Lectures on Modules 2

second course

The fourth stage

Mathematics Department

College of Education for Pure Sciences

Anbar University

the first lecturer

4.1 INTRODUCTION

In last chapter, we have studied some more results on modules and rings. In Section, 4.2, we study more results on noetherian and artinian modules and rings. In next section, Weddernburn theorem is studied. Uniform modules, primary modules, noether-laskar theorem and smith normal theorem are studied in next two section. The last section is contained with finitely generated abelian groups.

4.2 MORE RESULTS ON NOETHERIAN AND ARTINIAN MODULES AND RINGS

4.2.1 Theorem. Every principal ideal domain is Noetherian.

Solution. Let D be a principal ideal domain and $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_n \subseteq \ldots$be an ascending chain of ideals of D. Let $I = \bigcup_{i \geq 1} I_i$. Then I is an ideal of D. Since D is principal ideal domain, therefore, there exist $b \in D$ such that $I = \langle b \rangle$. Since $b \in D$, therefore, $b \in I_n$ for some n. Consequently, for $m \geq n$, $I \subseteq I_n \subseteq I_m \subseteq I$. Hence $I_n = I_m$ for $m \geq n$ implies that the given chain of ideals becomes stationary at some point i.e. R is Noetherian.

(2) (Z,+,.) is a Notherian ring.

(3) Every field is Notherian ring.

(4) Every finite ring is Notherian ring.

4.2.2 Theorem. (**Hilbert basis Theorem**). If R is Noetherian ring with identity, then R[x] is also Noetherian ring.

Proof. Let I be an arbitrary ideal of R[x]. To prove the theorem, it is sufficient to show that I is finitely generated. For each integer $t \geq 0$, define;

$$I_t = \{r \in R : a_0 + a_1 x + \ldots + r x^t\} \cup \{0\}$$

Then I_t is an ideal of R such that $I_t \subseteq I_{t+1}$ for all t. But then $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ is an ascending chain of ideals of R. But R is Noetherian, therefore, there exist an integer n such $I_n = I_m$ for all $m \geq 0$. Also each ideal I_i of R is finitely generated. Suppose that $I_i = \langle a_{i1}, a_{i2}, \ldots, a_{im_i} \rangle$ for i=0, 1, 2, 3, …, n, where a_{ij} is the leading coefficient of a polynomial $f_{ij} \in I$ of degree i. We will show that $m_0 + m_1 + \ldots + m_n$ polynomials $f_{01}, f_{02}, \ldots, f_{0m_0}, f_{11}, f_{12}, \ldots, f_{1m_1}, \ldots, f_{n1}, f_{n2}, \ldots, f_{nm_n}$ generates I. Let $J = \langle f_{01}, f_{02}, \ldots, f_{0m_0}, f_{11}, f_{12}, \ldots, f_{1m_1}, \ldots, f_{n1}, f_{n2}, \ldots, f_{nm_n} \rangle$. Trivially $J \subseteq I$. Let $f (\neq 0) \in R[x]$ be such that $f \in I$ and of degree t (say): $f = b_0 + b_1 x + \ldots + b_{t-1} x^{t-1} + b x^t$. We now apply induction on t. For t=0, $f = b_0 \in I_0 \subseteq J$. Further suppose that every polynomial of I whose degree less than t also belongs to J. Consider following cases:

Case 1. $t > n$. As $t > n$, therefore, leading coefficient b (of f) $\in I_t = I_n$ (because $I_t = I_n \ \forall \ t \geq n$). But then $b = r_1 a_{n1} + r_2 a_{n1} + \ldots + r_{m_n} a_{nm_n}$, $r_i \in R$. Now $g = f - (r_1 f_{n1} + r_2 f_{n1} + \ldots + r_{m_n} f_{nm_n}) x^{t-n} \in I$ having degree less than t (because the coefficient of x^t in g is $b - r_1 a_{n1} + r_2 a_{n1} + ... + r_{mn} a_{nm_n} = 0$, therefore, by induction, $f \in J$.

Case (2). $t \le n$. As $b \in I_t$, therefore, $b = s_1 a_{t1} + s_2 a_{t2} + ... + s_{mt} a_{tm_t}$; $s_i \in R$.

Then $h = f - (s_1 f_{n1} + s_2 f_{n1} + ... + s_{mn} f_{nm_n}) \in I$, having degree less than t. Now by lsinduction hypothesis, $h \in J \Rightarrow f \in J$. Consequently, in either case $I \subseteq J$ and hence $I = J$. Thus I is finitely generated and hence R[x] is Noetherian. It prove the theorem.

4.2.3 Definition. A ring R is said to be an Artinian ring iff it satisfies the descending chain condition for ideals of R.

4.2.4 Definition. A ring R is said to satisfy the minimum condition (for ideals) iff every non empty set of ideals of R, partially ordered by inclusion, has a minimal element.

4.2.5 Theorem. Let R be a ring. Then R is Artinian iff R satisfies the minimum condition (for ideals).

Proof. Let R be Artinian and f be a nonempty set of ideal of R. If I_1 is not a minimal element in f, then we can find another ideal I_2 in f such that $I_1 \supset I_2$. If f has no minimal element, the repetition of this process we get a non terminating descending chain of ideals of R, contradicting to the fact that R is Artinian. Hence f has minimal element.

Conversely suppose that R satisfies the minimal condition. Let $I_1 \supseteq I_2 \supseteq I_3 \ldots$ be an descending chain of ideals of R. Consider $\mathbf{F} = \{I_t : t=1, 2, 3, \ldots\}$. $I_1 \in \mathbf{F} \Rightarrow \mathbf{F}$ is non empty. Then by hypothesis, F has a minimal element I_n for some positive integer n $\Rightarrow I_m \subseteq I_n \ \forall\ m \ge n$.

Now $I_m \ne I_n \Rightarrow I_m \notin F$ (By the minimality of I_n) , which is not possible. Hence $I_m = I_n \ \forall\ m \ge n$ i.e. R is Artinian.

4.2.6 Theorem. Prove that an homomorphic image of a Noetherian(Artinian) ring is also Noetherian(Artinian).

Proof. Let f be a homomorphic image of a Noetherian ring R onto the ring S. Consider the ascending chain of ideals of S:

$$J_1 \subseteq J_2 \subseteq \ldots \subseteq \ldots \qquad (1)$$

Suppose $I_r = f^{-1}(J_r)$, for r=1, 2, 3, ….

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq \ldots \qquad (2)$$

Relation shown in (2) is an ascending chain of ideals of R. Since R is Noehterian, therefore, there exist positive integer n such that $I_m = I_n$ $\forall$ $m \geq n$. This shows that $J_m = J_n$ $\forall$ $m \geq n$. But then S becomes Noetherian and the result follows.

4.2.7 Corollary. If I is an ideal of a Noetherian(Artinian) ring, then factor module $\frac{R}{I}$ is also Noetherian(Artinian).

Proof. Since $\frac{R}{I}$ is homomorphic image of R, therefore, by Theorem 4.2.10, $\frac{R}{I}$ is Noehterian.

The second lecture

4.2.8 Theorem. Let I be an ideal of a ring R. If R and $\frac{R}{I}$ are both Noehterian rings, then R is also Noetherian.

Proof. Let $I_1 \subseteq I_2 \subseteq \ldots \subseteq \ldots$ be an ascending chain of ideals of R. Let f: R→ $\frac{R}{I}$. It is an natural homomorphism. But then $f(I_1) \subseteq f(I_2) \subseteq \ldots \subseteq$ is an ascending chain of ideals in $\frac{R}{I}$. Since $\frac{R}{I}$ is Noetherian, therefore, there exist a positive integer n such that $f(I_n) = f(I_{n+i})$ $\forall$ $i \geq 0$. Also $(I_1 \cap I) \subseteq (I_2 \cap I) \subseteq \ldots \subseteq \ldots$ is an ascending chain of ideals of I. As I is Noehterian, therefore, there exsit a positive integer m such that $(I_m \cap I) = (I_{m+i} \cap I)$. Let r=max{m, n}. Then $f(I_r) = f(I_{r+i})$ and $(I_r \cap I) = (I_{r+i} \cap I)$ $\forall$ $i \geq 0$. Let $a \in I_{r+i}$, then there exist $x \in I_r$ such that f(a)=f(x) i.e. a+I=x+I. Then $a-x \in I$ and also $a-x \in I_{r+i}$. This shows that $a-x \in (I_{r+i} \cap I) = (I_r \cap I)$. Hence $a-x \in I_r \Rightarrow a \in I_r$ i.e. $I_{r+i} \subseteq I_r$. But then $I_{r+i} = I_r$

for all $i \geq 0$. Now we have shown that every ascending chain of ideals of R terminates after a finite number of steps. It shows that R is Noetherian.

4.2.9 Definition. An Artinian domain R is an integral domain which is also an Artinian ring.

4.2.10 Theorem. Any left Artinian domain is a division ring.

Proof. Let a is a non zero element of R. Consider the ascending chain of ideals of R as: $\langle a\rangle \supseteq \langle a^2\rangle \supseteq \langle a^3\rangle \supseteq \ldots\ldots$ Since R is an Artinian ring, therefore, $\langle a^n\rangle = \langle a^{n+i}\rangle\ \forall\ i \geq 0$. Now $\langle a^n\rangle = \langle a^{n+1}\rangle \Rightarrow a^n = ra^{n+1} \Rightarrow ar = 1$ i.e. a is invertible $\Rightarrow$ R is a division ring.

4.2.11 Theorem. Let M be a finitely generated free module over a commutative ring R. Then all the basis of M are finite.

Proof. let $\{e_i\}_{i\in\wedge}$ be a basis and $\{x_1, x_2, \ldots, x_n\}$ be a generator of M. Then each x_j can be written as $x_j = \sum_i \beta_{ij} e_i$ where all except a finite number of β_{ij}'s are zero. Thus the set of all e_i's that occurs in the expression of x_j's, $j=1,2,\ldots,n$.

4.2.12 Theorem. Let M be finitely generated free module over a commutative ring R. Then all the basis of M has same number of element.

Proof. Let M has two bases X and Y containing m and n elements respectively. But then $M \cong R^n$ and $M \cong R^m$. But then $R^m \cong R^n$. Now we will show that m=n. Let m< n, f is an isomorphism from R^m to R^n and $g=f^{-1}$. Let $\{x_1, x_2, \ldots, x_m\}$ and $\{y_1, y_2, \ldots, y_n\}$ are basis element of R^m and R^n respectively. Define

$f(x_i) = a_{1i}y_1 + a_{2i}y_2 + \ldots + a_{ni}y_n$ and $g(y_j) = b_{1j}x_1 + b_{2j}x_2 + \ldots + b_{mj}x_m$. Let $A(a_{ji})$ and $B=(b_{kj})$ be n×m and m×n matrices over R. Then $g f(x_i) = g(\sum_{j=1}^{n} a_{ji}y_j) = \sum_{j=1}^{n} a_{ji}g(y_j) = \sum_{k=1}^{m}\sum_{j=1}^{n} b_{kj}a_{ji}x_k$. $1 \leq i \leq m$. Since $gf = I$, therefore, $x_i = \sum_{k=1}^{m}\sum_{j=1}^{n} b_{kj}a_{ji}x_k$ i.e. $\sum_{j=1}^{n} b_{1j}a_{ji}x_1 + \ldots + \sum_{j=1}^{n}(b_{ij}a_{ji} - 1)x_i + \ldots + \sum_{j=1}^{n} b_{mj}a_{ji}x_m = 0$. As x_i's are linearly independent, therefore,

$\sum_{j=1}^{n} b_{kj} a_{ji} x_k = \delta_{ki}$. Thus $BA=I_m$ and $AB=I_n$. Let $A^*=[A\ 0]$ and $B^*=\begin{bmatrix} B \\ 0 \end{bmatrix}$, then $A^*B^*= I_n$ and $B^*A^*=\begin{bmatrix} I_m & 0 \\ 0 & 0 \end{bmatrix}$. But then $\det(A^*B^*)=I_n$ and $\det(B^*A^*)=0$.

Since A^* and B^* are matrices over commutative ring R, so $\det(A^*B^*)$ $\det(B^*A^*)$, which yield a contradiction. Hence $M \geq N$. By symmetry $N \geq M$ i.e. $M=N$.

4.3 RESULT ON H_R(M, M) AND WEDDENBURN ARTIN THEOREM

4.3.1 Theorem 4. Let $M= \sum_{i=1}^{k} M_i$ be a direct sum of R-modules M_i. Then

$$\mathrm{Hom}_R(M, M) \simeq \begin{bmatrix} \mathrm{Hom}_R(M_1, M_1) & \mathrm{Hom}_R(M_2, M_1) & \ldots & \mathrm{Hom}_R(M_k, M_1) \\ \mathrm{Hom}_R(M_1, M_2) & \mathrm{Hom}_R(M_2, M_2) & \ldots & \mathrm{Hom}_R(M_k, M_2) \\ \vdots & \vdots & & \vdots \\ \mathrm{Hom}_R(M_1, M_k) & \mathrm{Hom}_R(M_2, M_k) & \ldots & \mathrm{Hom}_R(M_k, M_k) \end{bmatrix}$$

as a ring (Here right hand side is a ring T(say) of K×K matrices $f=(f_{ij})$ under the usual matrix addition and multiplication, where f_{ij} is an element of $\mathrm{Hom}_R(M_j, M_i)$).

Proof. We know that for are submodules X and Y, $\mathrm{Hom}_R(X, Y)$ (=set of all homomorphisms from X to Y) becomes a ring under the operations $(f +g) x=f(x) +g(x)$ and $fg(x)=f(g(x))$, $f , g \in \mathrm{Hom}_R(X, Y)$ and $x \in X$. Further $\lambda_j: M_j \to M$ and $\pi_i: M\to M_i$ are two mappings defined as:

$\lambda_j(x_j)=(0, \ldots, x_j,\ldots,0)$ and $\pi_i(x_1, \ldots, x_i, \ldots,x_k) = x_i$. (These are called inclusion and projection mappings). Both are homomorphisms. Clearly, $\pi_i \varphi \lambda_j: M_j \to M_i$ is an homomorphism, therefore, $\pi_i \varphi \lambda_j \in \mathrm{Hom}_R(M_j , M_i)$. Define a mapping $\sigma : \mathrm{Hom}_R(M, M)\to T$ by $\sigma(\varphi)= (\pi_i \varphi \lambda_j)$, $\varphi \in \mathrm{Hom}_R(M , M)$ and $(\pi_i \varphi \lambda_j)$ is k×k matrix whose $(i, j)^{th}$ enrty is $\pi_i \varphi \lambda_j$. We will show that σ is an isomorphism. Let $\varphi_1, \varphi_2 \in \mathrm{Hom}_R(M , M)$. Then

$\sigma (\varphi_1 + \varphi_2) = (\pi_i (\varphi_1+ \varphi_2)\lambda_j)= (\pi_i \varphi_1\lambda_j + \pi_i \varphi_2\lambda_j) = (\pi_i \varphi_1\lambda_j) + (\pi_i \varphi_2\lambda_j)$

$=\sigma (\varphi_1) + \sigma (\varphi_2)$ and $\sigma (\varphi_1) \sigma (\varphi_2) = (\pi_i \varphi_1 \lambda_j) (\pi_i \varphi_2 \lambda_j) = \sum_{l=1}^{k} \pi_i \varphi_1\lambda_l \pi_l\varphi_2\lambda_j$

$= \pi_i \varphi_1\lambda_1\pi_1\varphi_2\lambda_j + \pi_i \varphi_1\lambda_2\pi_2\varphi_2\lambda_j + ... + \pi_i \varphi_1\lambda_k \pi_k \varphi_2\lambda_j$

$= \pi_i \varphi_1(\lambda_1\pi_1 + ... + \lambda_k \pi_k)\varphi_2\lambda_j$. Since for $(x_1,\ldots, x_i, \ldots,x_k) = x \in M$, $\lambda_i\pi_i(x) = \lambda_i(x_i) = (0,\ldots, x_i, \ldots,0)$, therefore, $(\lambda_1\pi_1 + \lambda_2\pi_2 + ... + \lambda_k \pi_k)(x) = (\lambda_1\pi_1(x) + \lambda_2\pi_2(x) + ... + \lambda_k \pi_k(x) = (x_1, \ldots,0)+ (0, x_2, \ldots,0)+\ldots+ (0,\ldots, x_k) = (x_1, x_2, \ldots,x_k) = x$. Hence $(\lambda_1\pi_1 + \lambda_2\pi_2 + ... + \lambda_k \pi_k) = I$ on M. Thus $\sigma(\varphi_1)\sigma(\varphi_2) = \pi_i \varphi_1\varphi_2\lambda_j = \sigma(\varphi_1\varphi_2)$. Hence σ is an homomorphism. Now we will show that σ is one-one. For it let $\sigma(\varphi) = (\pi_i \varphi \lambda_j) = 0$. Then $\pi_i \varphi \lambda_j = 0$ for each i, j ; $1 \le i, j \le k$. But then $\pi_1 \varphi \lambda_j + \pi_2 \varphi \lambda_j +\ldots+ \pi_k \varphi \lambda_j = 0$. Since $\sum_{i=1}^{k} \pi_i$ is an identity mapping on M, therefore, $(\sum_{i=1}^{k} \pi_i)\varphi\lambda_j \Rightarrow \varphi\lambda_j = 0$. But then $\varphi \sum_{j=1}^{k} \lambda_j =$ 0 and hence $\varphi = 0$. Therefore, the mapping is one-one. Let $f = (f_{ij}) \in T$, where $f_{ij} : M_j \to M_i$ is an R-homomorphism. Set $\psi = \sum_{i,j} \lambda_i f_{ij}\pi_j$. Since for each i and j, $\lambda_i f_{ij} \pi_j$ is an homomorphism from M to M, therefore, $\sum_{i,j} \lambda_i f_{ij}\pi_j$ is also an element of Hom(M, M). Since $\sigma(\varphi)$ is a square matrix of order k, whose (s, t) entry is f_{st}, therefore, $\sigma(\psi) = (\pi_s(\sum_{j} \lambda_i f_{ij}\pi_j)\lambda_t)$. As $\pi_p \lambda_q = \delta_{pq}$, therefore, $\pi_s(\sum_{i,j} \lambda_i f_{ij}\pi_j)\lambda_t = f_{st}$. Hence $\sigma(\psi) = (f_{ij}) = f$ i.e. mapping is onto also. Thus σ is an isomorphism. It proves the result.

Third lecture

4.3.2 Definition. Nil Ideal. A left ideal A of R is called nil ideal if each element of it nilpotent.

Example. Every Nilpotent ideal is nil ideal.

4.3.3 Theorem. If J is nil left ideal in an Artinian ring R, then J is nilpotent.

Proof. Suppose $J^k \neq (0)$. For some positive integer k. Consider a family $\{J, J^2, \ldots\}$. Because R is Artinian ring, this family has minimal element say $B = J^m$. Then $B^2 = J^{2m} = J^m = B$ implies that $B^2 = B$. Now consider another family $f = \{A|$ A is left ideal contained in B with BA≠(0). As BB=B≠(0), therefore, f is non empty. Since it is a family of left ideals of an Artinian ring R, therefore, it has minimal element. Let A be that minimal element in *f*. Then BA $\neq$(0) i.e. there exist a in A such that Ba$\neq$(0) Because A is an ideal, therefore, Ba $\subseteq$ A and B(Ba)=B^2a=Ba $\neq$(0). Hence Ba$\in$ *f*. Now the minimality of A implies that Ba=A. Thus ba=a for some b$\in$B. But then $b^i a = a$ $\forall$ i $\geq$1. Since b is nilpotent element, therefore, a=0, a contradiction. Hence for some integer k, J^k=(0).

Theorem. Let R be Noetherian ring. Then the sum of nilpotent ideals in R is a nilpotent ideal.

Proof. Let B = $\sum_{i\in\Lambda} A_i$ be the sum of nilpotent ideals in R. Since R is noetherian, therefore, every ideal of R is finitely generated. Hence B is also finitely generated. Let B=<x_1, x_2, …, x_t> . Then each x_i lies in some finite number of A_i's say A_1, A_2, …, A_n. Thus B=A_1+A_2+…+A_n. But we know that finite sum of nilpotent ideals is nilpotent. Hence B is nilpotent.

4.3.4 Lemma. Let A be a minimal left ideal in R. Then either A^2=(0) or A=Re.

Proof. Suppose that $A^2$$\neq$(0). Then there exist a$\in$A sucht that Aa$\neq$(0). But Aa $\subseteq$A and the minimality of A shows that Aa =A. From this it follows that there exist e in A such that ea=a. As a is non zero, therefore, ea$\neq$0 and hence e$\neq$0. Let B={c$\in$A | ca=0}, then B is a left ideal of A. Since ea $\neq$ 0 , therefore, e$\notin$ B. Hence B is proper ideal of A. Again minimality of A implies that B=(0). Since e^2a=eea=ea $\Rightarrow$ (e^2-e)a=0, therefore, (e^2-e) $\in$B=(0). Hence e^2=e. i.e e is an idempotent in R. As 0$\neq$ e=e^2= e.e$\in$Re, therefore, Re is a non zero subset of A. But then Re=A. It proves the result.

4.3.5 Theorem. (Wedderburn-Artin). Let R be a left (or right) artinian ring with unity and no nonzero nilpotent ideals. Then R is isomorphic to a finite direct sum of matrix rings over the division ring.

Proof. First we will show that each non zero left ideal in R is of the form Re for some idempotent. Let A be a non-zero left ideal in R. Since R is artinian, therefore, A is also artinian and hence every family of left ideal of A contains a minimal element i.e. A has a minimal ideal M say. But then M^2=(0) or M=Re for some idempotent e of R. If M^2=(0), then

$(MR)^2=(MR)(MR)=M(RM)R=MMR=M^2R=(0)$. But then MR is nilpotent. Thus by given hypothesis MR=(0). Now MR = (0) implies that M = (0), a contradiction. Hence M=Re. This yields that each non zero left ideal contains a nonzero idempotent. Let f ={R(1-e)∩A | e is a non-zero idempotent in A}. Then f is non empty. Because M is artinian, f has a minimal member say R(1-e)∩A. We will show that R(1-e)∩A=(0). If R(1-e)∩A≠(0) then it has a non zero idempotent e_1. Since $e_1 = r(1-e)$, therefore, $e_1e=r(1-e)e= r(e-e^2)=0$. Take $e^* = e + e_1 - ee_1$. Then $(e^*)^2 =(e + e_1 - ee_1)(e + e_1 - ee_1)= ee + e_1e - ee_1e + ee_1 + e_1e_1 - ee_1e_1 - eee_1- e_1ee_1 + ee_1ee_1= e + 0 – e0 + ee_1 + e_1 - ee_1 -ee_1- 0e_1 + e0e_1= e + e_1 - ee_1 = e^*$ i.e. we have shown that e^* is an idempotent. But $e_1e^* =e_1e + e_1e_1$

$- e_1ee_1= e_1\neq 0$ implies that $e_1 \notin R(1-e^*) \cap A$. (Because if $e_1\in R(1-e^*) \cap A$, then $e_1 = r(1-e^*)$ for some $r\in R$ and then $e_1e^* = r(1-e^*) e^* = r(e^* - e^* e^*)=0$). More

over for $r(1-e^*)\in R(1-e^*)$, $r(1-e^*)= r(1- e - e_1 + ee_1)= r(1- e - e_1(1- e))= r(1-e_1)(1- e)= s(1-e)$ for $s = r(1-e_1)\in R$, therefore, Hence $R(1-e^*)\cap A$ is proper subset of R(1-e)∩A. But it is a contradiction to the minimality of R(1-e)∩A in f. Hence R(1-e)∩A=(0). Since for $a\in A$, $a(1-e)\in R(1-e)\cap A$, therefore, a(1-e)=(0) i.e. a=ae. Then $A \supseteq Re \supseteq Ae \supseteq A \Rightarrow A=Re$.

For an idempotent e of R, Re∩ R(1-e)=(0). Because if $x\in Re\cap R(1-e)$, then x=re and x=s(1-e) for some r and s belonging to R. But then $re=s(1-e)\Rightarrow ree=s(1-e)e \Rightarrow re= s(e-e^2)=0$ i.e. x=0. Hence Re ∩ R(1-e)=(0). Now let S be the sum of all minimal left ideals in R. Then S=Re for some idempotent e in R. If R(1-e)≠(0), then there exist a minimal left ideal A in R(1-e). But then $A \subseteq Re \cap R(1-e)=(0)$, a contradiction. Hence , R(1-e)=(0) i.e

$R=Re=S= \sum_{i\in\Lambda} A_i$ where $(A_i)_{i\in\Lambda}$ is the family of minimal left ideals in R. But

then there exist a subfamily $(A_i)_{i\in\Lambda^*}$ of the family $(A_i)_{i\in\Lambda}$ such that $R = \oplus\sum_{i\in\Lambda^*} A_i$. Let $1 = e_{i_1} + e_{i_2} + ... + e_{i_n}$. Then $R= Re_{i_1} \oplus ... \oplus Re_{i_n}$ (because for $r\in R$, $1 = e_{i_1} + e_{i_2} + ... + e_{i_n} \Rightarrow r = re_{i_1} + re_{i_2} + ... + re_{i_n}$). After reindexing if necessary, we may write $R = Re_1\oplus Re_2 \oplus ... \oplus Re_n$, a direct sum of minimal left ideals. In this family of minimal left ideals $Re_1, Re_2, ..., Re_n$, choose a largest subfamily consisting of all minimal left ideals that are not isomorphic to each other as left R-modules. After renumbering if necessary, let this subfamily be $Re_1, Re_2, ..., Re_k$. Suppose the number of left ideal in the family (Re_i), $1\le i \le n$, that are isomorphic to Re_i is n_i. Then

$$R = \overbrace{[Re_1 \oplus ...]}^{n_1 \text{ summands}} \oplus \overbrace{[Re_2 \oplus ...]}^{n_2 \text{ summands}} \oplus ... \oplus \overbrace{[Re_k \oplus ...]}^{n_k \text{ summands}}$$

where each set of brackets contains pair wise isomorphic minimal left ideals, and no minimal left ideal in any pair of bracket is isomorphic to minimal left ideal in another pair. Since $Hom_R(Re_i , Re_j)=(0)$ for $i\neq j$, $1\le i , j\le k$ and $Hom_R(Re_i , Re_i) =D_i$ is a division ring(by shcur's lemma). Thus by Theorem 4, we get $Hom_R(R,R)\cong$

$$\begin{pmatrix} \begin{vmatrix} D_1 & \cdots & D_1 \\ \vdots & & \vdots \\ D_1 & \cdots & D_1 \end{vmatrix} & 0 & 0 \\ 0 & \begin{vmatrix} D_2 & \cdots & D_2 \\ \vdots & & \vdots \\ D_2 & \cdots & D_2 \end{vmatrix} & \ddots \\ 0 & & \begin{vmatrix} D_k & \cdots & D_k \\ \vdots & & \vdots \\ D_k & \cdots & D_k \end{vmatrix} \end{pmatrix} \qquad \begin{pmatrix} (D_1)_{n_1} & & \\ & \ddots & \\ & & (D_k)_{n_k} \end{pmatrix}$$

$\cong (D_1)_{n1}$ ... $(D_k)_{nk}$. But since $Hom_R(M, M) \cong R^{op}$ (under the mapping f: $R^{op} \rightarrow Hom_R(M, M)$ given by $f(a)=a^*$ where $a^*(x)=a\circ x=xa$) as rings and the opposite ring of a division ring is a division ring. Since $R^{op} \cong R$, therefore, R is finite direct sum of matrix rings over division rings.

4.4 UNIFORM MODULES, PRIMARY MODULES AND NOETHER-LASKAR THOEREM

4.4.1 Definition. Uniform module. A non zero module M is called uniform if any two nonzero submodules of M have non zero intersection.

Example. Z as Z-module is uniform as: Since Z is principal ideal domain, therefore, the two sub-modules of it are <a> and <b> say, then <ab> is another submodule which is contained in both <a> and <b> . Hence intersection of any two nonzero sub-modules of M is non zero. Thus Z is a uniform module over Z.

4.4.2 Definition. If U and V are uniform modules, we say U is sub-isomorphic to V provided that U and V contains non zero isomorphic sub-modules.

4.4.3 Definition. A module M is called primary if each non zero sub-module of M has uniform sub-module and any two uniform sub-modules of M are sub-isomorphic.

Example. Z is a primary module over Z.

Fourth lecture

4.4.4 Theorem. Let M be a Noetherian module or any module over a Noetherian ring. Then each non zero submodule contains a uniform module.

Proof. Let N be a non zero submodule of M. Then there exist $x(\neq 0) \in N$. Consider the submodule xR of N. Then it is enough to prove that xR contains a uniform module. If M is Noetherian, then the every submodule of M is noetherian and hence xR is also noetherian and if R is Noethrian then, being a homomorphic image of Noetherian ring R, xR is also Noetherian. Thus, for both cases, xR is Noetherian.

Consider a family ***f*** of submodules of xR as: ***f*** $=\{N|$ N has a zero intersection with at least one submodule of xR$\}$. Then $\{0\} \in$ ***f***. Since xR is noetherian, therefore, ***f*** has maximal element K(say). Then there exist an submodule U of xR such that $K \cap U=\{0\}$. We claim U is uniform. Otherwise, there exist submodules A, B of U such that $A \cap B=\{0\}$. Since $K \cap U=\{0\}$, therefore, we can talk about $K \oplus A$ as a submodule of xR such that $K \oplus A \cap B=\{0\}$. But then $K \oplus A \in$ ***f***, a contradiction to the maximality of K. This contradiction show that U is uniform. Hence $U \subseteq xR \subseteq N$. Thus every submodule N contains a uniform submodule.

4.4.5 Definition. If R is a commutative noetherian ring and P is a prime ideal of R, then P is said to be associated with module M if R/P imbeds in M or equivalently, $P=r(x)$ for some $x \in M$, where $r(x)=\{a \in R \mid xa =0\}$.

4.4.6 Definition. A module M is called P- primary for some prime ideal P if P is the only prime associated with M.

4.4.7 Theorem. Let U be a uniform module over a commutative noetherain ring R. Then U contains a submodule isomorphic to R/P for precisely one prime ideal P. In other words U subisomorphic to R/P for precisely one ideal P.

Proof. Consider the family *f* of annihilators of ideals r(x) for non zero x $\in$U. Being a family of ideals of noetherian ring R, *f* has a maximal element r(x) say. We will show that P=r(x) is prime ideal of R. For it let ab$\in$r(x), a$\notin$r(x). As ab$\in$r(x) $\Rightarrow$ (ab)x = 0. Since xa $\neq$ 0, therefore, b(xa) = 0 $\Rightarrow$ b$\in$r(xa). More over for t$\in$r(xa) $\Rightarrow$ t(xa)=0 $\Rightarrow$ (ta)x=0 $\Rightarrow$ r(xa) $\in$ *f*. Clearly r(x) $\subseteq$ r(xa). Thus the maximality of r(x) in *f* implies that r(xa)=r(x) i.e. b$\in$r(x). Hence r(x) is prime ideal of R. Define a mapping from R to xR by θ(r)=xr. Then it is an homomorphism from R to xR. Kernal θ ={ r$\in$R | xr=0}. Then Kernal θ = r(x). Hence by fundamental theorem on homomorphism, R/ r(x) $\cong$ xR = R/P. Therefore R/P is embeddable in U. Hence [R/P]=[R/Q]. this implies that there exist cyclic submodules xR and yR of R/P and R/Q respectively such that xR$\cong$yR. But then R/P$\cong$R/Q, which yields P=Q. It prove the theorem.

4.4.8 Note. The ideal in the above theorem is called the prime ideal associated with the uniform module U.

4.4.9 Theorem. Let M be a finitely generated ideal over a commutative noetherian ring R. Then there are only a finite number of primes associated with M.

Proof. Take a family *f* consisting of the direct sum of cyclic uniform submodules of M. Since every submodule M over a noehtrian ring contains a uniform submdule, therefore, *f* is non empty. Define a relation ≤, on the set of elements of *f* by $\oplus\sum_{i\in I} x_iR \leq \oplus\sum_{j\in J} x_jR$ iff I $\subseteq$ J and $x_iR \subseteq y_jR$ for some j$\in$J.

This relation is a partial order relation on *f* . By Zorn's lemma F has a maximal member K = $\oplus\sum_{i\in I} x_iR$. Since M is noetherian, therefore, K is finitely generated. Thus K = $\oplus\sum_{i=1}^{t} x_iR$. By theorem, 4.2.7, there exist $x_ia_i \in x_i R$ such that $r(x_i a_i)=P_i$, the ideal associated with $x_i R$. Set $x_i^* = x_i a_i$ and $K^* = \oplus \sum_{i=1}^{t} x_i^* R$.

Let $Q = r(x)$ be the prime ideal associated with M. We shall show that $Q = P_i$ for some i, $1 \le i \le t$.

Since K is a maximal member of *f*, therefore, K as well as K^* has the property that each has non zero intersection with each submodule L of M. Now let $0 \neq y \in xR \cap K^*$. Write $y = \oplus \sum_{i=1}^{t} x_i^* b_i = xb$. We will show that $r(x_i^* b_i) = r(x_i^*)$ whenever $x_i^* b_i \neq 0$. Clearly, $r(x_i^*) \subseteq r(x_i^* b_i)$. Let $x_i^* b_i c = 0$. Then $b_i c \in r(x_i^*) = P_i$ and so $c \in P_i$ since $b_i \notin P_i$. Hence, $c \in r(x_i^*)$.

Further, we note $Q = r(x) = r(y) = \bigcap_{i=1}^{t} r(x_i^* b_i) = \bigcap_{i \in \Lambda} P_i$, omitting those terms from $x_i^* b_i = 0$, where $\Lambda \subset \{1, 2, ..., t\}$. Therefore, $Q \subseteq P_i$ for all $i \in \Lambda$. Also $\prod_{i \in \Lambda} P_i \subset \bigcap_{i \in \Lambda} P_i = Q$. Since Q is a prime ideal, at least one P_i appearing in the product $\prod_{i \in \Lambda} P_i$ must be contained in Q. Hence $Q = P_i$ for some i.

4.4.10 Theorem.(Noether-Laskar theorem). Let M be a finitely generated ideal over a commutative noetherian ring R. Then there exist a finite family $N_1, N_2, \ldots, N_t$ of submodules of M such that

(a) $\bigcap_{i=1}^{t} N_i = (0)$ and $\bigcap_{\substack{i=1 \\ i \neq i_0}}^{t} N_i \neq (0)$ for $1 \le i_0 \le t$.

(b) Each quotient module M/N_i is a P_i - primary module for some prime ideal P_i.

(c) The P_i are all distinct, $1 \le i \le t$.

(d) The primary component N_i is unique iff P_i does not contain P_j for some $j \neq i$.

Proof. Let U_i, $1 \le i \le t$, be a uniform sub module obtained as in the proof of the Theorem 4.4.9. Consider the family { K | K is a subset of M and K contains no submodule subisomorphic to U_i }. Let N_i be a maximal member of this family, then with this choice of N_i, (a), (b) and (c) follows directly.

Fifth lecture

4.5 SMITH NORMAL FORM

4.5.1 Theorem. Obtain Smith normal form of given matrix. Or if A is $m \times n$ matrix over a principal ideal domain R. Then A is equivalent to a matrix that has the diagonal form $\begin{pmatrix} a_1 & & & & \\ & a_2 & & O & \\ & & \ddots & & \\ & & & a_r & \\ & & & & O \end{pmatrix}$ where $a_i \neq 0$ and $a_1 \mid a_2 \mid a_3 \mid \ldots \mid a_r$.

Proof. For non zero a, define the length $l(a)$=no of prime factors appearing in the factorizing of , $a=p_1p_2 \ldots p_r$ (p_i need not be distinct primes). We also take l(a) if a is unit in R. If A=0, then the result is trivial otherwise, let a_{ij} be the non zero element with minimum $l(a_{ij})$. Apply elementary row and column operation to bring it (1, 1) position. Now a_{11} entry of the matrix so obtained is of smallest l value i.e. the non zero element of this matrix at (1, 1) position. Let a_{11} does not divide a_{1k}. Interchanging second and k^{th} column so that we may suppose that a_{11} does not divide a_{12}. Let $d=(a_{11}, a_{12})$ be the greatest common divisor of a_{11} and a_{12}, then $a_{11}=du$, $a_{12}=dv$ and $l(d) < l(a_{11})$. As $d=(a_{11}, a_{12})$, therefore we can find s and t R such that $d=(sa_{11}+ta_{12})= d(su + vt)$. Then we get that $A \begin{pmatrix} u & t & & & \\ v & -s & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}$ is a matrix whose first row is $(d, 0, b_{13}, b_{14}, \ldots b_{1n})$ where $l(d) < l(a_{11})$. If $a_{11} \mid a_{12}$, then $a_{12}=ka_{11}$. On applying, the operation C_2- kC_1 and $\frac{1}{u} C_1$ we get the matrix whose first row is again of the form $(d, 0, b_{13}, b_{14}, \ldots b_{1n})$. Continuing in this way we get a matrix whose first row and first column has all its entries zero except the first entry. This matrix is $P_1AQ_1 \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{pmatrix}$, where A_1 is (m-1)×(n-1) matrix, and P_1 and Q_1 are m×m and n×n invertible matrices respectively. Now applying the same process of A_1, we get that $P_2' A_1 Q_2' = \begin{pmatrix} a_2 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_2 & \\ 0 & & & \end{pmatrix}$, where A_2 is (m-2)×(n-2) matrix, and P_2' and Q_2' are (m-1)×(m-1) and (n-1)×(n-1) invertible matrices respectively. Let $P_2 = \begin{bmatrix} 1 & 0 \\ 0 & P_2 \end{bmatrix}$ and $Q_2 = \begin{bmatrix} 1 & 0 \\ 0 & Q_2 \end{bmatrix}$. Then $P_2P_1AQ_1Q_2 =$

$$\begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & & \\ \vdots & & A_2 & \\ 0 & & & \end{bmatrix}$$

. Continuing in this way we get matrices P and Q such that

$PAQ = \text{diag}(a_1, a_2, \ldots, a_r, 0, \ldots 0)$. Finally we show that we can reduce PAQ so that $a_1 | a_2 | a_3 | \ldots$. For it if a_1 does not divide a_2, then add second row to the first row and obtain the matrix whose first row is $(a_1, a_2, 0, 0, \ldots, 0)$. Again multiplying PAQ by a matrix of the form

$$\begin{bmatrix} u & t & & & \\ v & -s & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix}$$

we can obtain a matrix such that $a_1 | a_2$. Hence we can always obtain a matrix of required form.

4.5.2 Example. Obtain the normal smith form for a matrix $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{bmatrix}$.

Solution.

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{bmatrix} \xrightarrow{R_2 - 4R_1} \begin{bmatrix} 1 & 2 & 3 \\ 0 & -3 & -12 \end{bmatrix} \xrightarrow{C_2 - 2C_1,\, C_3 - 3C_1} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & -12 \end{bmatrix} \xrightarrow{C_3 - 4C_2}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & -12 \end{bmatrix} \xrightarrow{C_3 - 4C_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{bmatrix} \xrightarrow{-R_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix}.$$

4.6 FINITELY GENERATED ABELIAN GROUPS

4.6.1 Note. Let $G_1, G_2, \ldots G_n$ be a family of subgroup of G and let $G^* = G_1 \ldots G_n$.

Then the following are equivalent.

(i) $G_1 \times \ldots \times G_n \quad G^*$ under the mapping $(g_1, g_2, \ldots, g_n)$ to $g_1g_2 \ldots g_n$

(ii) G_i is normal in G^* and every element x belonging to G^* can be uniquely expressed as $x = g_1g_2 \ldots g_n$, $g_i \; G_i$.

(iii) G_i is normal in G^* and if $e = g_1g_2 \ldots g_n$, then each x_i=e.

(iv) G_i is normal in G^* and $G_i \cap G_1 \ldots G_{i-1} G_{i+1} \ldots G_n = \{e\}$, $1 \le i \le n$.

4.6.2 Theorem.(Fundamental theorem of finitely generated abelian groups). Let G be a finitely generated abelian group. Then G can be decomposed as a direct sum of a finite number of cyclic groups C_i i.e. $G = C_1 \oplus C_2 \oplus \ldots \oplus C_t$ where either all C_i's are infinite or for some j less then k, $C_1, C_2, \ldots C_j$ are of order $m_1, m_2, \ldots m_j$ respectively, with $m_1 | m_2 | \ldots | m_j$ and rest of C_i's are infinite.

Proof. Let $\{a_1, a_2, \ldots, a_t\}$ be the smallest generating set for G. If t=1, then G is itself a cyclic group and the theorem is trivially true. Let t > 1 and suppose that the result holds for all finitely generated abelian groups having order less then t. Let us consider a generating set $\{a_1, a_2, \ldots, a_t\}$ of element of G with the property that , for all integers $x_1, x_2, \ldots, x_t$, the equation

$$x_1 a_1 + x_2 a_2 + \ldots + x_t a_t = 0$$

implies that

$$x_1 = 0, x_2 = 0, \ldots, x_t = 0.$$

But this condition implies that every element in G has unique representation of the form

$$g = x_1 a_1 + x_2 a_2 + \ldots + x_t a_t, x_i \in Z.$$

Thus by Note 4.6.1,

$$G = C_1 \oplus C_2 \oplus \ldots \oplus C_t$$

where $C_i = \langle a_i \rangle$ is cyclic group generated by a_i, $1 \le i \le t$. By our choice on element of generated set each C_i is infinite set (because if C_i is of finite order say r_i , then $r_i a_i$ =0). Hence in this case G is direct sum of finite number of infinite cyclic group.

Now suppose that that G has no generating set of t elements with the property that $x_1 a_1 + x_2 a_2 + \ldots + x_t a_t = 0 \Rightarrow x_1 = 0, x_2 = 0, \ldots, x_t = 0$. Then, given any generating set $\{a_1, a_2, \ldots, a_t\}$ of G, there exist integers $x_1, x_2, \ldots, x_t$ not all zero such that

$$x_1 a_1 + x_2 a_2 + \ldots + x_t a_t = 0.$$

As $x_1 a_1 + x_2 a_2 + \ldots + x_t a_t = 0$ implies that $-x_1 a_1 - x_2 a_2 - \ldots - x_t a_t = 0$, therefore, with out loss of generality we can assume that $x_i > 0$ for at least one i. Consider all possible generating sets of G containing t elements with the property that $x_1 a_1 + x_2 a_2 + \ldots + x_t a_t = 0$ implies that at least one of $x_i > 0$. Let X is the set of all such $(x_1, x_2, \ldots x_t)$ t -tuples. Further let m_1 be the least positive integers that occurring in the set t-tuples of set X. With out loss of generality we can take m_1 to be at first component of that t-tuple $(a_1, a_2, \ldots, a_t)$

i.e. $m_1 a_1 + x_2 a_2 + \ldots + x_t a_t = 0$ (1) By division algorithm, we can write, $x_i=q_i m_1 + s_i$, where $0 \le s_i < m_1$. Hence (1) becomes,

$m_1 b_1 + s_2 a_2 + \ldots + s_t a_t = 0$, where $b_1= a_1 + q_2 a_2 + \ldots + q_t a_t$.

Now if $b_1=0$, then $a_1 = -q_2 a_2 - \ldots - q_t a_t$. But then G has a generator set containing less then t elements, a contradiction to the assumption that the smallest generator set of G contains t elements. Hence $b_1 \neq 0$. Since $a_1 = -b_1 - q_2 a_2 - \ldots - q_t a_t$, therefore, $\{b_1, a_2, \ldots, a_n\}$ is also a generator of G. But then by the minimality of m_1, $m_1 b_1 + s_2 a_2 + \ldots + s_t a_t = 0 \Rightarrow s_i =0$ for all i. $2\le i \le t$. Hence $m_1b_1=0$. Let $C_1 = \langle b_1\rangle$. Since m_1 is the least positive integer such that $m_1b_1=0$, therefore, order of $C_1=m_1$.

Let G_1 be the subgroup generated by $\{a_2, a_3, \ldots, a_t\}$. We claim that $G = C_1 \oplus G_1$. For it, it is sufficient to show that $C_1 \cap G_1 =\{0\}$. Let $d \in C_1 \cap G_1$. Then $d=x_1b_1$, $0 \le x_1 < m_1$ and $d = x_2 a_2 + \ldots + x_t a_t$. Equivalently, $x_1b_1 +(-x_2)a_2 +\ldots + (-x_t)a_t =0$. Again by the minimal property of m_1, $x_1=0$. Hence $C_1 \cap G_1 =\{0\}$.

Now G_1 is generated by set $\{a_2, a_2, \ldots, a_t\}$ of t-1 elements. It is the smallest order set which generates G_1(because if G_1 is generated by less then t-1 elements then G can be generated by a set containing t-1 elements, a contradiction to the assumption that the smallest generator of G contains t elements). Hence by induction hypothesis,

$G_1= C_2 \oplus \ldots \oplus C_t$

where $C_2, \ldots, C_k$ are cyclic subgroup of G that are either all are infinite or, for some $j \le t$, $C_2, \ldots , C_j$ are finite cyclic group of order $m_2, \ldots, m_j$ respectively such that $m_2| m_3 | \ldots| m_j$, and C_i are infinite for $i > j$.

Let $C_i =[b_i]$, i=2, 3, …, k and suppose that C_2 is of order m_2. Then $\{b_1, b_2, \ldots, b_t\}$ is the generating set of G and $m_1b_1 + m_2b_2 + 0.b_3 +\ldots+ 0.b_k =0$. By repeating the argument given for (1), we conclude that $m_1|m_2$. This completes the proof of the theorem.

4.6.3 Theorem. Let G be a finite abelian group. Then there exist a unique list of integers $m_1, m_2, \ldots, m_t$ (all $m_i > 1$) such that order of G is $m_1\, m_2 \ldots m_t$ and G $= C_1 \oplus C_2 \oplus \ldots \oplus C_t$ where $C_1, C_2, \ldots, C_t$ are cyclic groups of order $m_1, m_2, \ldots, m_k$ respectively. Consequently, $G \cong Z_{m_1} \oplus Z_{m_1} \oplus \ldots \oplus Z_{m_t}$.

Proof. By theorem 4.6.2, $G = C_1 \oplus C_2 \oplus \ldots \oplus C_t$ where $C_1, C_2, \ldots, C_t$ are cyclic groups of order $m_1, m_2, \ldots, m_t$ respectively, such that $m_1 | m_2 | \ldots | m_t$. As order of $S \times T$ = order of S $\times$ order of T, therefore, order of G $= m_1\, m_2 \ldots m_t$. Since a cyclic group of order m is isomorphic to Z_m group of integers under the operation addition mod m, therefore,

$$G \cong Z_{m_1} \oplus Z_{m_1} \oplus \ldots \oplus Z_{m_t} .$$

We claim that m_1 , $m_2, \ldots, m_t$ are unique. For it, let there exists $n_1, n_2, \ldots, n_r$ such that $n_1 | n_2 | \ldots | n_r$ and $G = D_1 \oplus D_2 \oplus \ldots \oplus D_r$ where D_j are cyclic groups of order n_j. Since D_r has an element of order n_r and largest order of element of G is m_t , therefore, $n_r \le m_t$. By the same argument, $m_t \le n_r$. Hence $m_t = n_r$.

Now consider $m_{t-1}\, G = \{m_{t-1} g \mid g \in G\}$. Then by two decomposition of G we get

$$m_{t-1}\, G = (m_{t-1}\, C_1) \oplus (m_{t-1}\, C_2) \oplus \ldots \oplus (m_{t-1}\, C_t)$$
$$= (m_{t-1}\, D_1) \oplus (m_{t-1}\, D_2) \oplus \ldots \oplus (m_{t-1}\, D_{r-1}).$$

As $m_i \mid m_{t-1}$ (it means m_i divides m_{t-1})for all i, $1 \le i \le t-1$, therefore, for all such i, $m_{t-1}\, C_i = \{0\}$. Hence order of (m_{t-1} G) i.e. $| m_{t-1}\, G | = |(m_{t-1}\, C_t)| = |(m_{t-1}\, D_r)|$. Thus $|(m_{t-1}\, D_j)| = 1$ for j=1, 2, …, r-1. Hence $n_{r-1} \mid m_{t-1}$. Repeating the process by taking m_{r-1} G, we get that $m_{t-1} \mid n_{r-1}$. Hence $m_{t-1} = n_{r-1}$. Continuing this process we get that $m_i = n_i$ for i=t, t-1, t-2, …. But $m_1 m_2 \ldots m_t = |G| = n_1\, n_2 \ldots n_r$, therefore, r = t and $m_i = n_i$ for all i, $1 \le i \le k$.

4.6.3 Corollary. Let A be a finitely generated abelian group. Then $A \cong Z^s \oplus \frac{Z}{a_1 Z} \oplus \ldots \oplus \frac{Z}{a_r Z}$, where s is a nonnegative integer and a_i are nonzero non-unit in Z, such that $a_1 | a_2 | \ldots | a_r$. Further decomposition of A shown above is unique in the sense that a_i are unique.

Sixth lecture

4.6.4 Example.

The abelian group generated by x_1 and x_2 subjected to the condition $2x_1 = 0$, $3x_2 = 0$ is isomorphic to Z/<6> because the matrix of these equation is $\begin{matrix} 2 & 0 \\ 0 & 3 \end{matrix}$ has the smith normal form $\begin{matrix} 1 & 0 \\ 0 & 6 \end{matrix}$

4.7 KEY WORDS

Uniform modules**,** Noether Lashkar, wedderburn artin, finitely generated.

4.8 SUMMARY

In this chapter, we study about Weddernburn theorem, uniform modules, primary modules, noether-laskar theorem, smith normal theorem and finitely generated abelian groups. Some more results on noetherian and artinian modules and rings are also studied.

4.9 SELF ASSESMENT QUESTIONS

(1) Let R be an artinain rings. Then show that the following sets are ideals and are equal:

(i) N= sum of nil ideals , (ii) U = some of nilpotent ideals, (iii) Sum of all nilpotent right ideals.

(2) Show that every uniform module is a primary module but converse may not be true

(3) Obtain the normal smith form of the matrix $\begin{matrix} -x & 4 & -2 \\ -3 & 8-x & 3 \\ 4 & -8 & -2-x \end{matrix}$ over the ring Q[x].

(4) Find the abelian group generated by $\{x_1, x_2, x_3\}$ subjected to the conditions $5x_1 + 9x_2 + 5x_3=0$, $2x_1 + 4x_2 + 2x_3=0$, $x_1 + x_2 - 3x_3=0$

4.10 SUGGESTED READINGS

(1) Modern Algebra; SURJEET SINGH and QAZI ZAMEERUDDIN, Vikas Publications.

(2) Basic Abstract Algebra; P.B. BHATTARAYA, S.K.JAIN, S.R. NAGPAUL, Cambridge University Press, Second Edition.