϕ is a group homomorphism satisfying $\phi(ar) = \phi(a)r$ for all $a \in A$, $r \in R$.

3.7 Definition : Zorn's Lemma : If every simply ordered subset of a nonempty ordered set $(S, \leq)$ has an upper bound in S, then S has at least one maximal element m in the sense that $m \leq s$ for any $s \in S$ implies $m = s$.

3.8 Definition : Axiom of Choise : The Cartesion product of a non-empty family of non-empty sets is non-empty. i.e., If $\{S_\alpha\}_{\alpha \in \Delta}$ is a family of sets where $\Delta \neq \phi$ and $S_\alpha \neq \phi$ $\forall \alpha \in \Delta$, then there is at least one map $f: \Delta \to \bigcup_{\alpha \in \Delta} S_\alpha$ such that $f(\alpha) \in S_\alpha$ $\forall \alpha \in \Delta$.

3.9 Theorem : Let T be any subset of the module A_R. Then any submodule B of A_R which has no element in common with T except possibly O is contained in a submodule M which is maximal with respect to this property.

Proof : Let P be the set of all submodules of A_R, which contains B and whose intersection with T is contained in the submodule $\{0\}$. Since $B \in P$, it follows that $P \neq \phi$. Now P is an ordered set under set inclusion. Let $\{B_\alpha\}_{\alpha \in \Delta}$ be any simply ordered family of submodules in P. Put $B = \bigcup_{\alpha \in \Delta} B_\alpha$ Since $\{B_\alpha\}$ is a simply ordered family, it follows that B is also a submodule of A. Suppose if possible an element $0 \neq x \in B \cap T \Rightarrow x \in B_\alpha$ for some $\alpha \in \Delta \Rightarrow 0 \neq x \in B_\alpha \cap T$. Which is a contradiction since each B_α has no element common with T except possibly 0. Hence $B \cap T \subseteq \{0\}$. Hence $B \in P$, clearly B is an upper bound of $\{B_\alpha\}$ since $B_\alpha \subseteq B$ $\forall \alpha$. Thus every simply ordered set in P has an upper bound in P. Hence by Zorn's Lemma, P has at least one maximal element M. $\Rightarrow M$ is a submodule of A which is maximal w.r.t. the property that it has no element in common with T except possibly 0.

3.10 Definition : If R is a ring, then a submodule of the right R - module R_R is called a right ideal of R.

3.11 Definition : An ideal (right ideal) of a ring R is said to be a proper ideal (right ideal) if it does not contain 1.

3.12 Theorem : Every proper ideal (right ideal) of a ring R is contained in a maximal proper ideal (right ideal).

Proof : Take $T=\{1\}$ or $\{0,1\}$. Let P be any proper ideal of R. Let $\mathbb{P}$ be the set of all ideals whose intersection with T is contained in $\{0\}$. Since P is a proper ideal, $1 \notin P$ Hence $P \cap T \subseteq \{0\}$.

Hence $p \in \mathbb{P} \Rightarrow \mathbb{P} \neq \phi$. Now $\mathbb{P}$ is an ordered set under set inclusion. If $\{A_\alpha\}$ is any simply ordered family of elements of $\mathbb{P}$. Put $A = UA_\alpha$. Since $\{A_\alpha\}$ is simply ordered, A is an ideal of R. Since each $A_\alpha \in \mathbb{P}$, we have $1 \notin A_\alpha \ \forall \alpha \Rightarrow 1 \notin A$. Hence A is also a proper ideal and hence $A \cap T \subseteq \{0\} \Rightarrow A \in \mathbb{P}$. Clearly $A_\alpha \subseteq A \ \forall \alpha \Rightarrow A$ is an upper bound of $\{A_\alpha\}$. Thus we have that every simply ordered set has an upper bound in $\mathbb{P}$. By Zorn's lemma, $\mathbb{P}$ has a maximal element M. Now M is a maximal proper ideal containing P.

3.13 Definition : If $\{A_\alpha\}_{\alpha \in \Delta}$ is any family of sets. The Cartesian Product of $\{A_\alpha\}$ is defined as the set of all mappings $x : \Delta \to \underset{\alpha \in \Delta}{U} A_\alpha$ such that $x(\alpha) \in A_\alpha \ \forall \alpha$. If x is any element of the Cartesian product of $\{A_\alpha\}_{\alpha \in \Delta}$, then x is denoted by $x = \{x_\alpha\}$. Where $x_\alpha = x(\alpha)$ for every α. The Cartesian product is denoted by pA_α or πA_α.

3.14 Remark : If $\{A_\alpha\}_{\alpha \in \Delta}$ where $\Delta = \{1,2,....,n\}$, then the Cartesian product is denoted by $A_1 \times A_2 \times ...... \times A_n$ Any element x in $A_1 \times A_2 \times ...... \times A_n$ is written as $x = (x_1, x_2, ..., x_n)$ where $x_i \in A_i$ for $i = 1, 2, ...n$.

3.15 Definition : Suppose $\{R_\alpha\}_{\alpha \in I}$ is a family of Rings. Let πR_α be the Cartesian product of the sets $\{R_\alpha\}_{\alpha \in I}$. We define all the ring operations by

(1) $\overline{O} = \{O_\alpha\}$ where $O_\alpha = 0$ in $R_\alpha \ \forall \alpha$.

(2) $\overline{1} = \{1_\alpha\}$ where $1_\alpha = 1$ in $R_\alpha \ \forall \alpha$

(3) For any $x=\{x_\alpha\}, -x=\{-x_\alpha\}$ where $-x_\alpha$ is the additive inverse of x_α in $R_\alpha\ \forall\alpha$.

(4) For any $x=\{x_\alpha\}$ and $y=\{y_\alpha\}$ in πR_i, $x+y=\{x_\alpha+y_\alpha\}$ and $xy=\{x_\alpha\, y_\alpha\}$ where $x_\alpha+y_\alpha\in R_\alpha$ and $x_\alpha\, y_\alpha\in R_\alpha\ \forall\alpha$.

So that πR_α is a ring with the above operations. i.e., $\left(\pi R_\alpha, \bar{0}, \bar{1}, -, +, \cdot\right)$ is a ring.

3.16 Definition : Suppose $\{A_\alpha\}_{\alpha\in\Delta}$ is a family of R - modules. The Caresian product. πA_α is called the direct product of R - modules $\{A_\alpha\}$ if we define all module opertions on πA_α which makes πA_α as an R - module.

3.17 Remark : We define the module operations on $A=\pi A_\alpha$ as follows.

(1) $\bar{0}=\{0_\alpha\}$ where 0_α is the zero element of $A_\alpha\ \forall\alpha$.

(2) If $x=\{x_\alpha\}$ in A, then $-x=\{-x_\alpha\}$.

(3) If $x=\{x_\alpha\}$, $y=\{y_\alpha\}$ in A, then $x+y=\{x_\alpha+y_\alpha\}$.

(4) If $x=\{x_\alpha\}$ in A and $r\in R$, then $xr=\{x_\alpha r\}$.

3.18 Definition : If $\{A_\alpha\}_{\alpha\in\Delta}$ is any family of subgroup of an abelian additive group A, then the sum of $\{A_\alpha\}_{\alpha\in\Delta}$ is defined as the set of all elements of the form $\sum\limits_{\alpha\in\Delta} a_\alpha$ where $a_\alpha\in A_\alpha\ \forall\alpha$ and all but a finite no. of a_α's are zeroes. The sum is denoted by $\sum\limits_{\alpha\in\Delta} A_\alpha$. We say that the sum $\sum\limits_{\alpha\in\Delta} A_\alpha$ is a direct sum if 0 can not be written non trivially as a sum of elements of the A_α's i.e. if $0=\sum\limits_{\alpha\in\Delta} a_\alpha$ where $a_\alpha\in A_\alpha$ then $a_\alpha=0\ \forall\alpha\in\Delta$.

3.19 Definition : An element a of a ring R is said to be an idempotent if $a^2=a$.

3.20 Definition : An element a of a ring R is said to be a central element if $ar=ra\ \forall\ r\in R$.

3.21 Definition : Suppose $A_1, A_2, \ldots, A_n$ are subgroups of a group A. We say that A is the direct sum of $A_1, A_2, \ldots, A_n$ if every element a of A can be uniquely expressed as $a=a_1+a_2+\ldots+a_n$ where $a_i\in A_i$ for $i=1,\ldots,n$.

3.22 Definition : Suppose $\{A_\alpha\}_{\alpha\in\Delta}$ is a family of subgroups of a group A. We say that A is the direct sum of $\{A_\alpha\}_{\alpha\in\Delta}$ if every element $a \in A$ can be uniquely expressed as $a = \sum_{\alpha\in B} a_\alpha$ where $a_\alpha \in A_\alpha$ and all most all the a_α's are zeroes except for finite number.

3.23 Problem : Suppose $\{B_\alpha\}_{\alpha\in\Delta}$ is a family of submodules of a module A_R. Then the sum $\sum_{\alpha\in\Delta} B_\alpha$ is direct iff $B_\alpha \cap \sum_{r\neq\alpha} B_r = 0$, $\forall\ \alpha \in \Delta$.

Proof : Suppose $\sum_{\alpha\in\Delta} B_\alpha$ is direct $\Rightarrow 0$ cannot be written nontrivially as a sum of elements of the B_α's. Let $x \in B_\alpha \cap \sum_{r\neq\alpha} B_r$

$$\Rightarrow x \in B_\alpha \text{ and } x \in \sum_{r\neq\alpha} B_r \Rightarrow x = \sum_{r\neq\alpha} b_r$$

Put $x = b_\alpha$. Now $\sum_{r\neq\alpha} b_r - x = 0 \Rightarrow \sum_{r\neq\alpha} b_r - b_\alpha = 0$

$\Rightarrow \sum b_r = 0 \Rightarrow b_r = 0\ \forall r \in \Delta$. In particular $b_\alpha = 0 \Rightarrow x = 0$.

Thus $B_\alpha \cap \sum_{r\neq\alpha} B_r = 0$

Conversly suppose that $B_\alpha \cap \sum_{r\neq\alpha} B_r = 0\ \forall\ \alpha$.

Suppose $0 = \sum a_r$ where at least one $a_\alpha \neq 0$

$$\Rightarrow 0 = a_\alpha + \sum_{r\neq\alpha} a_r \Rightarrow \sum_{r\neq\alpha} a_r = -a_\alpha$$

But $a_\alpha \in B_\alpha$ and $\sum_{r\neq\alpha} a_r \in \sum_{r\neq\alpha} B_r$

$$\Rightarrow a_\alpha \in B_\alpha \cap \sum_{r\neq\alpha} B_r \Rightarrow B_r \cap \sum_{r\neq\alpha} B_r \neq 0 \qquad (\because a_\alpha \neq 0)$$

Which is a contradiction. $\therefore$ 0 cannot be written as non-trivially as the sum of elements of the B_α's.

3.24 Theorem : Let R be a ring. Then the following are equivalent.

(a) R is isomorphic to a finite direct product of rings $R_i\,(i=1,2,...n)$.

(b) There exist central orthogonal idempotents $e_i \in R$ such that $1=\sum_{i=1}^{n} e_i$ and $e_i R \cong R_i$

(c) R is a finite direct sum of ideals $K_i \cong R_i$ for $i=1,2,...n$.

Proof : Assume (a) Let $\phi : R \to R_1 \times R_2 \times ... R_n$ be an isomprphism of R onto the direct product of rings $R_i\,(i=1,2,...n)$.

Let $\epsilon_i = (0.0,...0,1,0,....0)$ which is an n tuple with 1 in ith place and 0 else where for $i=1,2,...n$. Since ϕ is an isomorphism for every i, $\exists$ is a unique e_i in $R \ni \phi(e_i)=\epsilon_i$, since $\epsilon_i^2=\epsilon_i$ for $i=1,2,....n$ we have $\phi\left(e_i^2\right)=\phi(e_i)\,\forall i$. Since ϕ is one one, $e_i^2=e_i$ for $i=1,2,....n$. Since $\phi(e_1+....+e_n) = \epsilon_1+\epsilon_2+.....+\epsilon_n = (1,1,.....,1)$ which is the unity element in the direct product it follows that $e_1+.....+e_n$ is the unity in R.

$$\Rightarrow e_1+e_2+....+e_n=1$$

Define $\phi_i : e_i R \to R_i$ by $\phi_i(e_i r) = \pi_i(\phi(r))\,\forall i$

Clearly ϕ_i is a homomorphism. Since it is the composition of homomorphisms π_i and ϕ.

Suppose $\phi_i(e_i r)=\phi_i(e_i s) \Rightarrow \pi_i(\phi(r))=\pi_i(\phi(s))$

$$\Rightarrow \epsilon_i \phi(r)=\epsilon_i \phi(s)$$

$$\Rightarrow \phi(e_i)\phi(r) = \phi(e_i)\phi(s)$$

$$\Rightarrow \phi(e_i r)=\phi(e_i s)$$

$$\Rightarrow e_i r = e_i s$$

Hence ϕ_i is one one. Let $r_i \in R_i$. Since ϕ is on to, $\exists\, r \in R \ni \phi(r)=(0,0,.....,r_i,0,0,....,0)$ where r_i is in the i^{th} place, zero else where. $\Rightarrow \phi_i(\phi(r))=r_i \Rightarrow \pi_i\phi(r)=r_i \Rightarrow \phi_i(e_i r)=r_i$. Hence ϕ_i is on to. Thus ϕ_i is an isomorphism of $e_i R$ on to R_i. Hence $(a)\Rightarrow(b)$ assume (b).

Put $K_i = e_i R$, clearly K_i is an ideal of R for $i = 1, 2, \ldots n$ and $K_i \cong R_i \ \forall i$.

Let $r \in R \Rightarrow r = 1.r = (e_1 + \ldots + e_n) r = e_1 r + \ldots + e_n r$

$\Rightarrow r \in K_1 + K_2 + \ldots + K_n \Rightarrow R = K_1 + K_2 + \ldots + K_n$

Let $x \in K_i \cap \sum_{j \neq i} K_j$ for some i.

$\Rightarrow x = e_i r_i$ and $x = e_1 r_1 + \ldots + e_{i-1} r_{i-1} + e_{i+1} r_{i+1} + \ldots + e_n r_n$.

$\Rightarrow x = e_i x = e_i r_i = e_i \left(e_1 r_1 + \ldots + e_{i-1} r_{i-1} + e_{i+1} r_{i+1} + \ldots + e_n r_n \right) = 0$

This is true for $i = 1, 2, \ldots n$. Hence the sum $\sum_{i=1}^{n} K_i$ is a direct sum

Hence $(b) \Rightarrow (c)$

Assume (c) Let ϕ_i be an isomorphism of K_i on to R_i.

Define $\phi : R \to R_1 \times R_2 \times \ldots \times R_n$ as follows. Let $r \in R$.

$\Rightarrow r = a_1 + a_2 + \ldots + a_n$ for some unique set of elements $a_1, a_2, \ldots, a_n$, where $a_i \in k_i$ for $i = 1, 2, \ldots n$.

Define $\phi(r) = (\phi_1(a_1), \phi_2(a_2), \ldots\ldots, \phi_n(a_n))$

Clearly ϕ is a homomorphism.

Suppose $\phi(r) = \phi(s)$ suppose $r = a_1 + a_2 + \ldots + a_n$

$s = b_1 + b_2 + \ldots + b_n$

$\Rightarrow \phi_i(a_i) = \phi_i(b_i)$ for $i = 1, 2, \ldots n$

$\Rightarrow a_i = b_i$ for $i = 1, 2, \ldots n$

$\Rightarrow r = s$ $\quad \therefore \phi$ is one one

Let $(r_1, r_2, \ldots r_n) \in (R_1 \times R_2 \times \ldots \times R_n)$

Put $a_i = \phi^{-1}(r_i) \forall i$. Put $r = a_1 + \ldots + a_n$

Now $r \in R$ and $\phi(r) = (r_1, r_2, \ldots, r_n)$

$\therefore \phi$ is on to. Hence ϕ is an isomorphism of R onto $R_1 \times R_2 \times \ldots \times R_n$

Hence $(c) \Rightarrow (a)$

Lesson : 4 DIRECT SUM OF MODULES

4.0 Introduction : In this lesson, the direct sum of a family of modules is defined and some equivalent condition to a direct sum of a modules is given.

4.1 Definition : Suppose $A = \underset{\alpha \in \Delta}{\pi} A_\alpha$ is the direct product of R-modules. If $\pi_\alpha : A \to A_\alpha$ and $K_\alpha : A_\alpha \to A$ are the canonical epimorphism and monomorphism respectively, then

$$\pi_\alpha 0 k_\beta = 1 \text{ if } \alpha = \beta$$

$$= 0 \text{ if } \alpha \neq \beta$$

4.2 Definition : A submodule A of the direct product $\underset{i \in I}{\pi} A_i$ of R-modules consisting of all $a \in \underset{i \in I}{\pi} A_i$ such that $a(i) = 0$ for all but finite number.

4.3 Definition : A submodule A of the direct product $\underset{i \in I}{\pi} A_i$ of R - modules consisting of all $a \in \underset{i \in I}{\pi} A_i \ni a_i = 0$ for all but finite number of i's is called the (external) direct sum of R - modules $\{A_i\}_{i \in I}$. It is denoted by $\overset{*}{\underset{i \in I}{\Sigma}} A_i$.

4.4 Remark : If $\{A_i\}_{i \in I}$ is a family of R - modules and $A = \overset{*}{\underset{i \in I}{\Sigma}} A_i$ is the direct sum of R modules and for every $i \in I$ $\pi_i : A \to A_i$ is the canonical epimorphism and $k_i : A_i \to A$ is the canonical monomorphism, then $\underset{i \in I}{\Sigma} K_i 0 \pi_i(a) = a$ for all $a \in A$.

Proof : Let $a \in A \Rightarrow a(i) = 0 \,\forall\, i \neq i_1, i_2, \ldots, i_n$ for some $i_1, i_2, \ldots, i_n$ in I.

For any $i \neq i_1, i_2, \ldots i_n$ $K_i 0 \pi_i(a) = 0$

Hence $\underset{i \in I}{\Sigma} k_i 0 \pi_i(a) = \sum_{r=1}^{n} K_{i_r} 0 \pi_{i_r}(a) = a$

4.5 Definition : Let A be an R - module. A family $\{f_i\}_{i\in I}$ of endomorphism of A is said to be a complete system of orthogonal idempotent endomorphisms.

if (1) $f_i \, 0 \, f_j = 0$ for $i \neq j$

(2) $f_i \, 0 \, f_i = f_i$ for all i.

(3) $\sum\limits_{i\in I} f_i(a)$ is a finite sum and is equal to a for all $a \in A$.

4.6 Theorem : The following statements are equivalent concerning R - modules

(1) A_R is isomorphic with the (external) direct sum of R - modules $\{A_i\}_{i\in I}$

(2) A_R has a complete system of orthogonal idempotent endomorphisms

$\{\in_i\}_{i\in I} \ni \in_i A \cong A_i \ \forall i$

(3) A_R is the (internal) direct sum of submodules $\{B_i\}_{i\in I}$ where $B_i \cong A_i \ \forall i$.

Proof : Assume (1)

Let ψ be an isomorphism of A_R on to $\sum\limits_{i\in I} A_i$. Let π_i be the canonical epimorphism of $\sum\limits_{i\in I} A_i$ onto A_i and let K_i be the canonical monomorphism of A_i into $\sum\limits_{i\in I} A_i$

Put $\in_i = \psi^{-1} \, 0 \, K_i \, 0 \, \pi_i \, 0 \, \psi$. Clearly $\in_i$ is an endomorphism of A_R for all i. Now we show that $\{\in_i\}_{i\in I}$ is a complete system of orthogonal idempotent endomorphisms.

Suppose $i \neq j$ then $\in_i 0 \in_j = \left(\psi^{-1} 0 \, k_i 0 \, \pi_i 0 \, \psi\right) 0 \left(\psi^{-1} \, 0 \, k_j 0 \, \pi_j 0 \, \psi\right) = 0$

Suppose $i = j$. Then $\in_i \, 0 \in_i = \left(\psi^{-1} 0 \, K_i \, 0 \pi_i \, 0 \psi\right) 0 \left(\psi^{-1} 0 \, K_i \, 0 \pi_i \, 0 \psi\right) = \in_i$

Let $a \in A \Rightarrow \psi(a) \in \sum\limits_{i\in I} A_i = \psi(a)(i) = 0$ for all i except for finite number of i's (sa

$i_1, i_2, ..., i_n$.

$\sum\limits_{i\in I} \in_i (a) - \sum\limits_{i\in I}\left(\psi^{-1}\, 0\, K_i\, 0\, \pi_i\, 0\, \psi\right)(a) - \sum\limits_{i=i_1}^{i_n}\left(\psi^{-1}\, 0\, K_i\, 0\, \pi_i\, 0\, \psi\right)(a)$ which is a finite sum

and $\sum\limits_{i\in I} \in_i (a) = \sum\limits_{i\in I}\left(\psi^{-1}\, 0\, K_i\, 0\, \pi_i\, 0\, \psi\right)(a)$

$$= \psi^{-1}\left(\sum_{i\in I}(K_i\, 0\, \pi_i)(\psi(a))\right)$$

$$= \psi^{-1}(\psi(a)) = a$$

$\therefore \{\in_i\}_{i\in I}$ is a complete system of orthogonal idempotent endomorphisms of A_R.

Further $\in_i (A) = \left(\psi^{-1}\, 0\, K_i\, 0\, \pi_i\, 0\, \psi\right) A$

$$= \left(\psi^{-1}\, 0\, K_i\, 0\, \pi_i\right)(\psi(A))$$

$$= \left(\psi^{-1}\, 0\, K_i\right)\left(\pi_i\left(\sum_{i\in I} A_i\right)\right)$$

$$= \left(\psi^{-1}\, 0\, K_i\right) A_i \cong \psi^{-1}(A_i) \cong A_i \;\forall i$$

Thus $(1) \Rightarrow (2)$

Assume (2)

Let $\{\in_i\}_{i\in I}$ be a complete system of orthogonal idempotent endomorphisms of A_R such that $\in_i A \cong A_i$ for all i.

Put $B_i = \in_i A$ for every i. Clearly each B_i is a submodule of A and $B_i \cong A_i$.

Now we show that A_R is the (internal) direct sum of submodules $\{B_i\}_{i\in I}$. Let $a \in A$.

By the hypothesis $\sum\limits_{i\in I} \in_i (a) = a$ and the sum is finite.

For each $i \in I, \in_i (a) \in B_i \Rightarrow a \in \sum_{i \in I} B_i$

$$\therefore A = \sum_{i \in I} B_i$$

Let $a \in B_i \cap \sum_{j \neq i} B_j \Rightarrow a = b_i$ for some $b_i \in B_i$ and

$$a = b_{j_1} + b_{j_2} + b_{j_3} + \ldots\ldots + b_{j_n} \text{ where } \quad i \neq j_1, j_2, \ldots., j_n$$

$$\Rightarrow b_i = b_{j_1} + b_{j_2} + \ldots.. + b_{j_n}$$

$$\Rightarrow b_i = \in_i (b_i) = \in_i \left(b_{j_1} + b_{j_2} + \ldots.. + b_{j_n}\right) = 0$$

$$\Rightarrow a = 0 \Rightarrow B_i \cap \sum_{j \neq i} B_j = 0 \ \forall\ i \in I$$

$\therefore A_R$ is the internal direct sum of submodules $\{B_i\}_{i \in I}$ where $B_i \cong A_i \ \forall i$.

Thus $(2) \Rightarrow (3)$

Assume (3)

Let ψ_i be an isomorphism of B_i onto A_i for every i.

Define $\psi : A \to \sum_{i \in I} A_i$ as follows.

Let $a \in A$.

Since A_R is the internal direct sum of submodules $\{B_i\}_{i \in I}$, we have $a = \sum_{i \in I} b_i$ where $b_i \in B_i \ \forall i$ and $b_i = 0$ except for finite number of $i's$.

Now define $\psi(a) = \{\psi_i(b_i)\}_{i \in I}$.

Clearly $\psi_i(b_i) = 0$ except for finite number of $i's$.

Hence $\{\psi_i(b_i)\} \in \sum_{i \in I} A_i$

Clearly ψ is a homomorphism.

Suppose $\psi(a)=\psi(a')$ where $a=\sum_{i\in I} b_i$ and $a'=\sum_{i\in I} b_i'$

$$\Rightarrow \{\psi_i(b_i)\}_{i\in I}=\{\psi_i(b_i')\}_{i\in I}$$

$$\Rightarrow \psi_i(b_i)=\psi_i(b_i')\ \forall i$$

$$\Rightarrow b_i=b_i' \Rightarrow a=a'$$

$\therefore \phi$ is one one.

Let $\{a_i\}_{i\in I} \in \sum_{i\in I} A_i$

Since ψ_i is on to $\forall i$, $\exists b_i \in B_i \ni \psi_i(b_i)=a_i\ \forall i$

Put $a=\sum_{i\in I} b_i$

Now $a\in A$ and $\psi(a)=\{\psi_i(b_i)\}_{i\in I}=\{a_i\}_{i\in I}$

$\therefore \psi$ is onto

$\therefore \psi$ is isomorphism.

Thus $(3)\Rightarrow(1)$

Problem : Prove that the sum $\sum_{i\in I} B_i$ of submodules of A_R is direct $\Leftrightarrow \forall i\in I,\ B_i \cap \sum_{j\neq i} B_j=0$

Proof : Suppose $B=\sum_{i\in I} B_i$ is a direct sum of submodules of A_R.

$\Rightarrow$ every element $a\in B$ can be uniquely expressed as $a=\sum b_i$

where $b_i\in B_i$ and the sum is finite.

Let $a\in B_i \cap \sum_{j\neq i} B_j \Rightarrow a=b_i$ and

$a=\sum_{j\neq i} b_j$ where $b_i\in B_i$ and $b_j\in B_j$ for all $j\neq i$.

Suppose $a=b_{j_1}+b_{j_2}+.....+b_{j_n}$

$$\Rightarrow b_i=b_{j_1}+b_{j_2}+.....+b_{j_n} \Rightarrow 0=-b_i+b_{j_1}+b_{j_2}+....+b_{j_n}$$

Since $\sum B_i$ is a direct sum, we must have $b_i=0=b_{j_1}+b_{j_2}+....+b_{j_n}$

$$\Rightarrow B_i \cap \sum_{j\neq 1} B_j=0$$

Conversly suppose that $B_i \cap \sum_{i\neq j} B_j=0$

Let $a \in \sum_{i\in I} B_i$. By definition 'a' can be written as

$a=\sum_{i\in I} b_i$ where $b_i \in B_i$ and the sum is finite.

Suppose $a=\sum_{i\in I} b_i = \sum_{i\in I} b_i'$ where $b_i, b_i' \in B_i$

Fix some $i_0 \in I$, now $b_{i_0}-b_{i_0}' = \sum_{\substack{i\in I\\ i\neq i_0}} (b_i'-b_i)$

$$\Rightarrow b_{i_0}-b_{i_0}' \in B_{i_0} \cap \sum_{j\neq i_0} B_j=0$$

$$\Rightarrow b_{i_0}=b_{i_0}'$$

This is true for every $i_0 \in I$

$$\therefore b_i=b_i' \quad \forall\ i \in I$$

Thus every element of $\sum B_i$ can be uniquely expressed as the sum of elements of B_i.

$\Rightarrow \sum_{i\in I} B_i$ is a direct sum.

Prof. G. Koteswara Rao
Department of Mathematics
Acharya Nagarjuna University

Lesson : 5 CLASSICAL ISOMORPHISM THEOREMS - 1

5.1 Introduction : In this lesson we introduce some important types of modules namely Artinian and Noetherian modules. An important characterization of Noetherian module is proved.

5.2 Theorem : If ϕ is a homomorphism of an R - module A into an R - module B, then $\phi(A) \cong A/\phi^{-1}(0)$ where $\phi(A)$ is the image of ϕ and $\phi^{-1}(0)$ is the kernel of ϕ.

Proof : Define $\psi : A/\phi^{-1}(0) \to \phi(A)$ by $\psi\left(x+\phi^{-1}(0)\right) = \phi(x) \forall x \in A$.

Suppose $\psi\left(x+\phi^{-1}(0)\right) = \psi\left(y+\phi^{-1}(0)\right) \Rightarrow \phi(x) = \phi(y)$

$$\Rightarrow \phi(x-y) = 0$$

$$\Rightarrow x-y \in \phi^{-1}(0)$$

$$\Rightarrow x+\phi^{-1}(0) = y+\phi^{-1}(0)$$

$\therefore \psi$ is one - one.

Let $b \in \phi(A) \Rightarrow b = \phi(x)$ for some $x \in A$.

Now $x+\phi^{-1}(0) \in A/\phi^{-1}(0)$ and $\psi\left(x+\phi^{-1}(0)\right) = \phi(x) = b$

$\therefore \psi$ is onto.

Let $x+\phi^{-1}(0), y+\phi^{-1}(0) \in A/\phi^{-1}(0)$ and $\alpha \in R$.

Now $\psi\left[\left(x+\phi^{-1}(0)\right)+\left(y+\phi^{-1}(0)\right)\right] = \psi\left[(x+y)+\phi^{-1}(0)\right]$

$$= \phi(x+y)$$

$$= \phi(x)+\phi(y)$$

$$= \psi\left(x+\phi^{-1}(0)\right)+\psi\left(y+\phi^{-1}(0)\right)$$

Also $\psi\left(\alpha\left(x+\phi^{-1}(0)\right)\right)=\psi\left(\alpha x+\phi^{-1}(0)\right)=\phi(\alpha x)=\alpha\phi(x)$

$$=\alpha\psi\left(x+\phi^{-1}(0)\right)$$

$\therefore \psi$ is a module homomorphism.

Therefore ψ is a module isomorphism of $A/\phi^{-1}(0)$ on to $\phi(B)$.

Hence $A/\phi^{-1}(0) \cong \phi(A)$

5.3 Theorem : Let C be a submodule of A_R. Every sub-module of A/C has the form B/C where $C \subset B \subset A$ and $A/B \cong \dfrac{(A/C)}{(B/C)}$.

Proof : Let B' be any submodule of the quotient module A/C and Let $\pi : A \to A/C$ be the canonical epimorphism of A onto $A/C \Rightarrow \pi^{-1}(B')$ is a sub-module of A. Put $B=\pi^{-1}(B')$. Since $\pi^{-1}(0) \subseteq \pi^{-1}(B')$ where $C \subseteq \pi^{-1}(B')=B \Rightarrow C \subset B$ and $\pi(B)=B' \Rightarrow B/C=B'$.

Thus we have B/C is asub-module of A/C.

Let $\pi' : A/C \to \dfrac{(A/C)}{(B/C)}$ be the canonical epimorphism of A/C onto $\dfrac{(A/C)}{(B/C)}$

$\Rightarrow \pi' 0 \pi$ is an epimorphism of A onto $\dfrac{(A/C)}{(B/C)}$

Now $Ker(\pi' 0 \pi)=(\pi' 0 \pi)^{-1}(0)=\pi^{-1}\left(\pi'^{-1}(0)\right) \quad =\pi^{-1}\left(B/C\right)$

$$=\pi^{-1}(B')=B$$

$\therefore$ By the above theorem $A/B \cong \dfrac{(A/C)}{(B/C)}$

5.4 Theorem : If B and C are sub-modules of A, then $\dfrac{B+C}{B} \cong \dfrac{C}{B \cap C}$.

Proof : We have that $B+C$ is again an R - module and B is a submodule of $B+C$.

Let $\pi : B+C \to \dfrac{B+C}{B}$ be the canonical epimorphism.

Let $K : C \to B+C$ be the canonical monomorphism defined by $k(x) = x$.

For every $x \in C \Rightarrow \pi o k$ is a module homomorphism of C into $\dfrac{B+C}{B}$.

Put $\phi = \pi o k$. Now $x \in \ker \phi \Leftrightarrow \phi(x) = 0$ and $x \in C$

$\Leftrightarrow \pi o k(x) = 0$ and $x \in C$

$\Leftrightarrow \pi(x) = 0$ and $x \in C$

$\Leftrightarrow x + B = B$ and $x \in C$

$\Leftrightarrow x \in B$ and $x \in C$

$\Leftrightarrow x \in B \cap C$

$\therefore \ker \phi = B \cap C$

Further $\phi(C) = \pi o k(C) = \pi(C) = \pi(B) + \pi(C)$

$= \pi(B+C)$

$= B+C/B$

But we have $\dfrac{C}{\phi^{-1}(0)} \cong \phi(C) \to \dfrac{C}{B \cap C} \cong \dfrac{B+C}{B}$

5.5 Lemma (Zasson Laws) : If $B' \subset B \subset A$ and $C' \subseteq C \subseteq A$ are modules over R, then

$$\frac{B'+B\cap C}{B'+B\cap C'} \cong \frac{C'+B\cap C}{C'+C\cap B'}.$$

Proof : Now we show that both the R.H.S. and L.H.S. are isomorphic to $\dfrac{B\cap C}{(B'\cap C+B\cap C')}$.

Put $B_1 = B' + (B \cap C')$

$B_2 = B \cap C$.

By the above theorem we have $\dfrac{B_1+B_2}{B_1} \cong \dfrac{B_2}{B_1 \cap B_2}$

But $B_1 + B_2 = B' + (B\cap C') + (B \cap C)$

$= B' + (B\cap C)$ $(\because B\cap C' \subset B \cap C)$

Also $B_1 \cap B_2 = \left[B' + (B\cap C')\right] \cap (B \cap C)$

$= (B\cap C') + \left[B' \cap (B\cap C)\right]$ (By modular law since $B\cap C' \subset B \cap C$ and B' is any module)

$= (B\cap C') + (B' \cap C)$

Thus we have $\dfrac{B'+(B\cap C)}{B'+(B\cap C')} \cong \dfrac{B\cap C}{(B\cap C')+(B'\cap C)}$

Similarly, we have $\dfrac{C'+(B\cap C)}{C'+(B'\cap C)} \cong \dfrac{B\cap C}{(B\cap C')+(B'\cap C)}$

Therefore we have $\dfrac{B'+(B\cap C)}{B'+(B\cap C')} \cong \dfrac{C'+(B\cap C)}{C'+(B'\cap C)}$

5.6 Definition : A sequence of submodules $A_0 \subset A_1 \subset \ldots\ldots \subset A_m = A$ of A where each A_i is a submodule of A_{i+1} for $i = 0, 1, 2, \ldots\ldots, m-1$, is called a chain of submodules of A_R and m is called the length of the chain and $\dfrac{A_{i+1}}{A_i}$ for $i = 0, 1, 2, \ldots\ldots m-1$ are called the factors of the chain

5.7 Definition : A chain of submodules of A given by $A_0 \subset A_1 \subset .... \subset A_m = A$ is called a refinement of the chain $B_0 \subset B_1 \subset .... \subset B_n = A$ of submodules of A if $\{B_0, B_1, ... B_n\} \subseteq \{A_0, A_1, A_2 ....., A_m\}$. In particular if $\{B_0, B_1, ..., B_n\}$ is a proper subset of $\{A_0, A_1, ... A_m\}$, then we say that chain $A_0 \subset A_1 \subset .... \subset A_m = A$ is a proper refinement of the chain $B_0 \subset B_1 \subset ...... \subset B_n = A$.

5.8 Theorem : Given two chains of submodules of A_R

$B = A_0 \subset A_1 C ...... \subset A_m = A$ and $B = B_0 \subset B_1 \subset .... \subset B_n = A$, then both the chains can be refined. So that the resulting refinements have the same length and the factors of the refinements are isomorphic in some or other order.

Proof : For $i = 0, 1, 2, ..., m-1$, we introduce the chain of submodules $A_{i_0} \subset A_{i_1} \subset A_{i_2} \subset ..... \subset A_{i_n}$ between A_i and A_{i+1} such that $A_i = A_{i_0}$ and $A_{i_n} = A_{i+1}$.

For $j = 0, 1, 2, ..., n-1$, we introduce the chain of submodules, $B_{0_j} \subset B_{1_j} \subset B_{2_j} \subset .... \subset B_{m_j}$ between B_j and B_{j+1} such that $B_j = B_{0_j}$ and $B_{m_j} = B_{j+1}$ as follows.

For any $i = 0, 1, 2, ... m-1$, and $j = 0, 1, 2, ... n$ we define $A_{i_j} = A_i + (A_{i+1} \cap B_j)$

For any $i = 0, 1, 2, ..., m$ and $j = 0, 1, 2, ..., n$, we define $B_{i_j} = B_j + (B_{j+1} \cap A_i)$

Thus we have the following chains

$$B = A_0 = A_{0_0} \subset A_{0_1} \subset .... \subset A_{0_n} = A_1 = A_{1_0} \subset A_{1_1} \subset .... \subset A_{1_n}$$

$$= A_{2_0} \subset ..... \subset A_{m-2_n} = A_{m-1} = A_{m-1_0} \subset A_{m-1_1} .... = A_m$$

and

$$B = B_0 = B_{0_0} \subset B_{1_0} \subset .... \subset B_{m_0} = B_1 = B_{0_1} \subset B_{1_1} \subset .... \subset B_{m_1}$$

$$= B_{0_2} \subset ..... \subset B_{m_{n-2}} = B_{n-1} = B_{0_{n-1}} \subset B_{1_{n-1}} .... = B_n$$

The above two chains are refinements of $B = A_0 \subset A_1 \subset .... \subset A_m = A$ and $B = B_0 \subset B_1 \subset ..... \subset B_n = A$ respectively and lengths of these two refinements are same each of which is equal to 'mn'.

Further for any fixed 'i', $0 \leq i \leq m-1$ and for $j = 0, 1, 2, ... n$ we have $A_i \subset A_{i+1}$ and

$B_{j-1} \subset B_j$. By Zasson - Laws Lemma, we have

$$\frac{A_i + \left(A_{i+1} \cap B_j\right)}{A_i + A_{i+1} \cap B_{j-1}} \cong \frac{B_{j-1} + B_j \cap A_{i+1}}{B_{j-1} + B_j \cap A_i}$$

$$\Rightarrow \frac{A_{i_j}}{A_{i_{j-1}}} \subseteq \frac{B_{i+1_{j-1}}}{B_{i_{j-1}}}$$

Similarly for any fixed $j \ni 0 \le j \le n-1$ and for every $i = 0,1,2,\dots m$ we have by using $A_{i-1} \subset A_i$ and $B_j \subset B_{j+1}$.

$$\frac{A_{i-1} + A_i \cap B_{j+1}}{A_{i-1} + A_i \cap B_j} \cong \frac{B_j + \left(B_{j+1} \cap A_i\right)}{B_j + B_{j+1} \cap A_{i-1}}$$

$$\Rightarrow \frac{A_{i-1_{j+1}}}{A_{i-1_j}} \cong \frac{B_{ij}}{B_{i-1_j}}$$

Hence the factors are isomorphic in some or other order.

5.9 Definition : A chain of sub-modules of A which is of the form $0 = A_0 \subset A_1 \subset \dots\dots \subset A_m = A$ where $A_i \ne A_{i+1}$ for $i = 0,1,2,\dots. m-1$ is called a composition series of the module A if it cannot be properly refined i.e., it has no proper refinement.

5.10 (JORDAN HOLDER)

Let $0 = A_0 \subset A_1 \subset \dots \subset A_m = A$ and $0 = B_0 \subset B_1 \subset \dots \subset B_n = A$ be two composition series of A. Then $m = n$ and there exists a permuatation e of the numbers $0,1,2,\dots m-1$ such that

$\frac{A_{i+1}}{A_i} \cong \frac{B_{e(i)+1}}{B_{e(i)}}$ for $i = 0,1,2,\dots. m-1$.

Proof : By Schreier's theorem, the given two chains can be refined such that the resulting refinements are of same length and the factors of the refinements are isomorphic in some or other order. Since both of the given chains are composition series of A, they cannot be properly refined. Hence any refinements of the given chains are themselves. Hence they must have same lengths and the factors of them are isomorphic in some or other order $\Rightarrow m = n$ and there is a permutation e on the set $\{0,1,2,....m-1\}$ such that $\frac{A_{i+1}}{A_i} \cong \frac{B_{e(i)+1}}{B_{e(i)}}$

5.11 Definition : A module 'A' is said to be Artinian if every non-empty set of submodules has a minimal element.

5.12 Remark : A module A is Artinian iff every descending sequence of submodules becomes ultimately stationary.

Proof : Assume that A is Artinian. Suppose $A_1 \supseteq A_2 \supseteq .....$ be a descending sequence of submodules of A.

Put $\mathcal{A}=\{A_i / i \in N\}$. Now $\mathcal{A}$ is a non-empty set of submodules. Since A is Artinian, $\mathcal{A}$ has a minimal element say $A_{n_0} \Rightarrow A_{n_0} \subseteq A_i \ \forall i$. But $A_n \subseteq A_{n_0}$ for $n \geq n_0 \Rightarrow A_n = A_{n_0}$ for $n \geq n_0$. Thus the sequence is stationary from $n = n_0$. Conversely suppose that every descending sequence of submodules becomes ultimately stationary. Let $\mathcal{A}$ be any non-empty set of submodules of A. Suppose $\mathcal{A}$ has no minimal element. Choose an element A_1 in $\mathcal{A}$. Since A_1 is not a minimal element, $\exists$ an element $A_2 \ni A_1 \supseteq A_2$ and $A_1 \neq A_2$. Again since A_2 is not minimal, $\exists$ an element $A_3 \ni A_2 \supseteq A_3$ and $A_2 \neq A_3$. Continuing this process we get a descending sequence of submodules of A given by $A_1 \underset{\neq}{\supset} A_2 \underset{\neq}{\supset} A_2 \underset{\neq}{\supset} ....$ which is not ultimately stationary which is a contradiction. Hence '$\mathcal{A}$' has a minimal element therefore A is Artinian.

5.13 Definition : A module A is said to be Noetherian if every non-empty set of submodules has a maximal element.

5.14 Remark : A module A is Noetherian iff every ascending sequence of submodules of A is ultimately stationary.

5.15 Theorem : A module is Noetherian iff every submodule is finitely generated.

Proof : Suppose A module A is Noetherian. Let 'B' be any sub-module of A. Let $\Im$ be the set of all finitely generated submodules of B. Since A is Noetherian, $\Im$ has a maximal element say C. Suppose if possible $C \neq B \Rightarrow \exists$ an element $b \in B$ such that $b \notin C$. Put $C_1 = C + bR$. Now C_1 is also finitely generated submodules if B [C_1 is generated by the set of generaters of C together with b]. Hence $C_1 \in \Im$. Also C_1 contains C. Since C is maximal in $\Im$, We have $C_1 = C \Rightarrow b \subset C$ which is a contradiction. Hence $C = B$. Therefore, B is finitely generated.

Conversly suppose that every submodule of A is finitely generated. Let $A_1 \subseteq A_2 \subseteq ....$ be an ascending sequence of submodules of A. Put $B = \bigcup A_i$. Clearly B is a submodule of A. By hypothesis B is finitely generated. Suppose B is generated by $\{b_1, b_2, \ldots. b_k\} \Rightarrow b_1, b_2, \ldots b_k$ are all in $\bigcup A_i \Rightarrow \exists A_{n_o}$ which contains all the b_i's for $i = 1, 2, \ldots, k \Rightarrow B \subseteq A_{n_0}$. But $A_{n_0} \subseteq B$. Thus we have $A_{n_0} = B \Rightarrow$ for $n \geq n_0$, $A_n = A_{n_0}$. Hence the given ascending sequence of submodules of A is ultimately stationary. Therefore A is Noetherian.

5.16 Let B be a sub-module of A_R. Then A is Artinian (Noetherian) if and only if B and A/B are Artinian (Noetherian).

Proof : Assume that A is Artinian

Let $B_1 \supseteq B_2 \supseteq \ldots$ be a descending sequence of submodules of $B \Rightarrow$ This is a descending sequence of submodules of A. Since A is Artinian, the given sequence is ultimately stationary. Hence B is Artinian.

Let $C_1 \supseteq C_2 \supseteq \ldots$ be a descending sequence of submodules of A/B. Since C_i is a sub-module of A/B, we have $C_i = {A_i}/{B}$ for some same sub-module A_i of A containing B. This is true for every $i \Rightarrow \exists$ a sequence $\{A_n\}$ of sub-module of A each of them containing B such that $C_i = {A_i}/{B}\ \forall i \Rightarrow {A_1}/{B} \supseteq {A_2}/{B} \supseteq \ldots$ is an ascending sequence of submodules of A/B $\Rightarrow A_1 \supseteq A_2 \supseteq A_3 \supseteq \ldots$ is an ascending sequence of submodules of A. Since A is Noetherian, we have that there exists a positive integer n_0 $\ni$ for $n \geq n_0$, $A_n = A_{n_0}$.

$\Rightarrow {A_n}/{B} = {A_{n_0}}/{B}\ \forall n \geq n_0 \Rightarrow C_n = C_{n_0}\ \forall n \geq n_0$. Hence the given descending sequence of submodules of A/B is ultimately stationary. $\therefore$ A/B is Noetherian. Conversely for every submodule B of A, B and A/B are Artinian. Let $A_1 \supseteq A_2 \supseteq A_3 \supseteq \ldots$ be any descending sequence of submodules $\Rightarrow A_1 \cap B \supseteq A_2 \cap B \supseteq A_3 \cap B \supseteq \ldots$ is a descending sequence of submodules of B. Since B is Artinian, $\exists$ a positive integer $N_1 \ni n \geq N_1 \Rightarrow A_n \cap B = A_{n_1} \cap B$. (Since B is Artinian, $\exists$).

Since $A_i \supseteq A_{i+1}\ \forall i$ we have $A_i + B \supseteq \dfrac{A_{i+1}}{B}\ \forall i \Rightarrow \dfrac{A_i + B}{B} \supseteq \dfrac{A_{i+1} + B}{B}\ \forall i$ and $\dfrac{A_i + B}{B}$ is a submoduleof $\dfrac{A}{B}\ \forall i \Rightarrow \dfrac{A_1 + B}{B} \supseteq \dfrac{A_2 + B}{B} \supseteq \ldots$ is a descending sequence of submodules of A/B.

Since A/B is Noetherian, $\exists$ a positive integer $N_2 \ni$ for $n \geq N_2$, $\frac{A_n + B}{B} = \frac{A_{N_2} + B}{B}$. Let $N = \max\{N_1, N_2\} \Rightarrow$ for $n \geq N$, where $A_n \cap B = A_N \cap B$ and $\frac{A_n + B}{B} = \frac{A_N + B}{B}$.

Now for any $n \geq N$,

$$A_n = A_n \cap (A_n + B) = A_n \cap (A_N + B) = A_n + (B \cap A_n) = A_N + (B \cap A_N) = A_N$$

$\therefore$ The given descending sequence of submodules of A is ultimately stationary. Hence A is Artinian.

5.17 Corollary : A finite direct product of modules is Artinian (Noetherian) if and only if each factor is Artinian (Noetherian).

Proof : It is enough to prove this corrolary in the case of direct product of two modules.

Suppose $A = B \times C$ is the direct product of two modules B and C. Assume that 'A' is Artinian we have $O \times C$ is a submodule of $A = B \times C$ and $\frac{A}{O \times C} \cong B$ and also $O \times C \cong C$.

Since A is Artinian, $O \times C$ is Artinian and $\frac{A}{O \times C}$ is Artinian $\Rightarrow B$ and C are Artinian.

Conversely assume that B and C are Artinian $\Rightarrow O \times C$ is Artinian $(\because O \times C \cong C)$.

Since $\frac{A}{O \times C} \cong B$ and B is Artinian. We have $\frac{A}{O \times C}$ is Artinian. Thus $O \times C$ is a submodule of A such that $\frac{A}{O \times C}$ and $O \times C$ are Artinian $\Rightarrow A$ is Artinian.

Prof. G. Koteswara Rao
Department of Mathematics
Acharya Nagarjuna University

Lesson : 6 CLASSICAL ISOMORPHISM THEOREMS - 2

6.1 Introduction : In this lesson a famous Lemma known as Fittings Lemma is proved and a famous theorem which is proved by great mathematicians Krull, Remak, Schmidt, and Wedderburn is given.

6.2 Theorem : A module A has a composition series if and only if it is Artinian and Noetherian.

Proof : Assume that A has a composition series of length 'n'. Let $A_1 \supseteq A_2 \supseteq .....\supseteq A_n ....$ be a descending sequence of submodules of A. Suppose if possible this sequence is not ultimately stationary $\Rightarrow \exists n+1$ submodules $A_1, A_2 ....A_{n+1}$ such that $A_i \neq A_{i+1}$ and $A_1 \supseteq A_2 \supseteq A_3 \supseteq ....\supseteq A_{n+1}$

$\Rightarrow 0 = A_{n+1} \subseteq A_n \subseteq .... \subseteq A_1 \subseteq A_0 = A$ is a chain of length more than 'n'. Since the length of a composition series is n, we cannot have a chain of length more than n. Hence the given descending sequence is ultimately stationary.

Similarly if $A_1 \subseteq A_2 \subseteq ....\subseteq A_n \subseteq ......$ is an ascending chain of submodules which is not ultimatley stationary, we can get a chain of submodules of length more than 'n', which is also not possible. Hence every ascending sequence of submodules of A is also ultimately stationary. Therefore A is Artinian and Noetherian. Conversely suppose that A is Artinian and Noetherian. Since A is Artinian, $\exists$ a minimal submodule $A_1 \neq 0$ Again if we consider the set of all submodules of A which contains A_1 properly, it contain a minimal element say A_2. Continuing this process, we get an ascending sequence of submodules of A, such that

$(0) = A_0 \subseteq A_1 \subseteq ....$ and for each i, A_{i+1} is a minimal element among the sub modules of A containing A_i properly $\Rightarrow$ for each i there cannot be any submodule $B \ni A_i \underset{\neq}{\subset} B \underset{\neq}{\subset} A_{i+1}$.

Since A is Noetherian. This sequence is ultimately stationary say from A_N. $\Rightarrow$ There is no submodule of A containing A_N properly. $\Rightarrow A_n = A$ for $n \geq N$. Hence $(0) = A_0 \subset A_1 \subset ......\subseteq A_N = A$ is a composition series of A. Therefore A has a composition series.

6.3 Theorem : An endomorphism of an Artinian (Noetherian) module is an automorphism if and only if it is mono (epi).

Proof : Let f be an endomorphism of an Artinian module A. If f is an automorphism, then clearly it is mono. Conversely suppose that f is mono. Now $f(A)$ is a submodule of A and $f^2(A)$ is a submodule of $f(A)$, etc.....Hence $A \supseteq f(A) \supseteq f^2(A) \supseteq$......... is a descending sequence of submodules of A. Since A is Artinian, $\exists$ an integer $N \ni$ for $n \geq N$, $f^n(A) = f^N(A)$. In partiicular $f^N(A) = f^{N+1}(A)$.

Let $b \in A \Rightarrow f^N(b) \in f^N(A) = f^{N+1}(A) \Rightarrow f^N(b) = f^{N+1}(a)$ for some $a \in A$. Since f is mono, we have f^N is also mono. $\Rightarrow b = f(a)$. Thus f is onto. Hence f is an automorphism.

Let f be an endomorphims of a Noetherian module A. If f is an autiomorphism, then clearly f is an eepimorphism. Conversely assume that f is an epimorphism. Now $f^{-1}(0)$ is a submodule of A. Also $f^{-2}(0) = f^{-1}\left(f^{-1}(0)\right)$ is a submodule of A containing $f^{-1}(0)\left[x \in f^{-1}(0) \Rightarrow f(x) = 0 \Rightarrow f(f(x)) = 0 \Rightarrow f(x) \in f^{-1}(0) \Rightarrow x \in f^{-1}\left(f^{-1}(0)\right)\right]$.

Continuing this process for every n, we have an ascending sequence of submodules of A given by $0 \subset f^{-1}(0) \subseteq f^{-2}(0) \subseteq f^{-3}(0) \subseteq$.............

Since A is Noetherian, this sequence is ultimately stationary $\Rightarrow \exists$ an integer N such that for $n \geq N$, $f^{-n}(0) = f^{-N}(0)$. In particular $f^{-N}(0) = f^{-(N+1)}(0)$. Suppose $f(a) = 0$ for some $a \in A$. Since f is epimorphism, we have that f^n is also epimorphism

$$\Rightarrow \exists\, b \in B \ni f^N(b) = a \Rightarrow f\left(f^N(b)\right) = f(a) = 0$$

$$\Rightarrow f^{N+1}(b) = 0$$

$$\Rightarrow b \in f^{-(N+1)}(0) = f^{-N}(0) \Rightarrow f^N(b) = 0 \Rightarrow a = 0$$

$\therefore f$ is mono. Hence f is an automorphism.

6.4 Fitting's Lemma : If f is an endomorphism of the Artinian and Noetherian module A_R, then for same $n, A = f^n(A) + f^{-n}(0)$ as a direct sum.

Proof : We know that $f(A)$ is a submodule of A and $f^2(A)$ is a submodule of $f(A)$ etc., Hence we have a descending sequence of submodules of A given by $A \supseteq f(A) \supseteq f^2(A) \supseteq$....... since A is Artinian, $\exists$ a positive integer n such that $f^n(A) = f^{n+1}(A) = f^{2n}(A)$. Since $f^n(A)$ is a submodule of A and since A is Noetherian, we have $f^n(A)$ is a Noetherian module. Now if we restrict the f^n to $f^n(A)$ we get that f^n is endomorphism of $f^n(A)$ which is epimorphism. Hence f^n is an automorphism of $f^n(A)$. Hence f^n is mono $\Rightarrow f^{-n}(0) \cap f^n(A) = 0$.

Let $a \in A \Rightarrow f^n(a) \in f^n(A)$. Since $f^n : f^n(A) \to f^n(A)$ is an epimorphism, $\exists f^n(b) \in f^n(A)$ such that $f^n\left(f^n(b)\right) = f^n(a)$

$$\Rightarrow f^{2n}(b) = f^n(a) \Rightarrow f^n\left(a - f^n(b)\right) = 0$$

$$\Rightarrow a - f^n(b) \in f^{-n}(0) \Rightarrow a \in f^n(A) + f^{-n}(0)$$

$$\therefore A = f^n(A) + f^{-n}(0) \text{ and } f^n(A) \cap f^{-n}(0) = 0$$

Hence A is the direct sum of $f^n(A)$ and $f^{-n}(0)$.

Definition : A non-zero module is called an indecomposable module if it is not isomorphic to 'irect product of non-zero modules. equivalently if it is not the direct sum of non-zero submodules.

orrollary : If A_R is indecomposable, Artinian and Noetherian, then endo-morphism of A_R is nilpotent or an automorphism.

: Let f be an endomorphism of A_R which is indecomposable, Artinian and Noetherian. By 's Lemma, $\exists$ a positive integer 'n' such that A is the direct sum of the submodules, $f^n(A)$ $^{-n}(0)$. Since A is indecomposable, either $f^n(A) = 0$ or $f^{-n}(0) = 0$. If $f^n(A) = 0$ we have $\Rightarrow f$ is nilpotent. If $f^{-n}(0) = 0$ it follows that f^n is mono $\Rightarrow f$ is also automorphism.

eorem : If A_R is indecomposable, Artinian and Noetherian, and $g = f_1 + f_2 + \ldots\ldots + f_n$ is an orphism where $f_i \in Hom_R(A, A)$. Then some f_i is an automorphism.

Proof : First we prove this in the case $n=2$. Suppose 'g' is an automorphism of A which is indecomposable, Artinian and Noetherian and $g=f_1+f_2$ where f_1 and f_2 are endomorphism of A.

Since $g=f_1+f_2$ we have $I=g^{-1}f_1+g^{-1}f_2$. Now $g^{-1}f_1$ is an endomorphism of $A \Rightarrow$ either $g^{-1}f_1$ is nilpotent or an automorphism. If $g^{-1}f_1$ is an automorphism, we have $g\left(g^{-1}f_1\right)=f_1$ is an automorphism. Suppose $g^{-1}f_1$ is nilpotent $\Rightarrow I-g^{-1}f_1$ is an automorphism. [since if 'h' is nilpotent and $h^n=0,\ 1-h$ has inverse $1+h+.....+h^{n-1}$] $\Rightarrow g^{-1}f_2$ is an automorphism $\Rightarrow f_2$ is an automorphism. Suppose $n>2$. i.e., $g=f_1+f_2+......+f_n$ is an automorphism. Assume that the truth of the result for $n-1$. Put $h=f_2+......+f_n$. Now $g=f_1+h$ $\Rightarrow$ either f_1 is an automorphism or h is an automorphism. If f_1 is not an automorphism, then h is an automorphism. By induction hypothesis, same f_i where $2\le i\le n$ is an automorphism. Hence the result.

6.8 Lemma : Let λ be an isomorphism of the Artinian module $A=A_1\times A_2$ onto $B=B_1\times B_2$ such that $\lambda(a_1,0)$ = $(\alpha a_1,\ \beta a_1)$ where α is an isomorphism of A_1 onto B_1 and β is a homomorphism of A_1 into B_2. Then $A_2\cong B_2$.

Proof : Suppose $\beta(A_1)=0 \Rightarrow \lambda(a_1,0)=(\alpha a_1,0)\ \forall a_1\in A_1$.

Now $A_2\cong\dfrac{A}{A_1\times 0}\cong\dfrac{\lambda(A)}{\alpha(A_1)\times 0}=\dfrac{B}{B_1\times 0}\cong B_2$. Suppose $\beta(A_1)\ne 0$. Now we produce an isomorphism μ of A onto B. Such that $\mu(a_1,0)=(\alpha(a_1),0)$ for every $a_1\in A_1$.

Define $\mu: A_1\times A_2\to B_1\times B_2$ as follows. Let $(a_1,\ a_2)$ belongs to $A_1\times A_2$ and Suppose $\lambda(a_1,a_2)=(b_1,b_2)$. Now define $\mu(a_1,a_2)=\left(b_1,b_2-\beta\alpha^{-1}(b_1)\right)$.

For any $a_1\in A_1, \lambda(a_1,0)=(\alpha a_1,\beta a_1)$.

$\therefore \mu(a_1,0)=\left(\alpha a_1,\beta a_1-\beta\alpha^{-1}(\alpha a_1)\right)=(\alpha a_1,0)$

Now we show that μ is one - one. Suppose $\mu(a_1,a_2)=(0,0)$. Supppose

$\lambda(a_1,a_2) = (b_1,b_2) \Rightarrow \mu(a_1,a_2) = \left(b_1,\ b_2 - \beta\alpha^{-1} b_1\right) \Rightarrow \left(b_1, b_2 - \beta\alpha^{-1}(b_1)\right) = 0 \Rightarrow b_1 = 0$ and $b_2 = 0$

$\Rightarrow \lambda(a_1, a_2) = (0,0)$. Since λ is one -one. We have $a_1 = a_2 = 0 \therefore \mu$ is one - one. $\Rightarrow \lambda^{-1}\mu$ is a monomorphism which is an endomorphism of the Artinian module A.

$\Rightarrow \lambda^{-1}\mu$ is an automorphism.

$\Rightarrow \mu$ is an isomorphism.

Thus μ is an isomorphism of $A_1 \times A_2$ onto $B_1 \times B_2$ such that $\mu(a_1,0) = (\alpha a_1, 0)\ \forall\, a_1 \in A_1 \Rightarrow A_2 \cong B_2$

6.9 Theorem : Let the Artinian and Noetherian module $A = A_1 \times A_2 \times ...... \times A_m$ be isomorphic with $A' = A_1' \times A_2' \times .... \times A_n'$ where each A_i and A'_j are indecomposable for $i = 1,2,.....,m$ and $j = 1,2,......n$ then $m = n$ and $A_i \cong A'_j$ after some renumbering.

Proof : Let $\lambda : A \longrightarrow A'$ be the given isomorphism. Let K_i, K'_j and π_i, π'_j be canonical monomorphism and epimorphisms respectively for $i = 1, 2, ..., m$ and $j = 1, 2, ..., n$ associated with the corresponding products. Put $\alpha_i = \pi_1' \, 0\, \lambda \, 0\, K_i$ and $\beta_i = \pi_i \, 0\, \lambda^{-1} \, 0\, K_1'$ for $i = 1, 2, ..., m$ and $j = 1, 2, ..., n$

we know that $\sum_{i=1}^{m} K_i \, 0\, \pi_i$ is the identity mapping on A. $\Rightarrow \sum_{i=1}^{m} \alpha_i \, 0\, \beta_i$ is the identity mapping of A_1'. Since A' is Artinian and Noetherian, we have A_1' is also Artinian and Noetherian. $\Rightarrow A_1'$ is an indecomposable, Artinian and Noetherian module such that $\sum_{i=1}^{m} \alpha_i \, 0\, \beta_i$ is an automorphism of $A_1' \Rightarrow$ Atleast one $\alpha_i \, 0\, \beta_i$ say $\alpha_1 \, 0\, \beta_1$ is an automorphism of A_1'.

$\Rightarrow \beta_1 \ 0\ \alpha_1$ is not nilpotent (if $\beta_1 \, 0\, \alpha_1$ is nilpotent where $(\beta_1 \, 0\, \alpha_1)^n = 0$)

$\Rightarrow \alpha_1 \, 0 (\beta \, 0\, \alpha_1)^n = 0 \Rightarrow (\alpha_1 \, 0\, \beta_1)^{n+1} = 0$ which cannot happen since $\alpha_1 \, 0\, \beta_1$ is an automorphism.

$\therefore \beta_1 0 \alpha_1$ is an endomorphism of the Artinian, Noetherian and indecompsable module A_1 and $\beta_1 0 \alpha_1$ is not nilotent $\Rightarrow \beta_1 0 \alpha_1$ is an automorphism.

$\therefore \alpha_1$ is an isomorphism of A_1 onto A_1'.

Further $\lambda(a_1, 0, 0, \ldots\ldots 0) = (\lambda 0 K_1(a_1))$

$\Rightarrow \pi_1'(\lambda(a_1, 0, \ldots\ldots\ldots\ldots, 0)) = \pi_1' \, 0 \, \lambda 0 K_1(a_1) = \alpha_1(a_1)$.

Hence $\lambda(a_1, 0, 0, \ldots\ldots. 0) = (\alpha_1(a_1), *, *, \ldots\ldots\ldots *)$ where α_1 is an isomorphism of A_1 onto A_1'. Therefore by the above Lemma $A_2 \times \ldots\ldots\ldots \times A_m \cong A_1' \times \ldots\ldots\ldots \times A_n'$.

Assume that $n \geq m$. We repeat this process until A_m is left on one side. Since A_m is indecomposable, there cannot be more than one on the right-side.

Hence $n = m$ and $A_m \cong A_n'$.

6.10 Theorem : The central idempotents of a ring R form a Boolean Algebra $B(R)$.

Proof : Let $B(R)$ be the set of all central idempotents of R. Clearly $0 \in B(R)$. Suppose $e \in B(R)$ Put $e' = 1 - e$. Now $(e')^2 = (1-e)(1-e) = (1-e) = e'$ and for any $r \in R$,

$$e'r = (1-e)r = r - er = r - re = r(1-e) = re'$$

$\therefore e'$ is also a central idempotent of R. Hence $e' \in B(R)$.

Suppose e and f are in $B(R) \Rightarrow e f \in B(R)$

Further for any e_1, e_2, e_3 in $B(R)$, $(e_1 \cdot e_2)e_3 = e_1(e_2 \cdot e_3)$. $\therefore (B(R), .)$ is a semigroup which satisfy idempotent law and commutative laws.

$\therefore (B(R), \bullet)$ is a semi-lattice. Now $0 \in B(R)$ and ' is a unary operation on $B(R)$. For any $e, f \in B(R)$, $ef' = 0$ iff $e(1-f) = 0$ iff $ef = e$.

$\therefore (B(R), 0, ', \bullet)$ is a Bolean Algebra.

6.11 Definition : A minimal non-zero element of a Boolean Algebra is called an 'atom'.

6.12 Lemma : If e is a central idempotent in R then eR is indecomposable if and only if e is an atom of $B(R)$.

Proof : Suppose eR is indecomposable. Suppose if possible e is not an atom of $B(R)$.

$\Rightarrow$ there exists a non-zero element f in $B(R) \ni f < e$.

$\Rightarrow e = f + (e-f)$ where f and $(e-f)$ are orthogonal non-zero idempotents.

$\Rightarrow eR = fR + (e-f)R$ is a direct sum of ideal which are non-zero.

$\Rightarrow$ eR is not indecomposable. Which is a contradiction.

$\therefore e$ is an atom of $B(R)$.

Conversely suppose that e is an atom. Suppose if possible eR is decomposable.

$\Rightarrow eR$ is the direct sum of non-zero ideals.

Suppose $eR = A \oplus B$ where A and B are ideals of R.

Since $e \in eR$, $e = f + g$ for some unique $f \in A$ and $g \in B$.

Since $fg \in A \cap B = 0$ we have f and g are orthogonal.

$$e = e^2 = f^2 + g^2 \Rightarrow f^2 + g^2 = f + g$$

$$\Rightarrow f^2 - f = g^2 - g \in A \cap B = 0$$

$$\Rightarrow f^2 = f \text{ and } g^2 = g$$

Also for any $r \in R$, $er = fr + gr$ and $re = rf + rg$

But $er = re \Rightarrow fr = rf$ and $gr = rg$.

$\therefore f$ and g are orthogonal central idempotents of R. Since $ef = f$ where $f < e$ and since $eg = g$ we have $g < e$. Hence e is not an atom, which is a contradiction. $\therefore eR$ is indecomposable.

6.13 Theorem : If R is a direct sum of indecomposable ideals, then there are the only indecomposable direct summands of R

Proof : Suppose R is the direct sum of ideals $K_1, K_2, \ldots\ldots, K_n$ of R which are indecomposable. $\Rightarrow$ there exists central orthogonal idempotents $e_1, e_2, \ldots\ldots\ldots, e_n$ in R such that $e_1 + e_2 + \ldots\ldots\ldots + e_n = 1$ and $K_i = e_i R$ for $i = 1, 2, \ldots\ldots, n$; so that $R = e_1 R + \ldots\ldots + e_n R$. Since each $e_i R$ is indecomposable, we have that each e_i is an atom of $B(R)$. Suppose if possible e is another atom of $B(R)$ such that $e \neq e_i$ for $i = 1, 2, \ldots. n$.

$$\Rightarrow e = e \cdot 1 = \sum_{i=1}^{n} e e_i = 0$$

$\therefore$ The only atoms of $B(R)$ are $e_1, e_2 \ldots\ldots\ldots e_n$

$\Rightarrow e_1 R, e_2 R, \ldots\ldots\ldots e_n R$ are the only indecomposable direct summands of R.

Prof. G. Koteswara Rao
Department of Mathematics
Acharya Nagarjuna University

Lesson : 7 SELECTED TOPICS ON COMMUTATIVE RINGS

7.0 Introduction : In this lesson, the radical and prime radical of a commulative ring are defined and characterised. The famous Birchoff's theorem is also proved.

7.1 Definition : An element r of a ring R is called a unit, if $\exists$ an element

$$s \in R \ni rs = sr = 1$$

7.2 Definition : An element r of a ring R is called a zero-divisor if $\exists$ an element $s \neq 0 \ni$ either $rs = 0$ or $sr = 0$.

Remark : A unit is not a zero-divisor.

Proof : Let r be a unit $\Rightarrow \exists$ an element $s \in R \ni rs = sr = 1$

Suppose if possible r is a zero-divisior $\Rightarrow \exists$ an element $t \neq 0 \ni$ either $rt = 0$ or $tr = 0$.

Suppose $rt = 0$

Now $t = 1.t = (sr)t = s.0 = 0$, a contradiction. $\therefore r$ is not a zero-divisor.

7.3 Definition : A commutative ring is called a field if $0 \neq 1$ and every non-zero element is a unit.

7.4 : A commutative ring is called an integral domain if $0 \neq 1$ and 0 is the only zero-divisor.

7.5 Lemma : An element of a commutative ring is a unit if and only if it lies in no proper ideal and this is true if and only if it lies in no maximal ideal.

Proof : Let r be any element of a commutative ring R.

Suppose r is a unit $\Rightarrow \exists$ an element $s \in R \ni rs = 1$. If A is an ideal containing r, then $rs \in A \Rightarrow 1 \in A$. Hence $A = R$. Thus r lies in no proper ideal.

Conversely suppose that r lies in no proper ideal of R. Since rR is an ideal of R and $r \in rR$, we must have rR is not proper $\Rightarrow rR = R$.

$$\Rightarrow rs = 1 \text{ for some } s \in R \Rightarrow r \text{ is a unit.}$$

Suppose r does not lie in any proper ideal of R. Since every maximal ideal is also a proper ideal, it follows that r does not lie in any maximal ideal.

Conversely suppose that r does not lie in any maximal ideal since any proper ideal is contained in a maximal ideal, it follows that r does not lie in any proper ideal.

7.6 Definition : A proper ideal P in a ring is called a prime ideal if for any two ideals A and B, $ABCP$ implies either $A \subseteq P$ or $B \subseteq P$

7.7 Theorem : The proper ideal M of the commutative ring R is maximal if and only if for every $r \notin M, \exists x \in R \ni 1 - rx \in M$.

Proof : Suppose M is a maximal ideal of R. Let $r \notin M$. Now $M + rR$ is an ideal containing M properly. (Since $r \in M + rR$ and $r \notin M$)

Since M is a maximal ideal we must have that $M + rR = R$.

$\Rightarrow 1 \in M + rR \Rightarrow 1 = m + rx$ for some $x \in R$ and for some $m \in M$.

$\Rightarrow 1 - rx \in M$ for some $x \in R$.

Conversely suppose that for every $r \notin M, \exists$ an element $x \in R \ni 1 - rx \in M$

Suppose M_1 is any ideal containing M properly $\Rightarrow \exists r \in M_1$ and $r \notin M$.

$\Rightarrow \exists$ an $x \in R \ni 1 - rx \in M \Rightarrow 1 - rx \in M_1$. But $r \in M_1 \Rightarrow rx \in M_1 \Rightarrow 1 \in M_1$.

Hence $M_1 = R$.

Therefore M is a maximal ideal of R.

7.8 Theorem : The proper ideal P of the commutative ring R is prime if and only if for all elements a and b, $ab \in P$ implies $a \in P$ or $b \subset P$.

Proof : Suppose that P is prime. Suppose $ab \in P$ where a and b are elements of $R \Rightarrow (aR)(bR) \subseteq (ab) R \subseteq P$

Now aR and bR are ideals of R and P is prime $\Rightarrow$ either $aR \subseteq P$ or $bR \subseteq P$. If $aR \subseteq P$, then $a \in P$. If $bR \subseteq P$ then $b \in P$. Hence $a \in P$ or $b \in P$.

Conversely suppose that $ab \in P$ implies either $a \in P$ or $b \in P$.

Suppose A and B are ideals of R $AB \subseteq P$. Suppose $A \not\subseteq P$

$\Rightarrow \exists$ an element $a \in A \ni a \notin P$. Let b' be any element of B.

$\Rightarrow ab \in AB \subseteq P$. By hypothesis either $a \in P$ or $b \in P$. But $a \notin P$.

$\Rightarrow b \in P$ This is true for every $b \in B$ Hence $B \subseteq P$ $\therefore$ P is prime.

7.9 Theorem : The ideal M of the commutative ring R is maximal if and only if $\frac{R}{M}$ is a field.

Proof : Suppose M is maximal. Let $r+M$ be a non-zero element of $\frac{R}{M} \Rightarrow r \notin M$.

Since M is maximal, $\exists$ an element $x \in R \ni 1-rx \in M$.

$\Rightarrow 1+M = rx+M = (r+M)(x+M) = (x+M)(r+M)$

Hence $(r+M)$ is a unit in $\frac{R}{M}$. Thus every non-zero element of $\frac{R}{M}$ is a unit $\Rightarrow \frac{R}{M}$ is a field.

Conversly suppose that $\frac{R}{M}$ is a field. Let $r \notin M \Rightarrow r+M$ is a non-zero element of $\frac{R}{M} \Rightarrow r+M$ is a unit in $\frac{R}{M}$.

$\Rightarrow \exists$ en element $x+M$ in $\frac{R}{M} \ni (r+M)(x+M) = 1+M$

$\Rightarrow rx+M = 1+M \Rightarrow 1-rx \in M$ for some $x \in R \Rightarrow M$ is maximal.

7.10 Theorem : The ideal P of a commutative ring R is prime if and only if $\frac{R}{P}$ is an integral domain.

Proof : Suppose P is prime. Suppose $(r+P)(s+P) = P$ in $\frac{R}{P} \Rightarrow rs+P = P$.

$\Rightarrow rs \in P$. Since P is prime, either $r \in P$ or $s \in P$.

$\Rightarrow$ either $r+P = P$ or $s+P = P$. Hence $\frac{R}{P}$ is an integral domain. Conversely suppose that $\frac{R}{P}$ is an integral domain. Let a and b be two elements such that $ab \in P \Rightarrow ab+P = P$ $\Rightarrow (a+P)(b+P) = P$ in $\frac{R}{P}$. Since $\frac{R}{P}$ is an integral domain, we have either $a+P = P$ or $b+P = P \Rightarrow$ either $a \in P$ or $b \in P \Rightarrow P$ is a prime ideal.

Remark : Every field is an integral domain.

Proof : Let R be a field $\Rightarrow R$ is a commutative ring with $1 \neq 0$ in which every non-zero element is a unit. But we know that every unit is not a zero-divisor.

$\Rightarrow$ every non-zero element is not a zero-divisor.

$\Rightarrow$"0" is only the zero-divisor of $R \Rightarrow R$ is an integral domain.

7.11 Theorem : Every maximal ideal of commutative ring is a prime ideal.

Proof : Let M be a maximal ideal of a commutative ring R.

$\Rightarrow \frac{R}{M}$ is a field $\Rightarrow \frac{R}{M}$ is an integral domain $\Rightarrow M$ is a prime ideal.

Remark : A prime ideal need not be a maximal ideal in a commutative ring.

Ex : Let z be the ring of integers. In this commutative ring (0) is a prime ideal but not a maximal ideal.

7.12 Theorem : If the ideal A is contained in the prime ideal B, there exist minimal elements in the set of all prime ideals P such that $A \subseteq P \subseteq B$.

Proof : Let $\Im$ be the set of all prime ideals P such that $A \subseteq P \subseteq B$. Clearly $\Im$ is non-empty since $B \in \Im$. Now $\Im$ is a partially ordered set under set inclusion.

Let $\{P_\alpha\}_{\alpha \in \Delta}$ be any chain of elements in $\Im$. Put $P = \bigcap_{\alpha \in \Delta} P_\alpha$. Now we show that P is a prime ideal. Let $ab \in P \Rightarrow ab \in P_\alpha \ \forall \alpha \in \Delta$. Suppose $a \notin p \Rightarrow \exists \alpha_0 \in \Delta \ni a \notin P_{\alpha_0}$. Now we show that $b \in P$. Let P_β be any element of $\{P_\alpha\}$. Since $\{P_\alpha\}$ is a chain, we have either $P_\beta \subseteq P_{\alpha_0}$ or $P_{\alpha_0} \subseteq P_\beta$.

Suppose $P_\beta \subseteq P_{\alpha_0} \Rightarrow a \notin P_\beta \left(\because a \notin P_{\alpha_0}\right)$. But $ab \in P_\beta$ and P_β is prime.

Hence $b \in P_\beta$.

Suppose $P_{\alpha_0} \subseteq P_\beta$ Since $ab \in P_{\alpha_0}$ and $a \notin P_{\alpha_0}$ we must have $b \in P_{\alpha_0} \Rightarrow b \in P_\beta$. Thus $b \in P_\beta$ for every $\beta \in \Delta \Rightarrow b \in \bigcap_{\alpha \in \Delta} P_\alpha = P$.

$\therefore P$ is prime.

Since $A \subset P_\alpha \subset B \ \forall \alpha \in \Lambda$, we have $A \subseteq \bigcap_{\alpha \in \Delta} P_\alpha \subseteq B \Rightarrow A \subseteq P \subseteq B$.

$\Rightarrow P \in \mathfrak{I}$. Also $P \subseteq P_\alpha \ \forall \alpha \in \Delta$

$\Rightarrow P$ is a lower bound of $\{P_\alpha\}_{\alpha \in \Delta}$

Thus every chain in $\mathfrak{I}$ has a lower bound in $\mathfrak{I}$. Hence by Zorn's lemma $\mathfrak{I}$ has a minimal element.

7.13 Definition : The intersection of all maximal ideals of a commutative ring R is called the radical of R and it is denoted by $Rad\ R$.

7.14 Definition : The intersection of all maximal prime ideals of a ring R is called the prime radical of R and it is denoted by $rad\ R$.

7.15 Theorem : The radical of R consists of all elements $r \in R$ such that $1-rx$ is a unit for all $x \in R$.

Proof : Let $r \in Rad\ R \Rightarrow r \in M$ for every maximal ideal M. Let $x \in R$. $\Rightarrow rx \in M$ for every maximal ideal $M \Rightarrow 1-rx \notin M$ for every maximal ideal $M \Rightarrow 1-rx$ is a unit.

(If $1-rx$ is not a unit, then the ideal generated by $1-rx$ is a proper ideal and which is contained in a maximal ideal say M, $\Rightarrow 1-rx \in M_1$.)

Thus $1-rx$ is a unit $\forall x \in R$.

Conversely let r be any element of $R \ni 1-rx$ is a unit $\forall x \in R$.

$\Rightarrow 1-rx \notin M$ for every maximal ideal $\forall x \in R \Rightarrow r \in M$ for every maximal ideal $\Rightarrow r \in Rad\ R$.

$\therefore Rad\ R = \{r / 1-rx \text{ is a unit } \forall x \in R\}$

7.16 Definition : An element $r \in R$ is called nilpotent if $r^n = 0$ for some natural number n.

7.17 Theorem : The prime radical of a commutative ring R consists of all nilpotent elements of R.

Proof : Let r be any nilpotent element and suppose $r^n = 0$. Let P be any prime ideal of $R \Rightarrow r^n \in P \Rightarrow r.\, r^{n-1} \in P \Rightarrow$ either $r \in P$ or $r^{n-1} \in P$. Continuing this process we get that $r \in P$ This is true for every prime ideal P. Hence $r \in rad\ R$.

Conversely suppose that $r \in rad\ R$. Suppose if possible $r^n \neq 0$ for every positive integer n, put $T = \{1, r, r^2, r^3, ...\}$ clearly $0 \notin T$. Let P be an ideal of R which is maximal with respect to the property that it does not meet T.

Suppose $a \notin P$ and $b \notin P \Rightarrow P+aR$ and $P+bR$ are ideals which contain P properly

$\Rightarrow P+aR$ and $P+bR$ meet T.

$\Rightarrow \exists r^m \in (P+aR)\bigcap T$ and $r^n \in (P+bR)\bigcap T$.

$\Rightarrow r^{m+n} = r^m\ r^n \in (P+aR)(P+bR) \subseteq P+abR$

$\Rightarrow P+ab\,R$ meets T.

$\Rightarrow P\ +ab\,R$ must contain P properly.

$\Rightarrow ab \notin P$

Thus $a \notin P$ and $b \notin P \Rightarrow ab \notin P$. $\therefore P$ is prime.

Since P does not meet T we have $r \notin P$. Thus $r \notin rad\ R$ which is a contradiction... r is nilpotent.

Thus $rad\ R = \{\ r / r$ is nilpotent dement of $R\}$.

7.18 Lemma : If T is a subset of a commutative ring which is closed under finite products and does not contain 0, then any ideal which is maximal in the set of ideals not meeting T is a prime ideal.

Proof : Since T is closed under finite products and 1 is treated as an empty product, it follows that $1 \in T$.

Now T has the properties (1) $t_1, t_2 \in T \Rightarrow t_1 t_2 \in T$.

(2) $1 \in T$

(3) $0 \notin T$.

Let $\mathfrak{I}$ be the family ideals A such that A does not meet T. Let M be a maximal element in $\mathfrak{I}$. Now we show that M is prime. Suppose $a \notin M$ and $b \notin M \Rightarrow M+aR$ and $M+bR$ contain M properly.

Hence they meet $T \Rightarrow \exists t_1 \in (M+aR)\bigcap T$ and $t_2 \in (M+bR)\bigcap T$. Now $t_1 t_2 \in (M+aR)(M+bR) \subseteq (M+abR)$ and also $t_1 t_2 \in T$.

$\Rightarrow M+ab\,R$ contains M properly $\Rightarrow ab \notin M$. $\therefore$ M is a prime ideal.

7.19 Definition : A commutative ring R is called semiprimitive if it's radical is 0.

7.20 Definition : A commutative ring R is called semiprime if its prime radical is 0.

Remark : (1) R is semi-primitive - iff for any $r \neq 0, 1-rx$ is not a unit for some $x \in R$.

(2) R is semiprime iff it has no non-zero nilpotent elements.

(3) If R is a commutative ring then rad $R \subseteq Rad\ R$ ($\because$ every maximal ideal is a prime ideal)

7.21 Theorem (1) : If R is a commutative ring, then $\frac{R}{Rad\ R}$ is semiprimitive and $\frac{R}{rad\ R}$ is semi prime.

Proof : Let $\pi : R \to \frac{R}{Rad\ R}$ be the canonical epimorphism. Let $\pi(r)$ be any element in the radical of $\frac{R}{Rad\ R} \Rightarrow$ for any $\pi(x)$ in $\frac{R}{Rad\ R}$, $\pi(1) - \pi(r)\pi(x)$ is a unit $\Rightarrow \pi(1-rx)$ is a unit for every $x \in R$. Let x be any element of $R \Rightarrow \pi(1-rx)$ is a unit $\Rightarrow \exists y \in R \ni \pi(1-rx)\pi(y) = \pi(1)$ $\Rightarrow \pi\left(1-(1-rx)y\right) = 0$

$\Rightarrow 1-(1-rx)y \in Rad\ R \Rightarrow (1-rx)y$ is a unit in $R \Rightarrow 1-rx$ is a unit in R.

$\Rightarrow r \in Rad\ R \Rightarrow \pi(r) = 0$. $\therefore Rad\left(\frac{R}{Rad\ R}\right) = 0 \Rightarrow \frac{R}{Rad\ R}$ is a semiprimitive.

(2) Let $\pi : R \to \frac{R}{rad\ R}$ be the canonical epimorphism.

Suppose $\pi(r)$ be any nilpotent element of $\frac{R}{rad\ R} \Rightarrow (\pi(r))^n = 0$ for some n.

$\Rightarrow \pi\left(r^n\right) = 0 \Rightarrow r^n \in Rad\ R \Rightarrow \left(r^n\right)^k = 0$ for some $K \Rightarrow r^{nk} = 0 \Rightarrow r$ is nilpotent.

$\Rightarrow r \in rad\ R \Rightarrow \pi(r) = 0$ $\therefore rad\left(\frac{R}{rad\ R}\right) = 0 \Rightarrow \frac{R}{rad\ R}$ is semiprime.

7.22 Definition : We say that a ring R is a subdirect product of a family of rings $\{S_i / i \in I\}$ if there is a monomorphism $k:R \to S = \underset{i\in I}{\pi} S_i$ such that for any i, $\pi_i 0 k$ is an epimorphism of R onto S_i where π_i is the canonical epimorphism of πS_i onto S_i.

7.23 Theorem : R is a subdirect product of the rings $\{S_i / i \in I\}$ if and only if $\exists$ a family $\{K_i / i \in I\}$ of ideals of $R \ni S_i \cong \frac{R}{K_i} \forall i$ and $\bigcap K_i = 0$.

Proof : Suppose R is a subdirect product of the rings $\{S_i / i \in I\}$. For each i, let π_i be the canonical epimorphism of πS_i onto S_i. Let k be a monomorphism of R into πS_i such that $\pi_i 0 k$ is an epimorphism of R onto $S_i \forall i$.

Let K_i be the Kernel of $\pi_i 0 k \forall i \Rightarrow \{K_i / i \in I\}$ is a family of ideals of $R \ni \frac{R}{K_i} \cong S_i \forall i$.

Suppose $r \in \bigcap k_i \Rightarrow \pi_i K(r) = 0 \forall i \Rightarrow K(r) = 0$. Since k is mono, we have $r = 0$. Thus we have $\underset{i\in I}{\bigcap} K_i = 0$.

Conversely suppose that $\exists$ a family $\{K_i / i \in I\}$ of ideals $\ni \bigcap K_i = 0$ and $S_i \cong \frac{R}{K_i} \forall i$. Let ψ_i be an isomorphism of S_i onto $\frac{R}{K_i} \forall i$. Define $k: R \to \pi S_i$ by $K(r) = \{\psi_i^{-1} \pi_i(r)\} \forall r \in R$. It can be verified that k is a homomorphism. Suppose $k(r) = 0 \Rightarrow \psi_i^{-1} \pi_i(r) = 0 \ \forall i \Rightarrow \pi_i(r) = 0 \ \forall i$.

$$\Rightarrow r + K_i = K_i \forall i \Rightarrow r \in K_i \forall i \Rightarrow r \in \bigcap K_i = 0$$

$$\Rightarrow r = 0 \therefore k \text{ is a monomorphism.}$$

Further for any i, $\pi_i 0 K(r) = \pi_i\left(\psi_i^{-1} \pi_i(r)\right) = \psi_i^{-1} \pi_i(r)$

$\Rightarrow \pi_i 0 k = \psi_i^{-1} \pi_i \forall i$. Since ψ_i^{-1} and π_i are onto mappings, we have that $\pi_i 0 k$ is an epimorphism $\forall i$.

$\Rightarrow R$ is a subdirect product of the rings $\{S_i / i \in I\}$

7.24 Corollary : A commutative ring is a subdirect product of fields (integral domains) iff it is semiprimitive (semiprime).

Proof : Let R be a commutative ring. Suppose R is a subdirect product of fields $\{F_i / i \in I\} \Rightarrow \exists$ a family $\{K_i / i \in I\}$ of ideals $\ni F_i \cong \dfrac{R}{K_i}\ \forall i$ and $\bigcap K_i = 0$. Since F_i is a field we have that $\dfrac{R}{K_i}$ is a field $\forall i \Rightarrow K_i$ is a maximal ideal for every $i \in I$. Since $\bigcap\limits_{i \in I} K_i = 0$, it follows that the intersection of all maximal ideals is zero $\Rightarrow Rad\ R = 0 \Rightarrow R$ is semiprimitive conversely suppose that R is semiprimitive. Let $\{M_\alpha\}_{\alpha \in \Delta}$ be the family of maximal ideals of R. Since R is semiprimitive, we have $\bigcap\limits_{\alpha \in \Delta} M_\alpha = 0 \Rightarrow R$ is a subdirect product of the rings $\left\{\dfrac{R}{M_\alpha}\right\}_{\alpha \in \Delta}$.

Since each M_α is a maximal ideal, we have that $\dfrac{R}{M_\alpha}$ is a field $\forall \alpha$. $\therefore R$ is a subdirect product of fields.

(2) Suppose R is a subdirect product of integral domain $\{S_i\}_{i \in I} \Rightarrow \exists$ a family $\{K_i / i \in I\}$ of ideals of $R \ni S_i \cong \dfrac{R}{K_i}\ \forall i$ and $\bigcap K_i = 0$. Since S_i is an integral domain we have $\dfrac{R}{K_i}$ is an integral domain $\forall i \Rightarrow K_i$ is a prime ideal $\forall i$.

Since $\bigcap\limits_{i \in I} K_i = 0$, it follows that the intersection of all prime ideals is 0 $\Rightarrow$ rad $R = 0 \Rightarrow R$ is semiprime.

Conversely suppose that R is semiprime. Let $\{P_\alpha / \alpha \in \Delta\}$ be the family of all prime ideals of $R \Rightarrow \bigcap\limits_{\alpha \in \Delta} P_\alpha = 0$ ($\because R$ is semiprime, rad R = 0) $\Rightarrow R$ is a subdirect product of $\left\{R/P_\alpha\right\}_{\alpha \in \Delta}$.

Since each P_α is prime, we have that R/P_α is an integral domain $\forall \alpha$.

7.25 : A commutative ring R is semiprime iff it is isomorphic to a subring of a direct product of integral domains.

Proof : Suppose R is semiprime $\Rightarrow K$ is a subdirect product of a family of integral domains $\{S_i / i \in I\} \Rightarrow \exists a$ monomorphism. $k : R \to \pi S_i \Rightarrow R$ is isomorphic to a subring of πS_i.

Conversely suppose that R is isomorphic to a subring of the direct product of integral domain say $\{R_\alpha\}_{\alpha\in\Delta}$. Now $\underset{\alpha\in\Delta}{\pi} R_\alpha$ is a direct product of integral domain.

$\Rightarrow \underset{\alpha\in\Delta}{\pi} R_\alpha$ is also a subdirect product of integral domains.

$\Rightarrow \underset{\alpha\in\Delta}{\pi} R_\alpha$ is semiprime $\Rightarrow$ Every subring of $\underset{\alpha\in\Delta}{\pi} R_\alpha$ is also semiprime $\Rightarrow R$ is semiprime.

7.26 Corollary : A commutative ring R is semiprime iff it is isomorphic to subring of a direct product of fields

Proof : Suppose R is semiprime $\Rightarrow$ It is isomorphic to subring of direct product of integral domains say $\{R_\alpha\}_{\alpha\in\Delta}$. We know that every integral domain can be embeded in a field. Let F_α be a field $\ni R_\alpha$ is embeded in $F_\alpha\ \forall \alpha$. Now πR_α is a subring of the direct product of fields $\underset{\alpha\in\Delta}{\pi} F_\alpha$.

$\Rightarrow R$ is isomorphic to a subring of πF_α a direct product of fields. Conversely suppose that R is isomorphic to a subring of a direct product πF_α of fields. Since πF_α is a subdirect product of fields and hence integral domains, it follows that πF_α is semiprime $\Rightarrow R$ is semiprime since it is isomorphic to a subring of a semiprime ring.

7.27 Definition : A ring R is called subdirectly irreducible if the intersection of all non-zero ideals is non-zero.

7.28 Theorem : (Brikhoff) Every ring is a subdirect product of subdirectly irreducible rings.

Proof : Let $r \neq 0$ be any non-zero element of R. Let K_r be the ideal which is maximal in the set of all ideals that are contained in $R-\{r\}$. That is K_r is the ideal which is maximal with respect to the property that $r \notin K_r$.

Now consider the family $\{K_r\}_{r\in R^*}$ where R^* is the set of all non-zero elements of R.

Now $\bigcap\limits_{r\in R^*} K_r = 0$ (If $s \neq 0$, then $s \notin K_s$). Hence R is a subdirect product of rings $\{R/K_r\}_{r\in R^*}$.

Now we show that for each $r \in R^*$, $\dfrac{R}{K_r}$ is subdirectly irreducible. Let A/K_r be any non zero ideal of R/K_r $\Rightarrow$ A is an ideal of R containing K_r properly. By the property of K_r, we msut have $r \in A \Rightarrow r + K_r$ is in $\dfrac{A}{K_r}$. Thus every non-zero ideal of $\dfrac{R}{K_r}$ contains the non-zero element $r + K_r$.

Hence the intersection of all non-zero ideals of $\frac{R}{K_r}$ is non-zero. Hence $\frac{R}{K_r}$ is subdirectly irreducible.

Thus R is subdirect product of subdirectly irreducible rings.

7.29 Problem : (1) If r is nilpotent then $1-r$ is a unit.

Proof : Since r is nilpotent, $\exists$ a positive integer $n \ni r^n = 0$. We may assume that n is the least positive integer $\ni r^n = 0$. i.e. $r^{n-1} \neq 0$.

Now $(1-r)\left(1+r+r^2+.......+r^{n-1}\right)=1$. Hence $1-r$ is invertable $\Rightarrow 1-r$ is a unit.

(2) Show that an ideal P of a commutative ring is Prime iff $R-P$ is closed under finite products.

Proof : Suppose P is prime. Let $a_1 \in R-P$ and $a_2 \in R-P \Rightarrow a_1 \notin P$ and $a_2 \notin P$.

Since P is prime we have $a_1 a_2 \notin p \Rightarrow a_1 a_2 \in R-P$

$\Rightarrow a_1 \notin P$ and $a_2 \notin P$

Since P is prime we have $a_1 a_2 \notin P \Rightarrow a_1 a_2 \in R-P$.

Conversely suppose that $R-P$ is closed under products.

Let $ab \in P$. Suppose if possible $a \notin P$ and $b \notin P \Rightarrow ab \notin P$ which is a contradiction.

Therefore $a \in P$ or $b \in P \Rightarrow P$ is prime.

Prof. G. Koteswara Rao
Department of Mathematics
Acharya Nagarjuna University

Lesson : 8 PRIME IDEALS IN SPECIAL COMMUTATIVE RINGS

8.0 Introduction : In this lesson, a special class of commutative rings namely Boolean rings and commutative regular rings are studied.

8.1 Definition : A subset F of a Boolean Algebra $(S,0,',\wedge)$ is called a filter if

(1) $0' \in F$

(2) $a,b \in F \Rightarrow a \wedge b \in F$

(3) $a \in F$ and $a \leq b \Rightarrow b \in F$.

8.2 Definition : A filter F is said to be a proper filter if $0 \notin F$.

8.3 Definition : A maximal proper filter is called an ultrafilter.

Remark : The filters of a Boolean algebra $(S,1,',\vee)$ are called dual filters.

8.4 Theorem : If a Boolean algebra is regarded as a ring, the dual filters are precisely the ideals, hence the dual ultrafilters are precisely the maximal ideals.

Proof : Let K be a dual filter of a Boolean Algebra $(S,1,',\vee)$ since $1' \in K,$ we have $0 \in K$. Let $a \in K$ and $s \in S$. Then $as \leq a \Rightarrow as \in K$. Similarly $sa \in K$. Let $a,b \in K \Rightarrow ab' \in K$ and $ba' \in K$.

$\Rightarrow ab' \vee ba' \in K \Rightarrow a+b \in K$. $\therefore K$ is an ideal.

Conversely suppose that K is an ideal $\Rightarrow 0 \in K \Rightarrow 1' \in K$.

Suppose $a \in K$ and $b \leq a \Rightarrow b = ab \in K$

Suppose $a,b \in K \Rightarrow a \vee b = (a'b')' = ((1-a)(1-b))' = 1-(1-b-a+ab) = b+a-ab \in K$

$\therefore K$ is a dual filter.

Thus the dual filters of S are precisely the ideals of S .

8.5 Theorem : The following statements concerning the Boolean ideal K of a Boolean ring B are equivalent.

(a) K is maximal

(b) K is prime

(c) For every element, s of R, either $s \in K$ or $s' \in K$ but not both.

Proof : Assume (a). Since the Boolean ring is a commutative ring it follows that every maximal ideal is a prime ideal.

Hence $(a) \Rightarrow (b)$

Assume (b). Since K is a proper ideal, we have $1 \notin K$. Let $s \in B$. We have $s + s' = 1 \notin K \Rightarrow$ Both of s and s' cannot be in K.

But $s s' = s(1-s) = s - s^2 = 0 \in K$.

Since K is prime, either $s \in K$ or $s' \in K$. Hence $(b) \Rightarrow (c)$.

Assume (c) Since K is an ideal, we have $0 \in K \Rightarrow 0' \notin K \Rightarrow 1 \notin K$.

$\Rightarrow K$ is a proper ideal.

Let s be any element $\ni s \notin K \Rightarrow s' \in K$

Now $1 = s' + s \in K + sB \Rightarrow 1 - sx \in K$ for some $x \in B$

$\therefore K$ is a maximal ideal.

Hence $(c) \Rightarrow (a)$

8.6 Corollary : The following statements concerning the Boolean ring S are equivalent.

(a) S is a field

(b) S is an integral domain

(c) S has exactly two elements.

Proof : Let $K = (0)$ be the zero ideal of S which is a Boolean ideal. Assume (a) $\Rightarrow S$ is a field $\Rightarrow \frac{S}{K}$ is a field $\Rightarrow K$ is a maximal ideal $\Rightarrow K$ is a prime ideal $\Rightarrow \frac{S}{K}$ is an integral domain $\Rightarrow S$ is an integral domain. Hence $(a) \Rightarrow (b)$.

Assume $(b) \Rightarrow \frac{S}{K}$ is an integral domain $\Rightarrow K$ is prime.

$\Rightarrow$ For any $s \in S$, either $s \in K$ or $s' \in K$ but not both.

Since $s.s' = 0 \in K$ and K is prime, either s = 0 or $s' = 0$.

$\Rightarrow$ Either $s = 0$ or $s = 0' = 1$. Hence $s = \{0,1\}$. Hence $(b) \Rightarrow (c)$.

Assume (c) i.e., $S = \{0,1\}$. Then clearly S is a field. Hence $(c) \Rightarrow (a)$

8.7 Corollary : A boolean ring is semiprimitive. Thus an element of a Boolean ring is 0 iff it is mapped on to "0" by every homomorphism of the ring into the two element Boolean ring.

8.8 Definition : A ring R is said to be a regular ring, for every $a \in R$, the exists an element $a' \in R \ni a a' a = a$

8.9 Theorem : In a commutative regular ring R we have the following properties.

(1) Every non-unit is a zero - divisior

(2) Every prime ideal is maximal

(3) Every principal ideal is a direct summand

Proof (1) : Suppose "a" is not a zero-division. Since R is regular, $\exists$ an element $a' \in R \ni a = aa'a \Rightarrow a(1 - a'a) = 0$. Since "a" is not a zero-divisor we have $1 - a'a = 0 \Rightarrow a'a = 1 \Rightarrow$ "a" is a unit.

Hence every non-unit is a zero-divisor.

(2) Let P be a prime ideal suppose $a \notin p$. By regularity, $\exists a' \ni a a' a = a \Rightarrow a(a'a - 1) = 0 \in P$. Since P is prime and $a \notin P$, we have $a'a - 1 \in P$. Hence P is a maximal ideal.

(3) Let aR be a principal ideal. Let a' be an element $\ni aa'a = a$. Fu: $a'a = e \Rightarrow e^2 = a' aa'a = a'a = e \Rightarrow e$ is an idempotent. Hence R is the direct sum of eR and $(1-e)R$. But $eR = aR$.

$\therefore aR$ is a direct summand of R.

8.10 Theorem : Every commutative regular ring R is semiprimitive.

Proof : Suppose Rad $R \neq 0$. Let $0 \neq a \in Rad\, R$. Since R is regular, $\exists$ an element $a' \in R \ni a a' a = a \Rightarrow (1 - a a')a = 0 \Rightarrow 1 - aa'$ is a zero-divisor $\Rightarrow 1 - a a'$ is not a unit $\Rightarrow 1 - aa' \in M_1$ for some maximal ideal M_1.

But $a \in M_1 \Rightarrow aa' \in M_1 \Rightarrow 1 \in M_1$ which is a contradiction.

$\therefore Rad\ R = 0 \Rightarrow R$ is semiprimitive.

8.11 Definition : A commutative ring is called local if it has exactly one maximal ideal M.

8.12 Remark : If R is a local ring, then $Rad\ R$ is the unique maximal ideal of R. If R is an integral domain, then (0) is a prime ideal and hence $rad\ R = 0$.

Ex : We shall given an example of a local integral domain which is not a field Let R be the ring of formal power series.

$a(x) = a_0 + a_1 x + \ldots.$ over a field F. Clearly R is an integral domain.

An element $a(x) = a_0 + a_1 x + \ldots\ldots$ of R is a unit iff $a_0 \neq 0$. Hence $a(x) \in Rad\ R$ iff for every $b(x) \in R,\ 1 - a(x)\, b(x)$ is a unit iff for every $b(x) \in R,\ 1 - a_0 b_0 \neq 0$. Iff $a_0 = 0$.

Hence $Rad\ R = xR$. Which is the principal ideal generated by x.

Suppose $c(x) \in xR \Rightarrow c_0 \neq 0 \Rightarrow c(x)$ is a unit $\Rightarrow c(x) R = R$

$\therefore xR$ is a maximal ideal. Since $xR = Rad\ R$, it is the only maximal ideal of R. Hence R is a local ring.

8.14 Theorem : Let R be a commutative ring. The following conditions are equivalent.

(1) R has a unique maximal ideal M.

(2) All non-units of R are contained in a proper ideal M.

(3) The non-units form an ideal M.

Proof : Assume (1). Let x be any non-unit $\Rightarrow x$ is in a maximal ideal.

$$\Rightarrow x \in M$$

Hence every non-unit is in M. Therefore $(1) \Rightarrow (2)$

Assume (2) : All the non-units of R contained in the proper ideal M since M is proper, every element of M is a non unit. $\Rightarrow M$ is precisely the set of all non-units of R. Hence $(2) \Rightarrow (3)$.

Assume (3) : Let M be a ideal consisting of all non-units $\Rightarrow M$ is proper. Let M_1 be any maximal ideal $\Rightarrow$ Every element of M is a non-unit $\Rightarrow M_1 \subseteq M$. Since M_1 is maximal and M is proper, we must have $M_1 = M$. Therefore M is the only maximal ideal of R $\therefore (3) \Rightarrow (1)$.

8.15 Definition : A ring R is said to be fully primary if it has a unique prime ideal.

8.16 Theorem : Let R be a commutative ring, The following conditions are equivalent.

(1) Every zero-divisor is nilpotent

(2) R has a minimal prime ideal P and This contains all zero-divisors.

Proof : Assume (1). Let P be the set of all zero-divisors of R. Since every nilpotent element is a zero-divisor, if follows that P is the set of all nilpotent elements of R ($\because$ every zero-divisor is nilpotent)

$\Rightarrow P=$ rad $R \Rightarrow P$ is contained in every prime ideal of R. Suppose $a \notin p$ and $b \notin p$. Suppose $ab \in p \Rightarrow ab$ is a zero-divisor.

$\Rightarrow \exists s \neq 0 \ni abs=0$. If $bs=0$ then b is a zero-divisor. Hence $b \in P$. If $bs \neq 0$, then "a" is a zero-divisor and hence $a \in P$. Any way it is a contradiction. $\therefore ab \notin P$. Hence P is prime.

Thus P is a miniimal prime ideal which contains all zero-divisors.

Hence $(1) \Rightarrow (2)$

Assume (2) : Let P be a min' 'al prime ideal which contains all zero-divisors. Suppose r is a zero-divisor $\Rightarrow r \in P$. Suppose it possible r is not nilpotent. Let $T = \{ sr^k / s \notin P$ and $k \geq 0$ any natural number$\}$. Clearly $1 = 1.r^0 \in T$ and $r = 1\ r' \in T$. Also T is closed under finite products. [Let $a, b \in T$ and suppose $a = s\ r^m$ and $b = t\ r^n$ for some $s \notin P, t \notin P$ and $m \geq 0, n \geq 0$. Since P is prime ideal we have $st \notin P$. Now $ab = st\ r^{m+n} \in T$]. Suppose if possible $0 \in T \Rightarrow 0 = sr^k$ for some $s \notin p$ and $k \geq 0$ and $r^k \neq 0 \Rightarrow s$ is a zero-divisor $\Rightarrow s \in P$ which is a contradiction. $\therefore 0 \notin T$.

Let M be a maximal element among the set of all ideals which does not meet T. We know that M is prime $\Rightarrow M \subseteq R - T$.

If $s \in R - T$, then $s \in p$ (other wise $s \in T$) $\Rightarrow R - T \subseteq P$.

Thus we have $M \subseteq R - T \subseteq P \Rightarrow M \subseteq P$ where M and P are prime ideals and P is a minimal prime ideal $\Rightarrow M = P = R - T$. Since $r \in T$ we have $r \notin P$. Which is a contradiction. $\therefore r$ is nilpotent. Thus $(2) \Rightarrow (1)$.

8.17 Definition : A ring R is said to be primary if every zero-divisor is nilpotent or if R has a minimal prime ideal P and this contains all zero-divisors.

8.18 Theorem : Let R be a commutative ring, then the following conditions are equivalent.

(1) R has a unique prime ideal P.

(2) R is local and $Rad\ R = rad\ R$

(3) Every non-unit is nilpotent

(4) R is primary and all non-units are zero-divisors.

Proof : Assume (1) : Let P be the unique prime ideal. Since every maximal ideal is a prime ideal, there can be only one maximal ideal. Since P is proper, it is contained in a maximal ideal. Hence there is at least one maximal ideal. Hence P itself is the only maximal ideal.

$\Rightarrow R$ is local and $Rad\ R = rad\ R \therefore (1) \Rightarrow (2)$.

Assume (2) Let r be any non-unit $\Rightarrow r$ is in a maximal ideal. But R is local $\Rightarrow Rad\ R$ is the only maximal ideal $\Rightarrow r \in Rad\ R$. $\Rightarrow r \in rad\ R \Rightarrow r$ is a nilpotent. $\therefore (2) \Rightarrow (3)$.

Assume (3) Let r be any non-unit $\Rightarrow r$ is nilpotent. Let n be the least positive integer $\ni r^n = 0 \Rightarrow r\, r^{n-1} = 0$ where $r^{n-1} \neq 0 \Rightarrow r$ is a zero-divisor. Thus every non-unit is a zero-divisor.

Let r be any zero-divisor $\Rightarrow r$ is a non-unit $\Rightarrow r$ is nilpotent.

Therefore R is primary. Hence $(3) \Rightarrow (4)$.

Assume (4) : Let P be the set of all zero-divisors which is minimal prime ideal. Suppose $r \notin P \Rightarrow r$ is not a zero-divisor $\Rightarrow r$ is a unit. Hence P is a maximal ideal $\Rightarrow P$ is the only prime ideal. Hence $(4) \Rightarrow (1)$.

8.19 Definition : If K is any subset of the commutative ring R, then we write $K^* = \left\{ r \in R \middle/ rK = 0 \right\}$ and is called the annihilator of K.

8.20 Remark : K^* is always an ideal and we denote $(K^*)^*$ by K^{**} and $A \subseteq B \Rightarrow B^* \subseteq A^*$.

8.21 Theorem (Mechoy) : Let R be a subdirectly irreducible commutative ring with smallest non-zero ideal J. then the annihilator J^* of J is the set of all zero-divisors and J^* is a maximal ideal and $J^{**} = J$.

Proof : Let r be any zero-divisor $\Rightarrow rs = 0$ for some $s \neq 0$

$\Rightarrow s \in r^*$ and $s \neq 0$

$\Rightarrow r^*$ is a non-zero ideal of R.

$\Rightarrow J \subseteq r^* \Rightarrow r \in J^*$

Hence $J*$ contains all zero-divisors. Let $r \in J* \Rightarrow rx=0 \forall x \in J$. $\Rightarrow ry=0$ for some non-zero $y \in J \Rightarrow r$ is a zero divisor.

Therefore $J*$ is the set of all zero-divisors.

Clearly $1 \notin J* \Rightarrow J*$ is proper $\Rightarrow J*$ is a proper ideal.

Suppose $r \notin J* \Rightarrow ry \neq 0$ for some $y \in J \Rightarrow ryR$ is a non zero ideal and $ryR \subseteq J\,(\because y \in J)$

Since J is the smallest non-zero ideal, we have $J=ryR \Rightarrow y=ryx$ for some $x \in R \Rightarrow y(1-rx)=0$

$\Rightarrow j(1-rx)=0 \forall j \in J \Rightarrow 1-rx \in J* \Rightarrow J*$ is maximal ideal.

Let $x \in J$. Now for any $y \in J*$, we have $xy=0 \Rightarrow x \in J** \Rightarrow J \subseteq J**$. Let $0 \neq a \in J**$. Now aR is a non-zero ideal. $\Rightarrow J \subseteq aR \Rightarrow ar \neq 0$ for some $r \in R$ such that $ar \in J$. Since $ar \neq 0$. We have $r \notin J*$ Since $J*$ is maximal, we have $1-rx \in J*$ for some $x \in R \Rightarrow a(1-rx)=0 \Rightarrow a=arx \in J \Rightarrow J** \subseteq J$. Hence $J=J**$.

8.22 Corollary : If R is subdirectly irreducible and semiprime, then R is a field.

Proof : Let J be the smallest non-zero ideal of R. Since R is semiprime, we have $rad\,R=0 \Rightarrow \exists$ no non-zro nilpotent element. $\Rightarrow J^2 \neq 0 \Rightarrow J \not\subseteq J*$ Hence $J*=0 \Rightarrow$ "0" is a maximal ideal. $\Rightarrow R$ is a field.

8.23 Theorem : A commutative ring R is subdirectly irreducible if and only if it contains an element j such that jR has non-zero intersection with all non-zero ideals and it's annihilator $j*$ is a maximal ideal.

Proof : Suppose R is subdirectly irreducible $\Rightarrow \exists$ a smallest non-zero ideal J. For any $0 \neq j \in J$, we have $jR=J$ and $j*=J*$. Hence $j*$ is maximal. Clearly jR has non-zero intersection with all non-zero ideal.

Conversely supposet hat, $\exists$ an element j such that jR has non-zero intersection with all non-zero ideals and $j*$ is maximal. Now we show that jR is contained in every non-zero ideal of R. Let A be any non-zero ideal of R. Let $0 \neq a \in A \Rightarrow aR \cap jR \neq 0$. Let $0 \neq x \in aR \cap jR$ $\Rightarrow x=ar=js$ for some $r \in R$ and $s \in R \Rightarrow s \notin j*$. Since $j*$ is maximal, $\exists t \in R \ni 1-st \in j* \Rightarrow j(1-st)=0$

$\Rightarrow j=jst=art$

$\Rightarrow jR \subseteq art\,R \subseteq ar \subseteq A$

Thus jR is contained in every non-zero ideal of R. Hence R is subdirectlly irreducible.

8.24 Problem : Show that in a regular ring R, for each element $r \in R$ $\exists$ an element $r' \ni r r' r = r$ and $r' r r' = r'$ and r' is uniquely determined by r.

Proof : Since R is regular, there exists an element $s \in R \ni r s r = r$.

Put $r' = srs$

Now $rr'r = rs rs r = rsr = r$ and $r' r r' = r'$

Clearly r' is uniquely determined by r.

Prof. G. Koteswara Rao
Department of Mathematics
Acharya Nagarjuna University

Lesson : 9 THE COMPLETE RING OF QUOTIENTS OF A COMMUTATIVE RING

9.0 Introduction : There are several ways of constructing the rational numbers from the integers, some of which go back to Euclid's theory of proportions. One of those such methods is the following. The fraction $4/6$ may be regarded as a partial endomorphism of the additive group of integers; its domain is the ideal 6z and it sends 6z onto 4z, where $z \in Z$, the ring of integers. Similarly the fraction $6/9$ has domain 9Z and sends 9z onto 6z. These two fractions are equivalent in the sense that they agree on the intersection of their domains, the ideal 18z, since both send 18z onto 12z. Ratios are then defined as equivalence classes of fractions. This method may also be applied to any commutative ring to construct its "complete ring of quotients" provided only certain ideals are admitted as domains.

9.1 Definition : An ideal D in a commutative ring R is called a dense ideal of R if, for all $r \in R$, $rD = (0)$ implies $r = 0$.

9.2 Remark : R is dense.

For let $r \in R$ such that $rR = (0) \Rightarrow r = r.1 = 0 \Rightarrow r = 0$.

$\therefore R$ is dense.

9.3 Remark : If D is dense and $D \subseteq D'$, then D' is dense.

For let $r \in R$ such that $rD' = (0) \Rightarrow rD = (0)$ $(\because D \subseteq D')$

$\Rightarrow r = 0$ ($\because$ D is dense)

$\therefore$ D' is dense.

9.4 Remark : If D and D' are dense, so are DD' and $D \cap D'$. For let $r \in R$ such that $rDD' = (0) \Rightarrow rdD' = (0)$ for all $d \in D \Rightarrow rd = 0$ for all $d \in D$ ($\because D'$ is dense)

$\Rightarrow rD = (0) \Rightarrow r = 0$ ($\because D$ is dense)

$\therefore DD'$ is dense.

Since $DD' \subseteq D \cap D'$ and DD' is dense, by remark 9.3, $D \cap D'$ is dense.

9.5 Remark : If $R \neq (0)$, then (0) is not dense.

For, since $R\neq(0)$, choose $r\in R$ such that $r\neq 0$. We know that $x0=0$ for any $x\in R\Rightarrow r0=0$. If (0) is a dense ideal of R, then $r=0$, a contradiction. So (0) is not dense ideal of R.

9.6 Definition : By a fraction we mean an element $f\in Hom_R(D,R)$, where D is a dense ideal of R. (i.e., every R-homomorphism from D into R, where D is a dense ideal of R, is called a fraction).

Thus f is a group homomorphism of D into R such that $f(dr)=(fd)r$ for any $d\in D$ and $r\in R$.

We define, for any $f\in Hom_R(D,R)$, $-f:D\to R$, a R-homomorphism, by $(-f)(d)=-(f(d))$ for all $d\in D$.

We also introduce fractions $\bar{0},\bar{1}\in Hom_R(R,R)$, by writing $\bar{0}(r)=0$ and $\bar{1}(r)=r$ for all $r\in R$. Addition and multiplication of fractions are defined as follows :

Let $f_i\in Hom_R(D_i,R)$ for $i=1,2$. Define $(f_1+f_2)(d)=f_1(d)+f_2(d)$ for all $d\in D_1\cap D_2$.

Then $f_1+f_2\in Hom_R(D_1\cap D_2,R)$.

$(f_1f_2)(d)=f_1(f_2(d))$ for all $d\in f_2^{-1}D_1$. Then $f_1f_2\in Hom_R\left(f_2^{-1}D_1,R\right)$

Here $f_2^{-1}D_1=\{r\in D_2\,/\,f_2(r)\in D_1\}$

By remark 9.4, D_2D_1 is a dense ideal of R. Since $D_2D_1\subseteq f_2^{-1}D_1$, by remark 9.3, $f_2^{-1}D_1$ is a dense ideal of R.

Let F be the set of all fractions.

9.7 Remark : $\left(F,\bar{0},+\right)$ is an additive abelian semigroup with zero.

For let $f_i\in Hom_R(D_i,R)$ for $i=1,2,3$ and D_i be a dense ideal of R for $i=1,2,3$,

First we show that f_1+f_2 is an R-homomorphism of $D_1\cap D_2$ into R.

For any $x,y\in D_1\cap D_2$, consider $(f_1+f_2)(x+y)=f_1(x+y)+f_2(x+y)$

$=f_1(x)+f_1(y)+f_2(x)+f_2(y)$ ($\because f_1$ and f_2 are R - homomorphisms).

$= f_1(x)+f_2(x)+f_1(y)+f_2(y)$ ($\because$ R is a commutative ring)

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

$\Rightarrow (f_1+f_2)(x+y)=(f_1+f_2)(x)+(f_1+f_2)(y)$ for all $x, y \in D_1 \cap D_2$

For any $d \in D_1 \cap D_2$ and $r \in R$, consider $(f_1+f_2)(dr)=$

$= f_1(dr)+f_2(dr)=f_1(d)r+f_2(d)r$ ($\because f_1$ and f_2 are R-homomorphisms)

$=(f_1(d)+f_2(d))r = ((f_1+f_2)(d))r$

$\therefore f_1+f_2$ is an R-homomorphisms of $D_1 \cap D_2$ into R.

Since D_1 and D_2 are dense ideals of R, $D_1 \cap D_2$ is also a dense ideal of R (by remark 9.4)

Hence $f_1+f_2 \in F$

Clearly $(f_1+f_2)(d) = (f_2+f_1)(d)$ for all $d \in D_1 \cap D_2$

$\Rightarrow f_1+f_2 = f_2+f_1$ on $D_1 \cap D_2$.

$\therefore f_1+f_2 = f_2+f_1$

It is easy to verify that $(f_1+f_2)+f_3$ and $f_1+(f_2+f_3)$ are R-homomorphisms of $D_1 \cap D_2 \cap D_3$ into R and they are equal on $D_1 \cap D_2 \cap D_3$ and so $(f_1+f_2)+f_3 = f_1+(f_2+f_3)$.

Let $f \in Hom_R(D, R)$, where D is a dense ideal of R.

For any $d \in D$, consider $(f+\bar{0})(d)=f(d)+\bar{0}(d)$

$= f(d)+0 = f(d)$

$\Rightarrow f+\bar{0} = f$ on D

$\therefore f+\bar{0} = f$

$\therefore (F, \bar{0}, +)$ is an additive abelian semigroup with zero.

9.8 Remark : For any $f \in F$, $f \cdot \overline{1} = \overline{1} \cdot f = f$

We define a relation θ on F as follows. For any $f_1, f_2 \in F$, define $f_1 \theta f_2$ if and only if f_1 and f_2 agree on the intersection of their domains; that is, $f_1(d) = f_2(d)$ for all $d \in D_1 \cap D_2$.

9.9 Lemma : For any $f_1, f_2 \in F$, $f_1 \theta f_2$ if and only if f_1 and f_2 agree on some dense ideal of R.

Proof : Let $f_1, f_2 \in F$

Suppose $f_1 \theta f_2$, where $f_i \in Hom_R(D_i, R)$ for $i = 1, 2$.

Then $f_1(d) = f_2(d)$ for all $d \in D_1 \cap D_2$

Since D_1 and D_2 are dense ideals of R, by remark 9.4, $D_1 \cap D_2$ is a dense ideal of R. So f_1 and f_2 agree on the dense ideal $D_1 \cap D_2$ of R.

Conversely suppose that f_1 and f_2 agree on some dense ideal D of R. Then $f_1(d) = f_2(d)$ for all $d \in D$.

For any $x \in D_1 \cap D_2$ and for any $d \in D$,

Consider $f_1(x)d = f_1(xd)$ ($\because f_1$ is an R-homomorphism)

$= f_2(xd)$ ($\because xd \in D$ and f_1 and f_2 agree on D).

$= f_2(x)d$ ($\because f_2$ is an R - homomorphism)

$\Rightarrow (f_1(x) - f_2(x))d = 0$ for all $d \in D$ and for all $x \in D_1 \cap D_2$

$\Rightarrow (f_1(x) - f_2(x))D = (0)$ for all $x \in D_1 \cap D_2$

$\Rightarrow f_1(x) - f_2(x) = 0$ for all $x \in D_1 \cap D_2$ ($\because D$ is a dense ideal of R).

$\Rightarrow f_1(x) = f_2(x)$ for all $x \in D_1 \cap D_2$

$\Rightarrow f_1 \theta f_2$

Thus $f_1 \theta f_2$ if and only if f_1 and f_2 agree on some dense ideal of R.

9.10 Lemma : θ is a congruence relation on the system $\left(F,\bar{0},\bar{1},-,+,\bullet\right)$.

Proof : Clearly θ is reflexive.

Suppose $f_1, f_2 \in F$ such that $f_1 \theta f_2$. Then f_1 and f_2 agree on some dense ideal D of R (By Lemma 9.9).

$\Rightarrow f_1(d)=f_2(d)$ for all $d \in D \Rightarrow f_2(d)=f_1(d)$ for all $d \in D \Rightarrow f_2$ and f_1 agree on the dense ideal D of R.

$\Rightarrow f_2 \theta f_1$

$\therefore \theta$ is symmetric

Suppose $f_1, f_2, f_3 \in F$ such that $f_1 \theta f_2$ and $f_2 \theta f_3$.

Then $f_1(d) = f_2(d)$ for all $d \in D_1 \cap D_2$

and $f_2(d)=f_3(d)$ for all $d \in D_2 \cap D_3$

Now $D_1 \cap D_2 \cap D_3$ is a dense ideal of R and $D_1 \cap D_2 \cap D_3 \subseteq D_1 \cap D_2$ and

$D_1 \cap D_2 \cap D_3 \subseteq D_2 \cap D_3$

$\Rightarrow f_1(d)=f_2(d)$ and $f_2(d)=f_3(d)$ for all $d \in D_1 \cap D_2 \cap D_3$

$\Rightarrow f_1(d)=f_3(d)$ for all $d \in D_1 \cap D_2 \cap D_3$.

$\Rightarrow f_1$ and f_3 agree on the dense ideal $D_1 \cap D_2 \cap D_3$

$\Rightarrow f_1 \theta f_3$ (by lemma 9.9)

$\therefore \theta$ is transitive and hence θ is an equivalence relation on F.

Clearly $\bar{0} \theta \bar{0}$ and $\bar{1} \theta \bar{1}$

Suppose f_1, $f_2 \in F$ such that $f_1 \theta f_2$. Then f_1 and f_2 agree on some dense ideal D of $R \Rightarrow f_1(d)=f_2(d)$ for all $d \in D$.

$\Rightarrow -f_1(d) = -f_2(d)$ for all $d \in D$

$\Rightarrow(-f_1)(d)=(-f_2)(d)$ for all $d \in D$

$\Rightarrow(-f_1)\theta(-f_2)$

Suppose $f_1, f_2, f_3, f_4 \in F$ such that $f_1 \theta f_3$ and $f_2 \theta f_4$. Then $f_1(d)=f_3(d)$ for all $d \in D_1 \cap D_3$ and $f_2(d)=f_4(d)$ for all $d \in D_2 \cap D_4$.

Now $D_1 \cap D_2 \cap D_3 \cap D_4$ is a dense ideal of R and $D_1 \cap D_2 \cap D_3 \cap D_4 \subseteq D_1 \cap D_3$ and $D_1 \cap D_2 \cap D_3 \cap D_4 \subseteq D_2 \cap D_4$.

For any $d \in D_1 \cap D_2 \cap D_3 \cap D_4$, consider $(f_1+f_2)(d) = f_1(d)+f_2(d)$

$= f_3(d)+f_4(d) = (f_3+f_4)(d)$

$\therefore f_1+f_2$ and f_3+f_4 agree on the dense ideal $D_1 \cap D_2 \cap D_3 \cap D_4$

Hence by Lemma 9.9, $(f_1+f_2)\theta(f_3+f_4)$

Since $f_1 \theta f_3$ and $f_2 \theta f_4$, we have $f_1(d)=f_3(d)$ for all $d \in D_1 \cap D_3$ and $f_2(d)=f_4(d)$ for all $d \in D_2 \cap D_4$

Now $f_1 f_2 \in Hom_R(f_2^{-1} D_1, R)$ and $f_3 f_4 \in Hom_R(f_4^{-1} D_3, R)$,

where $f_2^{-1} D_1 = \{d \in D_2 / f_2(d) \in D_1\}$ and $f_4^{-1} D_3 = \{d \in D_4 / f_4(d) \in D_3\}$

Since $f_2^{-1} D_1$ and $f_4^{-1} D_3$ are dense ideals of R, by remark 9.4,

$f_2^{-1} D_1 \cap f_4^{-1} D_3$ is a dense ideal of R

Let $d \in f_2^{-1} D_1 \cap f_4^{-1} D_3 \Rightarrow d \in f_2^{-1} D_1$ and $d \in f_4^{-1} D_3$

$\Rightarrow d \in D_2$ and $f_2(d) \in D_1$ and $d \in D_4$ and $f_4(d) \in D_3$

$\Rightarrow d \in D_2 \cap D_4 \Rightarrow f_2(d)=f_4(d) \in D_1 \cap D_3$.

$\Rightarrow f_1(f_2(d))=f_3(f_4(d)) \Rightarrow (f_1 f_2)(d)=(f_3 f_4)(d)$ for all

$d \in f_2^{-1} D_1 \cap f_4^{-1} D_3$

$\therefore f_1 f_2$ and $f_3 f_4$ agree on the dense ideal $f_2^{-1} D_1 \cap f_4^{-1} D_3$

So by lemma 9.9, $(f_1 f_2)\theta(f_3 f_4)$

$\therefore \theta$ is a congruence relation on $(F, \bar{0}, \bar{1}, -, +, \cdot)$.

For any $f \in F$, $\theta(f)$ denotes the equivalence class containing f, that is, $\theta(f) = \{g \in F / f\theta g\}$. We denote the class of all equivalence classes under θ by $(F, \bar{0}, \bar{1}, -, +, \cdot)/\theta = F/\theta$

Theorem 9.11 : If R is a commutative ring, then the system $(F, \bar{0}, \bar{1}, -, +, \cdot)/\theta = Q(R)$ is also a commutative ring. It extends R and will be called its complete ring of quotients.

Proof : Define +, • and – on F/θ as follows.

For any $\theta(f_1), \theta(f_2) \in F/\theta$, define $\theta(f_1) + \theta(f_2) = \theta(f_1 + f_2)$,

$\theta(f_1).\theta(f_2) = \theta(f_1 f_2)$ and $-\theta(f_1) = \theta(-f_1)$

Now we will show that +, • and – are well defined.

Suppose $\theta(f_1), \theta(f_2), \theta(f_3), \theta(f_4) \in F/\theta$ are such that

$\theta(f_1) = \theta(f_3)$ and $\theta(f_2) = \theta(f_4)$. Then $f_1 \theta f_3$ and $f_2 \theta f_4$

Since θ is a congruence relation, $(f_1 f_2)\theta(f_3 f_4)$, $(f_1 + f_2)\theta(f_3 + f_4)$

and $(-f_1)\theta(-f_3) \Rightarrow \theta(f_1 f_2) = \theta(f_3 f_4)$, $\theta(f_1 + f_2) = \theta(f_3 + f_4)$

and $\theta(-f_1) = \theta(-f_3) \Rightarrow \theta(f_1)\, \theta(f_2) = \theta(f_3)\theta(f_4)$;

$\theta(f_1) + \theta(f_2) = \theta(f_3) + \theta(f_4)$ and $-\theta(f_1) = -\theta(f_3)$

$\therefore$ +, • and – are well defined.

Let $\theta(f_1), \theta(f_2) \in F/_\theta$. We know that $f_1+f_2=f_2+f_1$ on the dense ideal $D_1 \cap D_2 \Rightarrow (f_1+f_2)\theta(f_2+f_1) \Rightarrow \theta(f_1+f_2)=\theta(f_2+f_1) \Rightarrow \theta(f_1)+\theta(f_2)=\theta(f_2)+\theta(f_1)$

$\therefore$ + is cummutative.

Let $\theta(f_1), \theta(f_2), \theta(f_3) \in F/_\theta$. We know that

$(f_1+f_2)+f_3 = f_1+(f_2+f_3)$ on the dense ideal $D_1 \cap D_2 \cap D_3$.

$\Rightarrow ((f_1+f_2)+f_3)\theta(f_1+(f_2+f_3))$

$\Rightarrow \theta((f_1+f_2)+f_3) = \theta(f_1+(f_2+f_3))$

$\Rightarrow (\theta(f_1)+\theta(f_2))+\theta(f_3) = \theta(f_1)+(\theta(f_2)+\theta(f_3))$

$\therefore$ + is associative.

Let $\theta(f) \in F/_\theta$. Then $f \in F$ and $\bar{0} \in F$. Suppose D is the domain of f. Then the domain of $f+\bar{0}$ and $\bar{0}+f$ is $D \cap R = D$ and $f+\bar{0}=f$ and $\bar{0}+f=f$ on D.

$\Rightarrow (f+\bar{0})\theta f$ and $(\bar{0}+f)\theta f$

$\Rightarrow \theta(f+\bar{0})=\theta(f)$ and $\theta(\bar{0}+f)=\theta(f)$

$\Rightarrow \theta(f)+\theta(\bar{0})=\theta(f)$ and $\theta(\bar{0})+\theta(f)=\theta(f)$

$\therefore \theta(\bar{0})$ is the additive identity in $F/_\theta$.

Let $\theta(f) \in F/_\theta$. Then $f \in F$. Suppose the domain of f is D, where D is a dense ideal of R. Then $-f \in F \Rightarrow \theta(-f) \in F/_\theta$

Now, for any $d \in D$, consider $(f+(-f))(d) = f(d)+(-f)(d)$

$= f(d)-f(d)=0=\bar{0}(d) \Rightarrow (f+(-f))(d)=\bar{0}(d)$ for all $d \in D \Rightarrow f+(-f)$ and $\bar{0}$ agree on the dense ideal D.

$\Rightarrow (f+(-f))\theta\,\bar{0} \Rightarrow \theta(f+(-f)) = \theta(\bar{0})$

$\Rightarrow \theta(f)+\theta(-f) = \theta(\bar{0})$

$\therefore \theta(-f)$ is the additive inverse of $\theta(f)$ in F/θ

Hence F/θ is an additive abelian group.

Let $\theta(f_1), \theta(f_2) \in F/\theta$ and assume that $f_i \in Hom_R(D_i, R)$ for $i=1,2$. Then by the definition of $f_1 f_2$, the domain of $f_1 f_2$ is $\left\{ x \in D_2 / f_2(x) \in D_1 \right\} = f_2^{-1} D_1$; which is a dense ideal of R. $\Rightarrow f_1 f_2 \in F \Rightarrow \theta(f_1 f_2) \in F/\theta$

$$\Rightarrow \theta(f_1)\,\theta(f_2) \in F/\theta$$

So "." is closed on F/θ

Let $\theta(f_1), \theta(f_2) \in F/\theta$. Then $f_i \in Hom_R(D_i, R)$ for $i=1,2$; where D_1 and D_2 are dense ideals of R. Then by remark 9.4, $D_1 D_2$ is a dense ideal of R.

For $x \in D_1$ and $y \in D_2$, consider $f_1 f_2(xy) = f_1 f_2(yx)$

$= f_1(f_2(yx)) = f_1(f_2(y)x)$ ($\because f_2$ is an R - homomorphism)

$= f_1(x f_2(y)) = f_1(x) f_2(y)$ ($\because f_1$ is an R - homomorphism)

$= f_2(y) f_1(x) = f_2(y f_1(x))$ ($\because f_2$ is an R-homomorphism)

$= f_2(f_1(x)y) = f_2(f_1(xy))$ ($\because f_1$ is an R-homomorphism)

$= f_2 f_1(x\,y)$

$\Rightarrow f_1 f_2(xy) = f_2 f_1(xy)$ for all $x \in D_1$ and for all $y \in D_2$ ---- (1)

Let $d \in D_1 D_2$. Then $d = x_1 y_1 + x_2 y_2 + \cdots\cdots\cdots + x_n y_n$, where $x_1, x_2, \cdots\cdots, x_n \in D_1$ and $y_1, y_2, \cdots\cdots, y_n \in D_2$.

Consider $f_1 f_2(d) = f_1 f_2(x_1 y_1 + x_2 y_2 + \cdots\cdots + x_n y_n)$

$= f_1(f_2(x_1 y_1 + x_2 y_2 + \cdots\cdots + x_n y_n))$

$= f_1(f_2(x_1 y_1) + f_2(x_2 y_2) + \cdots\cdots + f_2(x_n y_n))$

$= f_1(f_2(y_1)x_1 + f_2(y_2)x_2 + \cdots\cdots + f_2(y_n)x_n)$ ($\because f_2$ is an R - homomorphism).

$= f_1(f_2(y_1)x_1) + f_1(f_2(y_2)x_2) + \cdots\cdots + f_1(f_2(y_n)x_n)$

$= f_1(f_2(x_1 y_1)) + f_1(f_2(x_2 y_2)) + \cdots\cdots + f_1(f_2(x_n y_n))$

($\because f_2$ is an R-homomorphism and R is commutative)

$= f_1 f_2(x_1 y_1) + f_1 f_2(x_2 y_2) + \cdots\cdots + f_1 f_2(x_n y_n)$

$= f_2 f_1(x_1 y_1) + f_2 f_1(x_2 y_2) + \cdots\cdots + f_2 f_1(x_n y_n)$ (By (1))

= -

$= f_2 f_1(x_1 y_1 + x_2 y_2 + \cdots\cdots + x_n y_n) = f_2 f_1(d)$

$\therefore f_1 f_2(d) = f_2 f_1(d)$ for all $d \in D_1 D_2$

i.e. $f_1 f_2$ and $f_2 f_1$ agree on the dense ideal $D_1 D_2$.

$\Rightarrow (f_1 f_2)\theta(f_2 f_1) \Rightarrow \theta(f_1 f_2) = \theta(f_2 f_1)$

$\Rightarrow \theta(f_1)\theta(f_2) = \theta(f_2)\theta(f_1)$

$\therefore$ "." is commutative.

Let $\theta(f_i) \in F/\theta$ and assume that $f_i \in Hom_R(D_i, R)$, where D_i is a dense ideal of R for $i = 1, 2, 3$.

It is easy to verify that $f_3^{-1}\left(f_2^{-1}D_1\right)$ is the domain of $(f_1 f_2)f_3$ and $f_1(f_2 f_3)$ and $f_3^{-1}\left(f_2^{-1}D_1\right)$ is a dense ideal of R and also $(f_1 f_2)f_3$, $f_1(f_2 f_3)$ agree on $f_3^{-1}\left(f_2^{-1}D_1\right)$

$$\Rightarrow (f_1 f_2)f_3\,\theta\, f_1(f_2 f_3) \Rightarrow \theta((f_1 f_2)f_3) = \theta(f_1(f_2 f_3))$$

$$\Rightarrow (\theta(f_1)\theta(f_2))\theta(f_3) = \theta(f_1)(\theta(f_2)\,\theta(f_3))$$

$\therefore \bullet$ is associative on F/θ

Let $\theta(f_i) \in F/\theta$ and assume that $f_i \in Hom_R(D_i, R)$ for $i = 1,2,3$. Then $f_1(f_2 + f_3) \in F$ and $f_1 f_2 + f_1 f_3 \in F$,

Since $f_2^{-1}D_1$ and $f_3^{-1}D_1$ are dense ideals of R, by remark 9.4, $f_2^{-1}D_1 \cap f_3^{-1}D_1$ is a dense ideal of R.

For any $d \in f_2^{-1}D_1 \cap f_3^{-1}D_1$, consider $(f_1(f_2+f_3))(d)$

$$= f_1((f_2+f_3)(d)) = f_1(f_2(d)+f_3(d)) = f_1(f_2(d)) + f_1(f_3(d))$$

$$= f_1 f_2(d) + f_1 f_3(d) = (f_1 f_2 + f_1 f_3)(d)$$

$\Rightarrow f_1(f_2+f_3)$ and $f_1 f_2 + f_1 f_3$ agree on the dense ideal $f_2^{-1}D_1 \cap f_3^{-1}D_1$

$\Rightarrow f_1(f_2+f_3)\,\theta\,(f_1 f_2 + f_1 f_3)$ (By lemma 9.9)

$$\Rightarrow \theta(f_1(f_2+f_3)) = \theta(f_1 f_2 + f_1 f_3)$$

$$\Rightarrow \theta(f_1)(\theta(f_2)+\theta(f_3)) = \theta(f_1)\theta(f_2) + \theta(f_1)\theta(f_3)$$

$\therefore +$ and $\bullet$ satisfy the left distributive law.

Similarly we can prove the right distributive law also.

Hence F/θ is a commutative ring.

Now we will show that there is a monomorphism from R into $Q(R) = F/\theta$

Let $r \in R$

Define $\frac{r}{1}: R \to R$ as $\frac{r}{1}(s) = rs$ for all $s \in R$

Clearly $\frac{r}{1}$ is well defined.

For any $s_1, s_2 \in R$, consider $\frac{r}{1}(s_1 + s_2) = r(s_1 + s_2)$

$$= rs_1 + rs_2 = \frac{r}{1}(s_1) + \frac{r}{1}(s_2)$$

$$\Rightarrow \frac{r}{1}(s_1 + s_2) = \frac{r}{1}(s_1) + \frac{r}{1}(s_2) \text{ for all } s_1, s_2 \in R$$

$\therefore \frac{r}{1}$ is an additive group homomorphism.

For $x, y \in R$, consider $\frac{r}{1}(xy) = r(xy) = (rx)y = \frac{r}{1}(x)y$

$$\Rightarrow \frac{r}{1}(xy) = \frac{r}{1}(x)y$$

$\therefore \frac{r}{1}$ is an R - homomorphism and hence $\frac{r}{1} \in F$

$$\Rightarrow \theta\left(\frac{r}{1}\right) \in F/\theta$$

So for each $r \in R, \theta\left(\frac{r}{1}\right) \in F/\theta = Q(R)$

Now define $\psi: R \to Q(R)$ as $\psi(r) = \theta\left(\frac{r}{1}\right)$ for all $r \in R$.

Now we will show that ψ is a monomorphism.

Let $r_1, r_2 \in R$ such that $r_1 = r_2 \Rightarrow r_1 s = r_2 s$ for all $s \in R$.

$$\Rightarrow \frac{r_1}{1}(s) = \frac{r_2}{1}(s) \text{ for all } s \in R \Rightarrow \frac{r_1}{1} \text{ and } \frac{r_2}{1} \text{ agree on } R$$

$$\Rightarrow \frac{r_1}{1}\theta\frac{r_2}{1} \Rightarrow \theta\left(\frac{r_1}{1}\right) = \theta\left(\frac{r_2}{1}\right) \Rightarrow \psi(r_1) = \psi(r_2)$$

$\therefore \psi$ is well defined.

Let $r_1, r_2 \in R$. Then $r_1 + r_2 \in R$ and $r_1 \, r_2 \in R$

For any $s \in R$, consider $\frac{r_1 + r_2}{1}(s) = (r_1 + r_2)s = r_1 s + r_2 s = \frac{r_1}{1}(s) + \frac{r_2}{1}(s) = \left(\frac{r_1}{1} + \frac{r_2}{1}\right)(s)$

$$\Rightarrow \frac{r_1 + r_2}{1} \text{ and } \frac{r_1}{1} + \frac{r_2}{1} \text{ agree on } R.$$

$$\Rightarrow \left(\frac{r_1 + r_2}{1}\right)\theta\left(\frac{r_1}{1} + \frac{r_2}{1}\right) \Rightarrow \theta\left(\frac{r_1 + r_2}{1}\right) = \theta\left(\frac{r_1}{1}\right) + \theta\left(\frac{r_2}{1}\right)$$

$$\Rightarrow \psi(r_1 + r_2) = \psi(r_1) + \psi(r_2)$$

For any $s \in R$, consider $\frac{r_1 r_2}{1}(s) = (r_1 r_2)s = r_1(r_2 s)$

$$\Rightarrow \frac{r_1}{1}(r_2 s) = \frac{r_1}{1}\left(\frac{r_2}{1}(s)\right) = \left(\frac{r_1}{1}\frac{r_2}{1}\right)(s)$$

$$\Rightarrow \frac{r_1 r_2}{1} \text{ and } \frac{r_1}{1}\frac{r_2}{1} \text{ agree on } R.$$

$$\Rightarrow \left(\frac{r_1 r_2}{1}\right)\theta\left(\frac{r_1}{1}\frac{r_2}{1}\right)$$

$$\Rightarrow \theta\left(\frac{r_1 r_2}{1}\right) = \theta\left(\frac{r_1}{1}\frac{r_2}{1}\right) \Rightarrow \theta\left(\frac{r_1 r_2}{1}\right) = \theta\left(\frac{r_1}{1}\right)\theta\left(\frac{r_2}{1}\right)$$

$$\Rightarrow \psi(r_1 r_2) = \psi(r_1)\psi(r_2)$$

It is easy to verify that $\frac{0}{1} = \bar{0}$ and $\frac{1}{1} = \bar{1}$ on R.

$\Rightarrow \frac{0}{1}\,\theta\,\bar{0}$ and $\frac{1}{1}\,\theta\,\bar{1}$

$\Rightarrow \theta\left(\frac{0}{1}\right) = \theta\left(\bar{0}\right)$ and $\theta\left(\frac{1}{1}\right) = \theta\left(\bar{1}\right)$

$\Rightarrow \psi(0) = \theta\left(\bar{0}\right)$, which is the zero element in $Q(R)$.

and $\psi(1) = \theta\left(\bar{1}\right)$, which is the unity element in $Q(R)$.

For any $r \in R$, consider $\psi(-r) = \theta\left(\frac{-r}{1}\right) = -\theta\left(\frac{r}{1}\right) = -\psi(r)$

$\therefore \psi : R \to Q(R)$ is a ring homomorphism.

Suppose $r \in R$ such that $\psi(r) = \theta\left(\bar{0}\right) \Rightarrow \theta\left(\frac{r}{1}\right) = \theta\left(\bar{0}\right)$

$\Rightarrow \frac{r}{1}\,\theta\,\bar{0} \Rightarrow \frac{r}{1}$ and $\bar{0}$ agree on some dense ideal D of R.

$\Rightarrow \frac{r}{1}(d) = \bar{0}(d)$ for all $d \in D$.

$\Rightarrow rD = (0) \Rightarrow r = 0$ ($\because$ D is a dense ideal of R).

$\therefore \psi$ is one - one.

Thus $\psi : R \to Q(R)$ is a monomorphism and hence $Q(R)$ extends R.

9.12 Remark : The mapping $\psi\left(r \to \theta\left(\frac{r}{1}\right)\right)$ is called the canonical monomorphism of R into $Q(R)$

Let R be a commutative ring and $d \in R$ be a non-zero-divisor. Then dR is a dense ideal of R. Let $r \in R$. Define $\frac{r}{d} : dR \to R$ as $\frac{r}{d}(dx) = rx$ for any $x \in R$. Then it is easy to verify that $\frac{r}{d}$ is an R-homomorphism and hence $\frac{r}{d} \in Hom_R(dR, R)$ and this $\frac{r}{d}$ is called a classical fraction associated with the dense ideal dR.

7)

9.13 Theorem : The equivalence classes $\theta\left(\frac{r}{d}\right)$, $r \in R$, d not a zero-divisor, from a subring of $Q(R)$, which is called the classical ring of quotients of R and is denoted by $Q_{cl}(R)$.

Proof : Let R be a commutative ring.

Write $Q_{cl}(R) = \left\{ \theta\left(\frac{r}{d}\right) \middle/ r \in R \text{ and } d \in R \text{ and } d \text{ is not a zero-divisor} \right\}$

Claim : $Q_{cl}(R)$ is a subring of $Q(R)$.

Let $\theta\left(\frac{r_1}{d_1}\right)$ and $\theta\left(\frac{r_2}{d_2}\right) \in Q_{cl}(R)$. Then $\frac{r_1}{d_1}$ and $\frac{r_2}{d_2}$ are fractions. Now $d_1 d_2 R$ is a dense ideal of R and $\frac{r_1 d_2 + r_2 d_1}{d_1 d_2} \in Hom_R(d_1 d_2 R, R)$.

For $d_1 d_2 s \in d_1 d_2 R$, consider $\left(\frac{r_1}{d_1} + \frac{r_2}{d_2}\right)(d_1 d_2 s)$

$$= \frac{r_1}{d_1}(d_1 d_2 s) + \frac{r_2}{d_2}(d_2 d_1 s) = r_1 d_2 s + r_2 d_1 s$$

$$= (r_1 d_2 + r_2 d_1) s = \frac{(r_1 d_2 + r_2 d_1)}{d_1 d_2}(d_1 d_2 s)$$

$\therefore \frac{r_1}{d_1} + \frac{r_2}{d_2}$ and $\frac{r_1 d_2 + r_2 d_1}{d_1 d_2}$ agree on the dense ideal $d_1 d_2 R$.

$$\Rightarrow \left(\frac{r_1}{d_1} + \frac{r_2}{d_2}\right) \theta \left(\frac{r_1 d_2 + r_2 d_1}{d_1 d_2}\right)$$

$$\Rightarrow \theta\left(\frac{r_1}{d_1}\right) + \theta\left(\frac{r_2}{d_2}\right) = \theta\left(\frac{r_1 d_2 + r_2 d_1}{d_1 d_2}\right) \in Q_{cl}(R)$$

For $d_1 d_2 s \in d_1 d_2 R$, consider $\frac{r_1}{d_1} \frac{r_2}{d_2}(d_1 d_2 s) = \frac{r_1}{d_1}\left(\frac{r_2}{d_2}(d_1 d_2 s)\right)$

$$= \frac{r_1}{d_1}(r_2 d_1 s) = r_1 r_2 s = \frac{r_1 r_2}{d_1 d_2}(d_1 d_2 s)$$

$\therefore \frac{r_1}{d_1} \frac{r_2}{d_2}$ and $\frac{r_1 r_2}{d_1 d_2}$ agree on the dense ideal $d_1 d_2 R$.

$$\Rightarrow \left(\frac{r_1}{d_1} \cdot \frac{r_2}{d_2}\right) \theta \left(\frac{r_1 r_2}{d_1 d_2}\right)$$

$$\Rightarrow \theta\left(\frac{r_1}{d_1} \cdot \frac{r_2}{d_2}\right) = \theta\left(\frac{r_1 r_2}{d_1 d_2}\right)$$

$$\Rightarrow \theta\left(\frac{r_1}{d_1}\right) \cdot \theta\left(\frac{r_2}{d_2}\right) = \theta\left(\frac{r_1 r_2}{d_1 d_2}\right) \in Q_{cl}(R)$$

$\therefore Q_{cl}(R)$ is closed under addition and multiplication.

Let $\theta\left(\frac{r}{d}\right) \in Q_{cl}(R)$. Then $\frac{r}{d} \in Hom_R(dR, R)$

For any $ds \in dR$, consider $-\left(\frac{r}{d}\right)(ds) = -\left(\frac{r}{d}(ds)\right)$

$$-(rs) = (-r)s = \frac{-r}{d}(ds)$$

$\therefore -\left(\frac{r}{d}\right)$ and $\frac{-r}{d}$ agree on the dense ideal dR

$$\Rightarrow -\left(\frac{r}{d}\right) \theta \left(\frac{-r}{d}\right) \Rightarrow \theta\left(-\left(\frac{r}{d}\right)\right) = \theta\left(\frac{-r}{d}\right)$$

$$\Rightarrow -\theta\left(\frac{r}{d}\right) = \theta\left(\frac{-r}{d}\right) \in Q_{cl}(R)$$

Since $1 \in R$ and 1 is not a zero divisor, $\frac{1}{1}(1s) = 1s = s = \bar{1}(s)$

$$\Rightarrow \frac{1}{1} \text{ and } \bar{1} \text{ agree on } R \Rightarrow \frac{1}{1}\theta\bar{1} \Rightarrow \theta\left(\frac{1}{1}\right) = \theta\bar{1}$$

$$\rightarrow \theta(\bar{1}) \in Q_{cl}(R)$$

It is easy to verify that $\frac{0}{1}$ and $\bar{0}$ agree on R and hence

$$\theta\left(\frac{0}{1}\right) = \theta(\bar{0}) \Rightarrow \theta(\bar{0}) \in Q_{cl}(R)$$

Thus $Q_{cl}(R)$ is a subring of $Q(R)$.

9.14 Definition : A fraction f defined on a dense ideal D is said to be an irreducible fraction if there does not exist a fraction g defined on a dense ideal G such that $D \subset G$ properly and $g/_D = f$.

(simply a fraction is called irreducible if it cannot be extended to a larger domain).

9.15 Theorem : Every equivalence class of fractions contains exactly one irreducible fraction and this extends all fractions in the class.

Proof : Let $\theta(f)$ be the equivalence class containing f. For any $f_1, f_2 \in \theta(f)$, define $f_1 \leq f_2$ if and only if $D_1 \subseteq D_2$ where D_i is the domain of f_i for $i = 1, 2$. Then it is easy to verify that $(\theta(f), \leq)$ is an ordered set. Let $\{f_i / i \in I\}$ be a chain in $\theta(f)$. Then each f_i is a fraction defined on a dense ideal D_i of R. Write $D = \bigcup_{i \in I} D_i$. Then D is a dense ideal of R.

Define $g : D \rightarrow R$ as follows.

Let $d \in D$. Then $d \in D_i$ for some $i \in I$.

Put $g(d) = f_i(d)$ [If also $d \in D_j$, then $f_i(d) = f_j(d)$; since f_i and f_j agree on $D_i \cap D_j$]

Since each f_i is an R-homomorphism, it is easy to verify that $g : D \rightarrow R$ is an R -

homomorphism and hence $g \in Hom_R(D, R)$. Clearly g is an upper bound of $\left\{ f_i \big/ i \in I \right\}$. So by Zorn's Lemma, $\theta(f)$ contains a maximal element. Let h, with domain H, be a maximal element in $\theta(f)$. Now we will show that h is an irreducible fraction. Let ℓ be a fraction with domain L such that ℓ is an extension of h and $H \subseteq L$.

Then $\ell \big/ H = h \Rightarrow \ell$ and h agree on $H \Rightarrow \ell \theta h$

$\Rightarrow \ell \theta f \left(\because h \in \theta(f) \right) \Rightarrow \ell \in \theta(f)$

Since $\ell \in \theta(f)$ and $h \leq \ell$ and h is maximal in $\theta(f)$, we have $h = \ell$ and $L = H$. Therefore h is irreducible. Next we will show that h extends all fractions in $\theta(f)$. Let $g \in \theta(f)$. Then $f \theta g$. Since $f \theta h$ and $f \theta g$, we have $g \theta h$. Now g is a fraction on some dense ideal D_1 and h is a fraction on the dense ideal D_2, where $D_2 = H$. Then $D_1 + D_2$ is a dense dieal of R.

Define $k : D_1 + D_2 \to R$ as $k(d_1 + d_2) = g(d_1) + h(d_2)$ for all $d_1 + d_2 \in D_1 + D_2$, where $d_1 \in D_1$ and $d_2 \in D_2$.

Now we will show that k is well defined.

Suppose $d_1 + d_2 \in D_1 + D_2$ such that $d_1 + d_2 = 0$

$\Rightarrow d_1 = -d_2 \in D_1 \cap D_2$

Since $g \theta h$, g and h agree on $D_1 \cap D_2$.

$\Rightarrow g(d_1) = h(d_1) = h(-d_2) = -h(d_2)$

$\Rightarrow g(d_1) + h(d_2) = 0 \Rightarrow k(d_1 + d_2) = 0$

$\therefore k$ is well defined.

Since g and h are R-homomorphisms, it is easy to verify that k is an R-homomorphism and hence $k \in Hom_R(D_1 + D_2, R)$. Clearly k is an extension of g and h. Since h is an irreducible fraction, we have $h = k$. Therefore h is an extension of g.

Thus h extends all fractions in $\theta(f)$.

Let h' be another irreducible fraction in $\theta(f)$. Since h is an extension of every fraction in $\theta(f)$ and h' is irreducible, we have $h=h'$. Hence $\theta(f)$ contains exactly one irreducible fraction.

9.16 Theorem : The following statements concerning the commutative ring R are equivalent.

(1) Every irreducible fraction has domain R.

(2) For every fraction f there exists an element $s\in R$ such that $fd=sd$ for all $d\in D$, the domain of f.

(3) $Q(R)\cong R$ canonically.

Proof : Let R be a commutative ring.

Assume (1) : i.e., every irreducible fraction has domain R. Let f be any fraction with domain D. Then $\theta(f)$ is the equivalence class containing f. Then by theorem in 9.15, $\theta(f)$ contains an irreducible fraction h, which is also an extension of f. By our assumption, h has domain R. Put $h(1)=s$. Then for any $d\in D$, $f(d)=h(d)=h(1d) = h(1)d = sd$. Thus for f, there exists $s\in R$ such that $f(d)=sd$ for all $d\in D$.

So $(1)\Rightarrow(2)$

Assume (2) : i.e., for every fraction f, there exists an element $s\in R$ such that $f(d)=sd$ for all $d\in D$, the domain of f.

Define $\psi:R\to Q(R)$ as

$$\psi(r)=\theta\left(\frac{r}{1}\right) \text{ for all } r\in R.$$

Then ψ is a monomorphism (The proof is given in theorem 9.11)

Next we will show that ψ is onto.

Let $\theta(f)\in Q(R)$. Then f is a fraction with domain D, a dense ideal of R. By our assumption there exists $s\in R$ such that $f(d)=sd$ for all $d\in D$.

$\Rightarrow f(d) = \frac{s}{1}(d)$ for all $d \in D$.

$\Rightarrow f$ and $\frac{s}{1}$ agree on $D \Rightarrow f\,\theta\left(\frac{s}{1}\right)$

$\Rightarrow \theta(f) = \theta\left(\frac{s}{1}\right)$

Consider $\psi(s) = \theta\left(\frac{s}{1}\right) = \theta(f)$

$\therefore \psi$ is onto

Hence ψ is an isomorphism of R onto $Q(R)$.

i.e., $R \cong Q(R)$ canonically

So $(2) \Rightarrow (3)$

Assume (3) : i.e., $R \cong Q(R)$ canonically.

Let $\psi : R \to Q(R)$ be the canonical isomorphism. Let f be any irreducible fraction. Then $\theta(f) \in Q(R)$. Since ψ is onto, there exists $s \in R$ such that

$$\psi(s) = \theta(f) \Rightarrow \theta\left(\frac{s}{1}\right) = \theta(f) \Rightarrow f\,\theta\left(\frac{s}{1}\right)$$

$$\Rightarrow \frac{s}{1} \in \theta(f)$$

Now $\frac{s}{1}$ is irreducible. Since $\theta(f)$ contains exactly one irreducible fraction, we have $f = \frac{s}{1}$

$\Rightarrow$ The domain of f is R.

Thus every irreducible fraction has domain R

So $(3) \Rightarrow (1)$

9.17 Remark : If R satisfies any one of the equivalent conditions in the above theorem, we say that R is rationally complete.

9.18 Remark : We identify R with its canonical image in $Q(R)$. Thus we write $\theta\left(\frac{r}{1}\right)=r$.

9.19 Remark : For any $q\in Q(R)$, put $q^{-1}R=\left\{r\in R/qr\in R\right\}$. Then $q^{-1}R$ is a dense ideal of R.

For, It is easy to verify that $q^{-1}R$ is an ideal of R. Since $q\in Q(R)$, $q=\theta(f)$ for some fraction f with domain D.

For any $d\in D$, consider $qd=\theta(f)\theta\left(\frac{d}{1}\right)=\theta\left(f\frac{d}{1}\right)=\theta\left(\frac{f(d)}{1}\right)=f(d)$

$\Rightarrow qd\in R$ for any $d\in D$.

$\Rightarrow qD\subseteq R\Rightarrow D\subseteq q^{-1}R\Rightarrow q^{-1}R$ is dense ($\because$ D is dense)

9.20 Theorem : If R is any commutative ring, then $Q(R)$ is rationally complete.

Proof : Let R be a commutative ring.

Claim : $Q(R)$ is rationally complete.

Let ϕ be any fraction over $Q(R)$ and K be its domain.

Put $D=\{r\in K\cap R/\phi r\in R\}$

Now we will show that D is a dense ideal of R

Suppose $r\in R$ such that $rD=(0)$

Let $k\in K$. Then $\phi k\in Q(R)$.

Put $D'=k^{-1}R\cap(\phi k)^{-1}R$. Then by remark 9.19 and remark 9.4, D' is a dense ideal of R and $kD'\subseteq R$ and $(\phi k)D'\subseteq R$. Therefore $\phi(kD')\subseteq R$. So $kD'\subseteq R\cap K$ and $\phi(kD')\subseteq R$ and hence $kD'\subseteq D$.

Consider $(rk)D' = r(kD') \subseteq rD = (0) \Rightarrow (rk)D' = (0) \Rightarrow rk = 0$ ($\because D'$ is a dense ideal of R)

Since $k \in K$ is arbitrary, we have $rK = (0) \Rightarrow r = 0$ ($\because K$ is a dense ideal of $Q(R)$). Thus, for any $r \in R$, $rD = (0) \Rightarrow r = 0$.

Consequently D is a dense ideal of R.

Now define $f : D \to R$ as $f(d) = \phi d$ for all $d \in D$.

Then $f \in Hom_R(D, R) \Rightarrow \theta(f) \in Q(R)$

Now we will show that for any $k \in K$, $\phi k = \theta(f)k$

Let $k \in K$ and let $d' \in D' = k^{-1}R \cap (\phi k)^{-1} R$

Consider $(\phi k)d' = \phi(kd') = f(kd')$ $(\because kD' \subseteq D)$

$$= (\theta(f))(kd') = (\theta(f)k)d'$$

$$\Rightarrow (\phi k - \theta(f)k)d' = 0$$

Since $d' \in D'$ is arbitrary, we have $(\phi k - \theta(f)k)D' = (0)$.

$$\Rightarrow \phi k - \theta(f)k = 0 \quad (\because D' \text{ is a dense ideal of } R).$$

$$\Rightarrow \phi k = \theta(f)k.$$

Thus for the fraction ϕ over $Q(R)$ with domain K, there exists $\theta(f) \in Q(R)$, $\phi k = \theta(f)k$ for all $k \in K$.

Therefore, by theorem 9.16, $Q(R)$ is rationally complete.

9.21 Remark : If $\theta(f) \in Q(R)$ and D is a dense ideal of R such that $\theta(f)D = (0)$, then $\theta(f) = 0$.

For, let $\theta(f) \in Q(R)$ and D be a dense ideal of R such that $\theta(f)D = (0)$. Let D_1 be the domain of f.

For any $d \in D$ and $d_1 \in D_1$, $d\,d_1 \in D$. Then by our supposition, $\theta(f)dd_1 = 0$, which is the zero element in $Q(R)$.

$$\Rightarrow \theta(f)\,\theta\left(\frac{d\,d_1}{1}\right)=\theta(\bar{0})$$

$$\Rightarrow \theta\left(\frac{f(dd_1)}{1}\right)=\theta(\bar{0})$$

$\Rightarrow \psi(f(dd_1))=\psi(0)$, where ψ is the canonical monomorphism of R into $Q(R)$.

$\Rightarrow f(dd_1)=0$ ($\because \psi$ is one - one)

Thus for any $d\in D,\ d_1\in D_1, f(dd_1)=0=\bar{0}(d\,d_1)$

$\Rightarrow f$ and $\bar{0}$ agree on the dense ideal DD_1

$\Rightarrow f\,\theta\,\bar{0}\Rightarrow \theta(f)=\theta(\bar{0})$

Thus if $\theta(f)\in Q(R)$ and if D is a dense ideal of R such that $\theta(f)D=(0)$, then $\theta(f)=0$

9.22 Definition : Let S be a commutative ring. A sub group D of S is called dense if, for any $s\in S$, $sD=(0)$ implies $s=0$.

9.23 Definition : :Let S be a commutative ring and R be a sub ring of S. Then S is called the ring of quotients of R if and only if, for all $s\in S$, $s^{-1}R=\{r\in R / sr\in R\}$ is dense in S.

9.24 Remark : S is a ring of quotients of R if and only if, for all $s\in S$ and $t\in S, t\neq 0$ implies $t(s^{-1}R)\neq(0)$. In other words, for all $s\in S$, for all $0\neq t\in S$, these exists $r\in R$ such that $sr\in R$ and $tr\neq 0$.

9.25 Theorem : Let R be a subring of the commutative ring S. Then the following three statements are equivalent :

(1) S is a ring of quotients of R.

(2) For all $0\neq s\in S, s^{-1}R$ is a dense ideal of R and $s(s^{-1}R)\neq 0$.

(3) There exists a monomorphism of S into $Q(R)$ which induces the canonical

monomorphism of R into $Q(R)$.

Proof : Assume (1) : i.e., S is a ring of quotients of R. Then for any $s \in S$, $s^{-1}R$ is a dense ideal of R. $\Rightarrow$ for all $0 \neq s \in S$, $s^{-1}R$ is a dense ideal of R.

Let $0 \neq s \in S$. Since $s^{-1}R$ is dense in S, we have $s\left(s^{-1}R\right) \neq (0)$

So $(1) \Rightarrow (2)$

Assume (2) : i.e., for all $0 \neq s \in S, s^{-1}R$ is a dense ideal of R and $s\left(s^{-1}R\right) \neq (0)$

Let $s \in S$. Define $\hat{s} : s^{-1}R \to R$ as $\hat{s}(d) = sd$ for all $d \in s^{-1}R$. Then $\hat{s}$ is an R - homomorphism and hence $\hat{s} \in Hom_R\left(s^{-1}R, R\right)$. Consequently $\theta\left(\hat{s}\right) \in Q(R)$. So, for any $s \in S, \theta\left(\hat{s}\right) \in Q(R)$.

Define $\psi : S \to Q(R)$ as $\psi(s) = \theta\left(\hat{s}\right)$ for all $s \in S$.

Clearly ψ is well defined.

Now we will show that ψ is a ring homomorphism

Let $s_1, s_2 \in S$ and assume $s_1 \neq 0$ and $s_2 \neq 0$. Then by our assumption $s_1^{-1}R$ and $s_2^{-1}R$ are dense ideals of R. Then by a known result, $s_1^{-1}R \cap s_2^{-1}R$ is a dense ideal of R. Also $\hat{s}_2^{-1}\left(s_1^{-1}R\right)$ is a dense ideal of R.

For any $d \in s_1^{-1}R \cap s_2^{-1}R$, Consider $\widehat{s_1 + s_2}(d) =$

$$= (s_1 + s_2)d = s_1 d + s_2 d = \hat{s}_1(d) + \hat{s}_2(d) = \left(\hat{s}_1 + \hat{s}_2\right)(d)$$

$\Rightarrow \widehat{s_1 + s_2}$ and $\hat{s}_1 + \hat{s}_2$ agree on the dense ideal $s_1^{-1}R \cap s_2^{-1}R$.

$$\Rightarrow \left(\widehat{s_1 + s_2}\right) \theta \left(\hat{s}_1 + \hat{s}_2\right) \Rightarrow \theta\left(\widehat{s_1 + s_2}\right) = \theta\left(\hat{s}_1 + \hat{s}_2\right)$$

$$\Rightarrow \theta\left(\widehat{s_1+s_2}\right)=\theta\left(\widehat{s_1}\right)+\theta\left(\widehat{s_2}\right)$$

$$\therefore \psi(s_1+s_2)=\theta\left(\widehat{s_1+s_2}\right)=\theta\left(\widehat{s_1}\right)+\theta\left(\widehat{s_2}\right)=\psi(s_1)+\psi(s_2)$$

For any $d \in \hat{s}_2^{-1}\left(s_1^{-1}R\right)$, consider $\widehat{s_1 s_2}(d)=s_1 s_2(d)$

$$=s_1(s_2 d)=\widehat{s_1}(s_2 d)=\widehat{s_1}\left(\widehat{s_2}(d)\right)=\left(\widehat{s_1}\,\widehat{s_2}\right)(d)$$

$\Rightarrow \widehat{s_1 s_2}$ and $\widehat{s_1}\,\widehat{s_2}$ agree c :he dense ideal $\hat{s}_2^{-1}\left(s_1^{-1}R\right)$

$$\Rightarrow \left(\widehat{s_1 s_2}\right)\theta\left(\widehat{s_1}\,\widehat{s_2}\right) \Rightarrow \theta\left(\widehat{s_1 s_2}\right)=\theta\left(\widehat{s_1}\,\widehat{s_2}\right)$$

$$\Rightarrow \theta\left(\widehat{s_1 s_2}\right)=\theta\left(\widehat{s_1}\right)\theta\left(\widehat{s_2}\right)$$

$$\therefore \psi(s_1 s_2)=\theta\left(\widehat{s_1 s_2}\right)=\theta\left(\widehat{s_1}\right)\cdot\theta\left(\widehat{s_2}\right)=\psi(s_1)\psi(s_2)$$

Similarly we can show that $\psi(-s)=-\psi(s)$ for all $s \in S$ and $\psi(1)=\theta\left(\bar{1}\right)$ and $\psi(0)=\theta\left(\bar{0}\right)$

$\therefore \psi$ is a ring homomorphism.

Now we will show that ψ is one - one.

Suppose $s \in S$ such that $\psi(s)=0$ in $Q(R)$

$$\Rightarrow \theta\left(\hat{s}\right)=\theta\left(\bar{0}\right) \Rightarrow \hat{s}\,\theta\,\bar{0} \Rightarrow \hat{s}=\bar{0} \text{ on } s^{-1}R$$

$$\Rightarrow s\left(s^{-1}R\right)=(0) \Rightarrow s=0 \;\left(\because \text{ for } 0 \neq x \in S.\ x\left(x^{-1}R\right) \neq (0)\right)$$

$$\therefore \psi(s)=0 \Rightarrow s=0$$

So ψ is one - one and hence ψ is a monomorphism.

For any $r \in R, r^{-1}R=R$. Then $r(d)=rd=\frac{r}{1}(d)$ for all $d \in R \Rightarrow \hat{r}$ and $\frac{r}{1}$ agree on R.

$$\Rightarrow \hat{r}\,\theta\frac{r}{1} \Rightarrow \theta\left(\hat{r}\right)=\theta\left(\frac{r}{1}\right)$$

$$\therefore \psi(r)=\theta\left(\hat{r}\right)=\theta\left(\frac{r}{1}\right)$$ for all $r \in R$.

Hence $\psi/_R : R \to Q(R)$ is the canonical monomorphism of R into $Q(R)$.

Thus ψ induces the canonical monomorphism of R into $Q(R)$.

So $(2) \Rightarrow (3)$

Assume (3) :i.e., there exists a monomorphism of S into $Q(R)$ which induces the canonical monomorphism of R into $Q(R)$. So we may assume that $R \subseteq S \subseteq Q(R)$. To show S is a ring of quotients of R, it is enough if we show that, for any $s \in S$, $s^{-1}R$ is dense in S.

Let $s \in S$. Then $s \in Q(R)$ and $s = \theta(f)$ for some fraction f defined on a dense ideal D of R. Then $D \subseteq s^{-1}R$. Now we will show that $s^{-1}R$ is dense in S. Suppose $t \in S$ such that $t\left(s^{-1}R\right) = (0)$. Then $t = \theta(f')$ for some $\theta(f') \in Q(R)$. Since $t\left(s^{-1}R\right) = (0)$, we have $\theta(f')\left(s^{-1}R\right) = (0) \Rightarrow \theta(f')D = (0)$. Then by remark 9.21, $\theta(f') = 0$ and hence $t = 0$.

Thus $t\left(s^{-1}R\right) = (0)$ for any $t \in S$ implies $t = 0$

$\therefore s^{-1}R$ is dense in S. Hence S is a ring of quotients of R.

So $(3) \Rightarrow (1)$

Corollary 9.26 : If S is a ring of quotients of the commutative ring R and D is a dense ideal of R, then D is dense in S.

Proof : Suppose S is a ring of quotients of the commutative ring R and D is a dense ideal of R. Since S is a ring of quotients of R, by theorem 9.25, there exists a monomorphism of S into $Q(R)$ which induces the canonical monomorphism of R into $Q(R)$. So we may assume that $R \subseteq S \subseteq Q(R)$.

Suppose $t \in S$ such that $tD=(0)$. Since $S \subseteq Q(R)$, $t=\theta(f)$ for some $\theta(f) \in Q(R)$ then $\theta(f)D=(0)$. By remark 9.21, $\theta(f)=0$ and hence $t=0$. Thus for $t \in S$, $tD=(0)$ implies $t=0$. Hence D is dense in S.

9.27 Theorem : Upto isomorphism over R, $Q(R)$ is the only rationally complete ring of quotients of the commutative ring R.

Proof : Let S be any ring of quotients of R such that S is rationally complete. Now we will show that $Q(R)=S$. Since S is a ring of quotients of R, by theorem 9.25, we may assume that $R \subseteq S \subseteq Q(R)$. Let $q \in Q(R)$. Put $D=\{s \in S / qs \in S\}$. Then $q^{-1}R \subseteq D$. We know that $q^{-1}R$ is a dense ideal of R. By corollary 9.26, $q^{-1}R$ is dense in S. Since $q^{-1}R \subseteq D$, D is dense in S. But D is an ideal of S. So D is a dense ideal of S.

Define $g : D \to S$ as $g(d)=qd$ for all $d \in D$. Then g is a fraction over S. Since S is rationally complete, by theorem 9.16, there exists $s \in S$ such that $g(d)=sd$ for all $d \in D$. Then $qd=sd$ for all $d \in D$. Since $q^{-1}R \subseteq D$ is dense in $Q(R)$, $qx=sx$ for all $x \in q^{-1}R$ implies that $q=s$. This implies $q \in S$. Since $q \in Q(R)$ is arbitrary, $Q(R) \subseteq S$. Consequently $S=Q(R)$. Thus $Q(R)$ is the only rationally complete ring of quotients of the commutative ring R.

Dr. V. SAMBASIVA RAO
Department of Mathematics
Acharya Nagarjuna University

Lesson : 10 RINGS OF QUOTIENTS OF COMMUTATIVE SEMI-PRIME RINGS

10.0 Introduction : In this lesson, it is proved that if R is a commutative ring then $Q(R)$ is regular if and only if R is semiprime. Also it is proved that the annihilator ideals in a commutative semiprime ring form a Boolean algebra. Further the lower subset ~~of an ordered~~ set is defined and it is proved that the lower sets of a Boolean algebra, regarded as a ring, are its annihilator ideals.

10.1 Definition : Let R be a commutative ring and K be a sub set of R. Then $K^* = \{r \in R \,/\, rK = (0)\}$ is called the annihilator of K.

10.2 Remark : K^* is an ideal of R.

10.3 Remark : An ideal K of R is dense if and only if $K^* = (0)$.

10.4 Remark : For any sub groups K_1 and K_2 of R,

$$(K_1 + K_2)^* = K_1^* \cap K_2^*$$

10.5 Lemma : For any ideal K in a commutative semi - prime ring R, we have $K \cap K^* = (0)$, $K + K^*$ is dense.

Proof : Let K be an ideal of a commutative ring R, First we show that $K \cap K^* = (0)$.

Consider $\left(K \cap K^*\right)^2 \subseteq K^* K = (0) \Rightarrow \left(K \cap K^*\right)^2 = (0)$

$\Rightarrow K \cap K^*$ is a nilpotent ideal of R.

Since R is semi-prime, by a known result, (0) is the only nilpotent ideal of $R \Rightarrow K \cap K^* = (0)$.

Next we will show that $K + K^*$ is dense.

Since K^* is an ideal of R, by the above proof, we have $K^* \cap K^{**} = (0)$. But

$$\left(K+K^{*}\right)^{*} = K^{*} \cap K^{**} \Rightarrow \left(K+K^{*}\right)^{*} = (0)$$

$\Rightarrow K+K^{*}$ is a dense ideal of R.

10.6 Theorem : If R is a commutative ring, then $Q(R)$ is regular if and only if R is semi-prime.

Proof : Let R be a commutative ring. Then $Q(R)$ is also a commutative ring.

Assume $Q(R)$ is regular. Since every commutative regular ring is semi primitive, $Q(R)$ is semiprimitive. Then $Rad(Q(R))=(0)$. Since $rad(Q(R)) \subseteq Rad(Q(R))$, we have $rad(Q(R))=(0) \Rightarrow Q(R)$ is semiprime $\Rightarrow R$ is semi prime.

Thus if $Q(R)$ is regular, then R is semiprime

conversely suppose that R is semiprime.

To show $Q(R)$ is regular, it is enough if we show that, for $\theta(f) \in Q(R)$, there exists $(f') \in Q(R)$ such that $\theta(f)\,\theta(f')\,\theta(f) = \theta(f)$. i.e., $\theta(f\,f'\,f) = \theta(f)$

i.e., $f\,f'\,f\,\theta\,f$.

Let $\theta(f) \in Q(R)$. Then f is a fraction with domain D, a dense ideal of R. Let K be the Kernel of f. Then $K \subseteq D$. Since R is semi-prime, by lemma 10.5, $K \cap K^{*} = (0)$.

$\Rightarrow D \cap K \cap K^{*} = (0) \Rightarrow$ The restriction of f to $D \cap K^{*}$ is a monomorphism.

Write $E = f\left(D \cap K^{*}\right)$. Then E is an ideal of R. By lemma 10.5, $E+E^{*}$ is a dense ideal of R.

Define $f' : E+E^{*} \longrightarrow R$ as follows.

Let $x \in E+E^{*}$. Then $x = f(d)+r$, where $f(d) \in f\left(D \cap K^{*}\right)$ and $r \in E^{*}$.

Define $f'(x) = d$. Then $f'(f(d)) = d$ and $f'(r) = 0$,

First we show that f' is well defined

Suppose $x_1 = f(d_1) + r_1$ and $x_2 = f(d_2) + r_2 \in E + E^*$ such that

$x_1 = x_2 \Rightarrow f(d_1) - f(d_2) = r_2 - r_1 \in E \cap E^* = (0)$

$\Rightarrow f(d_1) = f(d_2)$ and $r_1 = r_2$

$\Rightarrow d_1 = d_2$ ($\because f$ is a monomorphism on $D \cap K^*$)

$\Rightarrow f'(x_1) = f'(x_2)$

$\therefore f'$ is well defined.

It is easy to verify that f' is an R-homomorphism.

$\therefore f'$ is a fraction over $E + E^* \Rightarrow \theta(f') \in Q(R)$

By Lemma 10.5, $K + K^*$ is a dense ideal of R. Since $K + K^*$ and D are dense ideals of R, we have $D \cap (K + K^*)$ is a dense ideal of R. By modular law, $K + (D \cap K^*) = D \cap (K + K^*)$
$\Rightarrow K + (D \cap K^*)$ is a dense ideal of R.

For any $x = k + d \in K + (D \cap K^*)$, consider $f f' f(x)$

$$= f f' f(k+d) = f f'(f(k+d))$$

$$= f f'(f(k) + f(d)) = f f'(f(d))$$ ($\because k \in K$ and K is the kernal of f.)

$$= f(f'(f(d))) = f(d) = f(k) + f(d) = f(k+d) = f(x)$$

$\Rightarrow f f' f$ and f agree on the dense ideal $K + (D \cap K^*)$.

$$\Rightarrow f f' f \, \theta \, f \Rightarrow \theta(f f' f) = \theta(f) \Rightarrow \theta(f)\theta(f')\theta(f) = \theta(f)$$

Thus for $\theta(f) \in Q(R)$, there exists $\theta(f') \in Q(R)$ such that

$\theta(f)\theta(f')\theta(f)=\theta(f) \Rightarrow Q(R)$ is regular

Hence the theorem is proved.

10.7 Lemma : For any subsets K and J of a commutative ring R, we have

(1) $K \subseteq J \Rightarrow J^* \subseteq K^*$

(2) $K \subseteq K^{**}$

(3) $K^{***} = K^*$

Proof : (1) Suppose $K \subseteq J$

Let $x \in J^*$. Then $xJ=(0) \Rightarrow xK=(0)$ $(\because K \subseteq J)$

$\Rightarrow x \in K^*$

$\therefore J^* \subseteq K^*$

(2) Since $KK^* = K^*K=(0)$, we have $K \subseteq K^{**}$.

(3) By (2), $K \subseteq K^{**} \Rightarrow K^{***} \subseteq K^*$ (By (1))

Again by (2), $K^* \subseteq K^{***}$

$\therefore K^* = K^{***}$

10.8 Definition : Let R be a commutative ring. An ideal J of R is called an annihilator ideal of R if $J=K^*$ for some subset K of R.

Note that for each subset K of R, K^* is an annihilator ideal of R. If J is an annihilator ideal of R, by lemma 10.7, $J=J^{**}$

10.9 Theorem : The annihilator ideals in a commutative semi prime ring form a complete Boolean algebra $B^*(R)$, wtih intersection as inf and $*$ as complementation.

Proof : Let R be a commutative semi-prime ring and let $B^*(R)$ be the set of all annihilator ideals of R.

It is easy to verify that $B^*(R)$ is an ordered set under set inclusion [Here the ordering on $B^*(R)$ is defined as $A \le B$ if and only if $A \subseteq B$ for any $A, B \in B^*(R)$]. For any family $\{K_i / i \in I\}$ of subsets of R, it is easy to verify that $\bigcap_{i \in I} K_i^* = \left(\sum_{i \in I} K_i\right)^*$. Then the intersection of any family of annihilator ideals is again an annihilator ideal of R and it belongs to $B^*(R)$. Hence $B^*(R)$ is a complete semilattice with intersection as inf. To show $B^*(R)$ is a Boolean algebra, it is enough if we show that $J \cap K^* = (0)$ if and only if $J \subseteq K$ for any $J, K \in B^*(R)$. Let $J, K \in B^*(R)$. Suppose $J \subseteq K$. Then $J \cap K^* \subseteq K \cap K^* = (0) \Rightarrow J \cap K^* = (0)$.

So $J \subseteq K \Rightarrow J \cap K^* = (0)$

Conversely suppose that $J \cap K^* = (0)$

Consider $JK^* \subseteq J$ and $JK^* \subseteq K^* \Rightarrow JK^* \subseteq J \cap K^*$

$\Rightarrow JK^* = (0)$ $(\because J \cap K^* = (0))$

$\Rightarrow J \subseteq K^{**} = K$

So $J \cap K^* = (0) \Rightarrow J \subseteq K$

Hence $B^*(R)$ is a complete Boolean algebra.

10.10 Lemma : If M_R is an R-submodule of $Q(R)$ and if $q(M \cap R) = (0)$, $q \in Q(R)$, then $qM = (0)$

Proof : Let M be a right R-submodule of $Q(R)$ and $q \in Q(R)$ such that $q(M \cap R) = (0)$. Let $m \in M$. Then $D = m^{-1}R = \{r \in R / mr \in R\}$ is dense in $Q(R)$. Now $mD \subseteq M$ and $mD \subseteq R$ and so $mD \subseteq M \cap R$. Consider $qmD \subseteq q(M \cap R) = (0)$

$\Rightarrow qmD=(0) \Rightarrow qm=0$ ($\because D$ is dense in $Q(R)$).

Since $m \in M$ is arbitrary, $qM=(0)$.

10.11 Theorem : The mapping $K \longrightarrow K \cap R$ is an isomorphism of $B^*(Q(R))$ onto $B^*(R)$.

Proof : Let $B^*(R)$ be the lattice of all annihilator ideals of R and $B^*(Q(R))$ be the lattice of all annihilator ideals of $Q(R)$.

Define $\psi : B^*(Q(R)) \longrightarrow B^*(R)$ as

$\psi(K)=K \cap R$ for all $K \in B^*(Q(R))$

Claim : ψ is a Boolean isomorphism.

First we show that, for any $K \in B^*(Q(R))$, $K \cap R \in B^*(R)$. Let $K \in B^*(Q(R))$. Then K is annihilator ideal of $Q(R)$. This implies $K=K^{**}$. write $M=K^*$. Then M is an ideal of $Q(R)$ and consequently an R-submodule of $Q(R)$. Now we will show that $K \cap R=(M \cap R)^*$.

Let $r \in K \cap R$. Then $r \in K$ and $r \in R \Rightarrow r \in M^*$ and $r \in R \Rightarrow rM=(0)$ and $r \in R$.

Since $M \cap R \subseteq M$, we have $r(M \cap R)=(0)$

$\Rightarrow r \in (M \cap R)^*$

$\therefore K \cap R \subseteq (M \cap R)^*$

Conversely let $x \in (M \cap R)^*$. Then $x(M \cap R)=(0)$.

By lemma 10.10, $xM=(0) \Rightarrow x \in M^*$ and $x \in R$.

$\Rightarrow x \in M^* \cap R \Rightarrow x \in K \cap R$

$\therefore (M \cap R)^* \subseteq K \cap R$ and hence $K \cap R=(M \cap R)^* \Rightarrow K \cap R \in B^*(R)$

This show that for any $K \in B^*(Q(R))$, $\psi(K) \in B^*(R)$

Clearly ψ is well defined and $\psi(0)=0$.

For any $K_1, K_2 \in B^*(Q(R))$, $\psi(K_1 \cap K_2) = K_1 \cap K_2 \cap R$

$$=(K_1 \cap R) \cap (K_2 \cap R) = \psi(K_1) \cap \psi(K_2)$$

Next we will show that, for any $K \in B^*(Q(R))$, $\psi\left(K^*\right) = (\psi(K))^*$

i.e., $K^* \cap R = (K \cap R)^*$

Let $K \in B^*(Q(R))$. Then K is an annihilator ideal of $Q(R)$.

Let $x \in K^* \cap R \Rightarrow x \in K^*$ and $x \in R \Rightarrow xK = (0)$ and $x \in R$.

$\Rightarrow x(K \cap R) = (0)$ and $x \in R \Rightarrow x \in (K \cap R)^*$

$$\therefore K^* \cap R \subseteq (K \cap R)^*$$

Conversely suppose that $x \in (K \cap R)^* \Rightarrow x(K \cap R) = (0)$ and $x \in R$

$\Rightarrow xK = (0)$ and $x \in R$ (By Lemma 10.10)

$\Rightarrow x \in K^* \cap R$

$\therefore (K \cap R)^* \subseteq K^* \cap R$ and hence $K^* \cap R = (K \cap R)^*$

$$\Rightarrow \psi\left(K^*\right) = (\psi(K))^*$$

Hence ψ is a Boolean homomorphism.

Next we will show that ψ is one - one.

Suppose $K \in B^*(Q(R))$ such that $\psi(K) = (0) \Rightarrow K \cap R = (0)$

Since $K \in B^*(Q(R))$, we have $K = M^*$ where $M = K^*$

Then $K \cap R = (M \cap R)^* \Rightarrow (M \cap R)^* = (0)$.

If possible suppose that $K \neq (0)$. Choose $r \in K$ such that $r \neq 0$. Then

$$r \in M^* \Rightarrow rM = (0) \Rightarrow r(M \cap R) = (0)$$

$$\Rightarrow r \in (M \cap R)^* \Rightarrow (M \cap R)^* \neq (0)$$; a controdiction.

So, $K = (0)$. Thus $\psi(K) = (0) \Rightarrow K = (0)$.

Hence ψ is one - one.

Next we will show that ψ is onto

Let $I \in B^*(R)$. Then $I = J^*$ for some $J \subseteq R$.

Write $K = \{q \in Q(R) / qJ = (0)\}$ Then K is an annihilator ideal of $Q(R)$. Now we show that $J^* = K \cap R$. Consider $x \in J^* \Leftrightarrow xJ = (0)$ and $x \in R \Leftrightarrow x \in K$ and $x \in R \Leftrightarrow x \in K \cap R$.

$$\therefore J^* = K \cap R$$

Consider $\psi(K) = K \cap R = J^* = I$

Hence ψ is onto.

Thus ψ is an isomorphism of $B^*(Q(R))$ onto $B^*(R)$.

10.12 Theorem : If R is commutative semiprime and rationally complete, every annihilator ideal of R is a direct summand.

Proof : Let R be a commutative semiprime and rationally complete ring and K be an annihilator ideal of R.

Since R is a commutative semiprime ring, by lemma 10.5, $K + K^*$ is a dense ideal of R.

Define $f: K + K^* \longrightarrow R$ as $f(a+b) = a$ for all $a+b \in K + K^*$, where $a \in K$ and $b \in K^*$. It is easy to verify that f is an R-homomorphism and so f is a fraction over R. For any $a \in K$, $f(a) = a$

and for any $b \in K^*$, $f(b)=0$. Since $K+K^*$ is dense and since R is rationally complete, by theorem 9.16, there exists an element $e \in R$ such that $f(a+b)=e(a+b)$ for all $a+b \in K+K^*$ $\Rightarrow a=e(a+b)$ for all $a+b \in K+K^*$ and $f(a)=ea$ for all $a \in K$. For any $a+b \in K+K^*$, consider $a=f(a+b)=e(a+b)$.

$$\Rightarrow e^2(a+b)=ee(a+b)=ea=f(a)=a=e(a+b)$$

$$\Rightarrow \left(e^2-e\right)(a+b)=0 \text{ for all } a+b \in K+K^*$$

$$\Rightarrow \left(e^2-e\right)\left(K+K^*\right)=(0) \Rightarrow e^2-e=0 \qquad (\because K+K^* \text{ is dense})$$

$$\Rightarrow e = e^2$$

Since $a=f(a)=ea$ for any $a \in K$, we have $K \subseteq eK$. Clearly $eK \subseteq K$. So $K=eK \subseteq eR$.

Since $f(a+b)=e(a+b)$ for any $a+b \in K+K^*$, we have $f(b)=eb$ for all $b \in K^*$. Since $f(b)=0$ for any $b \in K^*$ we have $eb=0$ for all $b \in K^*$

$$\Rightarrow (1-e)K^* = K^*$$

$$\therefore K^* = (1-e)K^* \subseteq (1-e)R$$

We know that $eR \oplus (1-e)R=R \Rightarrow eR \cap (1-e)R=(0)$

$$\Rightarrow eR(1-e)R=(0) \Rightarrow eR \subseteq ((1-e)R)^* \subseteq K^{**} \quad \left(\because K^* \subseteq (1-e)R\right)$$

$$\Rightarrow eR \subseteq K^{**} = K \qquad (\because K \text{ is an annihilator ideal})$$

$\therefore K=eR$ and hence K is a direct summand of R.

10.13 Corollary : If R is commutative semi prime and rationally complete, then $B^*(R) \cong B(R)$, the Boolean algebra of central idempotents of R.

Proof : Let R be a commutative semi prime and rationally complete ring. Then $B^*(R)$, the family of all annihilator ideals of R, is a Boolean algebra and $B(R)$, the set of all central idempotents of R, is a Boolean algebra.

Define $\psi : B(R) \longrightarrow B^*(R)$ as $\psi(e) = eR$ for all $e \in B(R)$.

Since $R = eR \oplus (1-e)R$ for any $e \in B(R)$, we have $eR \cap (1-e)R = (0) \Rightarrow eR(1-eR) = (0)$

$\Rightarrow eR = ((1-e)R)^*$ for any $e \in B(R)$

$\Rightarrow eR$ is an annihilator ideal of R and hence $eR \in B^*(R)$ for all $e \in B(R)$.

Now we will show that ψ is an isomorphism.

Clearly $\psi(0) = 0$.

For any $e, f \in B(R)$, $\psi(ef) = efR = eR \cap fR = \psi(e) \cap \psi(f)$

Let $e \in B(R)$. Then $1-e$ is the complement of e.

Consider $\psi(e') = \psi(1-e) = (1-e)R = (eR)^* = (\psi(e))^*$

$\therefore \psi(e') = (\psi(e))^*$ for any $e \in B(R)$

Thus ψ is a Boolean homomorphism.

Next we will show that ψ is one-one.

Suppose $e, f \in B(R)$ such that $\psi(e) = \psi(f)$

$\Rightarrow eR = fR$

Since $e \in eR$, we have $e \in fR \Rightarrow e = fr$ for some $r \in R$.

Similarly $f = es$ for some $s \in R$.

Consider $e = fr = f\,f\,r$ $\quad$ ($\because f$ is an idempotent)

$= f\,e = e\,f = e\,e\,s = e\,s = f$

$\Rightarrow e = f$

$\therefore \psi(e) = \psi(f) \Rightarrow e = f$

So ψ is one - one.

Next we will show that ψ is onto.

Let $K \in B^*(R)$. Then K is an annihilator ideal of R. Then by the above theorem, K is a direct summand of R. This implies there exists an idea J of R such that $R=K+J$ and $K \cap J=(0)$. Now $1 \in K+J \Rightarrow 1=e+f$ for some $e \in K$ and $f \in J$. For any $x \in K$ and $y \in J$, $xy \in K \cap J$. Then $xy=0$. Now $1-e=f \in J$.

Consider $e(1-e)=ef=0 \Rightarrow e^2=e \Rightarrow e$ is an idempotent. Clearly $eR \subseteq K$.

Let $x \in K$. Consider $(1-e)x=fx=0 \Rightarrow x=ex \in eR$

$\therefore K \subseteq eR$ and hence $K=eR$

Now consider $\psi(e)=eR=K \Rightarrow \psi$ is onto.

Hence $\psi : B(R) \to B^*(R)$ is an isomorphism.

10.14 Corollary : If R is commutative semi prime, then $B^*(R) \cong B^*(Q(R)) \cong B(Q(R))$.

Proof : Let R be a commutative semiprime ring. Then by theorem 10.6, $Q(R)$ is regular. Since $Q(R)$ is a commutative, regular ring, by a known theorem, $Q(R)$ is semiprimitive and hence $Q(R)$ is semiprime. By theorem 9.20, $Q(R)$ is rationally complete. Since $Q(R)$ is commutative semiprime and rationally complete, by corollary 10.13, $B^*(Q(R)) \cong B(Q(R))$. Also by theorem 10.11, $B^*(R) \cong B^*(Q(R))$. Hence $B^*(R) \cong B^*(Q(R)) \cong B(Q(R))$.

10.15 Lemma : If R is a Boolean ring, then $Q(R)$ is a Boolean ring.

Proof : Let R be a Boolean ring. Let $\theta(f) \in Q(R)$. Then $f \in Hom_R(D, R)$ for some dense ideal D of R. Then f^2 is defined on D^2 and $D=D^2$ ($\because$ R is a Boolean ring).

For any $d \in D$, consider $f^2(d)=f(f(d))=f(f(d.\,d))$

$$=f(f(d)\,d) \qquad (\because f \in Hom_R(D, R))$$

$= f(d)f(d) \qquad (\because f \in Hom_R(D,R))$

$= (f(d))^2 = f(d) \qquad (\because R$ is a Boolean ring).

$\Rightarrow f^2(d) = f(d)$ for all $d \in D$

$\Rightarrow f^2 \theta f \Rightarrow \theta(f^2) = \theta(f) \Rightarrow \theta(f)\theta(f) = \theta(f)$

$\therefore Q(R)$ is a Boolean ring.

Hence the theorem.

Let $(S,\leq)$ be any ordered set. With any subset X of S, we associate X^V = the set of all upper bounds of X and $X^\wedge$ = the set of all lower bounds of X. Write $(X^\vee)^\wedge = X^{\vee\wedge}$ and $(X^\wedge)^\vee = X^{\wedge\vee}$

10.16 Lemma : Let $(S,\leq)$ be an ordered set and X, Y be subsets of S. Then

(1) $X \subseteq Y \Rightarrow Y^\vee \subseteq X^\vee$ and $Y^\wedge \subseteq X^\wedge$

(2) $X \subseteq X^{\vee\wedge}$ and $X \subseteq X^{\wedge\vee}$

(3) $X^{\vee\wedge\vee} = X^\vee$ and $X^{\wedge\vee\wedge} = X^\wedge$

Proof : Given that $(S,\leq)$ is an ordered set and X and Y are subsets of S

(1) Suppose $X \subseteq Y$

Let $z \in Y^\vee$. Then z is an upper bound of $Y \Rightarrow y \leq z$ for all $y \in Y$. $\Rightarrow x \leq z$ for all $x \in X$ $(\because X \subseteq Y) \Rightarrow z$ is an upper bound of X.

$\Rightarrow z \in X^\vee$

$\therefore Y^\vee \subseteq X^\vee$

Similarly we can show that $Y^{\wedge} \subseteq X^{\wedge}$

(2) Let $x \in X$. Since every element in $X^{\vee}$ is an upper bound of X, we have $x \leq z$ for all $z \in X^{\vee} \Rightarrow x$ is a lower bound of $X^{\vee} \Rightarrow x \in X^{\vee\wedge}$

Since $x \in X$ is arbitrary, we have $X \subseteq X^{\vee\wedge}$

Similarly we can show that $X \subseteq X^{\wedge\vee}$

(3) From (2), we have $X^{\vee} \subseteq X^{\vee\wedge\vee}$

Again from (2), $X \subseteq X^{\vee\wedge}$. Then from (1), we have

$$X^{\vee\wedge\vee} \subseteq X^{\vee}$$

$$\therefore X^{\vee\wedge\vee} = X^{\vee}$$

Similarly we can show that $X^{\wedge\vee\wedge} = X^{\wedge}$

10.17 Remark : From lemma 10.16, it is easy to verify that $\vee\wedge$ and $\wedge\vee$ are closure operations on the set of all subsets of S.

10.18 Definition : Let $(S, \leq)$ be an ordered set. A sub set Y of S is called a lower set if $Y = X^{\wedge}$ for some subset X of S.

10.19 Remark : By (3) of lemma 10.16, $Y = Y^{\vee\wedge}$

10.20 Theorem : The lower sets of $(S, \leq)$ form a complete lattice $D(S)$. The canonical mapping $\mu : S \longrightarrow D(S)$ defined by $\mu(x) = \{x\}^{\vee\wedge}$ has the property that $x \leq y$ iff $\mu(x) \subseteq \mu(y)$ for any $x, y \in S$; thus $(D(S), \subseteq)$ may be regarded as an extension of $(S, \leq)$. Moreover each element of $D(S)$ is the sup and inf of subsets of $\mu(S)$.

Proof : Let $(S, \leq)$ be an ordered set and $D(S)$ be the set of all lower sets of S. Clearly $D(S)$ is an ordered set under set inclusion.

Let $\{Y_\alpha\}_{\alpha \in \Delta}$ be any sub class of $D(S)$

Claim : $\bigcap_{\alpha\in\Delta} Y_\alpha \in D(S)$

Since each Y_α is a lower set of S, we have $Y_\alpha = Y_\alpha^{\vee\wedge}$ for all $\alpha\in\Delta$. By Lemma 10.16,

$\bigcap_{\alpha\in\Delta} Y_\alpha \subseteq \left(\bigcap_{\alpha\in\Delta} Y_\alpha\right)^{\vee\wedge}$

Suppose $x\in\left(\bigcap_{\alpha\in\Delta} Y_\alpha\right)^{\vee\wedge} \Rightarrow x\le y$ for all $y\in\left(\bigcap_{\alpha\in\Delta} Y_\alpha\right)^{\vee}$

Fix $\beta\in\Delta$. Then each upper bound of Y_β is an upper bound of $\bigcap_{\alpha\in\Delta} Y_\alpha \Rightarrow x$ is a lower bound of $Y_\beta^{\vee}$

$\Rightarrow x\in Y_\beta^{\vee\wedge} = Y_\beta$

Since $\beta\in\Delta$ is arbitrary, we have $x\in \bigcap_{\alpha\in\Delta} Y_\alpha$

$\therefore \left(\bigcap_{\alpha\in\Delta} Y_\alpha\right)^{\vee\wedge} \subseteq \bigcap_{\alpha\in\Delta} Y_\alpha$ and hence $\bigcap_{\alpha\in\Delta} Y_\alpha = \left(\bigcap_{\alpha\in\Delta} Y_\alpha\right)^{\vee\wedge}$

$\Rightarrow \bigcap_{\alpha\in\Delta} Y_\alpha \in D(S)$

Clearly $\bigcap_{\alpha\in\Delta} Y_\alpha$ is the infimum of $\{Y_\alpha\}_{\alpha\in\Delta}$

Also clearly S is the greatest element in $D(S)$. So $D(S)$ is a complete lattice.

Define $\mu : S \longrightarrow D(S)$ as $\mu(x) = \{x\}^{\vee\wedge}$ for all $x\in S$.

Clearly μ is a mapping.

First we show that $x\le y$ if and only if $\mu(x)\le\mu(y)$ for any $x, y\in S$.

Let $x, y\in S$

Suppose $x \leq y$. Then $\{y\}^{\vee} \subseteq \{x\}^{\vee} \Rightarrow \{x\}^{\vee\wedge} \subseteq \{y\}^{\vee\wedge}$

$\Rightarrow \mu(x) \subseteq \mu(y)$

Conversely suppose that $\mu(x) \subseteq \mu(y)$

$\Rightarrow \{x\}^{\vee\wedge} \subseteq \{y\}^{\vee\wedge} \Rightarrow \{y\}^{\vee\wedge\vee} \subseteq \{x\}^{\vee\wedge\vee}$

$\Rightarrow \{y\}^{\vee} \subseteq \{x\}^{\vee} \Rightarrow$ for $t \in S$, $y \leq t$ implies that $x \leq t$.

Since $y \leq y$, we have $x \leq y$.

So $\mu(x) \subseteq \mu(y) \Rightarrow x \leq y$

Thus for any $x, y \in S$, $x \leq y$ if and only if $\mu(x) \subseteq \mu(y)$.

Now we will show that μ is one - one

Suppose $x, y \in S$ such that $\mu(x) = \mu(y) \Rightarrow \{x\}^{\vee\wedge} = \{y\}^{\vee\wedge}$

$\Rightarrow \{x\}^{\vee\wedge\vee} = \{y\}^{\vee\wedge\vee} \Rightarrow \{x\}^{\vee} = \{y\}^{\vee}$ (By lemma 10.16)

$\Rightarrow x = y$

$\therefore \mu$ is one-one. Hence $(D(S), \subseteq)$ is an extension of $(S, \leq)$.

Next we will show that for $X \in D(S)$, X is the supremum of some subset of μS and X is the infimum of some subset of μS.

Let $X \in D(S)$. Then X is a lower set of $S \Rightarrow X = X^{\vee\wedge}$.

First we will show that $X = \sup\{\mu(s) \,/\, \mu(s) \subseteq X\}$.

Clearly X is an upper bound of $\{\mu(s) / \mu(s) \subseteq X\}$

For any $s \in S$, $\mu(s) \subseteq X$

$\Rightarrow \{s\}^{\vee\wedge} \subseteq X$

$\Rightarrow s \in X \qquad \left(\because s \in \{s\}^{\vee\wedge}\right)$ -------- (1)

Suppose $Y \in D(S)$ such that Y is an upper bound of $\{\mu(s) / \mu(s) \subseteq X\}$ Then for any $s \in S$, $\mu(s) \subseteq X \Rightarrow \mu(s) \subseteq Y$. That is, for any $s \in S, s \in X \Rightarrow s \in Y$.

$\therefore X \subseteq Y$. Thus $X = \sup\{\mu(s) / \mu(s) \subseteq X\}$

Next we will show that $X = Inf\{\mu(s) / X \subseteq \mu(s)\}$

Clearly X is a lower bound of $\{\mu(s) / X \subseteq \mu(s)\}$

For any $s \in S$, $X \subseteq \mu(s) \Rightarrow X \subseteq \{s\}^{\vee\wedge} \Rightarrow \{s\}^{\vee} \subseteq X^{\vee}$

$\Rightarrow$ for $t \in S$, $s \leq t$ implies $t \in X^{\vee}$

Since $s \leq s$, we have $s \in X^{\vee}$.

Also if $s \in X^{\vee}$ and $s \leq t$, then $t \in X^{\vee}$ $\quad$ ($\because \leq$ is transitive)

$\therefore X \subseteq \mu(s)$ if and only if $s \in X^{\vee}$ for any $s \in S$ ----------- (2)

Suppose Y is a lower bound of $\{\mu(s) / X \subseteq \mu(s)\}$. Then $X \subseteq \mu(s) \Rightarrow Y \subseteq \mu(s)$.

i.e., $s \in X^{\vee} \Rightarrow s \in Y^{\vee}$ (by (2))

This shows that $X^{\vee} \subseteq Y^{\vee} \Rightarrow Y^{\vee\wedge} \subseteq X^{\vee\wedge} \Rightarrow Y \subseteq X$ ($\because X$ and Y are lower sets of S).

$\therefore X$ is infimum of $\{\mu(s) / X \subseteq \mu(s)\}$

10.21 Remark : $D(S)$ is called the Dedekind - Mac Neille completion of S.

10.22 Theorem : The lower sets of a Boolean algebra, regarded as a ring R, are its annihilator ideals, that is $D(R) = B^{*}(R)$

Proof : Let R be a Boolean algebra. Then R is a Boolean ring and the ordering $\leq$ on R is $a \leq b$ if and only if $a = ab$.

Let K be any subset of R. Now we will show that for any $r \in R$, $r \in K^{\vee}$ if and only if $1-r \in K^{*}$.

Let $r \in R$. Suppose $r \in K^{\vee}$ if and only if r is an upper bound of K if and only if $k \leq r$ for all $k \in K$ if and only if $k = kr$ for all $k \in K$ if and only if $k(1-r)=0$ for all $k \in K$ if and only if $1-r \in K^{*}$

$\therefore r \in K^{\vee}$ if and only if $1-r \in K^{*}$

Next we will show that $x \in K^{*}$ if and only if $1-x \in K^{\vee}$.

Consider $x \in K^{*}$ if and only if $xk=0$ for all $k \in K$

if and only if $(1-x)k=k$ for all $k \in K$ if and only if $1-x \in K^{\vee}$

$\therefore x \in K^{*}$ if and only if $1-x \in K^{\vee}$

Now we will show that $K^{**} = K^{\vee\wedge}$

Let $s \in K^{**} \Rightarrow sl=0$ for all $l \in K^{*}$ --------- (1)

For any $x \in K^{\vee}$, $1-x \in K^{*}$. Then by (1), $s(1-x)=0$ for any $x \in K^{\vee} \Rightarrow s \leq x$ for any $x \in K^{\vee} \Rightarrow s \in K^{\vee\wedge}$

$\therefore K^{**} \subseteq K^{\vee\wedge}$

Conversely let $r \in K^{\vee\wedge} \Rightarrow r$ is a lower bound of $K^{\vee}$.

$\Rightarrow r \leq x$ for any $x \in K^{\vee}$ ------- (2)

For any $y \in K^{*}$, $1-y \in K^{\vee}$. Then by (2), for any $y \in K^{*}$,

$r \leq 1-y \Rightarrow r = r(1-y)$ for any $y \in K^{*}$

$\Rightarrow r = r - ry$ for any $y \in K^{*}$

$\Rightarrow ry=0$ for any $y \in K^{*} \Rightarrow r \in K^{**}$

$K^{\vee\wedge} \subseteq K^{**}$ and hence $\therefore K^{\vee\wedge} = K^{**}$

Suppose $K \in D(R)$ if and only if K is a lower set of R, if and only if $K = K^{\vee\wedge}$ if and only if $K = K^{**}$ if and only if K is an annihilator ideal of R if and only if $K \in B^*(R)$.

Hence $B^*(R) = D(R)$

10.23 Corollary : If R is a Boolean ring, then its Dedekind - Mac Neille completion is isomorphic over R to its complete ring of quotients.

Proof : Let R be a Boolean ring. Then R is a commutative semiprime ring. By corollary 10.14, $B^*(R) \cong B^*(Q(R)) \cong B(Q(R))$. Since R is a Boolean ring, $Q(R)$ is also a Boolean ring. Then $B(Q(R)) = Q(R)$. Since R is a Boolean ring, R is also a Boolean algebra. Then by theorem 10.22, $D(R) = B^*(R)$. Hence $D(R) \cong Q(R)$.

Dr. V. SAMBASIVA RAO
Department of Mathematics
Acharya Nagarjuna University

Lesson - 11 Prime Ideal Spaces

11.0 Introduction : In this lesson, the properties of the topological space of all prime ideals of a commutative ring are studied. If π is a prime ideal space of a commutative ring R such that $\Delta\pi=(0)$, then it is proved that the complete Boolean algebra of annihilator ideals of R is isomorphic to the complete Boolean algebra of regular open subsets of π. Further it is proved that a Boolean algebra is isomorphic to the algebra of all subsets of a set if and only if it is complete and atomic.

A topological space is a system (X,T) where T is a set of subsets of X which is closed under union and finite intersection. The elements of T are called open sets. Thus we have the following:

1. Any union of open sets is open (In particular, the empty set is open).
2. If V_1 and V_2 are open, so is $V_1 \cap V_2$.
3. X is open.

A topological space is called compact if any family of open sets which covers the space contains a finite sub family which already covers the space. A set is called closed if its complement is open. The closure of a set is the intersection of all closed sets containing it.

Throught this lesson π denotes the set of all prime ideals of a commutative ring R unless otherwise stated.

11.1 Definition : Let R be a commutative ring. For any subset A of R, define $\Gamma(A)=\{P\in\pi / A\not\subseteq P\}$.

11.2 Remark : $\Gamma(A)=\Gamma(A')$, Where A' is the intersection of all prime ideals of R containing A, hence an ideal of R. Thus for each subset A of R, there exists an ideal B of R such that $\Gamma(A)=\Gamma(B)$.

11.3 Theorem : π becomes a topological space, if as open sets we take all sets of the form $\Gamma(A)=\{P\in\pi \ / \ A\not\subseteq P\}$, where A is any subset of R. If π contains all maximal ideals, then π is commpact.

Proof : Let R be a commutative ring, and π be the set of all prime ideals of R.

Write $T=\{\Gamma(A) / A\subseteq R\}$.

By remark 11.2, $T = \{\Gamma(A) / A \text{ is an ideal of } R\}$.

Claim : T is a topology on π.

Let $\{\Gamma(Ai) / i \in I\}$ be any sub family of T.

Consider $\underset{i \in I}{U} \Gamma(A_i) = \{P \in \pi \,/\, A_i \not\subseteq P \text{ for some } i \in I\}$

$$= \left\{P \in \pi / \sum_{i \in I} A_i \not\subseteq P\right\} = \Gamma\left(\sum_{i \in I} A_i\right)$$

$\therefore \underset{i \in I}{U} \Gamma(Ai) \in T$

So T is closed under arbitrary unions.

Let $\Gamma(A),\ \Gamma(B) \in T$.

Consider $\Gamma(A) \cap \Gamma(B) = \{P \in \pi / A \not\subseteq P \text{ and } B \not\subseteq P\}$

$$= \{P \in \pi / AB \not\subseteq P\} = \Gamma(AB)$$

$\therefore \Gamma(A) \cap \Gamma(B) \in T$ This shows that T is closed under finite intersections.

Consider $\Gamma(\{o\}) = \{P \in \pi / O \notin P\} = \phi$.

$\therefore \phi \in T$

Consider $\Gamma(R) = \{P \in \pi / R \not\subseteq P\} = \pi$

$\therefore \pi \in T$.

So T is a topology on π and hence (π, T) is a topological space.

Suppose π is the class of all maximal ideals of R.

Then $(\pi . T)$ is a topological space.

Now we will show that π is compact.

Suppose $\{\Gamma(Ai) / i \in I\}$ is an open conver for π. Then $\pi = \underset{i \in I}{U} \Gamma(A_i) = \Gamma\left(\sum_{i \in I} A_i\right) \Rightarrow \sum_{i \in I} A_i$ is contained in no maximal ideal of R and so $1 \in \sum_{i \in I} A_i$.

$\Rightarrow 1 = a_{i_1} + a_{i_2} + \ldots\ldots\ldots\ldots + a_{i_n}$ for some $a_{i_j} \in A_{i_J}$ where $1 \le J \le n$

$$\Rightarrow R = \sum_{j=1}^{n} A_{ij} \Rightarrow \pi = \Gamma(R) = \Gamma\left(\sum_{j=1}^{n} A_{ij}\right) = \bigcup_{j=1}^{n}\left(A_{ij}\right)$$

$\Rightarrow \pi$ is compact.

11.4 Remark : For any subset A of R, $\Gamma(A) = \bigcup_{a \in A} \Gamma(a)$, thus the sets $\Gamma(a)$ form a basis of the open sets of π, in the sense that they are open and every open set is a union of basic open sets.

11.5 Remark : Γ is a mapping from the set of subsets of R into the set of subsets of π.

11.6 Definition : For any sub set V of π, define $\Delta V = \bigcap_{P \in V} P$

11.7 Renark : $\Delta\pi$ is the prime radical of R, depending on whether π is the set of all prime ideals or only of all maximal ideals of R.

11.8 Remark : Δ is a mapping from the set of all subsets of π into the set of subsets of R.

11.9 Definition : Let V be a sub set of a topological space X. The union of all open sub sets of X contained in V is called the interior of V. The interior of the complement of V is called the exterior of V.

11.10 Remark : We denote the interior of V by Int (V) and the exterior of V by Ext(V).

11.11 Theorem : For any sub set V of π, $\Gamma \Delta V$ is the exterior of V. If $\Delta\pi = 0$, then for any subset A of R, $\Delta \Gamma A$ is the annihilator A^* of A.

Proof: Let V be a subset of π.

Consider $Q \in \Gamma\Delta V \Leftrightarrow \Delta V \not\subseteq Q \Leftrightarrow$ there exists $r \in R$ such that $r \in P$ for all $P \in V$ and $r \notin Q \Leftrightarrow Q \in \Gamma(r)$ and $P \notin \Gamma(r)$ for all $P \in V$ and this means that there exists a basic open set $\Gamma(r)$ containing Q and $\Gamma(r) \cap V = \phi \Leftrightarrow Q \in \Gamma(r) \subseteq V'$, which is the complement of V $\Leftrightarrow Q \in Int(V') \Leftrightarrow Q \in Ext(V)$.

Thus $\Gamma \Delta V = Ext(V)$

Suppose $\Delta\pi=(0)$. Now we will show that $\Delta\Gamma A=A^*$, the annihilator of A, for any subset A of R.

Let A be a subset of R.

Suppose $r\in\Delta\Gamma A \Rightarrow r\in P$ for all $P\in\Gamma(A)$.

$\Rightarrow r\in P$ for all $P\in\pi$ such that $A\not\subseteq P$.

$\Rightarrow$ for all $P\in\pi$, $A\not\subseteq P$ implies $r\in P$.

$\Rightarrow rA\subseteq P$ for all $P\in\pi \Rightarrow rA\subseteq\Delta\pi \Rightarrow rA=(0)$ $(\because \Delta\pi=0)$

$\Rightarrow r\in A^*$

$\therefore\ \Delta\Gamma A\subseteq A^*$

Conversely suppose that $r\in A^* \Rightarrow rA=(0)\Rightarrow rA\subseteq\Delta\pi$

$\Rightarrow rA\subseteq P$ for all $P\in\pi$

$\Rightarrow$ for $p\in\pi$, $A\not\subseteq P$ implies $r\in P$

$\Rightarrow r\in P$ for all $P\in\Gamma(A)$

$\Rightarrow r\in\Delta\Gamma A$

$\therefore\ A^*\subseteq\Delta\Gamma A$ and hence $\Delta\Gamma A=A^*$

11.12 Definition : A subset A of a topological space X is called a regular open set if A is the interior of $\overline{A}$, where $\overline{A}$ is the closure of A.

Remark 11.13: Let A be a subset of a topological space X. Then A is a regular open set if and only if A is the interior of some closed set if and only if A is the exterior of some open set.

For, let A be a subset of a topological space X. Suppose A is a regular open set. Then by definition, A is the interior of $\overline{A}$. Since $\overline{A}$ is closed, we have A is the interior of the closed set $\overline{A}$. So A is the interior of some closed set. Conversely suppose that A is the interior of B for some closed subset B of X. Then $A\subseteq B\Rightarrow\overline{A}\subseteq B$.

$\Rightarrow Int\left(\overline{A}\right)\subseteq Int\,(B)$

$\Rightarrow Int\left(\overline{A}\right) \subseteq A\ (\because\ A = Int(B))$

Since $A \subseteq \overline{A}$, we have $Int\,(A) \subseteq Int\left(\overline{A}\right)$.

Since A is the interior of B, which is an open set, we have $A = Int(A)$.

$\therefore Int(A) \subseteq Int\left(\overline{A}\right) \Rightarrow A \subseteq Int\left(\overline{A}\right)$

So $A = Int\left(\overline{A}\right)$ and hence A is a regular open set.

Thus A is a regular open set if and only if A is the interior of some closed set.

Next we will show that A is the interior of some closed set if and only if A is the exterior of some open set.

Suppose A is the interior of some closed set B.

Write $C = B'$. Then C is an open set and A is the interior of the complement of C. So A is the exterior of the open set C.

Conversely suppose that A is the exterior of some open set G. Then by definition, A is the interior of the complement of G. Since G is open, Complement of G is closed. Hence A is the interior of some closed set. Thus A is the interior of some closed set if and only if A is the exterior of some open set G.

11.14 Problem : For any subset E of topological space X, $(Int(E))' = \overline{E'}$

Solution : Let E be a subset of a topological space X.

Consider $x \in (Int(E))' \Leftrightarrow x \notin Int(E) \Leftrightarrow$ for every open set G containing x, $G \not\subseteq E \Leftrightarrow$ For every open set G containing x, there exists $y \in G$ such that $y \notin E \Leftrightarrow$ for every open set G containing x, $G \cap E' \neq \phi \Leftrightarrow x \in \overline{E'}$

$\therefore (Int(E))' = \overline{E'}$

11.15 Problem : Show that the interior of any closed set is the interior of its own closure.

Solution : Let X be a topological space and A be a closed subset of X.

Claim: $Int(A) = Int\left(\overline{Int(A)}\right)$

Suppose $x \in Int\left(\overline{Int(A)}\right) \Rightarrow$ there exists an open set G

such that $x \in G \subseteq \overline{Int\,(A)} \subseteq \overline{A} = A$ ($\because A$ is closed)

$\Rightarrow x \in G \subseteq A \Rightarrow x$ is an interior point of $A \Rightarrow x \in Int(A)$

$\therefore Int\left(\overline{Int(A)}\right) \subseteq Int(A)$

Clearly $Int(A) \subseteq \overline{Int(A)}$

Since $Int\left(\overline{Int(A)}\right)$ is the largest open set contained in $\overline{Int\,(A)}$ and since $Int(A)$ is an open set contained in $\overline{Int(A)}$, we have $Int\,(A) \subseteq Int\left(\overline{Int(A)}\right)$.

$\therefore Int(A) = Int\left(\overline{Int\,(A)}\right)$

11.16 Problem : If A is a regular open subset of a topological space X, then show that $Ext(Ext(A)) = A$.

Solution : Let A be a regular open subset of topological space X. Then $A = Int\left(\overline{A}\right)$.

Consider $Ext\,(Ext(A)) = Ext(Int(A')) = Int\left((Int(A'))'\right)$

$= Int\left(\overline{(A')}'\right)$ (By problem 11.14)

$= Int\left(\overline{A}\right) = A$

Thus $Ext(Ext(A)) = A$.

11.17 Problem : Prove that the regular open sets in any topological space form a Boolean algebra.

Solution : Let X be a topological space and $\mathscr{H}$ be the set of all regular open sets in X.

Claim : $\mathcal{H}$ is a Boolean algebra.

Colearly $\mathcal{H}$ is an ordered set under set inclusion.

Let A, $B \in \mathcal{H}$. The $A = Int\left(\overline{A}\right) and\ B = Int\left(\overline{B}\right)$

$\Rightarrow A \cap B = Int\left(\overline{A}\right) \cap Int\left(\overline{B}\right) = Int\left(\overline{A} \cap \overline{B}\right)$.

$\therefore A \cap B = Int\left(\overline{A} \cap \overline{B}\right)$ and $\overline{A} \cap \overline{B}$ is a closed set.

By remark 11.13, $A \cap B$ is a regular open set. So $A \cap B \in \mathcal{H}$

Define $*$ on $\mathcal{H}$ as $A^* = Ext(A)$ for any $A \in \mathcal{H}$.

Let $A \in \mathcal{H}$. Since every regular open set is an open set, A is an open set.

Consider $A^* = Ext(A) = Int(A')$, which is interior of the closed $A' \Rightarrow A^*$ is a regular open set (By remark 11.13)

$\Rightarrow A^* \in \mathcal{H}$

$\therefore$ $*$ is a unary operation on $\mathcal{H}$.

Since $\phi = Int\left(\overline{\phi}\right)$ and $X = Int\left(\overline{X}\right)$, we have ϕ , $X \in \mathcal{H}$..

Next we will show that $A \cap B^* = \phi \Leftrightarrow A \subseteq B$ for any A, $B \in \mathcal{H}$.

Let A, $B \in \mathcal{H}$. Suppose $A \cap B^* = \phi \Rightarrow A \cap Ext(B) = \phi$.

$\Rightarrow A \cap Int(B') = \phi \Rightarrow A \subseteq \left(Int(B')\right)' = \overline{(B')}'$ (By problem 11.14)

$\Rightarrow A \subseteq \overline{B}$

Since A is an open set and $Int\left(\overline{B}\right)$ is the largest open set contained in $\overline{B}$, we have $A \subseteq Int\left(\overline{B}\right)$.

$\Rightarrow A \subseteq B$ ($\because$ B is a regular open set)

So $A \cap B^* = \phi \Rightarrow A \subseteq B$.

Conversely suppose that $A \subseteq B$. Then $A \cap B' = \phi$

Consider $A \cap B^* = A \cap Ext(B) = A \cap Int(B') \subseteq A \cap B' = \phi$

$\Rightarrow A \cap B^* = \phi$

So $A \subseteq B \Rightarrow A \cap B^* = \phi$

Thus for any A, $B \in \mathcal{H}$, $A \cap B^* = \phi \Leftrightarrow A \subseteq B$

Hence $\mathcal{H}$ is a Boolean algebra.

11.18 Theorem : If π is a prime ideal space of the commutative ring R such that $\Delta\pi = (0)$, Γ is an isomorphism of the complete Boolean algebra of annihilator ideals of R onto the complete Boolean algebra of regular open sets of π. Moreover, if π contains all maximal ideals of R, Γ induces an isomorphism of the Boolean algebra of direct summands of R onto the Boolean algebra of the (simultaneously) closed and open sets in π.

Proof: Let R be a commutative ring and π be a space of prime ideals of R such that $\Delta\pi = (0)$.

By theorem 10.9, $B^*(R)$, the set of all annihilator ideals of R, is a complete Boolean algebra and by problem 11.17, the set $\mathcal{H}$ of all regular open sets in π is a Boolean algebra.

For any $A \in B^*(R)$, consider $\Gamma(A) = \Gamma\left(A^{**}\right) = \Gamma(\Delta\Gamma(\Delta\Gamma A))$

$= \Gamma\Delta(\Gamma\Delta(\Gamma(A))) = Ext(Ext(\Gamma(A)))$

$\Rightarrow \Gamma(A) = Ext(Ext(\Gamma(A))) \Rightarrow \Gamma(A) = Ext\left(Int\left((\Gamma(A))'\right)\right)$

$\Rightarrow \Gamma(A)$ is a regular open set.

So for any $A \in B^*(R)$, $\Gamma(A) \in \mathcal{H}$

For any $V \in \mathcal{H}$, consider $(\Delta\Gamma\Delta(V))^{**} = \Delta\Gamma(\Delta\Gamma(\Delta\Gamma\Delta(V)))$

$= \Delta\Gamma\Delta(\Gamma\Delta(\Gamma\Delta(V))) = \Delta\Gamma\Delta(Ext(Ext(V))) = \Delta\Gamma\Delta(V)$

$(\because V$ is a regular open set$)$

$\Rightarrow \Delta\Gamma\Delta(V)$ is an annihilator ideal of R

So $\Delta\Gamma\Delta(V) \in B^*(R)$ for any $V \in \mathscr{H}$.

First we show that Γ is a Boolean homomorphism.

For any A, $B \in B^*(R)$, consider $\Gamma(A \cap B) = \{P \in \pi / A \cap B \not\subseteq P\}$

$= \{P \in \pi / AB \not\subseteq P\} = \{P \in \pi / A \not\subseteq P \text{ and } B \not\subseteq P\} = \Gamma(A) \cap \Gamma(B)$

$\Rightarrow \Gamma(A \cap B) = \Gamma(A) \cap \Gamma(B)$

Consider $\Gamma((0)) = \{P \in \pi / (0) \not\subseteq P\} = \phi$

$\Rightarrow \Gamma((0)) = \phi$, which is the zero element in $\mathscr{H}$.

Let $A \in B^*(R)$. Consider $\Gamma(A^*) = \Gamma(\Delta\Gamma(A)) = \Gamma\Delta(\Gamma(A))$

$= Ext(\Gamma(A)) \Rightarrow \Gamma(A^*) = (\Gamma(A))^*$, which is the complement of $\Gamma(A)$ in $\mathscr{H}$.

$\therefore \Gamma : B^*(R) \to \mathscr{H}$ is a Boolean homomorphism.

Next we will show that Γ and $\Delta\Gamma\Delta$ are inverses to each other.

For any $A \in B^*(R)$, consider $\Delta\Gamma\Delta\Gamma(A) = \Delta\Gamma(\Delta\Gamma(A))$

$= \Delta\Gamma(A^*) = A^{**} = A (\because A$ is an annihilator ideal of $R)$

$\Rightarrow \Delta\Gamma\, \Delta\Gamma(A) = A$ for any $A \in B^*(R)$.

For any $V \in \mathscr{H}$, consider $\Gamma\Delta\Gamma\Delta(V) = \Gamma\Delta(\Gamma\Delta(V))$

$= \Gamma\Delta(Ext(V)) = Ext(Ext(V)) = V$ $(\because V$ is a regular open set$)$

$\Rightarrow \Gamma\,\Delta\,\Gamma\,\Delta(V) = V$ for any $V \in \mathscr{H}$

$\because \Gamma$ and $\Delta\Gamma\Delta$ are inverse mappings to each other.

Hence Γ is an isomorphism.

Assume π is the space of all maximal ideals of R.

First we show that an ideal A of R is a direct summand of R if and only if A is an annihilator ideal of R for which $A + A^{*} = R$.

Suppose A is an ideal of R such that A is a direct summand of R. Then there exists an ideal J of R such that $A + J = R$ and $A \cap J = (0)$. Consider $AJ \subseteq A \cap J \Rightarrow AJ = (0)$ $\Rightarrow A \subseteq J^{*}$.

Let $x \in J^{*} \Rightarrow x\,j = 0$ for all $j \in J$

Since $R = A + J$, we have $1 \in A + J \Rightarrow 1 = e + f$, for

some $e \in A$ and for some $f \in J \Rightarrow 1 - e = f \in J$

$\Rightarrow x(1-e) = 0 \Rightarrow x = xe \in A$

This shows that $J^{*} \subseteq A$ and hence $A = J^{*}$

Similarly we can show that $J = A^{*}$

$\therefore A$ is an annihilator ideal of R and $A + A^{*} = R$.

Conversely suppose that A is an annihilator ideal of R such that $A + A^{*} = R$.

Let $x \in A \cap A^{*} \Rightarrow x \in A$ and $xy = 0$ for all $y \in A$

$\Rightarrow xx = 0 \Rightarrow x = 0$ ($\because R$ is a semi prime ring)

$\therefore A \cap A^{*} = (0)$. So $A + A^{*} = R$ and $A \cap A^{*} = (0)$ and hence A is a direct summand of R.

Thus an ideal A is a direct summand of R if and only if A is an annihilator ideal of R such that $A + A^{*} = R$.

Since π contains all maximal ideal of R, this is equivalent to $\Gamma\left(A + A^{*}\right) = \Gamma(R)$ and this is if and only if $\Gamma(A)\cup\Gamma\Delta\Gamma(A)=\pi\left(\because\Gamma\left(A+A^{*}\right)=\Gamma(A)\cup\Gamma\Delta\Gamma(A)\right)$

Now $\Gamma\Delta\Gamma(A)$ is the extenior of $\Gamma(A)$. Hence an annihirator ideal A is a direct summand of R if and only if the associated regular open set $\Gamma(A)$ is the complement of its exterior if and only if $\Gamma(A)$ is both open and closed. Hence Γ incluces an isomorphism of the Boolean algebra of direct summands of R onto the Boolean algebra of the (Simultaneously) closed and open sets of π.

11.19 Corollary : If π is the set of all prime (= maximal) ideals of the Boolean ring R, then R is isomorphic to the algebra of closed and open subsets of π. Moreover, its Dedekind-MacNeille completion is isomorphic to the algebra of regular open subsets of π.

Proof: Since R is a Boolean ring, R is semiprime and the maximal ideals of R are precisely the prime ideals of R and $R=B(R)$, the Boolean algebra of all idempotents of R. If $e\in B(R)$, then eR is a direct summand of R. Also it is clear that if A is a direct summand of R, then $A=eR$ for some $e\in B(R)$. Let $\mathscr{H}$ be the Boolean algebra of all direct summands of R. Define $\psi: B(R)\rightarrow\mathscr{H}$ as $\psi(e)=eR$ for all $e\in B(R)$. Then it is easy to verify that ψ is an isomorphism and hence $B(R)\cong\mathscr{H}$. By theorum 11.18, $\mathscr{H}$ is isomorphic to the Boolean algebra of both open and closed sets. Hence R is isomorphic to the Boolean algebra of all both open and closed sets. Since R is a Boolean ring, by theorum 10.22, $D(R)=B^{*}(R)$. By theorum 11.18, $B^{*}(R)$ is isomorphic to the Boolean algebra of all regular open subsets of π. Hence the Dedekind MacNeille completion is isomorphic to the algebra of all regular open subsets of π.

11.20 Definition : A Boolean algebra R is said to be Dedekind Complete if the cononical monomorphism $\mu: R\rightarrow D(R)$, the lower subsets of R, is an isomorphism (i.e. $\mu(r)=\{r\}^{\vee\wedge}$ for all $r\in R$).

11.21 Definition : A Boolean algebra R is said to be atomic if for every element $r\in R$ there exists an atom (minimal non-zero element) $a\in R$ such that $a\leq r$.

11.22 Theorem : A Boolean algebra is isomorphic to the algebra of all subsets of a set if and only if it is complete and atomic.

Proof: Let R be a Boolean algebra

Suppose R is isomorphic to the algebra of all subsets of a set X. i.e. $R\cong P(X)$.

Now we will show that $P(X)$ is atomic and complete.

Let $Y \in P(X)$ such $Y \neq \phi$. Choose $y \in Y$. Then $\{y\} \neq \phi$ and clearly $\{y\}$ is an atom in P(X) and $\{y\} \subseteq Y$. Therefore $P(X)$ is atomic.

Let $\mathscr{H}$ be a lower subset of $P(X)$. Then $\mathscr{H} = \mathscr{H}^{\vee\wedge}$. Write $A = \bigcup_{B \in \mathscr{H}} B$ Then $A \in P(X)$

Now we will show that $A^{\vee\wedge} = \mathscr{H}$

Consider $Y \in A^{\vee} \Leftrightarrow A \subseteq Y \Leftrightarrow B \subseteq Y$ for all $B \in \mathscr{H}$

$\Leftrightarrow Y \in \mathscr{H}^{\vee}$

$\therefore A^{\vee} = \mathscr{H}^{\vee} \Rightarrow A^{\vee\wedge} = \mathscr{H}^{\vee\wedge} = \mathscr{H}$ ($\because \mathscr{H}$ is a lower subset of $P(X)$)

This shows that if $\mathscr{H} \in D(P(X))$, there exists $A \in P(X)$ such that $\mu(A) = \mathscr{H}$

$\therefore$ The canonical monomorphism $\mu : P(X) \rightarrow D(P(X))$ is onto and hence an isomorphism.

So $P(X)$ is Dedikind complete

Hence $P(X)$ is atomic and Dedekind complete.

Since $R \cong P(X)$, R is atomic and Dedekind complete.

Conversely suppose that R is atomic and Dedekind complete.

First we show that for any atom $a \in R$, a^* is a maximal ideal of R. Let $a \in R$ be an atom. It is easy to verify that a^* is an ideal of R. Since $a \neq 0$, we have $1 \notin a^*$. So a^* is a proper ideal of R. Let M be any ideal of R such that $a^* \subseteq M \subseteq R$. Suppose $a^* \neq M$. Then there exists $r \in M$ such that $r \notin a^* \Rightarrow ar \neq 0$ and $ar \leq a \Rightarrow a = ar (\because a \text{ is atom})$

$\Rightarrow a(1-r) = 0 \Rightarrow 1-r \in a^* \Rightarrow 1-r \in M \Rightarrow 1 \in M \ (\because r \in M)$

$\Rightarrow M = R$

$\therefore a^*$ is a maximal ideal of R.

Let π be the set of all maximal ideals of the form a^*, where a is an atom of R.

i.e. $\pi = \left\{ a^* \middle/ a \text{ is an atom of } R \right\}$.

Suppose $r \in R$ such that $r \neq 0$. Since R is atomic, there exists an atom $a \in R$ such that $a \leq r$.

$\Rightarrow ar = a \neq 0 \Rightarrow r \notin a^* \Rightarrow r \notin \Delta\,\pi$

$\therefore \Delta\pi = (0)$.

Hence π is a space of all maximal ideal a^*, where a is an atom in R, such that $\Delta\pi = (0)$. Since R is a Boolean algebra, each maximal ideal of R is a prime ideal of R and conversely. By theorem 11.18, $B^*(R)$ is isomorphic to the Boolean algebra of all regular open subsets of π.

Suppose $a \in R$ is an atom. Now $\Gamma(a) = \left\{ b^* \in \pi \middle/ a \notin b^* \right\}$

Let $b^* \in \Gamma(a) \Rightarrow a \notin b^* \Rightarrow ab \neq 0$

Also $0 \neq ab \leq a$ and $0 \neq ab \leq b \Rightarrow a = ab = b$ ($\because$ a and b are atoms)

This shows that $\Gamma(a) = \{a^*\}$. Therefore every singleton set in π is an open set

$\Rightarrow$ Every subset of π is an openset $\Rightarrow$ every subset of π is both open and closed $\Rightarrow$ every subset of π is a regular open set. Hence $B^*(R)$ is isomorphic to the algebra of all subsets of π. Since R is a Boolean algebra, by theorum 10.22, $D(R) = B^*(R)$. Since R is Dedekind complete, $D(R) = R$. Hence R is isomorphic to the algebra of all subsets of π.

11.23 Corollary : If R is any atomic Boolean algebra, its completion is isomorphic to the algebra of all subsets of atoms of R.

Proof: Suppose R is an atomic Boolean algebra.

If we proceed as in the converse part of the above theorum 11.22, we have $D(R) = B^*(R)$ and $B^*(R)$ is isomorphic to the algebra of all subsets of π.

Let Δ be the set of all atoms of R.

Now we will show that there is a bijection betweeen Δ and π.

Define $f : \Delta \rightarrow \pi$ as $f(a) = a^*$ for all $a \in \Delta$

Clearly f is well defined and onto.

Now we will show that f is one - one.

Suppose a, $b \in \Delta$ such that $f(a)=f(b)$. Then $a^{*}=b^{*}$.

If $ab=0$, then $a \in b^{*} \Rightarrow a \in a^{*} \Rightarrow aa=0$

$\Rightarrow a=0$ ($\because$ R is a Boolean algebra), which is a contradiction to the fact that a is an atom.

$\therefore ab \neq 0$. Since $0 \neq ab \leq a$ and $0 \neq ab \leq b$ and since a and b are atoms, we have $a=ab$ and $b=ab$. and therefore $a=b$.

So $f(a)=f(b) \Rightarrow a=b$

$\therefore$ f is one - one and hence $f:\Delta \rightarrow \pi$ is a bijection.

Consequently $P(\pi) \cong P(\Delta)$

Since $D(R)=B^{*}(R)$, $P(\pi) \cong P(\Delta)$ and $B^{*}(R) \cong P(\pi)$, we have $D(R)$ is isomorphic to $P(\Delta)$, which is the algebra of all subsets of atoms of R. Thus if R is an atomic Boolean algebra, its completion $D(R)$ is isomorphic to the algebra of all subsets of atoms of R.

Dr. V. SAMBASIVA RAO
Department of Mathematics
Acharya Nagarjuna University

Lesson - 12 Primitive Rings

Introduction 12.0:

In this lesson primitive ideals of a ring and primitive rings are defined and studied. The Jacobson density theorem, which is one of the basic theorems in primitive rings is studied. Also a prime ideal of a ring is defined and it is shown that a primitive ideal is a prime ideal. R stands for an associative ring with unity 1 which is not necessarily commutative.

Definition 12.1:

A module A_R is called irreducible iff it has exactly two submodules.

So, if A_R is an irreducible module then $\{0\}$ and A are the only submodules of A_R and $\{0\} \neq A$.

We know that a right ideal M of R is a maximal right ideal of R if

1. $M \neq R$
2. U is a right ideal of R and $M \subseteq U \subseteq R$ implies $U = M$ or $U = R$.

We also know that a right ideal M of R is a minimal right ideal of R if

1. $M \neq \{0\}$
2. U is a right ideal of R and $\{0\} \subseteq U \subseteq M$ implies $U = \{0\}$ or $U = M$.

We know that if M is a right ideal of R then $R/M = \{r + M / r \in R\}$ is a right R - module, and if B is submodule of R/M then $B = K/M$, for some right ideal K of R containing M. Using this one can prove the following.

Remark 12.2:

Let M be a right ideal of R. Then R/M is an irreducible R - module if and only if M is a maximal right ideal of R.

Remark 12.3:

Let M be a right ideal of R. Then M_R is irreducible if and only if M is a minimal right ideal of R.

Definition: An element $r \in R$ is called right invertible (left invertible) in R if there exists an element $s \in R$ such that $rs = 1 \left(sr = 1\right)$ and r is called a unit in R if it is right invertible and left invertible.

Preposition 12.4:

The following conditions concerning the ring $R \neq \{0\}$ are equivalent.

1. $\{0\}$ is a maximal right ideal.
2. R is irreducible as a right R - Module.
3. Every non zero element is right invertible.
4. Every non-zero element is a unit.

Let $1'$, $2'$ and $3'$ be the conditions obtained from 1, 2 and 3 respectively by replacing 'right' by 'left'.

Under these conditions R is called a division ring.

Proof : Let R be a ring and $R \neq \{0\}$

$1 \Rightarrow 2$: Let K be a non zero submodule of the right R - module R. So K is a non zero right ideal of R.

Since {0} is a maximal right ideal of R, we get that $K = R$. Therefore, the right R - Module R has exactly two submodules {0} and R and hence R is an irreducible right R - Module.

$2 \Rightarrow 3$: Let $0 \neq r \in R$. Now $rR = \{rs / s \in R\}$ is a submodule of the right R - module R. Also $rR \neq \{0\}$ as $0 \neq r = r.1 \in rR$. Therefore, by our assumption, $rR = R$. So $1 \in R = rR$ and that $1 = rs$ for some $s \in R$. so r is right invertible.

$3 \Rightarrow 4$; Let $0 \neq r \in R$. By our assumption we get $s \in R$ such that $rs = 1$. Now $s \neq 0$. Again by our assumption we get $t \in R$ such that $st = 1$.

Now $t = 1 \cdot t = (rs)t = r(st) = r \cdot 1 = r$.

Therefore $rs = 1 = sr$ and hence r is a unit in R.

$4 \Rightarrow 1$: We have $\{0\} \neq R$

Suppose that K is a right ideal of R and $\{0\} \subseteq K \subseteq R$. Assume that $K \neq \{0\}$.

Let $0 \neq x \in K$. By our assumption, we get a $y \in R$ such that $xy = yx = 1$.

Since K is a right ideal and $x \in K$, $1 = xy \in K$.

Since $1 \in K$ we get that $K = R$.

Therefore $\{0\}$ is a maximal right ideal of R.

Similarly one can prove that the conditions $1', 2', 3'$ and 4 are equivalent.

Definition 12.5:

A ring R is called simple if it has exactly two ideals. i.e. $\{0\}$ is a maximal ideal of R. Let M be an ideal of a ring R. consider the quotient ring R/M. We know that an ideal X of R/M is of the form $X = K/M$ for some ideal K of R containing M. Therefore R/M is a simple ring iff M is a maximal ideal.

A division ring is simple. A commutative ring is simple if and only if it is a division ring if and only if it is a field.

Now we study primitive rings which contains the class of all simple rings.

Definition 12.6:

An ideal P of a ring R is called (right) primitive if it is the largest ideal contained in some maximal right ideal M. Thus $P = \left(R^{\cdot}_{\cdot} M\right) = \{r \in R / Rr \subseteq M\}$.

We say that an ideal P of a ring R is a (left) primitive ideal if it is the largest ideal contained in some maximal left ideal of R.

Definition 12.7:

A ring R is called (right) primitive if $\{0\}$ is a (right) primitive ideal of R. We say that a ring R is (left) primitive if $\{0\}$ is a (left) primitive ideal of R.

It is known that a (right) primitive ring need not be a (left) primitive ring.

Here after we omit the attribute "right" and we write primitive ring for (right) primitive ring and primitive ideal for (right) primitive ideal.

Definition 12.8:

A module A_R is called faithful if for any $0 \neq r \in R, Ar \neq \{0\}$.

Proposition 12.9 (JACOBSON):

The ring R is primitive if and only if there exists a faithful irreducible module A_R.

Proof: Let R be a ring. Suppose that R is primitive. Since R is primitive, there exists a maximal right ideal M such that $\left(R^{\cdot}_{\cdot} M\right) = \{0\}$

Let $A = R / M$. Now A_R is an irreducible right R - Module, as M is a maximal right ideal of R. Suppose that $r \in R$ and $Ar = \{0\}$.

Now $Rr \subseteq M$. So $r \in \left(R \cdot . M\right) = \{0\}$ and that $r = 0$.

Therefore A_R is a faithful irreducible right R - module. Conversely suppose that R has a faithful irreducible R - module A_R.

Let $0 \neq a \in A$, since $0 \neq a = a.1 \in ar$, $ar \neq \{0\}$.

Clearly $aR = \{ar / r \in R\}$ is a submodule of A_R.

Since A is irrducible we get that $aR = A$.

define $h : R \to A$ by h(r) = ar, for all $r \in R$.

Let r, $s \in R$ and $t \in R$. $h(r+s) = a(r+s) = ar + as = h(r) + h(s)$ and $h(rt) = a(rt) = (ar)t = h(r).t$. Therefore h is a homomorphism of right R - module R into the right R - module A.

Since $aR = A$, h is onto A and hence h is an epimorphism of R onto A. Let $M = Ker\, h$. Now $R / M \cong A$ as right R - modules. Since A is irreducible R / M is also irreducible.

Hence M is a maximal right ideal. Since $A \cong R / M$, we get an isomorphism g of the right R - module R / M onto A. Let $r \in \left(R \cdot . M\right)$. Now $Rr \subseteq M$ and that $\left(R/M\right)r = \{M\}$. Now $\{0\} = \{g(M)\} = g\left(\left(R/M\right)r\right) = \left(g\left(R/M\right)\right)r = Ar$.

Since A is faithful $r = 0$. Therefore $\left(R \cdot . M\right) = \{0\}$ and hence R is primitive.

Lemma 12.10 (Schur):

If A_R is an irreducible module, then its ring of endomorphisms $D = Hom_R(A, A)$ is a division ring.

Proof: Let A_R be an irreducible module.

Let $D = Hom_R(A, A)$ = $\{f / f \text{ is an } R\text{-homomorphism of } A \text{ into } A\}$. Then D in a ring with 1. Let $0 \neq d \in D$. since dA is a non zero submodule of A_R, $dA = A$.

Since $d^{-1}0 = \{a \in A / da = 0\} \neq A$ is a submodule of A_R, $d^{-1}0=\{0\}$.

Therefore d in an automorphism of A.

Hence d is a unit in D. Thus every non zero element of D is a unit and hence D is a division ring.

Let A_R be an irreducible module and $D = Hom_R(A, A)$.

Now $d(ar) = d(a)r$ for all $d \in D$, $a \in A$, $r \in R$.

Clearly A is a left D - module. From the above 'associative' condition we have that A is a bimodule ${}_DA_R$. Since D is a division ring A is called a vector space. Consider the ring $E = Hom_D(A, A)$. For f, $g \in E$, $(a)(f+g)=(a)f+(a)g$ and $(a)(fg) = ((a)f)g$ for all $a \in A$. E is called the ring of linear transormations of the vector space A over the division ring D.

We see now the Jacobson density theorem.

Theorem 12.11:

Let R be a primitive ring with faithful irreducible module A_R. Then $D = Hom_R(A, A)$ is a divison ring and R is canonically embedded in $E = Hom_D(A, A)$ so that for every $e \in E$ and every finitely generated submodule G of ${}_DA$, there exists an element $r \in R$ such that $G(e-r)=\{0\}$.

Proof: Let R be a primitive ring with faithful irreducible module A_R. Now $D = Hom_D(A, A)$ is a divison ring. Consider the ring $E = Hom_D(A, A)$. For $r \in R$, define $f_r : A \to A$ by $(a)f_r = ar$ for all $a \in A$. Now for $a, b \in A$ and $d \in D$.

$(a+b)f_r = (a+b)r = ar + br = (a)f_r + (b)f_r$ and $(da)f_r = (da)r = d(ar) = d(a)f_r$.

Therefore $f_r \in Hom_D(A, A) = E$. Define $T : R \to E$ by $T(r) = f_r$ for all $r \in E$.

Let r, $s \in R$. $(a)f_{r+s} = a(r+s) = ar + as = (a)f_r + (a)f_s = (a)(f_r + f_s)$ for all $a \in A$.

So $f_{r+s} = f_r + f_s$.

$(a)f_{rs} = a(rs) = (ar)s = ((a)f_r)f_s = (a)f_r f_s$ for all $a \in A$.

So $f_{rs} = f_r f_s$. Now $T(r+s) = f_{r+s} = f_r + f_s = T(r) + T(s)$ and

$T(rs)=f_{rs}=f_r\, f_s=T(r)T(s)$. Therefore T is a ring homomorphism.

Let $r \in \text{Kernel}\, T$. Now $T(r)=0$ i.e. $f_r=0$. So $(a)f_r=0$ for all $a \in A$.

i.e. $ar=0$ for all $a \in A$. i.e. $Ar=0$. Since A_R is faithful $r=0$.

Therefore T is one-one and hence R is canonically embedded in E

Let $e \in E$ and G be a finitely generated submodule of A_D.

We prove now that there exists an element $r \in R$ such that $G(e-r)=\{0\}$. i.e. $ge=gr$ for all $g \in G$. we define $G^r=\{s \in R / Gs=\{0\}\}$ and for any subset S of R, $S^l=\{a \in A / aS=\{0\}\}$. We prove by induction on the dimension (the number of generators) of the subspce G of ${}_DA$, that, 1. there exists an $r \in R$ such that $G(e-r)=\{0\}$ and $2 \cdot G^{rl}=G$. Suppose that $\dim G=0$

i.e. $G=\{0\}$. Now $O \in R$ and $G(e-0)=Ge=\{0\}\, e=\{0\}$ and $G^{rl}=\left(G^r\right)^l=\left(\{0\}^r\right)^l$

$=R^l=\{0\}=G$. Assume that the result holds for G and consider $G+Da$, $a \notin G$. If $\dim G=n$ then $\dim(G+Da)=n+1$. Now we get an element $r \in R$ such that $G(e-r)=\{0\}$ and $G^{rl}=G$.

Let $b=a(e-r)$ We claim that $aG^r=A$. Since aG^r is a submodule of A and A is irreducible, $aG^r=A$ or $aG^r=\{0\}$. If $aG^r=\{0\}$ then $a \in G^{rl}=G$ a contradiction. Therefore $aG^r=A$. We get $s \in G^r$ such that $as=b$. Let $g+da \in G+Da,\ g \in G, d \in D$.

$$(g+da)(e-(r+s))=(g+da)(e-r-s)=(g+da)(e-r)-(g+da)s=$$

$$g(e-r)+d(a(e-r)-as)-gs=0+d(b-b)+0=0$$

Therefore $(G+Da)(e-(r+s))=\{0\}$. We now show that $(G+Da)^{rl}=G+Da.$, Clearly $(G+Da)^{rl}=\left(G^r \cap \{a\}^r\right)^l$. Since $G+Da \subseteq (G+Da)^{rl}$ we have $G+Da \subseteq \left(G^r \cap \{a\}^r\right)^l$.

Let $y \in \left(G^r \cap \{a\}^r\right)^l$. Then $ys=0$, whenever $Gs=\{0\}$ and as=0. Now aG^r and yG^r are submodules of A_R. As seen above $aG^r=A^r$. Therefore $f: aG^r \to yG^r$ defined by

$f(as) = ys$, $s \in G^{r}$ is well defined. Moreover f is a R - homomorphism and that $f \in D$. Let $d_1 = f$. Now $d_1\,(as) \;=\; ys$ for all $s \in G^{r}$ and that $y - d_1\, a \in G^{rl} = G$. Therefore $y \in G + Da$. Hence $G + Da = (G + Da)^{rl}$. This completes the induction and hence the result.

Let $\{X_i \,/\, i \in I\}$ be a family of topological spaces. We consider product topology on $X = \underset{i \in I}{\pi} X_i$ whose basic open sets are all sets of the form $\bigcap_{i \in F} \pi_i^{-1}(V_i)$ where $\pi_i : X \to X_i$ is the canonical mapping, V_i is any basic open set of X_i and F is a finite subset of I. Now for each $i \in I$, we consider discrete topology on X_i in which all the subsets of X_i are open. Then the product topology on X is not discrete topology on X but has basic open sets $V = \bigcap_{i \in F} \pi_i^{-1}(\{x_i\}),\ x_i \in X_i$.

$V = \{x \in X \,/\, x(i) = x_i \text{ for all } i \in F\},\ \pi_i(x) = x(i)$. This topology on X is called the finite topology on X.

Let A_R be a faithful irreducible module. Let $D = Hom_R(A, A)$ and $E = Hom_D(A, A)$. E is subset of the set of all functions of A into A that is E is a subset of $\underset{a \in A}{\pi} A$.

We consider finite topology on $\underset{a \in A}{\pi} A$ and E is a topological space with respect to the relative topology.

Each open set V of E is of the form $V^1 \cap E$, V^1 is an open subset of $\underset{a \in A}{\pi} A$.

The basic open sets of E are of the form $V = \{e \in E / a_i\, e = b_i \text{ , for all } i \in F\}$, where F is a finite set of indices and a_i , $b_i \in A$.

A subset B of a topological space X is called dense if its closure is the whole space. i.e. $B \cap V$ is nonempty for every non empty open set V of X.

12.12 Corrollary :

A primitive ring is a dense subring of the ring of all linear transformations of a vector space.

Proof: Let R be a primitive ring. Let A_R be a faithful irreducible module. $D = Hom_R(A, A)$ is a division ring and R is canonically embedded in $E = Hom_D(A, A)$.

E is a topological space whose basic open sets are $V = \{e \in E \ / \ a_i e = b_i, \text{ for all } i \in F\}$, where F is a finite set of indices and $a_i, \ b_i \in A$. R can be treated as a subset of E. We show that R is dense in E. To prove that R is dense in E it is enough to showthat every non empty basic open subset of E has non empty intersection with R.

Let V be a non empty basic open subset of E.

now $V = \{e \in E / a_i e = b_i \text{ for all } i \in F\} \neq \phi$, where F is a finite set of indices and $a_i, b_i \in A$. So we have $e \in E$ and $a_i e = b_i$ for all $i \in F$. By theorem 12.11 we get $r \in R$ such that $a_i r = b_i e = b_i$ for all $i \in F$. So $r \in R \cap V$. Hence R is dense in E.

Theorem 12.11: together with corrollary 12.12 is called Jacobson density theorem.

12.13 Definition :

An ideal P of R is called prime if it is proper i.e. $P \neq R$ and $AB \subseteq P$, A and B ideals of R implies $A \subseteq P$ or $B \subseteq P$. R is called a prime ring if {0} is a prime ideal of R. So an ideal P is a prime ideal of R if and only if R / P is a prime ring. Also a commutative ring is prime if and only if it is an integral domain.

Proposition 12.14:

Let P be a proper ideal of R. P is a prime ideal of R if and only if for any elements a and b of R, $aRb \subseteq P$ implies $a \in P$ or $b \in P$.

Proof: Let P be a proper ideal of R. Suppose that P is a prime ideal of R. Let a, $b \in R$ and $aRb \subseteq P$.

now $RaR = \left\{ \sum_{i=1}^{K} r_i a s_i \Big/ r_i, s_i \in R \ K \text{, is a positive integer which is not fixed} \right\}$ is the ideal of R generated by a.

RbR is the ideal of R generated by b. Since $aRb \subseteq P$ we have that $(RaR)(RbR) \subseteq P$. Since P is a prime ideal $RaR \subseteq P$ or $RbR \subseteq P$. Now $a \in RaR$ & $b \in RbR$. So $a \in P$ *or* $b \in P$.

Conversely suppose that for any elements a nad b of R $aRb \subseteq P$ implies $a \in P$ or $b \in P$. Let $AB \subseteq P$, $A \& B$ be ideals of R. Suppose that $A \not\subseteq P$. We get $a \in A - P$.

Now $aRb \subseteq AB \subseteq P$ for all $b \in B$. So $b \in P$ as $a \notin P$ for all $b \in B$, by our assumption. Therefore $B \subseteq P$.

Hence P is a prime ideal of R.

Corrollary 12.15:

R is a prime ring if and only if $1 \neq 0$ and for all $a \neq 0$ and $b \neq 0$ in R, there exists $r \in R$ such that $arb \neq 0$.

Proof: Suppose that R is a prime ring.

So {0} is a prime ideal of R and that $R \neq \{0\}$.

Therefore $1 \neq 0$ as $R \neq \{0\}$. Let $0 \neq a$, $0 \neq b \in R$. If $arb = 0$ for all $r \in R$, then as {0} is a prime ideal of R, either $a = 0$ or $b = 0$, a contradiction to $a \neq 0$ & $b \neq 0$. Therefore there exists a $r \in R$ such that $arb \neq 0$. Conversely suppose that $1 \neq 0$ and for all $a \neq 0, b \neq 0$, there is an $r \in R$ such that $arb \neq 0$. $R \neq \{0\}$ as $1 \neq 0$. Let $a, b \in R$ and $aRb \subseteq \{0\}$. If $0 \neq a$, $0 \neq b$ then by our assumption we get $r \in R$ such that $arb \neq 0$, which is a controdiction to $aRb \subseteq \{0\}$. Therefore either $a = 0$ or $b = 0$. Hence {0} is a prime ideal of R i.e. R is a prime ring.

12.16 Proposition :

Every primitive ideal (ring) is prime.

Proof: Let P be a primitive ideal of R. We get a maximal right ideal M of R such that $P = (R \cdot\!\!. M) = \{r \in R / Rr \subseteq M\}$.

Let A and B be ideals of R such that $AB \subseteq P \subseteq M$.

Now $M \subseteq (M \,.\!\cdot B) = \{r \in R / rB \subseteq M\} \subseteq R$ Since M is maximal right ideal of R and $(M \,.\!\cdot B)$ is right ideal of R, either $M = (M \,.\!\cdot B)$ or $(M \,.\!\cdot B) = R$.

Since $AB \subseteq M$, $A \subseteq (M \,.\!\cdot B)$. Suppose that $M = (M \,.\!\cdot B)$.

Now $A \subseteq (M \,.\!\cdot B) \subseteq M$ and that $A \subseteq (R \cdot\!\!. M) = P$.

Suppose that $(M \,.\!\cdot B) = R$ now $B \subseteq RB = (M \,.\!\cdot B)B$ and that $B \subseteq (R \cdot\!\!. M) = P$. Therefore P is a prime ideal of R.

Exercises

12.17 Problem :

Let M be a maximal right ideal of R and $s \in R-M$. Then show that $s^{-1}M = \{r \in R / sr \in M\}$ is also a maximal right ideal of R and $R/s^{-1}M \cong R/M$.

Solution: Suppose that M is a maximal right ideal of R and $s \in R-M$. Consider the right R - modules R_R and R/M_R.

Define $f : R \to R/M$ by $f(r) = sr + M$ for all $r \in R$.

Let $r_1, r_2, t \in R$.

$$f(r_1 + r_2) = s(r_1 + r_2)M = (sr_1 + sr_2)M = (sr_1 + M) + (sr_2 + M) = f(r_1) + f(r_2).$$

$$f(r_1 t) = s(r_1 t) + M = (sr_1)t + M = (sr_1 + M)t = (f(r_1))t.$$

Therefore f is an R - homomorphism. Now $f(1) = s \cdot 1 + M = s + M \neq M$.

So $f \neq 0$. since M is maximal, R/M is irreducible.

now $f(R)$ is a non zero submodule of R/M and that $f(R) = R/M$ i.e. f is onto R/M.

$$Ker\, f = \{r \in R / f(r) = M\}$$

$$= \{r \in R / sr + M = M\}$$

$$= \{r \in R / sr \in M\}$$

$$= S^{-1}M.$$

Therefore $R/s^{-1}M \cong R/M$. Since R/M is an irreducible right R - module $R/s^{-1}M$ is also an irreducible right R - module. Hence $s^{-1}M$ is a maximal right ideal of R.

Problem 12.18:

Let M be a maximal right ideal of R. Then show that the associated primitive ideal $(R \cdot. M)$ is the intesection of all $s^{-1}M$, where s ranges over all elements of R not in M.

Solution: Suppose that M is a maximal right ideal of R.

Consider the primitive ideal $(R \cdot . M) = \{r \in R / Rr \subseteq M\}$

Let $P = (R \cdot . M)$. Let $S = R - M$ we prove that $P = \bigcap_{s \in S} s^{-1}R$, where $s^{-1}R = \{r \in R / sr \in M\}$. Obviously $P \subseteq M$. let $p \in P$.

Since P is an ideal $sp \in P \subseteq M$, for all $s \in S$ so $p \in S^{-1}R$ for all $s \in S$.

Therefore $P \subseteq \bigcap_{s \in S} s^{-1}R$ ....(1)

Let $x \in \bigcap_{s \in S} s^{-1}R$ now $sx \in M$ for all $s \in S$ also $x \in 1^{-1}R = M$ $(1 \in S)$.

Let $r \in R$. Now either $r \in M$ or $r \in R - M = S$.

If $r \in M$ then $rx \in M$, since M is a right ideal.

If $r \in S$, then $rx \in M$ as $x \in r^{-1}R$

Therefore $Rx \subseteq M$ and that $x \in P$. So $\bigcap_{s \in S} s^{-1}R \subseteq P$ ....(2)

From (1) & (2), $P = \bigcap_{s \in S} s^{-1}R$.

Problem 12.19:

Let R be a ring. Then show that R is a primering if and only if $1 \neq 0$ and $AB \neq 0$ for any two non zero right ideals A and B of R.

Solution: Let R a ring. Suppose that R is a prime ring. So {0} is a prime ideal of R. therefore $R \neq \{0\}$ i.e. $1 \neq 0$.

Let A and B be non zero right ideals of R. Suppose that $AB = \{0\}$

Let $0 \neq a \in A$ and $0 \neq b \in B$. now $aRb = \{0\}$ as $aR \subseteq A$.

Since {0} is prime, by proposition 12.14, either $a = 0$ or $b = 0$. This is a contradiction to $a \neq 0$ and $b \neq 0$. Therefore $AB \neq \{0\}$. Conversely suppose that in R, $1 \neq 0$ and $AB \neq \{0\}$ for any two non zero right ideals A and B of R.

Since $1 \neq 0$, $\{0\} \neq R$. Suppose that A and B are ideals of R and $AB \subseteq \{0\}$.

So $AB = \{0\}$. Since A and B are ideals of R they are right ideals of R. By our assumption if $AB \neq \{0\}$ and $B \neq \{0\}$, then $AB \neq \{0\}$. Since $AB = \{0\}$, either $A = \{0\}$ or $B = \{0\}$. Therefore $\{0\}$ is a prime ideal of R i.e. R is a prime ring.

Dr. R. SRINIVASA RAO
P.G. Department of Mathematics
P.B. Siddhardha College
Vijayawada

Lesson - 13 Radicals

13.0 Introduction :

In this lesson the prime radical and the Jacobson radical (radical) of a ring are defined and studied. Inparticular it is proved that the Jacobson radical of R is the largest ideal K such that for all $r \in K$ $1-r$ is a unit. A characterization of the Jacobson radical of a ring R interms of the primitive ideals of R is given. Also strongly nilpotent elements of a ring are defined. A characterization of the prime radical of a ring R is given in terms of the strongly nilpotent elements of R.

Definition 13.1:

The prime radical of R is the intersection of all prime ideals of R and is denoted by $rad\ R$.

We give an internal characterization of the prime radical of R.

Definition 13.2:

An element a of R is called strongly nilpotent if every sequence $a_0, a_1, a_2, \ldots\ldots\ldots\ldots$ in R such that $a_0 = a$, $a_{n+1} \in a_n R a_n$ for all integers $n \geq 0$ is ultimately zero. i.e., there is a positive integer K such that $a_k R a_k = \{0\}$ and that $a_{K+1} = 0$.

Remark 13.3:

Every strongly nilpotent element is nilpotent.

Suppose that a is strongly nilpotent. Therefore a is nilpotent.

strongly nilpotenet element in R.

Now the sequence $a, a^2, a^4, \ldots\ldots$ is ultimately zero as $a^2 \in aRa$, $a^4 \in a^2 R a^2$ .... and a is strongly nilpotent. Therefore a is nilpotent.

Remark 13.4:

If R is a commutative ring then every nilpotent element is strongly nilpotent.

Suppose that R is a commutative ring and $a \in R$ is nilpotent.

We get a positive integer n such that $a^n = 0$. Consider a sequence $a_0, a_1, a_2, \ldots\ldots\ldots$ in R such that $a_0 = a$, $a_{n+1} \in a_n R a_n$ for all integers $n \geq 0$.

now $a_1 = a x_1 a = a^2 x_1$, for some $x_1 \in R$ and $a_2 = \left(a^2 x_1\right) x_2 \left(a^2 x_1\right) = a^4 \left(x_1^2\ x_2\right)$ for some

$x_2 \in R$,............ we get a least positive integer K such that $n < 2^K$. Now $a_k = a^{2^k} y$ for some $y \in R$.

So $a_k = a^{2^k} y = a^n \left(a^{2^k - n} \right) y = 0. \left(a^{2^k - n} \right) y = 0$

Therefore a is strongly nilpotent.

Proposition 13.5:

The prime radical of R is the set of all strongly nilpotent elements of R.

Proof: The prime radical $rad\ R$ of the ring R is the intersection of all prime ideals of R. We prove that rad $rad\ R = \{a \in R / a \text{ is a strongly nilpotent element of } R\}$.

Let a be a strongly nilpotent element.

Suppose that $a \notin rad\ R$.

now we get a prime ideal P such that $a \notin P$.

Let $a_0 = a$

Since P is a prime ideal of R, $a_0 R a_0 \not\subseteq P$ as $a_0 \notin P$. So there exists an element $a_1 \in a_0 R a_0$ such that $a_1 \notin P$. Again since $a_1 \notin P$ and P is a prime ideal in R $a_1 R a_1 \not\subseteq P$. So we get an element $a_2 \in a_1 R a_1$ such that $a_2 \notin P$.

If we continue this, we get a sequence $a_0, a_1, a_2, ...a_{k+1}, ...$ such that $a_0 = a$, $a_1 \in a_0 R a_0$, $a_2 \in a_1 R a_1, ..., a_{k+1}, \in a_K R a_K$, ... and $a_n \notin P$ for all $n = 0,1,2,........$ so $a_n \neq 0$ for all $n = 0,1,2,........$

Therefore the sequence $a_0, a_1, a_2,$ .... is not ultimately zero.

This is a contradiction to an assumption that $a_0 = a$ is strongly nilpotent in R.

Therefore $a \in rad\ R$.

So the set of all stronly nilpotent elements in R is a subset of $rad\ R$ ....(1)

conversely, let $a \in rad\ R$.

We prove that a is strongly nilpotent.

Suppose that a is not strongly nilpotent.

There exists a sequence $a_0 = a$, $a_1 \in a_0 R a_0$, ..., $a_{n+1} \in a_n R a_n$.........

Such that $a_K \neq 0$ for all $k = 0,1,2,$.......

Let $T = \{a_0, a_1, a_2, ...\}$

now $T \subseteq R$ and $0 \notin T$

Let $A = \{I / I \text{ is an ideal of } R \text{ and } I \cap T = \phi\}$.

Since $\{0\} \in A$, A is non-empty

Using Zorn's Lemma, we can prove that A has a maximal element. Let P be a maximal element in A.

We prove now that the ideal P is a prime ideal.

Suppose that A and B are idelas of R and $A \not\subseteq P$ and $B \not\subseteq P$.

Since $P \underset{+}{\subset} A + P$ and $P \underset{+}{\subset} B + P$, by the definition of P, $(A+P) \cap T \neq \phi$ and $(B+P) \cap T \neq \phi$.

Let $a_i \in T \cap (A+P)$ and $a_j \in T \cap (B+P)$.

Without loss of generality suppose that $i \leq j$.

Now $a_j \in A + P$.

Therefore $a_{j+1} \in a_j R a_j \subseteq (A+P)(B+P) \subseteq AB + P$.

Now $a_{j+1} = x + y$ for some $x \in AB$ and $y \in P$. As $x + y = a_{j+1} \notin P$, $x \notin P$.

Therefore $AB \not\subseteq P$. Also $P \neq R$ and hence P is a prime ideal of R.

So P is a prime ideal of R and $a \notin P$.

This is a contradiction to our assumption that $a \in rad\ R$.

Therefore a is strongly nilpotenet.

So the prime radical of R, $rad\ R$ is a subset of the set of all strongly nilpotent elements of R ....(2)

From (1) and (2), we get the result.

Definition:

An ideal I of R is called nilpotent if $I^n = \{0\}$ for some positive integer n.

Proposition 13.6:

The following conditions concerning the ring R are equivalent

(1) $\{0\}$ is the only nilpotent ideal of R

(2) $\{0\}$ is an intersection of prime ideals, that is $rad\, R = \{0\}$.

(3) For any ideals A and B of R, $AB = \{0\}$ implies $A \cap B = \{0\}$

Proof:

$1 \Rightarrow 2$

$\{0\}$ is the only nilpotent ideal of R.

We prove that $rad\, R = \{0\}$.

Let $0 \neq a \in R$

Let $a_0 = a$

The ideal $\{0\} \neq Ra_0R$ is not nilpotent

If $a_0Ra_0 = \{0\}$ then $(Ra_0\, R)^2 = (Ra_0R)(Ra_0R) = \{0\}$, this is a contradiction to the fact that Ra_0R is not nilpotent.

Therefore we get $0 \neq a_1 \in a_0\, R\, a_0$

Continuing this we obtain a sequence $a_0 = a, a_1, a_2, \ldots\ldots\ldots\ldots\ldots$ in R such that $a_{n+1} \in a_n\, Ra_n$ for all $n = 0, 1, 2, \ldots\ldots\ldots\ldots$ and $a_n \neq 0$ for all $n = 0, 1, 2, \ldots\ldots\ldots$

Therefore by proposition 13.5, $a \notin rad\ \ R$.

Hence $rad\, R$ contains no non zero element (i.e., $rad\, R = \{0\}$).

$2 \Rightarrow 3$

We have that rad $R = \{0\}$.

Let A and B be ideals of R and $AB=\{0\}$.

Let P be a prime ideal of R.

Now $AB=\{0\}\subseteq P$.

So either $A\subseteq P$ or $B\subseteq P$.

Therefore $A\cap B\subseteq P$. Hence $A\cap B\subseteq rad\ R=\{0\}$.

i.e., $A\cap B=\{0\}$.

$3\Rightarrow 1$

We have that for any ideals A and B of R, $AB=\{0\}$ implies $A\cap B=\{0\}$.

Let I be an ideal of R and $I^n=\{0\}$, for some positive integer n.

If $n=1$ then $I=\{0\}$.

Suppose that $n>1$.

$\{0\}=I^n=I\,I^{n-1}$. So $I\cap I^{n-1}=\{0\}$.

Since $I^{n-1}\subseteq I$, $I^{n-1}=I\cap I^{n-1}=\{0\}$.

So, $\{0\}=I^{n-1}=I\,I^{n-2}$.

By the same argument we get that $I^{n-2}=\{0\}$.

Continuing this we get that $I=\{0\}$.

Therefore {0} is the only nilpotent ideal of R.

Definition:

A ring R is called semiprime if $rad\ R=\{0\}$.

Corollary 13.7:

The prime radical of R is the smallest ideal K of R such that R/K is semiprime.

Proof: Let I be an ideal of R

We know that any ideal of the quotient ring R/I is of the form J/I, where J is an ideal of R containing I. We see now that if P is an ideal of R and $I \subseteq P \subseteq R$ then P is a prime ideal of R if and only if P/I is a prime ideal of R/I.

Let $I \subseteq P \subseteq R$ and P be an ideal of R.

Suppose that P is a prime ideal of R.

We show that P/I is a prime ideal of R/I.

Let $A/I, B/I$ be ideals of R/I and $(A/I)(B/I) \subseteq P/I$.

Now $(AB+I)/I \subseteq P/I$ and that $AB \subseteq P$.

Since P is prime, $A \subseteq P$ or $B \subseteq P$.

So, either $A/I \subseteq P/I$ or $B/I \subseteq P/I$.

Since $P \neq R$, $P/I \neq R/I$. Therefore P/I is a prime ideal of R/I.

Conversely, suppose that P/I is a prime ideal of R/I

Since $P/I \neq R/I$, $P \neq R$.

Suppose that A and B are ideals of R and $AB \subseteq P$.

now $(A+I)/I$, $(B+I)/I$ are ideals of R/I and

$$((A+I)/I)((B+I)/I) = (AB+I)/I \subseteq P/I \text{ as } AB \subseteq P \text{ and } I \subseteq P.$$

Since P/I is prime, $(A+I)/I \subseteq P/I$ or $(B+I)/I \subseteq P/I$

So, either $A \subseteq P$ or $B \subseteq P$.

Therefore P is a prime ideal of R.

We know that rad R is the intersection of all prime ideals of R.

Consider the quotient ring $R/rad\ R$.

Since each prime ideal of R contains rad R, if P is a prime ideal of R then $P/rad\ R$ is a prime ideal of $R/rad\ R$.

Therefore the intersection of all prime ideals of $R/rad\ R$ is zero. i.e., $R/rad\ R$ is semiprime.

Let K be an ideal of R and R/K is semiprime.

Let $\left\{ {}^{P_\alpha}\!/\!{}_{K}\Big/ \alpha \in \Delta \right\}$ be the collection of all prime ideals of R/K.

Now $\{P_\alpha / \alpha \in \Delta\}$ is a collection of prime ideals of R.

As R/K is semiprime, $\bigcap_{\alpha\in\Delta} (P_\alpha / K)$ is zero. i.e., $\bigcap_{\alpha\in\Delta} P_\alpha = K$.

Therefore, $rad\ R \subseteq \bigcap_{\alpha\in\Delta} P_\alpha = K$. This completes the proof.

Definition 13.8:

The intersection of all maximal right ideals of R is called the Jacabson radical or the radical of R and it is denoted by $Rad\ R$.

We give a characterization of $Rad\ R$.

Proposition 13.9:

The radical of R is the set of all $r \in R$ such that $1-rs$ is right invertible for all $s \in R$.

Proof : $Rad\ R$, the radical of R is the intersection of all maximal right ideals of R.

Let $r \in R$

$r \in Rad\ R \iff r \in M$ for all maximal ideals M of R

$\iff 1 \notin M + rR$, for all maximal ideals M of R

$\iff 1 - rs \notin M$, for all maximal ideals M of R and forall $s \in R$

$\iff 1 - rs$ is right invertible for all $s \in R$.

Definition 13.10:

A ring R is called semiprimitive if $Rad\ R = \{0\}$.

Proposition 13.11:

The radical of R is an ideal of R and $R / Rad\ R$ is semiprimitive.

Proof: We first see that $Rad\ R$ is an ideal of R.

By definition $Rad\ R$ is a right ideal of R.

We prove that $Rad\ R$ is also a left ideal and hence an ideal.

Let $r \in Rad\ R$ and $x \in R$.

We have to prove that $xr \in Rad\ R$.

By proposition 13.9, it is enough to prove that $1 - xrs$ is right invertible forall $s \in R$.

Let $s \in R$

Let $rs = r_1$.

now $r_1 \in Rad\ R$

Since $r_1 x \in Rad\ R$, $1 - r_1 x$ is right invertible.

So we get $u \in R$ such that $(1 - r_1 x)u = 1$ *i.e.,* $1 + r_1 x u = u$

$$(1 - xr_1)(1 + xur_1) = 1 + xur_1 - x(1 + r_1 xu)r_1$$

$$= 1 + xur_1 - xur_1$$

$$= 1$$

Therefore $1 - xr_1 = 1 - xrs$ is right invertible. Since s is an arbitrary element in R, $1 - xrs$ is ght invertible for all $s \in R$ and that $xr \in Rad\ R$.

Therefore $Rad\ R$ is an ideal of R.

We prove now that $R / Rad\ R$ is semiprimitive.

i.e., $Rad(R/Rad\ R) = \{Rad\ R\}$.

Let M be a right ideal of R and $Rad\ R \subseteq M$.

Clearly M is a maximal right ideal of R if and only if $M / Rad\ R$ is a maximal right ideal of $/ Rad\ R$.

Let $r + Rad\ R \in Rad(R/Rad\ R)$.

Now, $r + Rad\ R \in \bigcap M/Rad\ R$

$M/Rad\ R$ is a maximal right

ideal of $R/Rad\ R$

$\Rightarrow r + Rad\ R \in M/Rad\ R$, for all maximal right ideals $M/Rad\ R$ of $R/Rad\ R$

$\Rightarrow r \in M$ for all maximal right ideals M of R.

$\Rightarrow r \in Rad\ R \Rightarrow r + RadR = RadR$

Therefore $Rad(R/Rad\ R) = \{Rad\ R\}$

So $R/Rad\ R$ is semiprimitive.

Proposition 13.12:

The radical of R is the largest ideal K suchthat forall $r \in K$, $1-r$ is a unit.

Proof: Let $r \in Rad\ R$

By proposition 13.9, $1-rs$ is right invertible for all $s \in R$.

Choosing $s = 1 \in R$, $1-r$ is right invertible.

So we get a $u \in R$ such that $(1-r)u = 1$.

So $1-u = -ru$.

Since $r \in Rad\ R$, $-ru = r(-u) \in Rad\ R$.

So $1-u \in Rad\ R$.

Therefore $1-(1-u)s$ is right invertible for all $s \in R$ and inparticular for $s=1$, $1-(1-u)$ is right invertible.

i.e., u is right invertible in R.

So we get an element $v \in R$ such that $uv = 1$

Since $1 = (1-r)u$, we have $v = (1-r)uv = (1-r)1$

$= 1-r$.

Therefore $u(1-r) = 1 = (1-r)u$.

Hence $1-r$ is a unit in R.

So, forall $r \in Rad\ R$, $1-r$ is a unit in R.

Let I be an ideal of R such that $1-x$ is a unit forall $x \in I$.

Let $y \in I$ and $s \in R$

now $ys \in I$.

By our supposition $1-ys$ is a unit in R and that $1-ys$ is right invertible in R.

Since $s \in R$ is arbitrary by proposition 13.9.

$y \in Rad\ R$

So $I \subseteq Rad\ R$

Hence $Rad\ R$ is the largest ideal of R such tht forall $r \in Rad\ R$, $1-r$ is a unit in R.

Corollary 13.13:

The radical of R is the intersection of all maximal left ideals of R.

Proof: Let J be the intersection of al maximal left ideals of R.

Using the fact that $Rad\ R$ is the intersection of all maximal right ideals of R, we have proved that $Rad\ R$ is the largest ideal of R such that $1-r$ is a unit in R. for all $r \in Rad\ R$ ....(1)

On the same lines we get that J is the largest ideal of R such that $1-s$ is a unit in R for all $s \in J$ ....(2)

From (1) and (2) we get that $J = Rad\ R$.

i.e., $Rad\ R$ is the intersection of all maximal left ideals of R.

Proposition 13.14:

The radical of R is the intersection of all primitive ideals of R.

Proof: Let $r \in R$

$r \in Rad\ R \quad \Leftrightarrow Rr \subseteq Rad\ R$ (as Rad R is an ideal of R)

$\Leftrightarrow Rr \subseteq M$ for all maximal right ideals M of R.

$\Leftrightarrow r \in \left(R^{\bullet}.\ M\right) = P$, for all primitive ideals P of R.

$\Leftrightarrow r \in \bigcap P$

P is a primitive

ideal of R

Therefore $Rad\ R$ is the intersection of all primitive ideals of R.

Proposition 13.15:

R is semiprime (semiprimitive) if and only if it is a subdirect product of prime (primitive) rings.

Proof: R is semiprime (Semi primitive)

$\Leftrightarrow rad\ R = \{0\}$ ($Rad\ R = \{0\}$)

$$\Leftrightarrow \bigcap_{\substack{P \text{ is a prime} \\ \text{ideal of } R}} P = \{0\} \left(\bigcap_{\substack{Q \text{ is a primitive} \\ \text{ideal of } R}} Q = \{0\} \right)$$

$\Leftrightarrow$ R is a sub direct product of prime rings R/P, P is a prime ideal of R.

(R is a subdirect product of primitive rings R/Q, Q is a primitive ideal of R).

Exercises

Problem 13.16:

Let S be a subset of R such that $1 \notin S$ and for any a and $b \notin S$, there exists $r \in R$ such that $arb \notin S$. If further more $0 \in S$, show that any ideal which is maximal in the set of ideals contained in S is prime.

Sol: Let $A = \{I / I \text{ is an ideal of } R \text{ and } I \subseteq S\}$

Since the ideal $\{0\} \subseteq S$, $A \neq \phi$

A is a poset under set inclusion.

Let I_α , $\alpha \in \Delta$ be a chain of ideals in A.

Let $I = \bigcup_{\alpha \in \Delta} I_\alpha$.

Clearly I is an ideal of R contained in S i.e., $I \in A$. As $I_\alpha \subseteq I\ \forall \alpha \in \Delta$, I is an upper bound for the chain. Therefore by Zorn's Lemma, A has a maximal element.

Let M be a maximal element in A.

We prove that M is a prime ideal of R.

M is an ideal and $M \neq R$ as $1 \notin S$ *imply* $1 \notin M \subseteq S$.

Let a, $b \in R$ and $aRb \subseteq M$

Suppose that $a \notin M$ *and* $b \notin M$

Let RaR, RbR be the ideals generated by $a \& b$ respectively.

now $M + RaR$, $M + RbR$ are ideals of R which contains M properly.

By the maximality of M. $M + RaR \not\subseteq S$ and $M + RbR \not\subseteq S$.

Let $x \in (M + RaR) - S$ *and* $y \in (M + RbR) - S$.

Now as $x \in M + RaR$, $x = m_1 + \sum_{i=1}^{n} r_i a t_i$, $r_i, t_i \in R$, $m_1 \in M$.

Also $y \in M + RbR$ implies $y = m_2 + \sum_{i=1}^{m} u_i b v_i$, u_i , $v_i \in R$, $m_2 \in M$

By our assumption we get $z \in R$ such that $xzy \notin S$.

$$xzy = \left(m_1 + \sum_{i=1}^{n} r_i a t_i \right) z \left(m_2 + \sum_{i=1}^{m} u_i b v_i \right)$$

$$= \left(m_1 z + \sum_{i=1}^{n} r_i a t_i z \right) \left(m_2 + \sum_{i=1}^{m} u_i b v_i \right)$$

$$= (m_1 z) m_2 + (m_1 z) \left(\sum_{i=1}^{m} u_i b v_i \right) + \left(\sum_{i=1}^{n} r_i a t_i z \right) m_2 + \left(\sum_{i=1}^{n} r_i a t_i z \right) \left(\sum_{i=1}^{m} u_i b v_i \right)$$

Since M is an ideal the first three terms in the above sum are in M.

Since $aRb \subseteq M$ and since M is an ideal, $\left(\sum_{i=1}^{n} r_i a t_i z \right) \left(\sum_{i=1}^{m} u_i b v_i \right) \in M$

Therefore $xzy \in M$.

So $xzy \in S$, a contradiction to xzy $\notin$ S.

Therefore $a \in M$ *or* $b \in M$

Hence M is a prime ideal of R.

Problem 13.17:

If A is any ideal and r is any element of the semiprime ring R then show that $Ar=\{0\}$ if and only if $rA=\{0\}$.

Proof: Let R be a semi prime ring and A is an ideal of R and $r \in R$.

Suppose that $Ar=\{0\}$.

Let $B=\{x \in R / Ax=0\}$.

Now $r \in B$, B is an ideal of R and $AB=\{0\}$.

Now $(BA)^2 = (BA)(BA) = B(AB)A = \{0\}$ *as* $AB=\{0\}$. So BA is a nilpotent ideal of R. Since R is semiprime, by proposition 13.6, $\{0\}$ the only nilpotent ideal of R. Therefore, $BA=\{0\}$.

Since $r \in B$, $rA = \{0\}$.

By a similar argument we get that $rA = \{0\} \Rightarrow Ar = \{0\}$.

Dr. R. SRINIVASA RAO
P.G. Department of Mathematics
P.B. Siddhardha College
Vijayawada.

Lesson - 14 Completely Reducible Modules

Introduction 14.0:

In this lesson radical and socle of a module A_R are defined. A completely irreducible module is introduced equivalent conditions for a completely reducible module are developed. Also homogeneous components of a completely reducible module A_R are defined and studied.

Definition 14.1:

The radical $Rad\,A$ of a module A_R is defined as the intersection of all maximal (proper) submodules of A_R. If A_R has no maximal (proper) submodules then $Rad\,A$ is defined as A itself.

Definition 14.2:

The socle $Soc\,A$ of a module A_R is defined as the sum of all minimal (non-zero) submodules of A_R. If A_R has no minimal (non zero) submodule then $Soc\,A$ is defined as $\{0\}$ (the zero submodule of A_R).

Proposition 14.3:

Let A_R be a module and $Soc\,A \neq \{0\}$. Then the socle of A_R is the direct sum of a subfamily of the family of all irreducible submodules of A_R. It is invarient under every endomorphism of A_R.

Proof: Let $A = \{A_i / i \in I\}$ be the family of all irreducible (minimal) submodules of A_R.

Since $Soc\,A \neq \{0\}$, A is non-empty.

Now $Soc\ A = \sum_{i \in I} Ai$. We say that a non-empty subset J of I is direct if $\sum_{j \in J} A_j$ is a direct sum.

Let B be the set of all direct subsets of I.

If $i \in I$ then $\{i\} \in B$. So B is non-empty.

For N, $L \in B$ define $N \leq L$ if and only if $N \subseteq L$. $(B, \leq)$ is aposet. we claim that B has a maximal element. Let $\{J_K / k \in K\} \neq \phi$ be a chain in B. Let $J = \underset{k \in K}{U}\ J_k$. We prove that J is a direct subset of I i.e., $\sum_{j\in J} Aj$ is a direct sum. Suppose that $\sum_{j\in J} aj=0$, where $a_j \in A_j$ and $T=\{j\in J/a_j\neq 0\}$ is finite. If T is empty there is nothing to prove. Suppose that T is non-empty. Since T is a non-empty finite subset of J, and $\{J_k/k\in K\}$ is a chain, we get that $T\subseteq J_k$ for some $k\in K$. Since J_K is a direct subset of I and $\sum_{j\in T} aj=0$, we get that $aj=0$ for all $j\in T$. This is a contradiction to the fact that $a_j\neq 0$ for all $j\in T$. Therefore, T is empty. Hence J is a direct subset of I. So $J\in B$ and $J_K \leq J$ for all $k\in K$. So J is an upperbound for the chain $\{J_k/k\in k\}$.

Therefore, by Zorn's lemma B has a maximal element P. Now $\sum_{i\in P} Ai$ is a direct sum. We claim that $Soc\ A=\sum_{i\in P} A_i$. Suppose that A_j is a minimal (non-zero) submodule of A and $A_j \not\subseteq \sum_{i\in P} A_i$. Then $A_j \cap \sum_{i\in P} A_i=\{0\}$ ....(1)

Let $a_j+\sum_{i\in P} a_i=0$, $a_j\in A_j$ and $a_i\in A_i$, $i\in P$. From (1), $a_j=0=\sum_{i\in P} a_i$. Since P is a direct subset of I, $a_i=0$ for all $i\in P$. Therefore $P\cup[j]$ is a direct subject of I and P is a proper subject of $P\cup[j]$. This is a contradiction to the maximality of P. So $A_j\subseteq \sum_{i\in P} A_i$. Therefore $\sum_{i\in P} A_i$ containg all the minimal (non-zero) submodules of A and that $Soc\ A\subseteq \sum_{i\in P} A_i$.

Obviously $\sum_{i\in P} A_i \subseteq Soc\ A$, by the definition of $Soc\ A$. Therefore $Soc\ A=\sum_{i\in P} A_i$ is a direct sum. Let $e\in Hom_R(A_i, A)$.

Let $A_i\in A$, since A_i is irreducible $Ker\, e\cap Ai$ is a submodule of A_i so $Ker\ e\cap A_i=\{0\}$ or $\ker e\cap A_i=A_i$. If $\ker e\cap A_i=\{0\}$ then $e(A_i)\cong A_i$ and hence $e(A_i)$ is an irreducible submodule of A. If $\ker e\cap A_i=A_i$ then $e(A_i)=\{0\}$. So $e(A_i)=\{0\}$ or $e(A_i)\cong A$. Therefore $e(A_i)\subseteq Soc\ A$ and hence $e(Soc\ A)\subseteq Soc\ A$.

Corollary 14.4:

The following conditions concerning the module A_R are equivalent where $Soc\ A \neq \{0\}$.

(1) $A = Soc\ A$

(2) A is the sum of minimal submodules

(3) A is isomorphic to a direct sum of irreducible modules

Proof: A_R is a module and $Soc\ A \neq \{0\}$

$1 \Rightarrow 2$. we have that $A = Soc\ A$.

By definition $Soc\ A$ is the sum of all minimal sub modules of A. So A is the sum of all minimal submodules of A.

$2 \Rightarrow 3$ Since A is the sum of all minimal submodules of A. By proposition 14.3, we get a sub family $\{B_i / i \in I\}$ of the family of all irreducible submodules of A_R, such that $A = \sum_{i \in I} B_i$, a direct sum of irreducible modules B_i, $i \in I$.

$3 \Rightarrow 1$ we have that A is isomorphic to B, where B is a direct sum of irreducible modules. We get a non-empty collection $\{B_i / i \in I\}$ of minimal (non-zero) submodules of B_R such that $B = \sum_{i \in I} B_i$ is a direct sum.

Let f be an isomorphism of A_R onto B_R. Let g be the inverse of f. g is an isomorphism of A_R onto B_R. where $g(b) = a$ iff $f(a) = b$, $a \in A, b \in B$. since g is an isomorphism $g(B_i)$ is also a minimal (non-zero) sumodule of A. we claim that $A = \sum_{i \in I} g(B_i)$. Let $a \in A$. Since $g(B) = A$, we get a $b \in B$ such that $g(b) = a$. since $B = \sum_{i \in I} Bi$, we get some $i_1, i_2, \ldots\ldots\ldots\ldots i_k \in I$, such that $b = b_{i_1} + b_{i_2} + \ldots\ldots\ldots\ldots + b_{i_k}$, where $b_{i_j} \in B_{i_j}$.

$$\text{now } a = g(b) = g\left(b_{i_1} + b_{i_2} + \ldots\ldots\ldots\ldots + b_{i_k}\right) = g\left(b_{i_1}\right) + g\left(b_{i_2}\right) + \ldots\ldots\ldots\ldots$$

$$+ g\left(b_{i_k}\right) \in g\left(B_{i_1}\right) + g\left(B_{i_2}\right) + \ldots\ldots\ldots\ldots + g\left(B_{i_k}\right) \subseteq \sum_{i \in I} g(Bi)$$

Therefore $A \subseteq \sum_{i\in I} g(B_i)$. But $\sum_{i\in I} g(B_i)$ is a submodule of A. Therefore $A = \sum_{i\in I} g(Bi)$.

Since $g(B_i)$ is a minimal submodule of A, $i \in I$, $\sum_{i\in I} g(B_i) \subseteq Soc\ A$. Therefore $A \subseteq Soc\ A$. But $Soc\ A \subseteq A$. Hence $A = Soc\ A$.

Definition 14.5:

A module A_R is said to be completely reducible if A is the sum of minimal submodules.

Definition 14.6:

A submodule B of a module A_R is called large if it has non-zero intersection with every non-zero submodule of A_R

Lemma 14.7:

If B is a submodule of A_R and C is maximal among the submodules of A such that $B \cap C = \{0\}$ then $B+C$ is large.

Proof: B is a submodule of A_R. C is a maximal among the sub modules of A suchthat $B \cap C = \{0\}$. $B+C$ is also a submodule of A. Let D be a submodule of A and $(B+C) \cap D = \{0\}$. We claim that $B \cap (C+D) = \{0\}$. Let $x \in B \cap (C+D)$.

Now $x = b = c + d$ for some $b \in B$, $c \in C$ and $d \in D$. Now $d = b - c \in D \cap (B+C) = \{0\}$. So $d = b - c = 0$ and that $b = c \in B \cap C = \{0\}$. So $b = c = 0$ and that $x = 0$. This shows that $B \cap (C+D) = \{0\}$. By the maximality of C, $D \subset C$ and that $D = (B+C) \cap D = \{0\}$. Hence $B+C$ is large.

Let B be a submodule of A_R. We know that a submodule C of A is called a complementary submodule of B if $B \cap C = \{0\}$ and $B + C = A$. A is complemented if every submodule B of A has a complementary submodule.

Lemma 14.8 :

Let B be a submodule of A_R. If $L(A)$ is complemented then so is $L(B)$.

Proof: B is a submodule of A_R. Suppose that $L(A)$ is complemented. Let C be a submodule of B. We get a sub module C' of A such that $C \cap C' = \{0\}$ and $C + C' = A$. now $B \cap C'$ is a submodule of B. We claim that $B \cap C'$ is a complementary submodule of C in B.

$$C \cap (C' \cap B) = (C \cap C') \cap B = \{0\} \cap B = \{0\}$$

Since $C \subseteq B$, by modular law $B \cap (C + C') = C + (B \cap C')$.

Therefore $C + (B \cap C') = (C + C') \cap B = A \cap B = B$

so $B \cap C'$ is a complementary submodule of C in B.

Hence $L(B)$ is complemented.

Lemma 14.9:

If $L(A)$ is complemented then Rad A = {0}.

Proof: suppose that $L(A)$ is complemented. Let $0 \neq a \in A$. By Zorn's lemema we get a submodule M of A which is maximal among the submodules of A not containing a. Suppose that N is a submodule of A and $M \subseteq N \subseteq A$. since $L(A)$ is complemented.

We get a submodule N' of A suchthat $N \cap N' = \{0\}$ and $N + N' = A$. Since $M \subseteq N$, by modular law $M + (N \cap N') = N \cap (M + N')$. Now $M = M + \{0\} = M + (N \cap N') = N \cap (M + N')$. Since $a \notin M$, either $a \notin N$ or $a \notin M + N'$. If $a \notin N$ then by the maximality of $M, N = M$. If $a \notin M + N'$ then by the maximality of $M, N' = \{0\}$ i.e., $N = A$.

Therefore, either $N = M$ or $N = A$.

Hence M is a maximal (proper) submodule of A

suchthat $a \notin M$. So $a \notin Rad\ A$. Therefore $Rad\ A = \{0\}$.

Proposition 14.10:

The following conditions concerening the module A_R are equivalent.

(1) A is completely reducible.

(2) A has no proper large submodule

(3) $L(A)$ is complenented.

Proof: Let A_R be a module.

$(1) \Rightarrow (2)$

we have that A is completely reducible. So, $Soc\, A = A$. Let M be a large sumodule of A. So M has non-zero intersection with every non-zero submodule of A. Let B be an irreducible submodule of A. Since $B \neq \{0\}$, $M \cap B \neq \{0\}$. But as B is irreducible either $M \cap B = B$ or $M \cap B = \{0\}$. Therefore $M \cap B = B$ i.e., $B \subseteq M$. Hence $Soc\, A \subseteq M$ i.e., $A \subseteq M$ i.e., $A = M$. So A has no proper large submodule.

$(2) \Rightarrow (3)$

We have that A has no proper large submodule. Let B be a submodule of A. By lemma 14.6, we get a submodule C of A suchthat $B \cap C = \{0\}$ and $B + C$ is a large submodule of A. By our assumption $B + C = A$. Therefore $L(A)$ is complemented.

$(3) \Rightarrow (1)$

We have that $L(A)$ is complemented. Since $Soc\, A$ is a submodule of A, we get a submodule C of A suchthat $Soc\, A + C = A$ and $Soc\, A \cap C = \{0\}$. Since $L(A)$ is complemented by lemma 14.7, $L(C)$ is also complemented. Now by lemma 14.8, $Rad\, C = \{0\}$. Suppose that $C \neq \{0\}$. Let $0 \neq x \in C$ Since $Rad\, C = \{0\}$, there exist a maximal submodule D of C suchthat $x \notin D$. Again since $L(C)$ is complemented we get a submodule D' of C such that $D \cap D' = \{0\}$ and $D + D' = C$. As D is maximal D' is an irreduvible submodule of C and hence an irreducible submodule of A. So $D^{|} \subseteq Soc\, A \cap C = \{0\}$, a contradiciton to the fact that D' is irreducible. Therefore $C = \{0\}$.

Hence $A = Soc\, A$. i.e., A is completely reducible.

Definition 14.11:

Let R and S be rings. Let A be a right R - module and Let A also be a left S - module T. Then A is called a $S - R$ - bimodule if $s(ar) = (sa)r$ for all $s \in S$, $a \in A$ and $r \in R$.

Example 14.12:

Let A be a right R - module. Let $E = Hom_R(A,A)$, the ring of all endomorphisms of the module A_R. It is obvious that A is a left E - Module. Also we have that $e(ar) = (e(a))r$ forall $e \in E, a \in A$ and $r \in R$. Therefore A is a $E - R$ module ${}_E A_R$.

Remark 14.13:

Let A_i be any irreducible submodule of A_R. Let $E = Hom_R(A,A)$ the ring of all endomorphisms of the module A_R. EA_i denotes the submodules of A_R, generated by all ea_i, $e \in E$ and $a_i \in A_i$. EA_i consists of all elements of the form $e_1a_1 + e_2a_2 + \ldots\ldots\ldots\ldots + e_ka_k$, where $e_1, e_2, \ldots\ldots\ldots\ldots, e_k \in E$ and $a_1, a_2, \ldots\ldots\ldots\ldots, a_k \in A_i$ (k is not fixed). Clearly EA_i is also a left E - module and that EA_i is an $E - R$ - submodule of ${}_E A_R$. For $e \in E$, eA_i is a homomorphic image of A_i and hence $eA_i = \{0\}$ or $eA_i \cong A_i$ as A_i is irreducible. So eA_i is either $\{0\}$ or irreducible.

Lemma 14.14:

Let A_i be an irreducible sub module of A_R. If A_R is completely reducible then EA_i is the sum of all irreducible submodules of A_R which are isomorphic to A_i. EA_i is called a homogeneous component of A_R.

Proof: A_i is an irreducible submodule of A_R and A_R is completely reducible. Let A_k be an irreducible sub module of A_R and $A_k \cong A_i$. Let B be the sum of all irreducible submodules of A_R which are isomorphic to A_i. Since $L(A_R)$ is complemented, we get a submodule A_i' of A suchthat $A_i \cap A_i' = \{0\}$ and $A = A_i + A_i'$. Let f be an isomorphism of A_{iR} onto A_{KR}. Define $e : A \to A$ by $e\left(a = a_i + a_i^1\right) = f(a_i)$, $a_i \in A_i$, $a_i^1 \in A_i^1$. Clearly e is an endomorphism of A_R. i.e., $e \in E$. obviously $e(A_i) = A_k$. so $A_k = e(A_i) \subseteq EA_i$. Therefore $B \subseteq EA_i$. By remark 14.13 $EA_i \subseteq B$. Hence $EA_i = B$.

Proposition 14.15:

Let A_R be the direct sum of a finite number of irreducible submodules Aj, $j \in J$ and let $E = Hom_R(A,A)$. Then every non-zero $E - R$ - submodules of ${}_E A_R$ is the direct sum of some of the homogeueous components EA_i.

Proof: Let A_R be the direct sum of a finite number of irreducible submodules Aj, $j \in J$ and $E = Hom_R(A, A)$. We may assume that $J = \{1,2,3,........,n\}$ and $A = A_1 \oplus A_2 \oplus ....\oplus A_n$, A_i are irreducible submodules of A_R. Let $1 \le i \le n$. Define $e_i : A \to A$ by $e_i(a_1 + a_2 + ...+ a_n) = a_i$, $a_j \in A_j$ for all $1 \le j \le n$. Clearly e_i is an endomorphism of A_R and that $e_i \in E$. Now $e_i(A) = A_i$, Also $e_1 + e_2 + ... + e_n = 1$, the identity map of A. Let B be a non-zero $E-R$ - submodule of $_EA_R$. Since $e_i(B) \subseteq A_i$ and A_i is irreducible, $e_i(B) = \{0\}$ or $e_i(B) = A_i$. Also $e_i(B) \subseteq B$. Let $I = \{i \in J / e_i(B) = A_i\}$. I is non empty as $B \ne \{0\}$. Now $B = (e_1 + e_2 + ... + e_n)(B) = \sum_{i \in J} e_i(B) = \sum_{i \in I} A_i$. For any $i \in I$, $EA_i \subseteq EB \subseteq B$. So $\sum_{i \in I} EA_i \subseteq B$. Since $e_i(A_i) = A_i$, $B = \sum_{i \in I} A_i \subseteq \sum_{i \in I} EA_i$. Therefore $B = \sum_{i \in I} EA_i$. We prove now that EA_i is a minimal submodule of $_EB_R$ for all $i \in I$. We know that EA_i is a submodule of $_EA_R$. So EA_i is a submodule of $_EB_R$ for all $i \in I$ as $EA_i \subseteq B$ for all $i \in I$. Let $i \in I$. Let $e \in E$ and $a_i \in A_i$. Since $e(a_i) \in EA_i \subseteq B = \sum_{i \in I} A_i$.

$e(a_i) = a_{i_1} + a_{i_2} + ... + a_{i_p}$. Where $0 \ne a_{i_l} \in A_{i_l}$, $i_l \in I$ and $1 \le l \le p$.

Since $a_{i_l} = e_{i_l} e(a_i)$, $A_i \simeq A_{i_l}$, $1 \le l \le p$.

Also $a_{i_l} = e_{i_l} e(a_i) \in EA_i$, $1 \le l \le p$. Now $A_{i_l} = a_{i_l} R \subseteq EA_i$, $1 \le l \le p$ ....(1)

Therefore $e(a_i) \in A_{i_1} + A_{i_2} + ... + A_{i_p}$, $A_i \simeq A_{i_l}$, $1 \le l \le p$. So we get $A_{i_1}, A_{i_2}, ..., A_{i_k}$ (say), $i_1, i_2, ...i_k \in I$ such that $A_i \cong A_{i_l}$ for all $1 \le l \le k$ and $EA_i \subseteq A_{i_1} + A_{i_2} + ... + A_{i_K}$. Using (1) we conclude that $A_{i_l} \subseteq EA_i$ for all $1 \le l \le k$.

Hence $EA_i = A_{i_1} + A_{i_2} + ... + A_{\cap_k}$ and $A_i \cong A_{i_l}$ for all $1 \le l \le k$.

Let C be a non zero submodule of $_EEA_{iR}$. Let $0 \ne x \in C$.

Since $x \in EA_i$, $x = a_1 + a_2 + ... + a_k$, $a_j \in A_{i_j}$, $1 \le j \le k$.

Since $x \neq 0$, without loss of generality we may assume that $a_1 \neq 0$. Now $a_1 \neq 0 \in A_{i_1}$. $a_1 = e_{i_1} x \in C$.

Since A_{i_1} is an irreducible sub module of A_R and $0 \neq a_1 \in A_{i_1}$, we have $a_1 R = A_{i_1}$. Since $A_i \cong A_{i_1}$, $EA_i = EA_{i_1}$. Now $EA_i = EA_{i_1} \subseteq Ea_1 R \subseteq EC \subseteq C$.

Therefore $C = EA_i$ and hence EA_i is a minimal submodule of ${}_E B_R$. Since $B = \sum_{i \in I} EA_i$ is a sum of minimal submodules EA_i, $i \in I$, we get that B is a direct sum of some of the minimal submodules EA_i, $i \in I$ of ${}_E A_R$.

Exercises

Problem 14.16:

Let A_R and C_R be R - modules and π be an epimorphism of C onto A. If B is a large submodule of A then showthat $\pi^{-1}(B)$ is a large submodule of C .

Solution: Let π be an epimorphism of a right R - module C onto the right R - module A. Suppose that B is a large submodule of A. We prove that $\pi^{-1}(B)$ is a large submodule of C. We know that $\pi^{-1}(B)$ is a submodule of C. Let $\{0\} \neq G$ be a submodule of C. Let $K = \pi^{-1}\{0\}$. K is a submodule of C contained in $\pi^{-1}(B)$. If $G \cap K \neq \{0\}$ then $G \cap \pi^{-1}(B) \neq 0$. Suppose that $G \cap K = \{0\}$. Now $\pi(G)$ is a non-zero submodule of A. So $\pi(G) \cap B \neq \{0\}$ as B is large. Let $0 \neq b \in B \cap \pi(G)$. We get $0 \neq a \in G$ such that $\pi(a) = b$. Now $a \in \pi^{-1}(b) \subseteq \pi^{-1}(B)$. Therefore $0 \neq a \in G \cap \pi^{-1}(B)$ and that $G \cap \pi^{-1}(B) \neq \{0\}$. Hence $\pi^{-1}(B)$ is a large submodule of C.

Problem 14.17:

Let C be a right R - module. Let A and B be submodules of C and $A \subseteq B \subseteq C$. Show that A is a large sumodule of C if and only if A is a large submoduleof B and B is a lage submodule of C.

Solution: Suppose that A is a large submodule of C. Let $\{0\} \neq D$ be a submodule of B. D is also a submodule of C. Since A is a large submoduleof C, $A \cap D \neq \{0\}$. Therefore A is a large submodules of B. Let $G \neq \{0\}$ be a submodule of C. Now $A \cap G \neq \{0\}$ as A is a large submodule of C. Since $A \subseteq B$, $\{0\} \neq A \cap G \subseteq B \cap G$. So $B \cap G \neq \{0\}$. Therefore B is a large submodule of C.

Conversely suppose that A is a large submodule of B and B is a large submodule of C. Let $\{0\} \neq H$ be a submodule of C. Since B is a large submodule of C, $B \cap H \neq \{0\}$. Since $\{0\} \neq B \cap H$ is a submodule of B and A is a large submodule of B, $A \cap (B \cap H) \neq \{0\}$. So $A \cap H \neq \{0\}$. Therefore A is a large submodule of C.

Problem 14.18:

Let B and C be large submodules of an R - module A_R. Then show that $B \cap C$ is a large submodule of A.

Solution: Let B and C be large submodules of an R - module A_R. Let $\{0\} \neq G$ be submodule of A. Since B is a large submodule of A, $B \cap G \neq \{0\}$. Since C is a large submodule of A, $C \cap (B \cap G) \neq \{0\}$. Therefore $(B \cap C) \cap G \neq \{0\}$.

Hence $B \cap C$ is a large submodule of A.

Dr. R. SRINIVASA RAO
P.G. Department of Mathematics
P.B. Siddhardha College
Vijayawada.

Lesson - 15 Completely Reducible Rings

Introduction 15.0:

In this lesson a completely reducible ring is defined. some equivalent conditions of a completely reducible ring are studied. If R is a semi prime then it is shown that R_R and R^R have the same socle and they have same homogeneous components which are minimal ideals. Also the minimal right ideals of a semiprime ring are studied and an equivalent condition for the R - modules eR and fR to be isomorphic is obtained, where e and f are idenpotents in R.

Proposition 15.1(Brauer):

Let K be a minimal right ideal of R. Then either $K^2 = \{0\}$ *or* $K = eR$, where $e^2 = e \in K$.

Proof: K is a minimal right ideal of R. Suppose that $K^2 \neq \{0\}$. We get a $k \in K$ such that $kK \neq \{0\}$.

Since $kK \neq \{0\}$ is also a right ideal of R contained in the minimal right ideal K, $kK = K$. We get $e \in K$ such that $ke = k$. Now $e \neq 0$. $k^* = \{r \in R / kr = 0\}$ is a right ideal of R. Since K is minimal and $kK \neq 0$, $k^* \cap K = \{0\}$. From $ke = k$ we get that $k(e^2 - e) = ke^2 - ke = (ke)e - k = ke - k = k - k = 0$. So $e^2 - e \in k^*$. Also $e \in K$. Therefore $e^2 - e \in k^* \cap K = \{0\}$ and that $e^2 = e \in K$. Now $0 \neq e \in eR \subseteq K$ as $e \in K$. Since K is minimal, $eR = K$.

Corollary 15.2:

A minimal right ideal of a semi simple ring R has the form eR, where $e^2 = e \in R$

Proof: Let K be a minimal right ideal of a semi simple ring R. By proposition 15.1, either $K^2 = \{0\}$ or $K = eR$, $e^2 = e \in K$. Suppose that $K^2 = \{0\}$. Let $k \in K$. Since $K^2 = \{0\}$ and $kR \subseteq K$, $kRk = \{0\}$. Therefore $\{0\} = kRk \subseteq P$ forall prime ideals P of R. So $k \in P$ for all prime ideals P of R by proposition 12.4. Therefore $k \in rad\ R = \{0\}$. Hence $K = \{0\}$; this is a controdiction to the fact that K is minimal. So $K = eR$ for some $e = e^2 \in K$.

Lemma 15.3:

If $e^2 = e \in R$ and $f \in R$ then there is a group isomorphism $Hom_R(eR, fR) \simeq fRe$. Moreover if $f = e$, this is a ring isomorphism.

Proof: $e^2 = e \in R$ and $f \in R$. $(fRe, +)$ is a group.

$(Hom_R(eR, fR), +)$ is also a group.

Let $r \in R$. Define $\phi_r : eR \to fR$ by $\phi_r(es) = (fre)es = fres$.

$\phi_r(es_1 + es_2) = \phi_r(e(s_1 + s_2)) = fre(s_1 + s_2)$

$= fres_1 + fres_2$

$= \phi_r(es_1) + \phi_r(es_2)$ for all $es_1, es_2 \in eR$

Also $\phi_r((es)t) = \phi_r(e(st)) = frest = (fres)t = (\phi_r(es))t$, for all $es \in eR$ and $t \in R$.

Therefore $\phi_r \in Hom_R(eR, fR)$ for all $r \in R$.

Define $\psi : fre \to Hom_R(eR, fR)$ by $\psi(fre) = \phi_r$ for all $r \in R$

ψ is well defined as $fr_1e = fr_2e$ implies $\phi_{r_1} = \phi_{r_2}$.

Let $r_1, r_2 \in R$. $\phi_{r_1+r_2}(es) = f(r_1 + r_2)es = fr_1es + fr_2es$

$= \phi_{r_1}(es) + \phi_{r_2}(es)$

$= (\phi_{r_1} + \phi_{r_2})(es)\ \forall\ es \in eR$

Therefore $\phi_{r_1+r_2} = \phi_{r_1} + \phi_{r_2}$.

So $\psi(fr_1e + fr_2e) = \psi(f(r_1 + r_2)e) = \phi_{r_1+r_2} = \phi_{r_1} + \phi_{r_2}$

$= \psi(fr_1e) + \psi(fr_2e)$ for all $fr_1e, fr_2e \in fRe$.

Therefore ψ is a group homomorphism.

We see now that ψ is one-one.

Suppose that $\psi(fr_1e) = \psi(fr_2e)$, $r_1, r_2 \in R$

Now $\phi_{r_1} = \phi_{r_2}$ and that $\phi_{r_1}(ee) = \phi_{r_2}(ee)$ and that

$fr_1e = fr_2e$. Therefore ψ is one-one. Let $\phi \in Hom_R(eR, fR)$

Let $\phi(e) = fr$, $r \in R$. We claim that $\phi = \phi_r$

$\phi(es) = \phi((e)es) = \phi(e)es = fres = \phi_r(es)$ forall $es \in eR$.

Therefore $\phi = \phi_r$. Now $fre \in fRe$ and $\psi(fre) = \phi_r = \phi$.

So ψ is onto $Hom_R(eR, fR)$. Hence $fRe \cong Hom_R(eR, fR)$

as groups. Suppose now that $f = e$ as seen above ψ is a group isomorphism of eRe onto $Hom_R(eR, eR)$. Now eRe, $Hom_R(eR, eR)$ are rings. We prove that ψ is a ring isomorphism. Let $r_1, r_2 \in R$. $\psi((er_1e)(er_2e)) = \psi(e(r_1er_2)e) = \phi_{r_1er_2}$. Now $\phi_{r_1er_2}(es) = er_1er_2es =$

$\phi_{r_1}(er_2es) = \phi_{r_1}(\phi_{r_2}(es)) = (\phi_{r_1}\phi_{r_2})(es)$, for all $es \in eR$.

Therefore $\phi_{r_1er_2} = \phi_{r_1}\phi_{r_2}$. So $\psi((er_1e)(er_2e)) = \phi_{r_1er_2} = \phi_{r_1}\phi_{r_2} = \psi(er_1e)\psi(er_2e)$.

Therefore ψ is a ring isomorphism.

Remark 15.4:

Let $e^2 = e \in R$. Now eRe is ring with unity e. By lemma 15.3 eRe and $Hom_R(eR, eR)$ are isomorphic rings. If eR is irreducible then by schure is lemma we get that $Hom_R(eR, eR)$ is a division ring.

Therefore eRe is a division ring. The converse is also true if R is semi prime..

Proposition 15.5 : If R is semi prime and $e^2 = e \in R$ then eR is a minimal right ideal if and only if eRe is a division ring.

Proof : R is a semi prime ring and $e^2 = e \in R$. If eR is a minimal right ideal of R then by the above remark we get that eRe is a division ring. Conversely suppose that eRe is a division ring. Let $0 \neq er \in eR$. Since R is semi prime as seen in the proof of collollary 15.2, $er\,\mathrm{Re}\,r \neq \{0\}$. So we get an $s \in R$ such that $erser \neq 0$ and that $erse \neq 0$. Since $erse$ is a non-zero element of the division ring eRe, we get $ete \in eRe$ such that $(erese)(ete) = e$. Therefore $e \in erR$ and that $eR \subseteq erR$. Obviously $erR \subseteq eR$. Therefore $erR = eR$.

Hence eR is minial right ideal of R.

Proposition 15.6: If R is semi prime and $e^2 = e \in R$ then eR is a minimal right ideal if and only if Re is a minimal left ideal of R.

Proof: R is a semi prime ring and $e^2 = e \in R$. The new results we get by replacing the term 'right ideal' by 'left ideal' and 'eR' by 'Re' in the statements of proposition 15.1, Corollary 15.2, and proposition 15.5 are also valid. So we get that eRe is a division ring if and only if Re a minimal left ideal of R. Therefore from proposition 15.5 we get that eR is a minimal right ideal if and only if Re is a minimal left ideal.

Proposition 15.7:

If $e^2 = e \in R$ and $f^2 = f \in R$ then $eR \cong fR$ as right R module if and only if there exist u, $v \in R$.

such that $vu = e$ and $uv = f$.

Proof: We have $e^2 = e \in R$ and $f^2 = f \in R$. Suppose that $eR \cong fR$ as right R - modules. As seen in the proof of lemma 15.3, $\psi : f\,\mathrm{Re} \to Hom_R(eR\,,\, fR)$ defined by $\psi(fre) = \phi_r$, is a group isomorphism, where $\phi_r(es) = fres$. Since $eR \cong fR$, there is an isomorphism ϕ of eR onto fR. We get a $r \in R$ such that $\psi(fre) = \phi_r = \phi$. Let $u = fre$. Now $\phi^{-1} : fR \to eR$ is an isomorphism. Again by the proof of lemma 15.3 $T : eRf \to Hom_R(fR\,,\, eR)$ defined by $T(erf) = g_r$ is a group isomorphism, where $g_r(fs) = erfs$. Since $\phi^{-1} \in Hom_R(fR\,, eR)$, we get a $t \in R$ such that $T(etf) = g_t = \phi^{-1}$. Let $v = etf$.

So, $e = \phi^{-1}\,\phi(e) = g_t(\phi_r(e)) = g_t(fre) = etfre = (etf)(fre) = vu$

and $f = \phi\phi^{-1}(f) = \phi_r(g_t(f)) = \phi_r(eff) = fretf = (fre)(eff) = uv$

Conversely, suppose that there are v, $u \in R$ such that

$e = vu$ and $f = uv$

Now $ue = u(vu) = (uv)u = fu$.

Define $\phi : eR \to fR$ by $\phi(er) = uer$

$\phi(er_1 + er_2) = \phi(e(r_1 + r_2)) = ue(r_1 + r_2) = uer_1 + uer_2$

$= \phi(er_1) + \phi(er_2)$ for all $er_1, er_2 \in eR$

$\phi((er)s) = \phi(e(rs)) = u(ers) = (u(er))s = (\phi(er))s$ for all $er \in eR$ and $s \in R$.

Therefore, ϕ is a R - homomorphism of eR into fR.

Suppose that $er_1 \,.\, er_2 \in eR$ and $\phi(er_1) = \phi(er_2)$.

Now $uer_1 = uer_2$ this implies $v(uer_1) = v(uer_2)$ and

this implies $(vu)er_1 = (vu)er_2$ i.e., $e(er_1) = e(er_2)$, i.e., $er_1 = er_2$.

Therefore ϕ is one-one. Let $fr \in fR$.

Now $evr \in eR$ and $\phi(evr) = (ue)vr = (fu)vr = f(uv)r$

$= ffr = fr$

So ϕ is onto fR. Hence ϕ is an R isomorphism of eR onto fR. eR and fR are isomorphic as right R modules.

Corollary 15.8:

If $e^2 = e \in R$ and $f^2 = f \in R$ then $eR \cong fR$ as right R modules if and only if $Re \cong Rf$ as left R modules.

Proof: $e^2 = e \in R$ and $f^2 = f \in R$.

By proposition 15.7 we have that $eR \cong fR$ as right R modules if and only if there exist v, $u \in R$, such that $e = vu$ and $f = uv$ ......(1). On the same lines we get that $Re \cong Rf$ as left P modules if and only if there exist x, $y \in R$ suchthat $e = xy$ and $f = yx$ .... (2).

From (1) and (2) we get that $eR \cong fR$ as right R modules if and only if $Re \cong Rf$ as left R modules.

Proposition 15.9:

If R is semi prime then R_R and R^R have the same homogeneous components and these are minimal ideals.

Proof: Let R be semiprime. Let S be the socle of R_R and S' be the socle of R^R. S is the sum of all minimal right ideals of R and S' is the sum of all minimal left ideals of R. Since R is semi prime by corollary 15.2, a minimal right ideal (left ideal) of R is of the form $eR(Re)$, $e^2 = e \in R$. We know that for $e^2 = e \in R$, $eR(Re)$ is a minimal right (left) ideal if and only if eRe is a division ring, as R is semi prime. Let $X = \{e \in R / e^2 = e \text{ and } eRe \text{ is a division ring}\}$.

So $S = \sum_{e \in X} eR$ and $S' = \sum_{e \in X} \text{Re}$

We show that S is an ideal. Clearly S is a right ideal of R. Let $r \in R$. $f_r : R \to R$ defined by $f_r(s) = rs$ is a R - homomorphism. So $f_r \in Hom_R(R, R)$. By proposition 14.3 $f_r(S) \subseteq S$. i.e., $rS \subseteq S$. Therefore S is a left ideal of R. Hence S is an ideal of R. By a similar argument we get that S' is also an ideal of R. Let $e \in X$. Now $e \in S$. Since S is an ideal, $Re \subseteq S$. Therefore $S' = \sum_{e \in X} Re \subseteq S$. Similarly we get that $S \subseteq S'$. Therefore $S = S'$. So R_R and R^R have the same socles. We prove now that $S \& S'$ have the same homogenous components. Let H be a homogeneous component of S. We get $f \in X$ such that H is the sum of all eR, $e \in X$. Such that $eR \cong fR$. We have that $eR \cong fR$ if and only if $Re \cong Rf$ by corollary 15.8. Now H' the sum of all Re, $e \in X$, such that $Re \cong Rf$ is the corresponding homogeneous component of S'. We claim that $H = H'$ clearly H is a right ideal. Let $r \in R$. t_r defined above is an R - homomorphism of R_R into R_R. By proposition 14.3, $f_r(H) \subseteq H$ i.e., $rH \subseteq H$. Therefore H is an ideal of R. Similarly we get that H' is also an ideal of R. Let $e \in X$ and $Re \cong fR$. So $eR \cong fR$. now $eR \subseteq H$ and that $e \in H$. Since H is an ideal $Re \subseteq H$. Therefore $H' \subseteq H$. Similarly we get that $H' \subseteq H$. Hence $H = H_1$. So S and S' have the same homogeneous components. We prove now that H

is a minimal ideal of R. Let K be a non-zero ideal of R contained in H. Since H_R is completely reducible and K is a sub module of H, K_R is also completely reducible. Let L be a minimal right ideal contained in K. $L = gR$, for some $g^2 = g$ and that $g \in X$. Now $gR \subseteq H$ as $K \subseteq H$. We claim that $gR \cong fR$ as R modules, since gR, fR are irreducible if $\phi \in Hom_R(gR , fR)$ then either $\phi = 0$ or an R - isomorphism. Suppose that gR is not R - isomorphic to fR. Then by lemma 15.3 $fRg \cong Hom_R(gR , fR) = \{0\}$ as groups. So $fRg = \{0\}$. We also get that $e \in X$ and $eR \cong fR$ implies $eRg = \{0\}$. Now $I = \{s \in R / sRg = 0\}$ is an ideal of R containing H. Since $g \in H$, $gRg = 0$ and that $g^2 = 0$. So $g = g^2 = 0$, a contradiction to the fact that gR is a minimal right ideal. Therefore $gR \cong fR$ as R - modules. By proposition 15.7, we get $u, v \in R$ such that $f = uv$ and $g = vu$. Now $f = uv = (uv)uv = u(vu)v = ugv$.

$$fR = (ugv)R \subseteq ugR = u(gR) \subseteq uk \subseteq K.$$

So, for each $e \in X$ with $eR \simeq fR$, $eR \subseteq K$.

Therefore H, the sum of all minimal right ideals isomorphic to fR is contained in K. Hence $H = K$. So H is a minimal ideal of R.

Proposition 15.10:

The following statements concerning the ring R are equivalent.

1. Every right R - module is completely reducible
2. R_R is completely reducible
3. Every left R module is completely reducible
4. ${}^R R$ is completely reducible.

Proof:

$1 \Rightarrow 2$ We have that every right R module is completely reducible. Since R_R is a right R module R_R is completely reducible.

$2 \Rightarrow 1$ We have that R_R is completely reducible. Let B_R be a right R module.

Since R_R is completely reducible, R is the sum of minimal right ideals A_i, $i \in I$. Now

$B = \sum_{b \in B} bR$, as $b \in bR$. Since $R = \sum_{i \in I} A_i$, $B = \sum_{b \in B} \sum_{i \in I} bA_i$.

Let $b \in B$. We claim that bA_i is either irreducible or {0}. Define $f : Ai \to bA_i$ by $f(r) = br$ forall $r \in A_i$. Clearly $f \in Hom_R(A_i, bA_i)$ and f is onto bA_i. Since A_i is a minimal right ideal $\ker f = \{0\}$ or A_i. If $\ker f = \{0\}$ then f is an isomorphism and that bA_i is also irreducible. If $\ker f = A_i$ then $f = 0$ i.e., $bA_i = \{0\}$. Therefore, either $bA_i = \{0\}$ or bA_i is an irreducible sub module of B.

Therefore B is the sum of irreducible sub modules of B_R. Hence B_R is completely reducible. Similarly we can prove that $3 \Leftrightarrow 4$.

$2 \Rightarrow 4$ We have that R_R is completely reducible.

By lemma 14.8, $Rad = \{0\}$. Since $rad\ R \subseteq Rad\ R\ \{0\}$. $rad\ R = \{0\}$. i.e., R is semi prime. Therefore by proposition 15.9, R_R and $^R R$ have the same socle. Since R_R is completely reducible, $Soc(R_R) = R$. Therefore the $Soc(^R R) = R$, i.e., $^R R$ is completely reducible. By symenetry we get $4 \Rightarrow 2$.

Definition 15.11:

A ring R is said to be completely reducible if R_R is completely reducible.

Corollary 15.12:

A vector space is completely reducible.

Proof: Let V_R be a vector space. Now R is division ring. So R_R is completely reducible. So by proposition 15.10, V_R is completely reducible.

Lemma 15.13:

Let R be a prime ring and assume that the socle S_R of R_R is not zero. Let $e^2 = e \in R$ such that eR is a minimal right ideal of R. Then $Hom_R(S, S)$ is isomorphic to the ring of linear transformations $Hom_{eRe}(Re, Re)$.

Proof: R is a prime ring and S_R the socle of R_R is not zero. So R is semi prime. Let eR be a minimal right ideal of R, $e^2 = e \in R$. Now eRe is a division ring and Re_{eRe} is a right eRe - module.

So Re is a vector space over the division ring eRe. Let H be a Homogeneous component of S. By proposition 15.9, H is a direct summand of S. We get an ideal K of R such that $S = H \oplus K$. now $HK \subseteq H \cap K = \{0\}$. Since R is a prime ring {0} is a prime ideal. So $H = \{0\}$ or $K = \{0\}$. Since H is a minimal ideal of R, $H \neq \{0\}$. So $K = \{0\}$. Therefore $S = H$.

Let $\{e_i R / i \in I\}$ be the set of all minimal right ideals of R, where $e_i^2 = e_i \in R$ for all $i \in I$. Now $S = \sum\limits_{i \in R} e_i R$. Also $e_i R \cong eR$ as right R - modules as S is a homogeneous components of S.

By proposition 15.7 there exist $v_i, u_i \in R$ such that $v_i u_i = e$ and $u_i v_i = e_i$, for all $i \in I$.

Now $u_i e v_i = u_i v_i u_i v_i = e_i^2 = e_i$ for all $i \in I$.

Let $\phi \in Hom_R(S, S)$. Since $e \in eR \subseteq S$ and S is an ideal, $Re \subseteq S$.

Define $\phi' : Re \to Re$ by $\phi'(re) = \phi(re) = \phi(ree) = \phi(re)e \in Re$.

$\phi^1(r_1 e + r_2 e) = \phi^1((r_1 + r_2)e) = \phi((r_1 + r_2)e) = \phi(r_1 e + r_2 e)$

$= \phi(r_1 e) + \phi(r_2 e) = \phi^1(r_1 e) + \phi^1(r_2 e)$ for all $r_1 e_1$ $r_2 e \in Re$

$\phi^1(r_1 e\ ere) = \phi(r_1 e\ ere) = (\phi(r_1 e))ere = (\phi^1(r_1 e))\ ere,$

for all $r_1 e \in Re$. $ere \in eRe$.

Therefore $\phi^1 \in Hom_{eRe}(Re, Re)$.

Define $\psi : Hom_R(S, S) \to Hom_{eRe}(Re, Re)$ by $\psi(\phi) = \phi'$.

Let $\phi_1, \phi_2 \in Hom_R(S, S)$ and $\psi(\phi_1) = \psi(\phi_2)$.

Now $\phi_1' = \phi_2'$. We prove that $\phi_1 = \phi_2$. Let $s \in S$.

$s = \sum e_i r_i$ for a finite number of $i \in I$, $r_i \in R$.

Now $s = \sum e_i r_i = \sum u_i e v_i r_i$

$\phi_1(s) = \phi_1(\sum u_i e v_i r_i) = \sum \phi_1(u_i e v_i r_i) = \sum \phi_1(u_i e) v_i r_i =$

$= \sum \phi_1' (u_i e) v_i r_i = \sum \phi_2' (u_i e) v_i r_i = \sum \phi_2 (u_i e) v_i r_i =$

$= \sum \phi_2 (u_i e v_i r_i) = \phi_2 (\sum u_i e v_i r_i) = \phi_2 (s)$.

Therefore $\phi_1 = \phi_2$ and that ψ is one - one. We prove now that ψ is onto $Hom_{e\text{Re}} (\text{Re}, \text{Re})$.

Let $g \in Hom_{e\text{Re}} (\text{Re}, \text{Re})$. Define $\phi : S \to S$ by

$\phi (s = \sum u_i e v_i r_i) = \sum g (u_i e) v_i r_i$. Clearly $\phi \in Hom_R (S, S)$.

Also $\phi' = g$. So $\psi(\phi) = g$ and hence ψ is onto $Hom_{eRe} (Re, Re)$. We prove now that ψ is ring homomorphism. $\psi(\phi_1 + \phi_2) = (\phi_1 + \phi_2)'$.

$(\phi_1 + \phi_2)' (re) = (\phi_1 + \phi_2)(re) = \phi_1 (re) + \phi_2 (re) = \phi_1' (re) + \phi_2' (re)$

$= (\phi_1' + \phi_2') (re)$ for all $re \in Re$.

Therefore $(\phi_1 + \phi_2)' = \phi_1' + \phi_2' = \psi(\phi_1) + \psi(\phi_2)$

So $\psi(\phi_1 + \phi_2) = \psi(\phi_1) + \psi(\phi_2)$

$(\phi_1 \phi_2)' (re) = (\phi_1 \phi_2)(re) = \phi_1 (\phi_2 (re)) = \phi_1 ((\phi_2 (re))e) =$

$= \phi_1' (\phi_2 (re)) = \phi' (\phi' (re))$ for all $re \in \text{Re}$.

Therefore $(\phi_1 \phi_2)' = \phi_1' \cdot \phi_2'$ and that $\psi(\phi_1 \phi_2) = \psi(\phi_1) \psi(\phi_2)$.

So ψ is a ring isomorphism of $Hom_R (S, S)$ onto $Hom_{e\text{Re}} (Re, Re)$.

Hence $Hom_R (S, S) \cong Hom_{e\text{Re}} (Re, Re)$ as rings.

Dr. R. SRINIVASA RAO
P.G. Department of Mathematics
P.B. Siddhardha College
Vijayawada.

Lesson - 16 WEDDERBURN - ARTIN THEOREM

Introduction 16.0:

In this lesson the wedderburn-Artin theorem is studies. Wedderburn - Artin theorem is a valuable and extremely important structure theorem in rings which describes a basic class of rings in terms of rings of $n \times n$ matrics over division rings.

Proposition 16.1 (Wedderburn - Artin theorem):

(a) A ring R is completely reducible if and only if it is isomorphic toa finite direct product of completely reducible simple rings.

(b) A ring R is completly reducible and simple if and only if it is the ring of all linear trasformations of a finite dimensional vector space.

Proof:

(a) Suppose that R is a completely reducible ring. So R is a direct sum of minimal right ideals.

Since $1 \in R$, 1 belongs to a finite sum of these minimal right ideals and that R is a direct sum of finitely many minimal right ideals. Since R is completely reducible, by lemma 14.8, $Rad\ R = \{0\}$. As $rad\ R \subseteq Rad\ R = \{0\}$, R is semi prime.

So, a minimal right ideal of R is of the form eR for some $e^2 = e \in R$. Since R is a direct sum of finitely many minimal right ideals by proposition 15.9, R is a direct sum of finitely many homogeneous components $H_1, H_2, ...H_n$ (say) and each H_i is a minimal ideal of R. So $R = H_1 \oplus H_2 \oplus .... \oplus H_n$ and H_i is a minimal ideal of R. Now $1 = e_1 + e_2 + ... + e_n$, for some $e_i \in H_i$. Then by proposition $e_1.e_2.................e_n$ are central orthogonal idempotenets and $H_i = e_i R = Re_i$, for all $1 \leq i \leq n$. Now each H_i is a ring with unity e_i.

Therefore R is isomorphic to the direct product of rings H_1, ...H_n. We see now that a right ideal of H_i, $1 \leq i \leq n$ is a right ideal of R. We have $R = H_1 \oplus H_2 \oplus .... \oplus H_n$. Let K be a right ideal ofthe ring H_i. Let $r \in R$. $r = e_1 x_1 + e_2 x_2 + ... + e_n x_n$.$e_j x_j \in H_j$.

Let $k \in K$. Now $k = e_i y$ for some $y \in R$ as $k \in H_i = e_i R$.

$kr = e_i y(e_1x_1 + e_2x_2 + ... + e_nx_n) = e_i ye_1x_1 + e_i ye_2x_2 + ... + e_i ye_nx_n =$

$= e_ie_1yx_1 + e_ie_2yx_2 + ... + e_ie_ntx_n = e_ie_iyx_i = e_iyx_i \in e_iR = H_i$ as e_i are central orthogonal idempotents. Therefore K is a right ideal of R. Similarly we get that an ideal of the ring H_i, $1 \le i \le n$ is an ideal of R. Obviousely any ideal (right ideal) of R contained in H_i, $1 \le i \le n$ is also an ideal (right ideal) of H_i Therefore $K \subseteq H_i$, $1 \le i \le n$ is an ideal (right ideal) of H_i if and only if it is an ideal (right ideal) of R. Since H_i, $1 \le i \le n$ is a minimal ideal of R by the above observation we get that H_i is a simple ring. Also since H_i, $1 \le i \le n$ is a direct sum of minimal right ideals of R, as seen above these are also minimal right ideals of H_i. Hence H_i is a completely reducible and simple ring and R is isomorphic to the direct product of these rings H_1, H_2, ...H_n.

Conversely suppose that R is isomorphic to a finite direct product of completely reducible simple rings. Let $R \cong R_1 \times R_2 \times .... \times R_n$, each R_i is a completely reducible simple ring.. By proposition $R = K_1 \oplus K_2 \oplus .... \oplus K_n$, where K_i are ideals of R and $K_i \cong R_i$ for all $1 \le i \le n$. Since R_i is completely reducible K_i is also a completely reducible ring. As seen above each minimal right ideal of K_i, $1 \le i \le n$ is also a minimal right ideal of R. Since $R = K_1 \oplus K_2 \oplus .... \oplus K_n$ and each K_i is a sum of minimal right ideals of R, R is a sum of minimal right ideals of R.

i.e., R is completely reducible.

(b) Let R be a completely reducible simple ring.

So $\{0\}$ and R are the only ideals of R and $\{0\} \neq R$. If $R^2 = \{0\}$ then 1 = 0, a contradiction to $R \neq \{0\}$. Therefore $R^2 \neq \{0\}$ and that $\{0\}$ is a prime ideal of R i.e. R is prime.

A minimal right ideal of R is of the form eR, for some $e^2 = e \in R$. Let eR be a minimal right ideal of R, $e^2 = e \in R$.

Since Socle $(R_R) = R$, by lemma 15.13, $Hom_R(R, R) \cong Hom_{eRe}(Re, Re)$. But $R \cong Hom_R(R, R)$. As eR is minimal, eRe is a division ring and that R is isomorphic to the ring of all linear transformations of the vector space,

Re_{eRe} (as $R \cong Hom_{eRe}(Re, Re)$). We have to provethat Re_{eRe} is a finite dimensional vector space. To verify that Re_{eRe} is finite dimenssional, it is enough to show that Re_{eRe} is Noetherian. Let $\{K_i / i \in I\}$ be a non-empty family of submodules of Re_{eRe}. Now $K_i R$ is a submodule of Re_{eRe} for all $i \in I$. Since R_R is noetherian and ReR is a submodule of R_R, Re, R_R is also noetherian.

For all $i \in I$, $K_i = K_i\ eRe = K_i\ Re$ (as $k_i e = k_i$) ....(1)

Since ReR_R is noetherian and $\{K_i R / i \in I\}$ is a non-empty family of submodules of ReR_R, this family has a maximal element $K_m R$. We claim that K_m is a maximal element in $\{K_i / i \in I\}$. Suppose that $K_m \subseteq K_i$, for some $i \in I$. Now $K_m\ R \subseteq K_i R$. Since $K_m R$ is maximal, $K_m R = K_i R$. So $K_m R e = K_i Re$. i.e., $K_m = K_i$ (by (1)).

Therefore K_m is a maximal element in $\{K_i / i \in I\}$ and hence Re_{eRe} is Noetherian. So Re_{eRe} is finite dimensional. Hence R is isomorphic to $Hom_{eRe}(Re, Re)$ and $Hom_{eRe}(Re, Re)$ is the ring of linear transformations of a finite dimensional vector space Re_{eRe}.

Conversely assume that $R = Hom_D(V, V)$, where V_D is a finite dimenssional vector space. Let $v_1, v_2, \ldots\ldots\ldots, v_n$ a basis of V_D.

$v \in V$ can be uniquely written as $v = v_1 d_1 + v_2 d_2 + \ldots\ldots\ldots\ldots + v_n d_n, d_i \in D$..

For $1 \le i, j \le n$, define $e_{ij} : V \to V$ by $e_{ij}(v_1 d_1 + v_2 d_2 + \cdots\cdots + v_n d_n) = v_i d_j$. Clearly e_{ij} is a linear transformation. So $e_{ij} \in R$.

For $1 \le i \le n$, Let $A_i = \sum_{j=1}^{n} e_{ij} D$ and let $B_i = \{r \in R / rV \subseteq v_i D\}$. We claim that $A_i = B_i, 1 \le i \le n.$

Let $a \in A_i$. $a = e_{i1} d_1 + e_{i2} d_2 + \ldots\ldots + e_{in} d_n$ for some $d_1, d_2, \ldots\ldots\ldots\ldots, d_n \in D$.

Let $u \in V$. Now $u = v_1 \alpha_1 + v_2 \alpha_2 + \cdots\cdots + v_n \alpha_n, \alpha_i \in D$

$au = (e_{i1}d_1 + e_{i2}d_2 + \ldots\ldots\ldots\ldots + e_{in}d_n)u = v_i d_1 \alpha_1 + v_i d_2 \alpha_2 + \ldots.. + v_i d_n \alpha_n \in v_i d$.

Therefore $a \in B_i$ and that $A_i \subseteq B_i$ Let $r \in R$ and $rV \subseteq v_i D$

Now $r(v_j) = v_i \beta_j$ for some $\beta_j \in D$ where $1 \le j \le n$

Now $b = e_{i1}\beta_1 + e_{i2}\beta_2 + \ldots\ldots\ldots\ldots + e_{in}\beta_n \in A_i$

$b(v_j) = (e_{i1}\beta_1 + e_{i2}\beta_2 + \ldots\ldots\ldots + e_{in}\beta_n)(v_j) = v_j\beta_j = r(v_j)$ for all $1 \le j \le n$.

Since $v_1, v_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots v_n$ is a basis, $b = r$. So $r = b \in A_i$.

Therefore $B_i \subseteq A_i$ and hence $A_i = B_i$ Clearly $B_i = \{r \in R / rV \subseteq v_i D\}$ is a right ideal of R. Therefore A_i is a right ideal of R.

Let $0 \ne a \in A_i$ and $a = e_{i1}d_1 + e_{i2}d_2 + \ldots\ldots\ldots\ldots + e_{in}d_n$, $d_1, d_2 \ldots\ldots\ldots\ldots\ldots d_n \in D$

Since $a \ne 0$, for some $1 \le k \le n$, $d_k \ne 0$. So $d_k^{-1} \in D$.

Now $ae_{k1} = e_{i1}d_k$ and that $e_{i1} = ae_{k1}d_k^{-1} \in aR$.

For $1 \le J \le n$, $e_{ij} = e_{i1}e_{1j} \in aR$ as $e_{i1} \in aR$ and aR is a right ideal.

So, $e_{ij}d \in aR$ for all $d \in D$ and $1 \le j \le n$

Therefore $A_i \subseteq aR$. But $aR \subseteq A_i$ as $a \in A_i$ and A_i is a right ideal of R. Hence $A_i = aR$ and that A_i is a minimal right ideal of R. Since $e_{ii} \in A_i$, we have $1 = e_{11} + e_{22} + \ldots\ldots\ldots\ldots + e_{nn} \in A_1 + A_2 + \ldots\ldots\ldots + A_n$.

Therefore $R = A_1 + A_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots + A_n$. So R is a sum of minimal right ideals A_1, A_2, $\ldots\ldots\ldots A_n$ and that R is completely reducible. We prove now that R is simple. Let $0 \ne r \in R$. To verify that R is simple, it is enough to prove that RrR, the ideal generated by r is R. We have $0 \ne r \in R$.

$r \in R = A_1 + A_2 + \ldots\ldots\ldots + A_n$. Now $r = a_1 + a_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots + a_n$, where $a_j \in A_j$.

Since $r \ne 0$ for some $1 \le i \le n$, $a_i \ne 0$. Now $0 \ne a_i = e_{ii}r \in \mathrm{R}\, rR$,

RrR is the ideal of R generated by r.

Since $a_i \in A_i = \sum_{j=1}^{n} e_{ij}D$, $\quad a_i = e_{i1}r_1 + e_{i2}r_2 + \ldots\ldots\ldots + e_{in}r_n$ for some $r_1, r_2, \ldots\ldots\ldots r_n \in D$.

Since $a_i \neq 0$ for some $1 \leq j \leq n$, $r_j \neq 0$.

Since $a_i \in RrR$, $e_{ij} = a_i e_{jj} r_j^{-1} \in RrR$.

For $1 \leq k \leq n$, $e_{kk} = e_{ki} e_{ij} e_{jk} \in RrR$.

Therefore $1 = e_{11} + e_{22} + \ldots\ldots\ldots\ldots + e_{nn} \in RrR$. Since RrR is an ideal and $1 \in RrR$, we get that $RrR = R$. Hence R is a completely reducible simple ring. This completes the proof.

Exercises

Problem 16.2 : If D is a division ring and V_D has dimension n, then showthat $Hom_D(V, V) \cong D_n$, the ring of $n \times n$ matrices over D.

Solution:

Suppose that V_D is an n - dimensional vector space over the division ring D.

Let $T \in Hom_D(V, V)$ and let $T(v_i) = \sum_{j=1}^{n} v_j \alpha_{ji}$ $i = 1, 2, \ldots\ldots\ldots\ldots, n$, $\alpha_{ji} \in D$.

We associate with T an $n \times n$ matrix $m(T) = \begin{bmatrix} \alpha_{11} & \alpha_{12} \ldots\ldots\ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} \ldots\ldots\ldots & \alpha_{1n} \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots & \ldots\ldots \\ \alpha_{n1} & \alpha_{n2} \ldots\ldots\ldots & \alpha_{nn} \end{bmatrix} \in D_n$

We prove that the mapping $T \to m(T)$ of $Hom \in D(V, V)$ into D_n is a ring isomorphism. Let $S \in Hom_D(V, V)$ and $S(v_i) = \sum_{j=1}^{n} v_j \beta_{ji}$, $i = 1, 2, \ldots\ldots, n$

Now $(T+S)(v_i) = \sum_{j=1}^{n} v_j (\alpha_{ji} + \beta_{ji})$, $i = 1, 2, \ldots., n$.

Therefore $m(T+S)=\left(\alpha_{ji}+\beta_{ji}\right)_{n\times n}=\left(\alpha_{ji}\right)_{n\times n}+\left(\beta_{ji}\right)_{n\times n}=m(T)+m(S)$

$$(TS)(v_i)=T(S(v_i))=T\left(\sum_{k=1}^{n} v_k\beta_{ki}\right)=$$

$$\sum_{k=1}^{n} T(v_k)\beta_{ki}=\sum_{k=1}^{n}\left[\sum_{j=1}^{n} v_j\,\alpha_{jk}\right]\beta_{ki}=\sum_{j=1}^{n} v_i\left[\sum_{k=1}^{n}\alpha_{jk}\,\beta_{ki}\right],$$

Therefore, $m(TS)=\left(r_{ji}\right)_{n\times n}$, where for $1\le i,\ j\le n$

$r_{ji}=\sum_{k=1}^{n}\alpha_{jk}\,\beta_{ki}$. So $m(TS)=m(T)m(S)$.

The above mapping is a ring homomorphism.

Supposethat $M(T)$ is the zero matrix. Then $T(v_i)=0$ forall $i=1,2,.....,n$.

Since $v_1, v_2, ..., v_n$ is a basis, $T=0$. Therefore the above mapping is one - one. Let $A=(a_{ji})_{n\times n}\in D_n$

Define $L(v_i)=\sum_{j=1}^{n} v_j a_{ji}$, $i=1, 2, ..., n$. Since $v_1, v_2, ... v_n$ is a basis,

L can be extended to a linear transformation of V into V. So $L\in Hom_D(V\ V)$.

Clearly $M(L)=A$.

so the mapping $T\to m(T)$ is onto D_n.

Hence $T\to m(T)$ is an isomorphism of $Hom_D(V\ V)$ onto D_n.

Problem 16.3 : Show that $R\ne\{0\}$ is completely reducible if and only if no maximal right ideal of R is large.

Solution : Suppose that R is completely reducible.

Since $1\in R$, R is a direct sum of a finite number of minimal right ideals. Let $R=K_1\oplus K_2\oplus..............\oplus K_n$ where $K_1, K_2, ..., K_n$ are minimal right ideals of R. Let M be a maximal right ideal of R. We claim that M is not large.

13

On the contrary, suppose that M is large. Now $K_i \cap M \neq \{0\}$ as $K_i \neq \{0\}$ and as M is large, where $1 \leq i \leq n$.

Therefore $K_i \cap M = K_i$ for all $i = 1, 2, ..., n$. So, $K_i \subseteq M$ for all $i = 1, 2, ..., n$ and that $K_i + K_2 + ...+ K_n \subseteq M$ $i.e. R \subseteq M$ a contradiction to $M \neq R$.

Therefore M is not large.

Conversely supposethat no maximal rightideal of R is large.

Let K be a right ideal of R. We get a right ideal L of R

such that $K \cap L = \{0\}$ and $K + L$ is large.

Suppose that $K + L \neq R$. Since $1 \in R$, $K + L$ is contained in a maximal right ideal M of R. Since $K + L$ is large, M is also large. A controdiction to the fact that no maximal right ideal of R is large. Therefore $K + L = R$. Therefore $L(R_R)$ is complemented and hence R_R is completely reducible i.e., R is completely reducible.

Problem 16.4:,

Show that the ring of 2×2 matrices over an infinite field has an infinite number of district minimal right ideals.

Solution:

Let F be an infinite field. Let F_2 be the ring of 2×2 matrics over F. $F \times F$ is an abelian group under component wise addition. For $(\alpha , \beta) \in F \times F$ and $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in F_2$,

define $(\alpha , \beta)\begin{bmatrix} a & b \\ c & d \end{bmatrix} = (\alpha a + \beta c , \alpha b + \beta d)$.

This makes $F \times F$, a right F_2 - module. For $(\alpha, \beta) \in F \times F$, define

$(\alpha, \beta)^r = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in F_2 \middle/ (\alpha , \beta)\begin{bmatrix} a & b \\ c & d \end{bmatrix} = (0,0) \right\}$. Clearly $(\alpha, \beta)^r$ is a right ideal of F_2 for all $(\alpha , \beta) \in F \times F$.

Fix $(\alpha , \beta) \in F \times F$, $\alpha \neq 0 , \beta \neq 0$. Clearly $0 \neq \begin{bmatrix} \beta & -\beta \\ -\alpha & \alpha \end{bmatrix} \in (\alpha , \beta)^r$ and $(\alpha, \beta)^r \neq F_2$ as $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin (\alpha , \beta)^r$. Since F is simple, we have that F_2 is simple and hence prime.

Now $K_2 = \left\{ \begin{pmatrix} 0 & 0 \\ x & y \end{pmatrix} \Big/ x , y \in F \right\}$ and $K_1 = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \Big/ x, y \in F \right\}$ are minimal right ideals of F_2 by proposition 15.5 as $K_1 = e_1 F_2$ and $K_2 = e_2 F_2$ and $e_1 F_2 e_1 \cong F$, $e_2 F_2 e_2 \cong F$, where $e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ are idempotents.

Also $F_2 = K_1 \oplus K_2$ So $\{0\} \subseteq K_1 \subseteq K_, \oplus K_2 = F_2$ is a composition series of ${F_2}_{F_2}$ of length 2.

Therefore, $\{0\} \underset{\neq}{\subset} (\alpha, \beta)^r \underset{\neq}{\subset} F_2$ is a composition series, of ${F_2}_{F_2}$, as $\{0\} \underset{\neq}{\subset} (\alpha, \beta)^r \underset{\neq}{\subset} F_2$ can be refined to obtain a composition series of ${F_2}_{F_2}$ and any two composition series have the same length. So $(\alpha, \beta)^r$ is a minimal right ideal of F_2.

Let $s \in R$ and $s \neq 0$ & $s \neq 1$.

Now $(\alpha, \beta s)^r$ is a minimal right ideal of F_2 and

$\begin{bmatrix} \beta & -\beta \\ -\alpha & \alpha \end{bmatrix} \notin (\alpha , \beta s)^r$. Therefore, the minimal right ideals

$(\alpha , \beta s)^r$ and $(\alpha , \beta)^r$ are distinct. Similarly we get that for $0 \neq s$, $0 \neq t$ in R, $(\alpha, \beta s)^r \neq (\alpha, \beta t)^r$, if $s \neq t$

Therefore, we get that $\left\{ (\alpha , \beta s)^r / 0 \neq s \in F \right\}$ is an infinite set of distinct minimal right ideals of F_2.

Dr. R. SRINIVASA RAO
P.G. Department of Mathematics
P.B. Siddhardha College

Lesson - 17 Artinian and Noetherian Rings

Introduction 17.0: In this lesson, Artinian and Noetherian rings are studied. It is proved that the radical of a right Artinian ring is the largest nilpotent ideal and the prime radical of a right Noetherian ring is the largest nilpotent right ideal. Finally Hilbert Basis theorem is proved.

17.1 Definition : A ring R is called right Artinian (Noetherian) if the right module R_R is Artinian (Noetherian).

Theorem 17.2: The radical, $Rad\ R$, of a right Artinian ring is nilpotent.

Proof : Let R be a right Artinian ring. Then R_R is right Artinian. This implies any non-empty family of sub modules of R_R (i.e., right ideals of R) has a minimal element and hence R satisfies the discending chain condition on right ideals. Now $Rad\ R$ is an ideal of R and $Rad\ R \supseteq (Rad\ R)^2 \supseteq (Rad\ R)^3 \supseteq$ .... is a descending chain of right ideals of R. since R satisfies the d.c.c. on right ideals of R, there exists a positive integer n such that $(Rad\ R)^n = (Rad\ R)^{n+1} =$ ....

Put $B = (Rad\ R)^n$. Then $B^2 = B$.

Now we will show that, $B = (0)$

If possible suppose that $B \neq 0$

Write $\mathscr{S} = \{A / A \text{ is a right ideal of } R \text{ such that } A \subseteq B \text{ and } AB \neq (0)\}$.

Since $B \in \mathscr{S}$, $\mathscr{S} \neq \phi$. Since R is Artinian, $\mathscr{S}$ contains minimal elements. So let A be a minimal element in $\mathscr{S}$. Then $AB \neq 0 \Rightarrow$ there exists an element $a \in A$ such that $a \neq 0$ and $aB \neq (0)$.

Now $aB \subseteq A \subseteq B$ and $aBB = aB^2 = aB \neq (0)$

$\therefore aB \in \mathscr{S}$

Since $(0) \neq aB \subseteq A$ and A is a minimal element in $\mathscr{S}$. We have $aB = A$. Since $a \in A$ we have $a = ab$ for some $b \in B$.

Now $b \in B$ and $B = (Rad\ R)^n \subseteq Rad\ R \Rightarrow 1-b$ is invertible. $\Rightarrow$ there exists $c \in R$ such that $(1-b)c=1$.

Consider $a=a\cdot 1=a(1-b)c=ac-abc=ac-ac=0\quad (\because a=ab)$

$\Rightarrow a=0$ a contradiction.

This contradiction arises due to our supposition $B \neq 0$. So $B=(0)$ and hence $(Rad\ R)^n=(0)$. Thus there exists a positive integer n such that $(Rad\ R)^n=(0)$ and hence $Rad\ R$ is nilpotent

Corollary 17.3 : In a right Artinian ring, the radical is the largest nilpotent ideal.

Proof: Let R be a right Artinian ring

Claim: $Rad\ R$ is the largest nilpotent ideal of R.

By the above theorem 17.2, $Rad\ R$ is a nilpotent ideal of R. We know that $rad\ R \subseteq Rad\ R$.

Now we will show that every nilpotent ideal of R is contained in $Rad\ R$.

Let I be any nilpotent ideal of R. Then $I^n=(0)$ for some positive integer $n \Rightarrow I^n \subseteq P$ for any prime ideal P of $R \Rightarrow I \subseteq P$ for any prime ideal P of R.

$\Rightarrow I \subseteq rad\ R \Rightarrow I \subseteq Rad\ R\ (\because rad\ R \subseteq Rad\ R)$. So $Rad\ R$ is the largest nilpotent ideal of R.

Corollary 17.4 : If R is right Artinian, then $Rad\ R = rad\ R$.

Proof: Suppose R is a right Artinian ring. Then by theorem 17.2, $Rad\ R$ is a nilpotent ideal of R. Since every nilpotent ideal is contained in the prime radical of R, we have $Rad\ R \subseteq rad\ R$. But $rad\ R \subseteq Rad\ R$. Hence $rad\ R = Rad\ R$.

We recall that a ring R is a regular ring if to each $a \in R$, there exists an element $x \in R$ such that $a=axa$, put $e=ax$. Then $e=e^2$ and $aR=eR$.

Remark 17.5 : A ring R is a regular ring if and only if every principal right ideal of R is a direct summand of R.

For let R be a ring.

Suppose R is a regular ring.

Let L be any prinicipal right ideal of R. Then $L=aR$ for some $a \in R$. Since R is regular, there exists $x \in R$ such that $a=axa$. Put $e=ax$. Then e is an idempotent.

consider $eR = axR \subseteq aR = axaR \subseteq axR = eR \Rightarrow eR = aR$

$\therefore$ $L = eR$ for some idemopotent $e \in R$.

We know that R is the direct sum of eR and $(1-e)R \Rightarrow R$ is the direct sum of L and $(1-e)R$. Hence L is a direct summand of R. Thus every prinicipal right ideal of R is a direct summand of R.

Conversely suppose that every principal right ideal of R is a direct summand of R.

Let $a \in R$.Then aR is a principal right ideal of R. By our supposition, these exists a right ideal L of R such that $R = aR \oplus L$. Since $1 \in R$, we have $1 \in aR + L$. Then $1 = e + f$ for some $e \in aR$ and $f \in L$.

Consider $1 = e + f \Rightarrow a = ea + fa \Rightarrow a - ea = fa \in L$

$\Rightarrow a - ea \in aR \cap L \; (\because e \in aR \text{ and } a \in aR)$

$\Rightarrow a - ea = 0 \; (\because aR \cap L = (0)) \Rightarrow a = ea$

Since $e \in aR$, we have $e = ax$ for some $x \in R$

Consider $a = ea = axa$

Thus , for $a \in R$, there exists $x \in R$ such that $a = axa$

$\therefore R$ is a regular ring.

Lemma 17.6 : In a regular ring every finitely generated right ideal is principal.

Proof: Let R be a regular ring and L be a finitely generated right ideal of R.

We prove this by induction on the number of generators of L.

If L is generated by a single element, then L is a principal right ideal of R.

Suppose L is generated by two elements a and b of R. Then $L = aR + bR$. Since R is a regular ring, there exists $r \in R$ such that $a = ara$. Put $e = ar$. Then e is an idempotent and $eR = aR$.

Now $1 = e + (1-e) \Rightarrow b = eb + (1-e)b \Rightarrow bR \subseteq ebR + (1-e)bR$ ....(1)

Consider $(1-e)bR = (b - eb)R \subseteq bR + ebR \subseteq bR + eR$ ....(2)

From (1) and (2), $L = aR + bR \subseteq eR + ebR + (1-e)\,bR \subseteq eR + (1-e)bR \subseteq aR + bR = L$

$\therefore\ L = eR + (1-e)bR$

Now $(1-e)bR$ is a principal right ideal of $R \Rightarrow$ there exists an idempotent $f \in R$ such that $(1-e)bR = fR \Rightarrow f = (1-e)\ bs$ for some $s \in R$.

Consider $ef = e(1-e)bs = 0$

Put $g = f(1-e)$. Then $gf = f(1-e)f = f(f - ef) = f^2 = f \quad (\because ef = 0) \Rightarrow gf = f$

Consider $g^2 = gf(1-e) = f(1-e) = g$

Consider $eg = ef\ (1-e) = 0 \quad (\because ef = 0)$

and $ge = f(1-e)e = 0$

So g is an idempotent in R such that $ge = eg = 0$.

Now $g = f(1-e) \in fR$ and $f = gf \in gR$

$\Rightarrow gR \subseteq fR$ and $fR \subseteq gR$

$\therefore\ fR = gR$

Consider $L = eR + (1-e)bR = eR + fR = eR + gR$

Now we will show that $eR + gR = (e+g)R$.

Clearly $(e+g)R \subseteq eR + gR$.

Let $x \in eR + gR \Rightarrow x = er + gt$ for some $r,\ t \in R$

Consider $(e+g)x = (e+g)(er+gt) = eer + egt + ger + ggt$

$= er + gt = x\ (\because eg = 0\ and\ ge = 0) \Rightarrow x = (e+g)x \in (e+g)R$

So $eR + gR \subseteq (e+g)R$ and hence $eR + gR = (e+g)R$.

Consequently $L = (e+g)R$, which is a prinicipal right ideal of R.

So the result is true for $n=2$.

Assume $n>2$ and the result is true for all $m<n$.

Suppose $a_1, a_2, ..., a_n$ are generators of L. Then $L = a_1R + a_2R + ... + a_nR$.

Write $M = a_1R + a_2R + ... + a_{n-1}R$. Then by our assumption M is a principal right ideal of R. This implies $M = aR$ for some $a \in R$. now $L = aR + a_nR$. Again by our assumption, L is a principal right ideal of R. Hence the result is true for all n.

Thus every finitely generated right ideal of a regular ring is a principal right ideal.

17.7 Theorm: The following statements concerning the ring R are equivalent:

(1) R is completely reducible

(2) R is right Artinian and regular

(3) R is right Artinian and semi primitive

(4) R is right Artinian and semiprime

(5) R is right Noetherian and regular

Proof : Assume (2) i.e. R is right Artinian and regular

Let $a \in Rad\ R$. Since R is regular, there exists $r \in R$ such taht $a = ara$. Then $(1-ar)a = 0$

Since $a \in Rad\ R$, we have $ar \in Rad\ R$. Then $1-ar$ is invertible. This implies there exists $s \in R$ such that $(1-ar)s = s(1-ar) = 1$

Consider $a = 1 \cdot a = s(1-ar)a = s \cdot 0 = 0$ $(\because (1-ar)a = 0) \Rightarrow a = 0$

Since $a \in Rad\ R$ is arbitrary, we have $Rad\ R = (0)$.

$\therefore$ R is semiprimitive and hence R is right Artinian and semiprimitive.

So $(2) \Rightarrow (3)$

Assume (3) i.e. R is right Artinian and semiprimitive

Then $Rad\ R = (0)$. Since $rad\ R \subseteq Rad\ R$, we have $rad\ R = (0)$. Therefore R is semiprime and hence R is right Artinian and semiprime.

So $(3) \Rightarrow (4)$

Assume (4) : i.e. R is right Artinian and semiprime.

Since R is right Artinian, by theorem 17.2, $Rad\ R$ is nilpotent. Then $Rad\ R$ is contained in every prime ideal of R. This implies $Rad\ R \subseteq rad\ R$. Since R is semi prime, $rad\ R = (0)$. This implies $Rad\ R = (0)$ and hence the intersection of all maximal right ideals of R is zero.

Since R contains 1, R has maximal right ideals.

Write

$$\mathscr{S} = \{L_1 \cap L_2 \cap \ldots\ldots\ldots \cap L_n / \text{each } L_i \text{ is a maximal right ideal of } R \text{ and } n \text{ is a positive integer}\}$$

Then $\mathscr{S} \neq \phi$. Since R is Artinian, $\mathscr{S}$ contains minimal elements. Let $B = L_1 \cap L_2 \cap \ldots\ldots\ldots\ldots \cap L_n$ be a minimal elements in $\mathscr{S}$. Now we will show that $B = (0)$. Let M be any maximal right ideal of R. Then $B \cap M \in \mathscr{S}$ and $B \cap M \subseteq B$. Since B is a minimal element in $\mathscr{S}$, we have $B \cap M = B$. This implies $B \subseteq M$. Since M is an arbitrary maximal ideal of R, we have $B \subseteq Rad\ R$. Since $Rad\ R = (0)$, We have $B = (0)$. So $L_1 \cap L_2 \cap \ldots\ldots\ldots \cap L_n = (0)$. Since B is a minimal element in $\mathscr{S}$, $L_i \not\supseteq \bigcap_{j \neq i} L_j$ for $i = 1, 2, \ldots\ldots, n$.

Put $A_i = \bigcap_{j \neq i} L_j$ for $i = 1, 2, \ldots\ldots, n$. Then $A_i \not\subseteq L_i$ for all i. Since L_i is maximal right ideal of R, we have $R = A_i + L_i$ for $i = 1, 2, \ldots\ldots, n$. Also $A_i \cap L_i = (0)$.

$\therefore R = A_i \oplus L_i$, the direct sum, for $i = 1, 2, \ldots\ldots, n$.

By a known result, $R/L_i \cong A_i$ for $i = 1, 2, \ldots\ldots, n$. Consequently, A_i is irreducible and hence A_i is a minimal right ideal of R.

Since $R = A_i + L_i$, we have $1 \in A_i + L_i$. Then $1 = e_i + f_i$ for some $e_i \in A_i$ and $f_i \in L_i$ for $i = 1, 2, \ldots\ldots, n$. It is easy to verify that e_i is an idempotent for $i = 1, 2, \ldots\ldots, n$.

Now $1 - e_i = f_i \in L_i$ for $i = 1, 2, \ldots\ldots, n$.

Put $e = \sum_{i=1}^{n} e_i$.

Now we will show that $e - 1 = 0$

For $j = 1, 2, \ldots\ldots, n$, $A_j \subseteq L_i$ for $i \neq j$. Then

$$e-1=(e_i-1)+\sum_{j\neq i} e_j \in L_i \text{ for } i=1,2,\ldots\ldots,n$$

$$\left(\because 1-e_i \in L_i \text{ and } e_j \in A_j' \text{ for } j=1,2,\ldots\ldots,n\right)$$

$$\Rightarrow e-1 \in \bigcap_{i=1}^{n} L_i \Rightarrow e-1=0 \left(\because \bigcap_{i=1}^{n} L_i=(0)\right)$$

$$\Rightarrow e=1 \Rightarrow \sum_{i=1}^{n} e_i=1 \Rightarrow 1 \in \sum_{i=1}^{n} A_i \Rightarrow R=\sum_{i=1}^{n} Ai$$

$\Rightarrow R$ is completely reducible.

So $(4) \Rightarrow (1)$.

Next we will show that (1) implies (2) and (5)

Assume (1) i.e. R is completely reducible.

Then R is a direct sum of a fimite number of minimal right ideals $A_1, A_2, \ldots\ldots\ldots A_n$. This implies $R = A_1 + A_2 + \ldots\ldots + A_n$ and each A_i is non-zero.

Consider $(0) \underset{\neq}{\subset} A_1 \underset{\neq}{\subset} A_1 + A_2 \underset{\neq}{\subset} \ldots\ldots\ldots \underset{\neq}{\subset} R$ is a composition series of $R_R \Rightarrow R$ is right Artinian and right Noetherian.

Since R is completely reducible, $L(R)$ is complemented. Then each right ideal of R is a direct summand of R and hence every principal right ideal of R is a direct summand of R. Then by remark 17.5, R is regular.

Hence (1) $\Rightarrow$ (2) and (1) $\Rightarrow$ (5)

Next we will show that (5) $\Rightarrow$ (1)

Assume (5) : i.e. R is right Noetherian and regular.

Since R is right Noetherian, every right ideal of R is finitely generated. Since R is regular, by lemma 17.6, every finitely generated right ideal is a principal right ideal. By remark 17.5, every principal right ideal of R is a direct summand of R. Threrefore every right ideal of R is a direct summand of R and hence $L(R)$ is complemented. By a known result, R is completely reducible.

So (5) $\Rightarrow$ (1)

Thus all conditions are equivalent.

17.8 Theorem : If R is right Artinian, then any right R - module is Noetherian if and only if it is Artinian.

Proof: Let R be a right Artinian ring.

Put $N = Rad\, R$. Since R is right Artinian, by theorem 17.2, N is nilpotent. Then there exists a positive integer n such that $N^n = (0)$.

Let A be any right R module such that A is Artinian.

Clearly AN^i is an R - submodule of A_R for $i = 1, 2, \ldots\ldots, n$.

Consider the chain of sub modules $A \supseteq AN \supseteq AN^2 \supseteq \ldots\ldots\ldots\ldots AN^{n-1} \supseteq AN^n = (0)$ with factor modules,

$$F_R = \frac{AN^{k-1}}{AN^k} \text{ for } k = 1, 2, \cdots\cdots, n$$

Define $\bullet : F_k \times \frac{R}{N} \to F_k$ as $\left(x + AN^k\right) \bullet (\alpha + N) = x\alpha + AN^k$ for all $x \in AN^{k-1}$ and for all $\alpha \in R$.

Then F_k is a right R/N - module and also F_k is an R - module. Also F_k is Artinian for $k = 1, 2, \cdots\cdots\cdots, n$. Since R is Artinian, by a known theorem, R/N is also Artinian.

Since R/N is Artinian and semi primitive, by theorem 17.7, R/N is completely reducible. Then by a known result, F_k is completely reducible as an R/N - module. This implies F_k is completely reducible as an R-module.

($\because R$ sub modules of F_k are precisely the R/N sub-modules of F_k).

Since F_k is completely reducible and F_k is Artinian, F_k is the direct sum of a finite number of irreducible R - submodules of F_k. Then F_k has a composition series and hence F_k is Noetherian as an R - module for $k = 1, 2, \ldots., n$.

Therefore $AN^{n-1} = F_n$ and $\frac{AN^{n-2}}{AN^{n-1}} = F_{n-1}$ are Noetherian. Then by a known theorem, AN^{n-2} is Noetherian. Continuing in this way $\frac{A}{AN}$ and AN are Noetherian and hence A is Noetherian.

Interchanging the words "Artinian" and "Noetherian" in the above proof, we get the converse part.

17.9 Corollary : Every right Artinian ring is right Noetherian.

Proof : Suppose R is a right Artinian ring. Then R_R is right Artinian. Since R is right Artinian, by theorem 17.8, R_R is right Noetherian and hence R is right Noetherian.

17.10 Reamrk : The converse of the above corollary need not be true.

Ex : The ring of integers is right Noetherian but not right Artinian.

17.11 Theorem : In a right Noetherian ring the prime radical is the largest nilpotent right ideal.

Proof : Let R be a right Noetherian ring.

The family $\mathscr{S}$ of all nilpotent right ideal . of R is non-empty. Since R is right Noetherian, $\mathscr{S}$ contains a maximal element say N. Since N is a nilpotent right ideal of R, there exists a positive integer p such that $N^p = (0)$.

Now we will show that N is the largest nilpotent right ideal of .

Let L be any nilpotent right ideal of R. Then there exists a positive integer k such that $L^k = (0)$.

Now $(N+L)^{p+k} = (0)$. This implies $N+L$ is a nilpotent right ideal of R. Since $N \subseteq N+L$ and N is a maximal element in $\mathscr{S}$, we have $N = N+L$ and hence $L \subseteq N$.

Therefore N is the largest nilpotent right ideal of R. Now we will show that N is an ideal of R. For this, it is enough if we show that $RN \subseteq N$

Consider $(RN)^k = RNRN$.............RN k times

$$\subseteq RN^k = (0) \Rightarrow (RN)^k = (0) \Rightarrow RN \text{ is nilpotent.}$$

Since N is nilpotent and RN is nilpotent, we have $N + RN$ is also nilpotent. Since $N \subseteq N + RN$ and N is maximal element in $\mathscr{S}$, we have $N = N + RN$ and hence $RN \subseteq N$. Therefore N is an ideal of R. Since N is a nilpotent ideal of R, we have $N \subseteq rad\, R$. Consider the ring $\frac{R}{N}$. Any right ideal of $\frac{R}{N}$ is of the form $\frac{A}{N}$ where A is a right ideal of R such that $N \subseteq A$. Let $\frac{M}{N}$ be any nilpotent right ideal of $\frac{R}{N}$. Then $\left(\frac{M}{N}\right)^s = (0)$ in $\frac{R}{N}$ for some positive integer s.

$\Rightarrow \ M^s \subseteq N \Rightarrow M^{sp} \subseteq N^p = (0) \Rightarrow M^{sp} = (0)$

Therefore M is a nilpotent right ideal of R.

Since N is the largest nilpotent right ideal of R, we have $M \subseteq N$ and hence $M = N$. This implies $\frac{M}{N} = (0)$ in $\frac{R}{N}$. This shows that $\frac{R}{N}$ has no non-zero nilpotent right ideals and hence $\frac{R}{N}$ has no non-zero nilpotent ideals. Then by a known theorem, $\frac{R}{N}$ is semiprime. We know that $rad\,R$ is the smallest ideal K of R such that $\frac{R}{K}$ is semiprime. Since N is an ideal of R such that $\frac{R}{N}$ is semiprime, we have $rad\ R \subseteq N$. Hence $rad\ R = N$. Therefore $rad\,R$ is the largest nilpotent right ideal of R.

17.12 Definition : A subset S of a ring R is called a nil sub set if every element of S is nilpotent.

17.13 Remark : The prime radical of any ring is a nil subset.

17.14 Theorem : In a right Noetherian ring the prime radical is the largest nil left ideal.

Proof : Let R be a right Noetherian ring.

Claim : The prime radical $rad\,R$ is the largest nil left ideal of R.

By a known result, every element of $rad\,R$ is nilpotent and so $rad\,R$ is a nil left ideal of R.

case (i) : Assume that R is semi prime

Since R is semiprime, $rad\,R = (0)$.

Let N be any nil left ideal of R.

Now we will show that $N = (0)$

If possible suppose that $N \neq (0)$.

For any $0 \neq n \in N$, the set $n^r = \{s \in R / ns = 0\}$ is a right ideal of R and $1 \notin n^r$.

Put $\mathscr{S} = \{n^r / 0 \neq n \in N\}$

Since $N \neq (0)$, we have $\mathscr{S} \neq \phi$. Since R is right Noetherian, $\mathscr{S}$ contains maximal elements.

So let n^r be a maximal element in $\mathscr{S}$. Then $n \neq 0$ and $n \in N$.

Now we will show that $nRn = (0)$.

Let x be any element in R. If $xn = 0$, then $nxn = 0$. Suppose $xn \neq 0$. Since $n \in N$ and N is a left ideal of R, we have $xn \in N$. Then xn is nilpotent. Let k be the smallest positive integer such that $(xn)^k = 0$. Then $k > 1$ and $(xn)^{k-1} \neq 0$. Now $\left((xn)^{k-1}\right)^r \in \mathscr{S}$ and $n^r \subseteq \left((xn)^{k-1}\right)^r$. Since n^r is a maximal element in $\mathscr{S}$, $n^r = \left((xn)^{k-1}\right)^r$. This implies $xn \in n^r$ and hence $nxn = 0$. Since $x \in R$ is arbitrary, we have $nRn = (0)$. Since R is semi prime, we have $n = 0$; which is a contradiction to the fact that $n \neq 0$. Therefore $N = (0)$

Next consider the general situation where R is no longer assumed to be semiprime. Let N be any nil left ideal of R and $\pi : R \to \frac{R}{rad\ R}$ be the canonical epimorphism. Since N is a nil left ideal of R, $\pi(N)$ is a nil left ideal of R. Consider $\pi(N) = \{n + rad\ R / n \in N\}$

$$= \frac{N}{rad\ R} = \frac{(N + rad\ R)}{rad\ R}$$

Since R is Noetherian, by a known result, $\frac{R}{rad\ R}$ is Noetherian. Also $\frac{R}{rad\ R}$ is semiprime. Then by case (i), $\frac{(N + rad\ R)}{rad\ R} = rad\ R$, which is the zero element in $\frac{R}{rad\ R}$. This implies $N + rad\ R \subseteq rad\ R$ and hence $N \subseteq rad\ R$. So if N is a nil left ideal of R, then $N \subseteq rad\ R$. Thus $rad\ R$ is the largest nil left ideal of R.

17.15 Corollary : In a right Noetherian ring every nil ideal is nilpotent.

Proof : Let R be a right Noetherian ring. Then by Theorem 17.11, $rad\ R$ is the largest nilpotent right ideal of R and so $rad\ R$ is a nilpotent ideal of R. Let I be any nil ideal of R. Then I is a nil left ideal of R. Then by the above theorem 17.14, $I \subseteq rad\ R$. Since $rad\ R$ is nilpotent, we have I is nilpotent. Thus every nil ideal in a right Noetherian ring is nilpotent.

The following important result is known as the Hilbert Basis Theorem.

17.16 Theorem : Let $R[x]$ be the ring obtained from the ring R by adjoining an indeterminate x which commutes with all elements of R. Then $R[x]$ is right Noetherian if R is.

Proof : Suppose R is a right Noetherian ring.

Given that $R[x]$ is the ring obtained from R by adjoining an indeterminate x which commutes with all elements of R.

Claim : $R[x]$ is right Noetherian.

Since R is right Noetherian, by a known result, every right ideal of R is finitely generated.

To show $R[x]$ is right Noetherian, it is enough if we show that every right ideal of $R[x]$ is finitely generated.

Let K be any right ideal of $R[x]$

For $i=0,1,2,\ldots\ldots\ldots$, put $K_i = \left\{ r \in R \middle/ \begin{array}{l} \text{there is a polynomial of degree } i \text{ in } K \text{ with leading} \\ \text{coefficient } r \text{ or } r=0 \end{array} \right\}$

Now we will show that K_i is a right ideal of R for $i=0,1,2,\ldots\ldots\ldots$. Since $0 \in K_i$, we have $K_i \neq \phi$ for $i=0,1,2,\ldots\ldots\ldots$.

Let $r_1, r_2 \in K_i$, Then there exist polynomials f and g in K such that $f = r_1 x^i + \ldots\ldots\ldots + c_1$ and $g = r_2 x^i + \ldots\ldots\ldots\ldots + c_2$

Consier $f-g=(r_1-r_2)x^i+\ldots\ldots\ldots+(c_1-c_2)$. This implies r_1-r_2 is the leading coefficient of $f-g$ and so $r_1-r_2 \in K_i$.

Let $r_1 \in K_i$ and $r \in R$. Then there exists a polynomial f in K such that $f = r_1 x^i + \ldots\ldots + c$.

Consider $fr = r_1 r x^i + \ldots\ldots\ldots\ldots + cr$. This implies $r_1 r$ is the leading coefficient of the polynomial fr and and so $r_1 r \in K_i$. Therefore K_i is a right ideal of R for $i=0,1,2,\ldots\ldots\ldots$

Next we will show that $K_i \subseteq K_{i+1}$ for $i=0,1,2,\ldots\ldots\ldots$

Let $r \in K_i$. If $r=0$ then $r \in K_{i+1}$.

Suppose $r \neq 0$. Then there exists a polynomial $f \in K$ such that $f = rx^i + ... + c$. Since $f \in K$ and since $x \in R[x]$ and K is a right ideal of $R[x]$, we have $fx \in K$ and $fx = rx^{i+1} + ... + cx$. Then $r \in K_{i+1}$. Therefore $K_i \subseteq K_{i+1}$.

Hence $\{K_i\}_{i=0}^{\alpha}$ is an ascending chain of right ideals in R. Since R is right Noehterian, there exists a positive integer n such that $K_n = K_{n+1} = ...$

Since R is right Noetherian, by a known result, $K_0, K_1, K_2, ..., K_n$ are finitely generated right ideals of R. So let $K_i = \sum_{j=1}^{mi} b_{ij} R$ for $i = 0, 1, 2, ..., n$.

Since $b_{ij} \in K_i$, there exists a polynomial $P_{ij} \in K$ of degree i with leading coefficient b_{ij}.

Write $X = \left\{ P_{ij} / 1 \leq j \leq m_i \text{ and } 0 \leq i \leq n \right\}$

Now we will show that K is generated by X.

i.e., $K = \langle X \rangle = \sum_{i=0}^{n} \sum_{j=1}^{mi} P_{ij} R[x]$, Clearly $\langle X \rangle \subseteq K$.

Suppose $K \neq \langle X \rangle$. Put $S = K \setminus \langle X \rangle$. Then $S \neq \phi$. Let $f \in S$ be a polynomial of minimal degree and let deg $f = t$. Write $f = cx^t + ... + c_0$. Now f is a polynomial in K of degree t, with leading coefficient c. Then $c \in K_t = \sum_{j=1}^{m_t} b_{tj} R$. This implies $c = \sum_{j=1}^{m_t} b_{tj} r_{tj}$ for some $r_{tj} \in R$ for $j = 1$, 2, ..., m_t.

Case (i) : Suppose $t < n$

Consider the polynomial $f - \sum_{j=1}^{m_t} P_{tj} r_{tj} \in K$ and deg $\left(f - \sum_{j=1}^{m_t} P_{tj} r_{tj} \right) \leq t - 1$. This implies $- \sum_{j=1}^{m_t} p_{tj} r_{tj} \notin S$. Consequently $f - \sum_{j=1}^{m_t} P_{tj} r_{tj} \in \langle X \rangle$ and hence $f \in \langle X \rangle$; a contradiction.

Case (ii) : Suppose $t \geq n$. Then $K_t = K_n$

Now $c \in K_t = K_n \Rightarrow c = \sum_{j=1}^{m_n} b_{nj} s_{nj}$ for some $s_{nj} \in R$ for $j = 1, 2, ..., m_n$. Then the polynomial

$f - \sum_{j=1}^{m_n} P_{nj} x^{t-n} s_{nj} \in K$ and the degree of this polynomial is less than or equal to $t-1$. This implies

$f - \sum_{j=1}^{m_n} P_{nj} x^{t-n} s_{nj} \notin S$. Consequently $f - \sum_{j=1}^{m_n} P_{nj} x^{t-n} s_{nj} \in \langle X \rangle$ and hence $f \in \langle X \rangle$; which is a contradiction.

Therefore $K = \langle X \rangle = \sum_{i=0}^{n} \sum_{j=1}^{m_i} P_{ij} R[x]$ and hence K is finitely generated.

Thus every right ideal of $R[x]$ is finitely generated. Hence by a known result, $R[x]$ is Noetherian.

17.17 Corollary : Let $R[x_1, x_2, ..., x_n]$ be the ring obtained from R by adjoining n indeterminates x_i which commute with all elements of R and with each other. Then this is right Noetherian if R is.

Proof : Suppose R is a right Noetherian ring. Then by Theorem 17.16, $R[x_1]$ is right Noetherian. Again by Theorem 17.16, $R[x_1][x_2]$ is right Noehterian. But $R[x_1, x_2] = R[x_1][x_2]$ and so $R[x_1, x_2]$ is right Noetherian. If we continue this process, we have $R[x_1, x_2, ..., x_n]$ is right Noetherian.

Dr. V. SAMBASIVARAO
Department of Mathematics
Acharya Nagarjuna University.

Lesson - 18 PROJECTIVE MODULES

18.0 Introduction :

In this lesson, the notion of projective modules is introduced. All projective modules are characterized in several ways and some examples are given. some important properties of projective modules are studied.

18.1 Definition :

We recall that the (external) direct sum $A = \overset{*}{\underset{i\in I}{\Sigma}} A_i$ of a family of modules consists of all

$a \in \underset{i\in I}{\pi} A_i$ such that $a(i)=0$ for all but a finite number of i.

For $i \in I$, the canonical mapping $K_i : A_i \to A$ is defined by $\left(K_i\left(a_i\right)\right)(j) = \begin{cases} a_i & if \quad j=i \\ 0 & if \quad j \neq i \end{cases}$

18.2 Remark :

$\underset{i\in I}{\Sigma} K_i\left(a(i)\right) = a$ for all a in $A = \overset{*}{\underset{i\in I}{\Sigma}} A_i$

18.3 Proposition :

If A is the direct sum of a family of modules $\{A_i\}_{i\in I}$ with canonical mappings $K_i : A_i \to A$ then, for every module B and for every family of homomorphisms $\phi_i : A_i \to B$, there exists a unique homomorphism $\phi : A \to B$ such that $\phi \cdot K_i = \phi_i$. More over, this property characterizes the direct sum up to isomorphism.

The proposition is illustrated by the "Commutative" diagram:

$$\begin{tikzcd} B & A \arrow[l, dashed, "\phi"'] \\ & A_i \arrow[u, "k_i"'] \arrow[ul, "\phi_i"] \end{tikzcd}$$

Proof: Suppose that A is the direct sum of family $\{A_i\}_{i\in I}$ of R - modules.

Let B be an R - module and Let $\phi_i : A_i \to B$ be a homomorphism for $i \in I$.

Let $a \in A$

Then $a = \sum_{i \in I} K_i(a(i))$

Define $\phi : A \to B$ by $\phi(a) = \sum_{i \in I} \phi_i(a(i))$

Now, we show that ϕ is an R - homomorphism.

Let $r \in R$ and Let $a, a^1 \in A$.

Then $a = \sum_{i \in I} K_i(a(i))$ and $a^1 = \sum_{i \in I} K_i(a^1(i))$

So $a + a^1 = \sum_{i \in I} K_i((a + a^1)(i))$ and $ar = \sum_{i \in I} K_i((ar)(i))$

Now $\phi(a + a^1) = \sum_{i \in I} \phi_i((a + a^1)(i)) = \sum_{i \in I} \phi_i(a(i) + a^1(i))$

$$= \sum_{i \in I} \phi_i(a(i)) + \sum_{i \in I} \phi_i(a^1(i))$$

$$= \phi(a) + \phi(a')$$

and $\phi(ar) = \sum_{i \in I} \phi_i((ar)(i)) = \sum_{i \in I} \phi_i(a(i)r)$

$$= \sum_{i \in I} \phi_i(a(i))r = \left(\sum_{i \in I} \phi_i(a(i))\right)r = \phi(a)r$$

$\therefore \phi$ is an R - homomorphism.

Fix j in I

Now, for any $a_j \in A_j$,

$$(\phi \cdot K_j)(a_j) = \phi(K_j(a_j)) = \sum_{i \in I} \phi_i(K_j(a_j)(i))$$

$$=\phi_j\left(K_j\left(a_j\right)(j)\right)=\phi_j\left(a_j\right).$$

Thus $\phi \cdot K_j = \phi_j$ for all j in I .

Uniqueness : Suppose $\psi : A \to B$ is an R - homomorphism such that $\psi \cdot K = \phi \;\; \forall\, i \in I$.

For any $a \in A$, $\phi(a) = \sum \phi\left(a(i)\right) = \sum \psi \cdot K\left(a(i)\right)$

$$= \sum_{i\in I} \psi\left(K_i\left(a(i)\right)\right) = \psi\left(\sum_{i\in I} K_i\left(a(i)\right)\right)$$

$$=\psi(a)$$

$$\Rightarrow \phi = \psi$$

Thus there exists a unique homomorphism $\phi \colon A \to B$ such that $\phi \circ K_i = \phi_i \;\; \forall i \in I$.

Converse:

Suppose that A^1 is another module with monomorphisms $K_i^1 : A_i \to A^1$ satisfying the conditions of the proposition.

i.e., given any module B, a family of homomorphisms $\phi_i \colon A_i \to B,\;\; i \in I$, there exists a unique homomorphism $\psi \colon A^1 \to B$ such that $\psi_0 K_i^1 = \phi_i$.

So the diagrams

$$\begin{tikzcd} B & A \arrow[l, dashed, "\phi"'] \\ & A_i \arrow[u, "k_i"'] \arrow[ul, "\phi_i"] \end{tikzcd} \qquad \begin{tikzcd} B & A^1 \arrow[l, dashed, "\psi"'] \\ & A_i \arrow[u, "k_i'"'] \arrow[ul, "\phi_i'"] \end{tikzcd}$$

(1) (2)

are commutative.

Take $B = A^1$ and $\phi_i = K_i^1$ in (1)

Then, by the first part of the proposition, we get a unique homomorphism $K^1 : A \to A^1$ such that $K^1 o K_i = K_i^1$

Take B = A and $\phi_i = K_i$ in (2)

Then, by our supposition, we get a unique homomorphism

$K : A' \to A$ Such that $KOK'_i = K_i$.

$\therefore\ KoK'oK_i = KoK' = K_i = I_A o K_i$ where I_A is the identity mapping of A.

By the uniqueness property, $KoK' = I_A$.

Similarly $K'oK = I_{A'}$ where $I_{A'}$ isthe identity mapping of A'.

$\therefore\ A \cong A'$

18.4 Corollary:

If A is isomorphic to the direct sum of modules $\{A_i\}$ with canonical mappings $K_i : A_i \to A$, then there exist mappings $\pi_i : A \to A_i$ (also called canonical) such that $\pi_i o K_i = 1$ and $\pi_i o K_j = 0$ when $i \neq j$.

Proof:

For fixed i, consider the mapping $\delta_{ij} : A_j \to A_i$

where $\delta_{ij} = \begin{cases} 1 & if \quad i = j \\ 0 & if \quad i \neq j \end{cases}$

By the above proposition, there exists a (unique) homomorphism $\pi_i : A \to A_i$ such that $\pi_i o K_j = \delta_{ij}$

$$\begin{tikzcd} A_i & A \arrow[l, dashed, "\pi_i"'] \\ & A_j \arrow[u, "k_j"'] \arrow[ul, "\delta_{ij}"] \end{tikzcd}$$

i.e., $\pi_i o K_i = 1$, the identity mapping of A_i and $\pi_i o K_j = 0$ when $i \neq j$

18.5 Remark:

The above corollary implies K_i is mono and π_i is epi for every i.

18.6 Definition:

A module M_R is called free if it has a basis $\{m_i\}_{i\in I}$, where $m_i \in M$, such that every element $m \in M$ can be written uniquely in the form $m = \sum_{i\in I} m_i r_i$ where $r_i \in R$ and all but a finite number of the r_i are 0.

18.7 Remark:

The above definition implies that $\sum_{i\in I} m_i r_i = 0$ only when all $r_i = 0$.

In particular, $m_i r = 0 \Rightarrow r = 0$.

18.8 Lemma:

A module M_R is free if and only if it is isomorphic to a direct sum of copies of R_R.

Proof:

Suppose M_R is free.

Then M has a basis, Let it be $\{m_i\}_{i\in I}$.

So every element $m \in M$ can be written uniquely as $m = \sum_{i\in I} m_i r_i$, where $r_i \in R$ and all but a finite number of the r_i's are 0.

Therefore, $M = \sum_{i\in I} m_i R$

Let $x \in m_i R \cap \sum_{j\neq i} m_j R$.

$\Rightarrow x = m_i r_i = \sum_{j\neq i} m_j r_j$, where $r_i, r_j \in R \; \forall \; j$

$\Rightarrow m_i r_i - \sum_{j\neq i} m_j r_j = 0$

$\Rightarrow r_i = 0 \; \forall \; i \in I$

$\Rightarrow x = 0$

$\therefore \sum_{i\in I} m_i R$ is a direct sum of right R - module and hence $M = \sum_{i\in I} m_i R$ as a direct sum.

Define $\phi_i : R \to m_i R$ by $\phi_i(r) = m_i r$

It is clear that each ϕ_i is an R - isomorphism

i.e., $m_i R \cong_R R \ \forall i \in I$

Hence M_R is isomorphic to a direct sum of $\{m_i R\}_{i\in I}$, where each $m_i R$ is a copy of R_R.

Conversely, suppose that $M \cong \overset{*}{\sum_{i\in I}} A_i$, where $(A_i)_R \cong R_R \ \forall i$.

Now we prove that M_R is a free module.

Since $M \cong \overset{*}{\sum_{i\in I}} A_i$, (by prop (4) of sec 1.4), $\exists$ sub modules B_i, $i \in I \ni M = \sum_{i\in I} B_i$ as a direct sum and $(B_i)_R \cong (A_i)_R \ \forall i$.

$\therefore B_i \cong R \ \forall i$

Let $\phi_i : R \to B_i$ be the R - isomorphism, $i \in I$.

Put $\phi_i(1) = m_i$.

Then $m_i \in B_i \Rightarrow m_i R \subseteq B_i$.

Let $x \in B_i \Rightarrow \exists r \in R \ni x = \phi_i(r) = \phi_i(1.r)$

$$= \phi_i(1) r = m_i r \in m_i R$$

So $x \in m_i R$. $\quad \therefore B_i \subseteq m_i R$ and hence $B_i = m_i R \ \forall i \in I$

Thus $M = \sum_{i\in I} m_i R$.

$\therefore \{m_i\}_{i\in I}$ is a basis of M_R

Hence M_R is free.

18.9 Definition :

A module M is said to be projective if it satisfies the following property:

If A and B are two modules with an epimorphism $\pi : B \to A$, then any homomorphism $\phi : M \to A$ can be "lifted" to a homomorphism $\psi : M \to B$ such that $\pi \circ \psi = \phi$.

i.e., $$\begin{tikzcd} M \arrow[r, dashed, "\psi"] \arrow[dr, "\phi"'] & B \arrow[d, "\pi"] \\ & A \end{tikzcd}$$ is commutative

18.10 Proposition:

Every free module is projective.

Proof:

Let M_R be a free module with basis $\{m_i\}_{i \in I}$.

Let A and B be two right R - modules with an epimorphism $\pi : B \to A$ and let $\phi : M \to A$ be a homomorphism .

For each $i \in I$, $\phi(m_i) \in A$.

Write $B_i = \{b \in B / \pi(b) = \phi(m_i)\}$.

clearly $B_i \neq \phi$,since π is onto.

so $\underset{i \in I}{\pi} B_i \neq \phi$

Let $\{b_i\}_{i \in I} \in \underset{i \in I}{\pi} B_i$.

Define $\psi : M \to B$ as follows:

Let $m \in M$. Then $m = \sum_{i \in I} m_i r_i$, where $r_i \in R$, and all but a finite number of the r_i are 0

Clearly ψ is well defined, since each $m \in M$ has a unique representation of the form $m = \sum_{i \in I} m_i r_i$ where $r_i \in R$.

It is easy to verify that ψ is an R - homomorphism.

Claim : $\pi o \psi = \phi$.

For any $m = \sum_{i \in I} m_i r_i$ in M,

$$(\pi \cdot \psi)(m) = \pi(\psi(m)) = \pi\left(\sum_{i \in I} b_i r_i\right) = \sum_{i \in I} \pi(b_i r_i)$$

$$= \sum_{i \in I} \pi(b_i) r_i = \sum_{i \in I} \phi(m_i) r_i = \sum_{i \in I} \phi(m_i r_i)$$

$$= \phi\left(\sum_{i \in I} m_i r_i\right) = \phi(m).$$

$\Rightarrow \pi\ o\ \psi = \phi$

Thus $\exists$ a homomorphism $\psi : M \to B \ni \pi\ o\ \psi = \phi$

$\therefore$ M is projective.

Remark:

The converse of the above proposition is not true.

i.e., A projective module need not be a free module.

Ex: Consider $Z_6 = \{0,1,2,3,4,5\}$.

There exist projective modules which are not free modules in $\mathbb{Z}_6$ over $\mathbb{Z}_6$.

$\mathbb{Z}_6$ is a free module as a $\mathbb{Z}_6$ module and hence a projective module.

Let $I = \langle 0,2,4 \rangle$ and $J = \langle 0,3 \rangle$

Then I and J are ideals of $\mathbb{Z}_6$ - and $\mathbb{Z}_6 = I + J$ as a direct sum. I and J are projective $\mathbb{Z}_6$ - modules but not free modules.

18.12 Corollary : R_R is projective.

Proof : Since R_R is generated by {1}, we have that {1} is a basis of R_R, and hence R_R is a free module.

So, by the above proposition, R_R is projective.

18.13 Proposition:

If M is the direct sum of a family of modules $\{M_i \ / \ i \in I\}$, then M is projective if and only if each M_i is projective.

Proof: First suppose that each M_i is projective.

Claims: M is projective

Let A nad B be any two modules with an epimorphism $\pi : B \to A$

and Let $\phi : M \to A$ be a homomorphism.

Consider the canonical mappings $k_i : M_i \to M, i \in I$

Then $\phi o\ k_i : M_i \to A$ is a homomorphism $\forall i \in I$.

Since M_i is projective $\exists$ a homomorphism $\psi_i : M_i \to B \ni \pi o \psi_i = \phi o K_i$

Since $M = \sum\limits_{i \in I}^{*} M_i$, by a known proposition, $\exists$ a unique homomorphism $\psi : M \to B \ni \psi o K_i = \psi_i \ \forall \ i \in I$.

Again, since $M = \sum\limits_{i \in I}^{*} M_i$, by the same proposition, $\exists$ a unique homomorphism

$h : M \to A \ni hok_i = \phi ok_i$ i.e., $h \circ k_i = \pi \circ \psi_i$

i.e., the following diagrams are commutative :

$$\begin{tikzcd} M_i \arrow[r, dashed, "\psi_i"] \arrow[dr, "\phi\, ok_i"'] & B \arrow[d, "\pi"] \\ & A \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, dashed, "\psi"] \arrow[dr, "k_i"'] & B \arrow[d, "\psi_i"] \\ & M_i \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, dashed, "h"] \arrow[dr, "k_i"'] & A \arrow[d, "\phi\, ok_i"] \\ & M_i \end{tikzcd}$$

Consider $\pi_o \ \psi_i = \pi o(\psi \circ k_i) = (\pi \circ \psi) \circ k_i$

By the uniqueness of h, we have $\pi \circ \psi = \phi$

Thus $\exists$ a homomorphism $\psi : M \to B \ni \pi \circ \psi = \phi$

$\therefore$ M is projective

Conversely, supposethat M is projective.

Claim: Each M_i is projective.

Let A and B be any two modules with an epimorphism $\pi : B \rightarrow A$ and Let $\phi_i : M_i \rightarrow A$ be a homomorphism.

Let $\pi_i : M \rightarrow M_i$ be the canonical homomorphism.

Then $\phi_i o \pi_i \; : M \rightarrow A$ is a homomorphism.

Since M is projective, there exists a homomorphism $\psi : M \rightarrow B$ such that $\pi \; o \; \psi = \phi_i \; o \; \pi_i$.

Now $\psi o K_i : M_i \rightarrow B$ is a homomorphism and

$$\pi o \left(\psi \; o \; K_i\right) = \left(\pi o \psi\right) o \; K_i$$

$$= \left(\phi_i \; o \; \pi_i\right) o \; K_i$$

$$= \phi_i \; o \left(\pi_i \; o \; K_i\right)$$

$$= \phi_i \; o \; I \qquad \left(\because \pi_i \; o \; K_i = I\right)$$

$$= \phi_i$$

Thus there exists a homomorphism $h = \psi \cdot K_i : M_i \rightarrow B$ such that $\pi \cdot h = \phi_i$

Therefore each M_i is projective.

18.14 Remark:

Any direct summand of a projective module is projective .

18.15 Remark:

Any direct summand of a free module is projective.

·· Result:

›r every non empty set S and for every ring R, there exists a free R - module on S.

Proof : Let S be a non empty set and Let R be a ring with $1 \neq 0$.

Write $F = \{f : S \to R \,/\, f(s) = 0 \text{ for all but a finite number of } s \in S\}$.

Let f, $g \in F$ and $r \in R$

Define $(f+g)(s) = f(s) + g(s)$

and $(fr)(s) = f(s)r$ for all $s \in S$.

Then F is a right R - module.

Claim: F is a free right R - module on S.

Let $s \in S$

Define $f_s : S \to R$ as $f_s(s) = 1$

and $f_s(l) = 0$ for all $l \neq s$ in S.

Then $f_s \in F$

Consider $\{f_s \mid s \in S\}$

Now we showthat $\{f_s \mid s \in S\}$ is a basis for F_R.

Let $f \in F$.

Then there exist $s_1, s_2, \ldots\ldots\ldots\ldots\ldots, s_n$ in S such that $f(s) = 0$ for all

$s \in S \setminus \{s_1, s_2, \ldots\ldots\ldots, s_n\}$

Put $r_i = f(s_i)$, i = 1, 2, ..., n and

$$g = \sum_{i=1}^{n} f_{s_i} r_i$$

Let $s \in S$

Then $g(s) = \sum_{i=1}^{n} (f_{s_i} r_i)(s) = \sum_{i=1}^{n} f_{s_i}(s) r_i$.

If $s \in \{s_1, s_2, \ldots\ldots\ldots\ldots\ldots, s_n\}$ then $s = s_j$ for some $j \ni 1 \leq j \leq n$.

So $g(s) = \sum_{i=1}^{n} f_{s_i}(s_j) r_i = f_{s_j}(s_j) r_j = 1 \cdot r_j = r_j = f(s_j) = f(s)$

If $s \notin \{s_1, s_2, \ldots\ldots\ldots\ldots, s_n\}$ then f(s) = 0

So $g(s) = \sum_{i=1}^{n} f_{s_i}(s) r_i = 0 = f(s)$

$\therefore g(s) = f(s)$ for all $s \in S$.

$\Rightarrow g = f$

Thus each $f \in F$ is a linear combination of lements of $\{f_s \mid s \in S\}$

Suppose $\sum_{s \in S} f_s r_s = 0$ where $r_s \in R$.

Then $\left(\sum_{s \in S} f_s r_s\right)(s^1) = 0$ for all $s^1 \in S$.

$\Rightarrow \sum_{s \in S} (f_s r_s)(s^1) = 0$ for all $s^1 \in S$

$\Rightarrow \sum_{s \in S} f_s(s^1) r_s = 0$ for all $s^1 \in S$

$\Rightarrow f_{s^1}(s^1) r_{s^1} = 0$ for all $s^1 \in S$

$\Rightarrow r_{s^1} = 0$ for all $s^1 \in S$

There fore F is a free right R - module on S.

18.17 Proposition:

Every module is isomorphic to a factor of a free module.

Proof: Let M be any right R - module.

Let S be the set of all generators of M (for example we can take S=M)

Write $F = \{f : S \to R \mid f(s) = 0 \text{ for all a finite number of } s \in S\}$.

Let f, $g \in F$ and $r \in R$

Define $(f+g)(s) = f(s) + g(s)$

and $(fr)(s) = f(s)r$ for all $s \in S$

Then F is a right R - module.

Let $s \in S$. Define $f_s : s \to R$ as $f_s(s) = 1$ and $f_s\left(s^1\right) = 0$ for $s^1 \neq s$

Then $f_s \in F$, $s \in S$

Now $\{f_s \mid s \in S\}$ is a basis for F_R

So F_R is a free module .

Define $\psi : F \to M$ as follows:

Let $f \in F$

Then $f = \sum_{s \in S} f_s r_s$ where $r_s \in R$ and al but a finite number of the r_s are 0.

Define $\psi(f) = \sum_{s \in S} s r_s$ $(Where\ sr_s \in M)$

It can be easily verified that ψ is an R - homomorphism

Now we show that ψ is onto.

Let $m \in M$

$\Rightarrow m = \sum s_i r_i$ where $s_i \in S$ and $r_i \in R$ $\quad (\because S \text{ generates } M)$

Put $f = \sum f_{s_i} r_i$

Then $f \in F$.

Now $\psi(f) = \sum s_i r_i = m$

Therefore ψ is onto and hence ψ is an R - epimorphism.

Consequently $F/Ker\ \psi \cong M$.

i.e., M is isomorphic to a factor module $F/_{Ker\ \psi}$ of a free module F_R.

18.18 Corollary:

Every module is isomorphic to a factor module of a projective module.

Proof:

By the above proposition, every module is isomorphic to a factor module of a free module.

We know that every free module is projective.

so every module is isomorphic to a factor module of a projective module.

18.19 Definition:

Let B and M be R-modules. An epimorphism $\pi : B \to M$ is said to be <u>direct</u> if there exists a homomorphism $K : M \to B$ such that $\pi \circ K = I_M$

18.20 Remark:

In the above definition,k is a monomorphism and $ko\pi$ is an idempotent endomorphism of B.

18.21 Remark:

If $\pi : B \to M$ is direct then M is isomorphic to a direct summand of B.

Proof:

Suppose $\pi : B \to M$ is direct.

Then there exists a homomorphism $k : M \to B$ such that $\pi \cdot k = I_M$.

Clearly k is a monomorphism.

Put $\in = Ko\pi$.

Then $\in$ is an idempotent endomorphism of B.

Put $B_1 = \in(B)$. $B_2 = (I - \in)(B)$

Then B_1 and B_2 are submodules of B.

For any $b \in B,\ b = b - \in(b) + \in(b)$

$$= (I - \in)(b) + \in(b) \in B_1 + B_2$$

So $B \subseteq B_1 + B_2$ *and hence* $B = B_1 + B_2$

Let $x \in B_i \cap B_2$

$\Rightarrow x = \in(b)$ and $x = (I - \in)\left(b^1\right)$ for some b, $b^1 \in B$.

So $x = \in(x) = \in(I - \in)\left(b^1\right) = 0$

$\therefore B_1 \cap B_2 = \{0\}$

Hence B is a direct sum of B_1 and B_2.

Consider $B_1 = \in(B) = (Ko\pi)(B) = K(\pi(B)) = K(M) \cong M$

$\therefore M \cong B_1$, a direct summand of B.

18.22 Propostion:

A module M is projective if and only if every epimorphism $\pi : B \to M$ is direct.

(or)

A module M is projective if and only if it is a direct summand of every module of which it is a factor module.

Proof :

Suppose M is projective.

Let B be any modue and Let $\pi : B \to M$ be an epimorphism

consider the identity mapping $I : M \to M$.

Since M is projective, there exists a homomorphism $K : M \to B$ such that $\pi \circ k = I$.

$$\begin{tikzcd} M \arrow[r, dashed, "K"] \arrow[dr, "I"'] & B \arrow[d, "\pi"] \\ & M \end{tikzcd}$$

Therefore π is direct.

Conversely, suppose that every epimorphism $\pi : B \to M$ is direct.

Claim: M is projective.

We know that any module is isomorphic to a factor module of a free module.

So we get a free module F and an epimorphism $\pi : F \to M$.

By our supposition, the epimorphism $\pi : F \to M$ is direct.

$\Rightarrow$ there exists a homomorphism $K : M \to F$ Such that

$\pi \circ K = I_M$

Clearly K is a monomorphism

Now $(K \circ \pi)(F)$ is a direct summand of F and $(K \circ \pi)(F) = K(\pi(F)) = k(M) \cong M$

Therefore M is isomorphic to a direct summand of a free module F and hence we get that M is projective.

18.23 Corollary:

A module M is projective if and only if it is isomorphic to a direct summand of a free module.

Proof : Suppose M is projective.

Since every module is isomorphic to a factor of a free module, there exists a free module F on M and an epimorphism $\pi : F \to M$.

Since M is projective, by the above proposition, $\pi : F \to M$ is direct.

$\Rightarrow$ there exists a homomorphism $K : M \to F$ such that $\pi \cdot K = I_M$.

Now $(K \circ \pi)(F)$ is a direct summand of F and $(K \circ \pi)(F) = K(M) \cong M$.

Thus M is isomorphic to a direct summand of a free module F.

Conversely, supposethat M is isomorphic to a direct summand of a free moduleF.

Since any direct summand of a free module is projective, we have that M is projective.

18.24 Proposition:

Every R - module is projective if and only if R is completely reducible.

Proof : Suppose that every R - module is projective.

Claim : R is completely reducible.

It is enough to show that $\mathcal{L}(R_R)$, the lattice of all submodules of R_R (i.e., all right ideals of R) is complemented.

Let L be a right ideal of R

Consider the right R - module R/L

By our supposition, R/L is projective.

By a known proposition, the canonical epimorphism $\pi : R \to R/L$ is direct.

$\Rightarrow$ There exists a homomorphism $K : R/L \to R$ such that $\pi \circ K = I_{R/L}$.

$\Rightarrow$ k is a monomorphism.

Put $\in = K \circ \pi$

Then $\in$ is an idempotent endomorphism of R and R is a direct sum of right ideals $\in(R)$ and $(I-\in)(R)$.

Claim : $(I-\in)(R) = L$

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

$= \{r \in R \mid k(\pi(r)) = 0\}$

$= \{r \in R \mid \pi(r) = 0\}$

$= Ker\ \pi$

$= L$

Therefore $Ker \in = L$

Since $\in(I - \in)(R) = \{0\}$ we have $(I - \in)(R) \subseteq Ker \in = L$

For any $x \in L$, $\quad x = I(x) - \in(x)$

$= (I - \in)(x) \in (I - \in)(R)$

Therefore $L \subseteq (I - \in)(R)$ and hence $L = (I - \in)(R)$.

Thus L is a direct summand of R.

Therefore $\mathcal{L}(R_R)$ is complemented.

So, R is completely reducible.

Conversely, suppose that R is completely reducible.

Let M_R be any right R - Module.

Since every module is isomorphic ot a factor of a free module, we get a free module F_R and an epimorphism $\pi : F \to M$.

Since R is completely reducible, we knowthat every right R - module is completely reducible.

So F is completely reducible.

Put $B = Ker\ \pi$.

Then B is a direct summand of F.

$\Rightarrow$ there exists a submodule B^1 of F such that F is a direct sum of B and B^1 .

Now $M \cong F/_{Ker\ \pi} = F/_B \cong B^1/_{B \cap B^1} = B^1/_{\{0\}} \cong B^1$ ....(1)

But B^1 is a direct summand of F.

Hence B^1 is projective $(\because F \text{ is a free module})$

So by (1), M is also projective.

K. SIVA PRASAD
P.G. Department of Mathematics
J.K.C. College, Guntur

Lesson : 19

INJECTIVE MODULES - I

19.0 Introduction : In this lesson, the direct product of modules is characterized. The notion of injectivity which dual to projectivity is introduced for modules.

Some important properties of injective modules are studied and some examples are given.

19.1 Remark : Let A be a direct product of a family of modules $\{A\}_{i \in I}$ i.e., $A = \underset{i \in I}{\pi} A_i$

Define $\pi_i : A \to A_i$ by $\pi_i(a) = a(i)$.

Then π_i is an epimorphism and is called the canonical epimorphism corresponding to the direct product $A = \underset{i \in I}{\pi} A,$ for $i \in I$.

19.2 Proposition : If A is the direct product of a family of modules $\{A_i\}_{i \in I}$ with canonical mappings $\pi_i : A \to A_i$ then for every module B and for every family of homomorphisms $\phi_i : B \to A_i$ there exists a unique homomorphism $\phi : B \to A$ such that $\pi_i \circ \phi = \phi_i$. Moreover, this property characterizes the direct product up to isomorphism.

$$\begin{tikzcd} B \arrow[r, dashed, "\phi"] \arrow[dr, "\phi_i"'] & A \arrow[d, "\pi_i"] \\ & A_i \end{tikzcd}$$ is commutative.

Proof : Let B be an R-module and let $\phi_i : B \to A_i$ be a homomorphism for $i \in I$.

Let $a \in A$.

Then $\pi_i(a) = a(i)$ for $i \in I$

Define $\phi : B \to A$ as $\phi(b)(i) = \phi_i(b)$ for all $b \in B$.

Clearly ϕ is well-defined.

Now, we show that ϕ is an R - homomorphism.

Let $b_1, b_2 \in B$ and $r \in R$.

Now $\phi(b_1+b_2)(i)=\phi_i(b_1+b_2)$

$$=\phi_i(b_1)+\phi_i(b_2)$$

$$=\phi(b_1)(i)+\phi(b_2)(i)$$

$$=(\phi(b_1)+\phi(b_2))(i)$$

This is true for every $i \in I$.

Therefore $\phi(b_1+b_2)=\phi(b_1)+\phi(b_2)$

Now $\phi(b_1 r)(i)=\phi_i(b_1 r)$

$$=\phi_i(b_1)r$$

$$=\phi(b_1)(i)r$$

$$=(\phi(b_1)r)(i)$$

This is true for every $i \in I$

Therefore $\phi(b_1 r)=\phi(b_1)r$

So ϕ is an R-homomorphism.

Now, for any $b \in B$, $(\pi_i 0 \phi)(b)=\pi_i(\phi(b))=\phi(b)(i)=\phi_i(b)$

$$\Rightarrow \pi_i 0 \phi=\phi_i$$

Uniqueness : Suppose $\psi: B \to A$ is another R-homomorphism such that $\pi_i 0 \psi=\phi_i$.

Claim : $\phi=\psi$

Let $b \in B$

For any $i \in I, \psi(b)(i)=\pi_i(\psi(b))=(\pi_i 0 \psi)(b)=\phi_i(b)=\phi(b)(i)$

$$\Rightarrow \psi(b)=\phi(b)$$

Therefore $\psi=\phi$

Thus there exists a unique homomorphism $\phi: B \to A$ such that $\pi_i 0 \phi=\phi_i$ for all $i \in I$.

Converse : Suppose that A' is another module with epimorphisms $\pi'_i : A' \to A_i$ satisfying the condition of the proposition. i.e., given any module B, a family of homomorphisms $\phi'_i : B \to A_i$, $i \in I$, there exists a unique homomorphism $\psi : B \to A'$ such that $\pi'_i \circ \psi = \phi'_i$.

So the diagrams

$$\begin{tikzcd} B \arrow[r, dashed, "\phi"] \arrow[dr, "\phi_i"'] & A \arrow[d, "\pi_i"] \\ & A_i \end{tikzcd} \qquad \begin{tikzcd} B \arrow[r, dashed, "\psi"] \arrow[dr, "\phi'_i"'] & A^1 \arrow[d, "\pi'_i"] \\ & A_i \end{tikzcd}$$

are commutative.

(1) (2)

Take $B = A'$ and $\phi_i = \pi'_i$

Then, by the first part of the proposition, we get a unique homomorphism $\pi' : A' \to A$ such that $\pi_i \circ \pi' = \pi'_i$.

Take $B = A$ and $\phi_i = \pi_i$

Then, by our supposition, we get a unique homomorphism

$\pi : A' \to A$ such that $\pi'_i \circ \pi = \pi_i$.

Therefore $\pi_i \circ \pi' \circ \pi = \pi'_i \circ \pi = \pi_i \circ I_A$, where I_A is the identity mapping of A.

By the uniqueness property, $\pi' \circ \pi = I_A$

Similarly $\pi' \circ \pi = I_{A'}$, where $I_{A'}$ is the identity mapping of A'.

Therefore $A \cong A'$

19.3 Corollary : If A is isomorphic to the direct product of modules $\{A_i\}_{i \in I}$ with canonical mappings $\pi_i : A \to A_i$, then there exist mappings $K_i : A_i \to A$ (also called canonical) such that $\pi_i \circ k_i = I$ and $\pi_i \circ k_j = 0$ if $i \neq j$.

Proof : For fixed i, consider the mapping $\delta_{ij} : A_i \to A_j$,

Where $\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$

By the above proposition, there exists a(unique) homomorphism $K_i : A_i \to A$

such that $\pi_j \circ K_i = S_{ij}$

$$\begin{tikzcd} A_i \arrow[r, dashed, "K_i"] \arrow[dr, "\delta_{ij}"'] & A \arrow[d, "\pi_j"] \\ & A_j \end{tikzcd}$$

i.e., $\pi_i \circ k_i = 1$, the identity mapping of A_i and $\pi_i \circ k_j = 0$ if $i \neq j$.

19.4 Remark : The above corollary implies k_i is mono.

19.5 Definition : A module M is said to be injective if it satisfies the following property :

If A and B are two modules with a monomorphism $k : A \to B$, then any homomorphism $\phi : A \to M$ can be "extended" to a homomorphism $\psi : B \to M$ such that $\psi \circ k = \phi$.

i.e., $$\begin{tikzcd} M & B \arrow[l, dashed, "\psi"'] \\ & A \arrow[u, "k"'] \arrow[ul, "\phi"] \end{tikzcd}$$ is commutative.

19.6 Proposition : If M is the direct product of a family of modules $\{M_i / i \in I\}$, then M is injective if and only if each M_i is injective.

Proof : First suppose that each M_i is injective.

Claim : M is injective.

Let A and B be any two modules with a monomorphism $k : A \to B$ and let $\phi : A \to M$ be a homomorphism.

Consider the canonical mappings $\pi_i : M \to M_i$, $i \in I$. Then $\pi_i \circ \phi : A \to M_i$ is a homomorphism, for all $i \in I$.

Since M_i is injective, there exists a homomorphism $\psi_i : B \to M_i$ such that $\psi_i \circ k = \pi_i \circ \phi$ for all $i \in I$.

Since $M = \underset{i \in I}{\pi} M_i$, by a known proposition, there exists a unique homomorphism $\psi : B \to M$ such that $\pi_i \circ \psi = \psi_i$, for all $i \in I$.

Again, since $M = \underset{i \in I}{\pi} M_i$, by the same proposition, there exists a unique homomorphism $h : A \to M$ such that $\pi_i \circ h = \pi_i \circ \phi$, for all $i \in I$.

[i.e., the following diagrams are commutative :

$$\begin{tikzcd} B \arrow[r, dashed, "\psi_i"] & M_i \\ A \arrow[u, "k"] \arrow[ur, "\pi_i \circ \phi"'] & \end{tikzcd} \qquad \begin{tikzcd} B \arrow[r, dashed, "\psi"] \arrow[dr, "\psi_i"'] & M \arrow[d, "\pi_i"] \\ & M_i \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, dashed, "h"] \arrow[dr, "\pi_i \circ \phi"'] & M \arrow[d, "\pi_i"] \\ & M_i \end{tikzcd}$$

consider $\psi_i \circ k = (\pi_i \circ \psi) \circ K = \pi_i \circ (\psi \circ K)$

By the uniqueness of h, we have $\psi \circ k = \phi = h$

Thus there exists a homomorphism $\psi : B \to M$ such that $\psi \circ k = \phi$.

Therefore M is injective.

Conversely, suppose that M is injective.

Claim : Each M_i is injective.

Let A and B be any two modules with a monomorphism $k : A \to B$ and let $\phi_i : A \to M_i$ be a homomorphism.

Since M is the direct product of $\{M_i / i \in I\}$ with canonical epimorphisms $\pi_i : M \to M_i$, there exist monomorphisms $k_i : M_i \to M$ such that $\pi_i \circ k_i = I_{M_i}$ and $\pi_i \circ k_j = 0$ if $i \neq j$.

Since M is injective, there exists a homomorphism $\psi : B \to M$ such that $\psi \circ k = k_i \circ \phi_i$.

Now $\quad (\pi_i \circ \psi) \circ k = \pi_i \circ (\psi \circ k)$

$$= \pi_i \circ (k_i \circ \phi_i)$$

$$= (\pi_i \circ k_i) \circ \phi_i$$

$$= I_{M_i} \circ \phi_i = \phi_i$$

Thus there exists a homomorphism $h = \pi_i \circ \psi : B \to M_i$, such that $h \circ k = \phi_i$

Therefore each M_i is injective.

19.7 Result : A module M is injective if and only if, for any modules A and B with $A \subseteq B$ and a homomorphism $\phi : A \to M$, there exists a homomorphism $\psi : B \to M$ such that $\psi / A = \phi$.

Proof : Suppose M is injective.

Let A be a submodule of a module B and let $\phi : A \to M$ be a homomorphism.

Consider the inclusion mapping $i : A \to B$, which is a monomorphism.

Since M is injective, there exists a homomorphism $\psi : B \to M$ such that $\psi \circ i = \phi$.

$i.e., (\psi \circ i)(a) = \phi$ for all $a \in A$

$i.e., \psi(a) = \phi(a)$ for all $a \in A$

$i.e., \psi / A = \phi$.

Conversely, suppose that M satisfies the condition.

Claim : M is injective.

Let A and B be two modules with nonmorphism $k : A \to B$ and let $\phi : A \to M$ be a homomorphism.

Now $k(A)$ is a submodule of B and $A \cong k(A)$.

Consider $\phi \circ k^{-1} : k(A) \to M$, which is a homomorphism

By our supposition, there exists a homomorphism

$\psi : B \to M$ such that $\psi / k(A) = \phi \circ k^{-1}$

$$i.e., \ \psi \circ i_{K(A)} = \phi \circ K^{-1}$$

$$i.e., \ \psi \circ i_{K(A)} \circ K = \phi$$

$$i.e., \ \psi \circ K = \phi$$

Therefore M is injective.

19.8 Bayer's Criterion For Injectivity :

A module M_R is injective if and only if, for every right ideal K of R and every $\phi \in Hom_R(K, M)$, there exists an $m \in M$ such that $\phi(k) = mk$ for all $k \in K$.

Proof : Suppose M_R is injective.

Let K be a right ideal of R and let $\phi : K \to M$ be a homomorphism.

Consider the inclusion mapping $i : K \to R$.

Since M is injective, there exists a homomorphism $\psi : R \to M$ such that $\psi \circ i = \phi$

Put $\psi(1) = m$

Then $m \in M$

Now, for any $k \in K$, $\psi(k) = \psi(1k) = \psi(1)k = mk$

Thus $\phi(k) = (\psi \circ i)(k) = \psi(k) = mk$ for all $k \in K$.

Conversely, suppose that for every right ideal K of R and every $\phi \in Hom_R(K, M)$, there exists an $m \in M$ such that $\phi(k) = mk$ for all $k \in K$.

Claim : M is injective.

Let A be a submodule of a right R-module B and let $\phi : A \to M$ be a homomorphism.

Write $\mathcal{S} = \left\{ (D, \psi) \middle| \begin{array}{l} D \text{ is a submodule of } B_R, A \subseteq D \text{ and} \\ \psi : D \to M \text{ is a homomorphism} \ni \psi / A = \phi \end{array} \right\}$

Clearly $\mathcal{S} \neq \phi$ ($\because (A, \phi) \in \mathcal{S}$)

Let $(D_1, \psi_1), (D_2, \psi_2) \in \mathcal{S}$

Define $(D_1, \psi_1) \leq (D_2, \psi_2)$ iff D_1 is a submodule of D_2 and ψ_2 is an extension of ψ_1.

Then ($\mathcal{S}$, $\leq$) is a poset.

Let $\{(D_\alpha, \psi_\alpha) / \alpha \in \Delta\}$ be a chain in $\mathcal{S}$

Put $D = \bigcup_{\alpha \in \Delta} D_\alpha$

Then D is a submodule of B and $A \subseteq D$.

Define $\psi : D \to M$ as follows :

Let $x \in D$

$\Rightarrow x \in D_\alpha$ for some $\alpha \in \Delta$.

Define $\psi(x)=\psi_\alpha(x)$

Claim : ψ is well - defined

Suppose $x \in D_\beta$ for some $\beta \in \Delta$

Then (D_α, ψ_α) and (D_β, ψ_β) are comparable.

Suppose $(D_\alpha, \psi_\alpha) \le (D_\beta, \psi_\beta)$, so that $D_\alpha \le D_\beta$ and ψ_β extends ψ_α.

Therefore $x \in D_\alpha$ and $\psi_\alpha(x)=\psi_\beta(x)$ and $x \in D_\beta$.

Therefore ψ is well-defined.

It can be easily verified that ψ is an R-homomorphism and ψ is an extension of each ψ_α and hence an extension of ϕ.

Therefore $(D,\psi) \in \mathscr{S}$ and each $(D_\alpha, \psi_\alpha) \le (D,\psi)$

So (D,ψ) is an upper bound of $\{(D_\alpha, \psi_\alpha) | \alpha \in A\}$

Hence by Zon's lemma, $\mathscr{S}$ contains a maximal element (D_0, ψ_0) (say).

So we have $A \subseteq D_0 \subseteq B$ and $\psi_0 : D_0 \to M$ is an extension of ϕ.

Claim : $D_0 = B$

Let $b \in B$

Put $K = \{r \in R / br \in D_0\}$.

Then K is a right ideal of R.

Define $\psi : K \to M$ as $\psi(k)=\psi_0(bk)$ for all $k \in K$.

Then ψ is an R-homomorphism.

So, by our supposition, there exists an $m \in M$ such that

$\psi(k) = mk$ for all $k \in K$.

i.e., $\psi_0(bk) = mk$ for all $k \in K$.

Define $\psi_0' : D_0 + bR \to M$ as follows.

Let $x \in D_0 + bR$

$\Rightarrow x = d_0 + br$ for some $d_0 \in D_0$ and $r \in R$

Define $\psi_0'(x) = \psi_0(d_0) + mr$

Claim : ψ_0' is well-defined.

Suppose $x = d_1 + br_1 = d_2 + br_2$ where $d_1, d_2 \in D_0$ and $r_1, r_2 \in R$.

So $d_1 - d_2 = b(r_2 - r_1) \in D_0$

$\Rightarrow r_2 - r_1 \in K$

Therefore $\psi(r_2 - r_1) = m(r_2 - r_1)$

i.e., $\psi_0(b(r_2 - r_1)) = m(r_2 - r_1)$

i.e., $\psi_0(d_1 - d_2) = m(r_2 - r_1)$

i.e., $\psi_0(d_1) + mr_1 = \psi_0(d_2) + mr_2$

Therefore ψ_0' is well defined.

It can be easily verified that ψ_0' is an R - homomorphism and ψ_0' is an extension of ψ_0

$(\because \psi_0'(d) = \psi_0(d) \forall d_0 \in D_0)$

Therefore $(D_0 + bR, \psi_0') \in \mathscr{S}$ and $(D_0, \psi_0) \leq (D_0 + bR, \psi_0')$

Since (D_0, ψ_0). is a maximal element in $\mathscr{S}$, we have that $D_0 = D_0 + bR$ and $\psi_0 = \psi_0'$

So $b \in D_0$

Therefore $B \subseteq D_0$ and hence $B = D_0$.

Therefore $\psi_0 : B \rightarrow M$ is an R-homomorphism and ψ_0 extends ϕ. Hence (by the above result) M is injective.

19.9 Definition : An Abelian group $M(=M_z)$ is called divisible if, for every $m \in M$ and every non-zero integer z, there exists an $m' \in M$ such that $m'z = m$.

19.10 Examples : $(Q,+)$, the additive group of rational numbers is divisible.

19.11 Remark : Any homomorphic image of a divisible group is divisible.

Proof : Let f be a homomorphism from an Abelian group G into an Abelian group H, where G is divisible.

Claim : $f(G)$ is divisible.

Let $x \in f(G)$

$\Rightarrow x = f(g)$ for some $g \in G$.

Let $n \in \mathbb{Z} \ni n \neq 0$.

Since G is divisible, there exists $g' \in G$ such that $g'n = g$.

So $f(g'n) = f(g) = x$

$\Rightarrow f(g')n = x$

Thus there exists $y = f(g') \inf(G)$ such that $yn = x$.

Therefore $f(G)$ is divisible.

19.12 Proposition : An Abelian group is injective if and only if it is divisible.

Proof : Let M be an Abelian group.

Then M is a $\mathbb{Z}$- module, where $\mathbb{Z}$ is the ring of integers.

Suppose M is divisible.

Claim : M is injective as a $\mathbb{Z}$-module.

Let K be any right ideal of $\mathbb{Z}$.

Then $K = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

We may assume that $K \neq \{0\}$, so that $n \neq 0$.

Let $\phi : K \to M$ be a $\mathbb{Z}$ - homomorphism.

Put $\phi(n) = m \in M$

Since M is divisible, there exists an $m' \in M$ such that $m'n = m$.

Let $x \in K$. Then $x = nz$ for some $z \in \mathbb{Z}$.

Now $\phi(x) = \phi(nz) = \phi(n)z = mz = m'nz = m'x$

Thus there exists an $m' \in M$ such that $\phi(x) = m'x$ for all $x \in K$.

So by a known lemma (Baer's lemma), M is injective.

Conversely, suppose M is injective as a $\mathbb{Z}$ - module.

Claim : M is divisible.

Let $m \in M$ and $0 \neq z \in \mathbb{Z}$

Put $K = zZ$

Then k is a right ideal of $\mathbb{Z}$.

Define $\phi : K \to M$ as $\phi(zx) = mx$ for all $x \in \mathbb{Z}$.

Then ϕ is a $\mathbb{Z}$ - homomorphism.

Since M is injective, there exists an $m' \in M$ such that $\phi(k) = m'k$ for all $k \in K$.

$\Rightarrow \phi(zx) = m'zx$ for all $x \in \mathbb{Z}$..

$\Rightarrow mx = m'zx$ for all $x \in \mathbb{Z}$.

$\Rightarrow m = m'z$ (take $x = 1$)

Thus there exists an $m' \in M$ such that $m'z = m$.

Therefore M is divisible.

19.13 Remark : Let Q be the additive group of rational numbers. Define '~' on Q as $a \sim b$ iff $a - b \in Z$ for all $a, b \in Q$. Then '~' is an equivalence relation on Q.

We denote, the class of all equivalence classes on '~' by $\frac{Q}{Z}$.

Define '+' on $\frac{Q}{Z}$ as $\bar{a}+\bar{b}=\overline{a+b}$ for all $\bar{a},\bar{b}\in\frac{Q}{Z}$. Then $\left(\frac{Q}{Z},+\right)$ is an Abelian group and hence it is a z-module.

19.14 Definition : Let M be an additive Abelian group. Then $Hom_Z\left(M,\frac{Q}{Z}\right)$ is called the character group of M, and is denoted by M^*.

Any element in M^* is called a character of M.

19.15 Remark : i) If M is a left R-module, then M^* is a right R-module by defining $(fr)(m)=f(rm)$ for all $f\in M^*$, $r\in R$ and $m\in M$.

ii) If M is a right R-module, then M^* is a left R-module.

We call M_R^* the character module of the left R-module $_RM$.

19.16 Lemma : If $0\neq m\in M$, then there exists $\Psi\in M^*$ such that $\Psi(m)\neq 0$.

Proof : Let $\pi:Q\to\frac{Q}{Z}$ be the canonical epimorphism.

Since Q is divisible and every homomorphic image of divisible group is divisible, we have that $\frac{Q}{Z}$ is divisible. Consequently, $\frac{Q}{Z}$ is injective as Z-module.

Let $0\neq m\in M$

Case (i) : Suppose $mz\neq 0$ for all $0\neq z\in Z$

Define $\phi:mZ\to\frac{Q}{Z}$ as $\phi(mz)=\pi\left(\frac{z}{2}\right)$ for all $z\in Z$.

Claim : ϕ is well-defined.

Let $mz\in mZ$ such that $mz=0$

$$\Rightarrow \pi\left(\frac{z}{2}\right)=0 \text{ in } \frac{Q}{Z}.$$

$$\Rightarrow Q(mz)=0$$

Therefore ϕ is well-defined.

It can be easily verified that ϕ is a z-homomorphism. Since $\frac{Q}{Z}$ is injective, there exists a Z-homomorphism $\Psi: m \rightarrow \frac{Q}{Z}$ such that $\Psi / mZ = \phi$

$$\Rightarrow \Psi \in M^* \text{ and } \Psi(m) = \phi(m) = \pi\left(\frac{1}{2}\right) \neq 0 \text{ in } \frac{Q}{Z}$$

Case - ii : Suppose $mz=0$ for some +ve integer z.

Let z_0 be the least +ve integer such that $mz_0=0$

Define $\phi: mZ \rightarrow \frac{Q}{Z}$ as $\phi(mz)=\pi\left(\frac{z}{z_0}\right)$ for all $z \in Z$.

Claim : ϕ is well-defined.

Let $mz \in mZ$ such that $mz=0$,

By division algorithm, $z = pz_0 + r$ for some integers p and r such that $0 \le r < z_0$.

$$\Rightarrow r = z - pz_0$$

$$\Rightarrow mr = m(z - pz_0) = mz - pmz_0 = 0 \quad (\because mz = 0 \text{ and } mz_0 = 0)$$

$\Rightarrow r=0$ since $0 \le r < z_0$ and z_0 is the least +ve integer such that $mz_0 = 0$.

So $z = pz_0$

$i.e., \frac{z}{z_0}$ is an integer.

So $\phi(mz)=\pi\left(\frac{z}{z_0}\right)=0$ in $\frac{Q}{Z}$.

Therefore ϕ is well-defined.

It can be easily verified that ϕ is a Z - homomorphism. Since $\frac{Q}{Z}$ is injective, there exists a Z - homomorphism $\Psi: M \to \frac{Q}{Z}$ such that $\Psi / mZ = \phi$.

$\Rightarrow \Psi \in M^*$ and $\Psi(m)=\phi(m)=\pi\left(\frac{1}{z_0}\right)\neq 0$ in $\frac{Q}{Z}$.

So in any case, for $0 \neq m \in M$, there exists $\Psi \in M^*$ such that $\Psi(m)\neq 0$.

19.17 Corollary : There is a canonical monomorphism of M into $\left(M^*\right)^*$.

Proof : Define $\phi: M \to \left(M^*\right)^*$ as follows :

Let $m \in M$.

Then, for any $\Psi \in M^*$, $\Psi(m) \in \frac{Q}{Z}$.

Define $\hat{m}: M^* \to \frac{Q}{Z}$ as $\hat{m}(\Psi)=\Psi(m)$

Then $\hat{m}$ is a Z - homomorphism, so $\hat{m} \in \left(M^*\right)^*$

Define $\phi(m)=\hat{m}$.

It can be easily verified that ϕ is a group of homomorphism.

Claim : ϕ is one-one.

Let $m \in M$ such that $\phi(m)=0$.

16

$\Rightarrow \hat{m}=0$

$\Rightarrow \hat{m}(\Psi)=0$ for all $\Psi \in M^*$.

$\Rightarrow \Psi(m)=0$ for all $\Psi \in M^*$

$\Rightarrow m=0$ (by above lemma)

Therefore ϕ is one-one

Thus there exists a canonical monomorphism ϕ of M into $\left(M^*\right)^*$

19.18 Remark : If M is a right R-module, then M^* is a left R-module and hence $\left(M^*\right)^*$ is a right R-module. So the mapping $\phi: M \rightarrow \left(M^*\right)^*$ defined by $\phi(m)=\hat{m}$ is a monomorphism of right R-modules.

Remark : If $\phi: A \rightarrow B$ is a homomorphism of modules then ϕ induces a homomorphism $\phi^*: B^* \rightarrow A^*$ given by $\phi^*(\Psi)(a)=\Psi(\phi(a))$ for all $\Psi \in B^*$ and $a \in A$

19.20 Lemma : If $\phi: A \rightarrow B$ is epi, then $\phi^*: B^* \rightarrow A^*$ is mono.

Proof : Suppose $\phi: A \rightarrow B$ is an epimorphism. It can be easily verified that the mapping $\phi^*: B^* \rightarrow A^*$ defined by $\phi^*(\Psi)(a) = \Psi(\phi(a))$ for all $\Psi \in B^*$ and $a \in A$ is a homomorphism.

Now we show that ϕ^* is one - one.

Let $\Psi \in B^*$ such that $\phi^*(\Psi)=0$

Claim : $\Psi=0$

Let $b \in B$

Since ϕ is onto, there exists $a \in A$ such that $\phi(a)=b$. So $\Psi(b)=\Psi(\phi(a))=\phi^*(\Psi)(a)=0$

Therefore $\Psi=0$.

So ϕ^* is one-one and hence ϕ^* is a monomorphism.

19.21 Proposition : Every module is isomorphic to a submodule of the character module of a free module.

Proof : Let M_R be a right R-module.

Then M^* is a left R-module and hence $\left(M^*\right)^*$ is a right R-module.

By corollary 19.17, there is a monomorphism of M into $\left(M^*\right)^*$ -------- (1)

we know that every module is isomorphic to a factor of a free module.

So there exists a free left R-module $_RF$ on $_RM^*$ and an epimorphism $\phi : F \to M^*$.

Hence by the above lemma, $\phi^* : F \to M^*$

Hence by the above lemma, $\phi^* : \left(M^*\right)^* \to F^*$ is a monomorphism. -------- (2)

From (1) and (2), there is a monomorphism of M into F^*.

Therefore M is isomorphic to a submodule of F^*, where F^* is the character module of free module F.

19.22 Proposition : If $_RF$ is a free module then F_R^* is injective.

Proof : Suppose $_RF$ is a free left R-module. Then its character module F^* is a right R-module.

Claim : F_R^* is injective.

Let K be any right ideal of R and let $\phi : K \to F^*$ be an R-homomorphism.

We show that there exists $\Psi \in F^*$ such that $\phi(k) = \Psi k$ for all $k \in K$.

Now KF is an additive subgroup of F consisting of all finite sums of terms kf, where $k \in K$ and $f \in F$

Since F is a free module, F has a basis, say $\{f_i\}_{i \in I}$.

so each element of KF has the form $\sum\limits_{i \in I} k_i f_i$, where $k_i \in K$ and all but a finite number of the k_i are zero.

Define $\psi : KF \to \frac{Q}{Z}$ by $\psi\left(\sum\limits_{i \in I} k_i f_i\right) = \sum\limits_{i \in I} \phi(k_i) f_i$

Claim : ψ is well defined.

Suppose $\sum\limits_{i \in I} k_i f_i = 0$, where each $k_i \in K$.

$\Rightarrow k_i = 0$ for all $i \in I$.

$\Rightarrow \phi(k_i) = 0$ for all $i \in I$

$\Rightarrow \sum\limits_{i \in I} \phi(k_i) f_i = 0$

$\Rightarrow \psi\left(\sum\limits_{i \in I} k_i f_i\right) = 0$

Therefore ψ is well-defined.

Clearly ψ is a Z - homomorphism.

But $\frac{Q}{Z}$ is injective as a Z - module.

So there exists a Z - homomorphism $\Psi : F \to \frac{Q}{Z}$ such that $\Psi / KF = \psi \Rightarrow \Psi \in F^*$.

Now for any $k \in K$ and $f \in F$,

$$(\phi(k))(f) = \psi(kf) = \Psi(kf) = (\Psi k)(f)$$

$$\Rightarrow (\phi(k))(f) = (\Psi k)(f) \text{ for all } k \in K \text{ and } f \in F.$$

$$\Rightarrow \phi(K) = \Psi k \text{ for all } k \in K.$$

Thus there exists $\Psi \in F^*$ such that $\phi(k) = \Psi k$ for all $k \in K$

So by Baer's lemma, F_R^* is injective.

19.23 Corollary : Every module is isomorphic to a submodule of an injective module.

Proof : Let M_R be a right R-module.

we know that every module is isomorphic to a submodule of the character module of a free module.

So there exists a free module $_R F$ such that M_R is isomorphic to a submodule of the character module F_R^*.

By the above proposition, F_R^* is injective.

Thus M_R is isomorhpic to a submodule of an injective module F_R^*.

K. SIVA PRASAD
P.G. Department of Mathematics
J.K.C. College, Guntur

Lesson - 20 INJECTIVE MODULES

20.0 Introduction : In this lesson, injective modules are characterized in several ways. The notion of injective hull of a module is introduced and given three equivalant conditions to the injective hull of a module.

20.1 Definition: A monomorphism $K : M \to B$, where M and B are two modules is said to be <u>direct</u> if there exists a homomorphism $\pi : B \to M$ such that $\pi \circ K = I$.

20.2 Remark: In the above definition, π is an epimorphism and $K \circ \pi$ is an idempotent endomorphism of B.

20.3 Remark: If $K : M \to B$ is direct then M is isomorphic to a direct summand of B.

20.4 Proposition : A module M is injective if and only if every monomorphism $K : M \to B$ is direct.

(or)

A module M is injective if and only if it is a direct summand of every module of which it is a submodule.

Proof :

Suppose M is injective

Let B be any module and Let $K : M \to B$ be a homomorphism.

Consider the identity mapping $I : M \to M$

Since M is injective there exists a homomorphism $\pi : B \to M$ such that $\pi \circ K = I$

$$\begin{tikzcd} M & & B \arrow[ll, dotted, "\pi"'] \\ & M \arrow[ul, "I"] \arrow[ur, "K"'] & \end{tikzcd}$$

Therefore k is direct.

Conversely supposethat, for any module B, every monomorphism of M into B is direct.

Claim : M is injective.

We know that every module is isomorphic to a submodule of an injective module.

So there exists an injective module B and a monomorphism $K : M \to B$

By our supposiiton, $K : M \to B$ is direct.

$\Rightarrow$ there exists a homomorphism $\pi : B \to M$ such that

$\pi \circ K = I_M$

Clearly π is an epimorphism

Put $\in \; = \; K \circ \pi$

Then $\in$ is an idempotent endomorphism of B and

$\in B \; = \; (k \circ \pi)(B) = K(\pi(B)) = k(M) \cong M$

But $B = \in B + (I - \in)B$ as a direct sum.

$\Rightarrow$ $\in B$ is a direct summand of injective module B.

$\Rightarrow$ $\in B$ is injective.

Thus M is isomorphic to injective module $\in B$.

$\Rightarrow$ M is also injective.

20.5 Corollary:

A module M is injective if and only if it is a direct summand of a character moduleof a free module.

Proof : Suppose M is injective.

We know that every module is isomorphic to a sub module of the character module of a free module. So there exists a free module F such that M is isomorphic to a sub module of the character module F^*. Hence there is a monomorphism $K : M \to F^*$. Since M is injective, by the above proposition, $K : M \to F^*$ is direct.

$\Rightarrow$ there exists a homomorphism $\pi : F^* \to M$ such that $\pi \circ K = I_M$.

Clearly π is an epimorphism.

Now $(K \circ \pi)(F^*)$ is a direct summand of F^* and $(K \circ \pi)(F^*) = K(M) \cong M$

Thus M is isomorphic to a direct summand of a character module F^* of a free module F.

Conversely, suppose that M is a direct summand of the character module F^* of a free module F.

By a known result (proposition 19.22), F^* is injective.

Therefore M is injective .

20.6 Proposition:

Every R - module is injective if and only if R is completely reducible.

Proof:

Supposethat every R - module is injective.

Claim:

R is completely reducible.

It is enough to showthat $\mathscr{L}(R_R)$ is complemented.

Let K be any right ideal of R.

Then by our supposition, the right R - module K_R is injective.

Consider the inclusion mapping $i_k : K \to R$.

Since K is injective, by proposition 20.4, i_k is direct .

$\Rightarrow$ there exists a homomorphism $\pi : R \to K$ such that $\pi \circ i_k = I_k$.

Clearly π is an epimorphism.

Put $\in = i_k \circ \pi$

Then $\in$ is an idempotent endomorphism of R and $\in R = (i_k \circ \pi)(R) = i_k(K) = K$.

But $R = \in R + (I - \in)R$ as a direct sum.

$\Rightarrow \in R$ is a direct summand of R.

Thus K is a direct summand of R.

Therefore $\mathscr{L}(R_R)$ is complemented.

Conversely, supposethat R is completely reducible.

Let M_R be any right R - module.

We know that every module is isomorphic to a submodule of an injective module.

So there exists a right R - module B_R , Which is injective such that M is isomorphic to a submodule C (say) of B_R.

Since R is completely reducible, we have B_R is completely reducible.

$\Rightarrow$ C is a direct summand of the injective module B.

$\Rightarrow$ C is also injective.

Thus M is injective $\left(\because M \cong_R C \right)$

20.7 Definition:

Let A and B be two R - modules. We say that B is an extension of A if A is a submodule of B.

20.8 Remark:

Any module can be extended to an injective module.

20.9 Definition:

An extension B of a module A is called an essential extension of A if every non zero sub module of B has non zero intersection with A.

20.10 Remark:

B is an essential extenssion of A iff A is a large sub module of B.

20.11 Definition:

Let B be an essential extension of A. We say that B is a maximal essential of A if no proper extension of B is an essential extension of A.

20.12 Lemma:

Let N be an essential extension of M and Let I be an injective module containing M, then the identity mapping of M can be extended to a monomorphism of N inot I.

Proof:

Consider the identity mapping $I_M : M \to M$

Then $I_M : M \to I$ is a homomorphism.

Since I is injective and $M \subseteq N$, by a known result, there exists a homomorphism $\phi : N \to I$ such that $\phi | M = I_M$

$\Rightarrow \phi(m) = I_M(m) = m$ for all $m \in M$.

Put $K = Ker\,\phi$

Then K is a sub module of N.

Let $x \in K \cap M$

$\Rightarrow x \in K$ and $x \in M$

$\Rightarrow \phi(x) = 0$

$\Rightarrow x = 0$

Therefore $K \cap M = \{0\}$.

Since N is an essential extension of M, we get that K = {0}.

i.e., $Ker\ \phi = \{0\}$

So $\phi : N \to I$ is a monomorphism, which is an extension of I_M

20.13 Proposition:

A module M is injective if and only if M has no proper essential extension.

Proof:

Suppose M is injective.

Let N be an essential extenssion of M.

Consider the inclusion mapping $i : M \to N$ which is a monomorphism.

Since M is injective, by a known result, $i : M \to N$ is direct.

So M is a direct summand of N.

$\Rightarrow$ there exists a sub module K of N such that N=M+K and $M \cap K = \{0\}$

Since N is an esential extension of M and $M \cap K = \{0\}$, we have $K = \{0\}$

So M = N.

There fore M has no proper essential extension.

Convensely, suppose that M has no proper essential extension.

Claim:

M is injective.

Let I be an injective module containing M.

Write $\mathscr{S}$= { A / A is a submodule of I such that $A \cap M = \{0\}$ }

Clearly $\mathcal{S} \neq \phi \quad (\because \{0\} \in \mathcal{S})$

Also clearly $\mathcal{S}$ is a poset under set inclusion, in which every chain has an upper bound.

So, by Zorn's lemma, $\mathcal{S}$ has a maximal element, say M^1.

Thus M^1 is a sub module of I and $M \cap M^1 = \{0\}$

Now we show that I/M^1 is an essential extension of $(M+M^1)/M^1$.

Let K/M^1 be a sub module of I/M^1 such that $K/M^1 \cap (M+M^1)/M^1 = \{0\}$.

Then $M^1 \subseteq K \subseteq I$ and $K \cap (M+M^1) \subseteq M^1$

$\Rightarrow K \cap M \subseteq M \cap M^1 = \{0\}$.

So $K \in \mathcal{S}$

By maximality of M^1, we have $K = M^1$.

Therefore $K/M^1 = \{0\}$ and hence I/M^1 is an essential extension of $(M+M^1)/M^1$

But $(M+M^1)/M^1 \cong M/M \cap M^1 \cong M$.

Since M has no proper essential extension, we have $(M+M^1)/M^1$ has no proper essential extension.

So $I/M^1 = (M+M^1)/M^1$

$\Rightarrow I = M + M^1$

Thus M is a direct summand of injective module I. Hence M is injective.

20.14 Proposition:

Every module M has a maximal essential extension N. This is unique in the following sense:

If N^1 is another maximal essential extension of M, then the identity mapping of M can be extended to an isomorphism of N^1 onto N.

Proof:

Let I be an injective module containing M.

Write $\mathscr{S} = \{S / S$ is a submodule of I and S is an essential extension of M$\}$

since $M \in \mathscr{S}$, we have $\mathscr{S} \neq \phi$.

Clearly $\mathscr{S}$ is a poset under set inclusion.

Let $\{S_\alpha\}_{\alpha \in \Delta}$ be a chain in $\mathscr{S}$.

Then each S_α is an essential extension of M Contained in I

Write $S = \underset{\alpha \in \Delta}{U} S_\alpha$

Then S is a submodule of I and $M \subseteq S$.

Now we show that S is an essential extension of M.

Let A be a sub module of S such that $A \neq \{0\}$

Then $A \cap S_\alpha \neq \{0\}$ for at least one $\alpha \in \Delta$ and $A \cap S_\alpha$ is sub module of S_α.

since S_α is an essential extension of M, we have $M \cap A \cap S_\alpha \neq \{0\}$.

$\Rightarrow M \cap A \neq \{0\}$

Therefore S is an essential extension of M and so $S \in \mathscr{S}$ clearly S is an upper bound of $\{S_\alpha\}_{\alpha \in \Delta}$.

So by Zorn's lemma, $\mathscr{S}$ contains a maximal element say N.

$\Rightarrow$ N is a maximal essentail extensionof M in I.

Claim : N is a maximal essentail extension of M, (not just in I, but absolutely).

Let N^1 be any essential extension of M containing N (not necessarily in I)

Then N^1 is an essential extension of N.

By the above lemma, the identity mapping of N can be extended to a monomorphism $\phi : N^1 \rightarrow I$.

So $\phi\left(N^1\right)$ is also an essential extension of N in I, and hence $\phi\left(N^1\right)$ is an essential extension of M and $\phi\left(N^1\right) \subseteq I$.

So $\phi\left(N^1\right) \in \mathscr{S}$

Since N is a maximal essential extensin of M, we have $\phi\left(N^1\right) = N$

$\Rightarrow \phi\left(N^1\right) = N = \phi\left(N\right)$

$\Rightarrow N^1 = N$

Therefore N is a maximal essential extensionof M, (not just in I, but absolutely).

Any essential extensionof N is an essential extension of M.

Therefore N has no proper essential extension and hence N is injective (by proposition)

Suppose L is any maximal esential extension of M.

Then by the above lemma, the identity mapping of M can be extended to a monomorphism ψ of L into N.

Since L is a maximal essential extension of M, we have $\psi(L) = N$.

Therefore $N \cong L$

20.15 Proposition:

Let N be an extension of M. The following statements are equivalent:

i) N is a maximal essential extenson of M.

ii) N is an essential extension of M and is injective

iii) N is a minimal injective extension of M.

Proof:

Assume (i) i.e., N is a maximal essential extenssion of M.

Then N has no proper esential extension and hence by a known result, N is injective.

So $(i) \Rightarrow (ii)$

Assume (ii) i.e., N is an essential extension of M and is injective.

Suppose $M \subseteq I \subseteq N$, where I is an injective extension of M.

Since I is injective , by a known result, I is a direct summand of N.

$\Rightarrow$ there exists a sub module I' of N such that $N = I + I'$ and $I \cap I' = \{0\}$.

Since N is an essential extension of I and $I \cap I' = \{0\}$, we have $I' = \{0\}$

Therefore N = I

So $(ii) \Rightarrow (iii)$

Assume (iii) i.e., N is a minimal injective extension of M.

Let N' be a maximal essential extension of M contained in N.

i.e., $M \subseteq N' \subseteq N$

Then N' is injective.

Since N is a minimal injective extension of M, we have $N = N'$

Therefore N is a maximal essential extension of M.

K. SIVA PRASAD
P.G. Department of Mathematics
J.K.C. College, Guntur