UNIT - III

LECTURE – I

In general, it is not true that every submodule of a free module is free.

Example 0.1. Let $R = \mathbb{Z}[x]$. Then R is a free R-module. The ideal $I = \langle 2, x \rangle$ of R is a submodule of R. If a and b are nonzero elements of I, then $ab - ba = 0$. Thus, no two nonzero elements of I are R-linearly independent. Therefore, if I is a free R-module, then it must be a cyclic submodule of R. But this is not the case as I is not a principal ideal of R.

Theorem 0.2. *Let R be a PID and let M be a free R-module. If N is a submodule of M, then N is a free R-module and $rank_R(N) \leq rank_R(M)$.*

Proof not required.

Corollary 0.3. *Let R be a PID and let M be a finitely generated R-module. If N is a submodule of M, then N is also finitely generated. In fact, if M is generated by m elements then N can be generated by n elements such that $n \leq m$.*

Proof. There is a free R-module F of rank m such that $M \simeq F/K$, for some submodule K of F. Then, there exists a submodule F_1 of

F containing K such that $N \simeq F_1/K$. By Theorem 0.2, F_1 is a free R-module and $\text{rank}_R(F_1) \leq \text{rank}_R(F)$. Thus, N is a finitely generated R-module with number of generators at most $\text{rank}_R(F_1)$.

PROPOSITION 0.4. *A free module over an integral domain is torsion free.*

Proof. Let M be a free module over an integral domain R and let $B = \{ x_i \mid i \in I \}$ be a basis of M. Then for $x = \sum_{i \in I} r_i x_i \in M \setminus \{0\}$, if $r \in R$ such that $rx = 0$, then $rr_i = 0$ for all $i \in I$. Since $x \neq 0$, $r_j \neq 0$ for some $j \in I$ and so $r = 0$.

LECTURE – II

The converse of the above Proposition is, in general, not true. For example, the $\mathbb{Z}$-module $\mathbb{Q}$ is torsion free but not free. However, we have the following:

THEOREM 0.5. *A finitely generated torsion free module over a PID is free.*

Proof. Let M be a torsion free module over a PID R with $X \subseteq M \setminus \{0\}$, a finite set of generators of M. Since M is a torsion free, $x \in M \setminus \{0\}$ and $rx = 0$ implies $r = 0$. So, every nonzero element of M is R-linearly independent. Therefore, let $S = \{x_1, \ldots, x_k\}$ be a maximal linearly independent subset of X.

Let $N = \langle S \rangle$. Then N is a free R-module with a basis S. If $y \in X \setminus S$, then there exist $r_y, r_1, \ldots, r_k$ in R, not all zero, such that $r_y y + r_1 x_1 + \cdots + r_k x_k = 0$. Clearly, $r_y \neq 0$, otherwise $r_i = 0$ for all i. Thus, $r_y y = -(r_1 x_1 + \cdots + r_k x_k) \in N$. Hence, to each $y \in X$, there exists $r_y \in R \setminus \{0\}$ such that $r_y y \in N$. Let $r = \prod_{y \in X} r_y$. Then $r \neq 0$ and $rx \in N$ for all $x \in X$, and so $rM \subseteq N$.

Define a mapping $f\colon M \to M$ by $f(x) = rx$. Then f is an R-module homomorphism with $\ker f = \{\, x \in M \mid rx = 0 \,\}$. Since M is torsion free, $\ker f = \{0\}$ and f is $1 - 1$. Hence, $M \simeq \operatorname{Im} f = rM \subseteq N$. Thus, M is isomorphic to a submodule of a free R-module N. Therefore, M is free by Theorem 0.2.

Corollary 0.6. *If M is a finitely generated module over a PID R, then*

$$M \simeq T(M) \oplus M/T(M).$$

Proof. We have the following short exact sequence:

$$0 \longrightarrow T(M) \longrightarrow M \longrightarrow M/T(M) \longrightarrow 0.$$

M is finitely generated implies, $M/T(M)$ is also finitely generated. Also, $M/T(M)$ is a torsion free module. By Theorem 0.5, $M/T(M)$ is a free module. So, the above sequence splits and $M \simeq T(M) \oplus M/T(M)$.

LECTURE – III

We have seen before that if M is a module over a division ring D, then every linearly independent subset of M can be extended to form a basis of M. If $0 \neq x \in M$, and M is a module over a division ring D, then $\{x\}$ is linearly independent and hence M has a basis containing x. In general, this is not true.

Example 0.7. Let R be a PID. R considered as an R-module is a torsion free cyclic module. R is commutative, hence eery basis of R contains only one element. Now for $r \in R \setminus \{0\}$, $\{r\}$ is linearly independent. If $\{r\}$ is a basis of R, then we must have $s \in R$ such that

$sr = 1$, i.e., r must be a unit in R. Conversely, if r is a unit in R, then $\{r\}$ is a basis of R. Thus if r is a non-unit, then R has no basis containing r.

EXAMPLE 0.8. Let $M = R \oplus R$, where R is a PID. Then M is a free R-module of rank 2 and is also torsion free. If r is a nonzero nonunit in R, then $\{x = (r, 0)\}$ is R-linearly independent. If $y = (a, b) \in M$, such that $\{x, y\}$ is R-linearly independent, then there do not exist α, $\beta \in R$ such that $(1, 0) = \alpha x + \beta y$. Indeed, if $\beta = 0$, then $\alpha x = (1, 0)$ implies that r is a unit in R; if $\beta \neq 0$, then $b = 0$. But then $(0, 1) \neq \alpha x + \beta y$ for any $\alpha, \beta \in R$. So $\{x\}$ can not be extended to form a basis of M

DEFINITION: Let M be a module over a ring R. A torsion free nonzero element $x \in M$ is **primitive** if $x = ry$ for some $y \in M$ and $r \in R$, then r is a unit in R.

EXAMPLE 0.9. In a module over a division ring D, every nonzero element is primitive.

EXAMPLE 0.10. In the $\mathbb{Z}$-module $\mathbb{Q}$, there are no primitive elements,. This is because for every $q \in Q$, $q = n.q/n$ but n is a unit in $\mathbb{Z}$ if and only if $n \neq \pm 1$.

EXAMPLE 0.11. An element x of a ring R is a primitive element of the R-module R if and only if x is a unit in R. This is because $x = x1$ and so if x is primitive, then x must be a unit.

LEMMA 0.12. *Let R be a PID and let M be a free R-module with a basis $B = \{\, x_i \mid i \in I \,\}$.*
(i) $x = \sum_{i \in I} r_i x_i \in M \setminus \{0\}$ is a primitive element if and only if $\gcd(\{\, r_i \mid i \in I \,\}) = 1$.

(ii) If $y = \sum_{i \in I} s_i x_i \in M \setminus \{0\}$ *and if* $r(y) = \gcd(\{ s_i \mid i \in I \})$*, then* $y = r(y)y'$*, and* y' *is a primitive element of* M*.*

Proof. (i) In a PID, gcd is unique up to multiplication by a unit. So, it is enough to show that $d = \gcd(\{ r_i \mid i \in I \})$ is a unit in R. Let $r_i = ds_i$ for all $i \in I$. Then $x = d(\sum_{i \in I} s_i x_i)$. Thus, if x is primitive, then d is a unit in R. Conversely, if $x = ay$, $a \in R$, $y = \sum_{i \in I} s_i x_i \in M$, then $r_i = as_i$, and so $a | r_i$ for all i. Thus, if $d = 1$, then a is a unit in R. Hence, x is a primitive element.

(ii) This is simple.

LECTURE – IV

THEOREM 0.13. *Let* M *be a free module over a PID* R*. If* x *is a primitive element of* M*, then* M *has a basis containing* x*.*

Proof. Let $\text{rank}_R(M) = n$. We prove the result by induction on n. If $n = 1$, and M has a basis $\{x_1\}$, then $x = rx_1$ for some $r \in R$. Since, x is primitive, r is a unit in R. Thus, $M = Rx_1 = Rx$. Hence, $\{x\}$ is also a basis of M.

Now assume that the statement is true for all free R-modules of rank at most $n-1$. Let $B = \{x_1, \ldots, x_n\}$ be a basis of M, and let $M_1 = \langle x_1, \ldots, x_{n-1} \rangle$. Then $x = \sum_{i=1}^{n} r_i x_i$ $(r_i \in R)$. If $r_n = 0$, then $x \in M_1$. Since $\text{rank}_R(M_1) = n-1$, by the induction hypothesis, M_1 has a basis $\{x, x_2', \ldots, x_{n-1}'\}$, and hence $\{x, x_2', \ldots, x_{n-1}', x_n\}$ is a basis of M. If $r_n \neq 0$, then let $y = \sum_{i=1}^{n-1} r_i x_i$. Then $y \in M_1$. If $y = 0$, then $x = r_n x_n$. Since x is primitive, so r_n is a unit in R, and so $\{x_1, \ldots, x_{n-1}, x\}$ is a basis of M. If $y \neq 0$, then by Lemma 0.12, there is a primitive element $y' \in M$ such that $y = ry'$, for some $r \in R$. By the induction hypothesis, M_1 has a basis $\{y', x_2', \ldots, x_{n-1}'\}$, and so M has a basis

$\{y', x'_2, \ldots, x'_{n-1}, x_n\}$. Now $x = r_n x_n + y = r_n x_n + ry'$, and $\gcd(r_n, r) = 1$ (Lemma 0.12). Then $ar_n + br = 1$ for some $a, b \in R$. Let $y'' = ay' - bx_n$. Then $x, y'' \in \langle x_n, y' \rangle$. Also x, y'' are linearly independent: if $ux + vy'' = 0$ for $u, v \in R$, then $(ur_n - bv)x_n + (ur + av)y' = 0$, and the linear independence of x_n and y' implies that $ur_n - bv = 0$ and $ur + av = 0$, and so on solving these equations for u and v, we get $u = v = 0$. Thus, $\{x, y''\}$ is a basis of $\langle x_n, y' \rangle$. Therefore, $\{x, x'_2, \ldots, x'_{n-1}, y''\}$ is a basis of M.

If M is of infinite rank with a basis $B = \{ x_i \mid i \in I \}$, then choose a finite subset $\{x_{i_1}, \ldots, x_{i_n}\}$ of B so that $x \in \langle x_{i_1}, \ldots, x_{i_n} \rangle = N$. Thus, x is a primitive element of a module N of finite rank. By the above argument, there is a basis $\{x, x'_2, \ldots, x'_n\}$ of N. Hence, $\{x, x'_2, \ldots, x'_n\} \cup \{ x_i \mid i \in I \setminus \{i_1, \ldots, i_n\} \}$ is a basis of M containing x.

Example 0.14. Let $x = (2, 4, 3) = 2e_1 + 3e_2 + 4e_3 \in \mathbb{Z}^3$, where $\{e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)\}$ is standard basis of $\mathbb{Z}^3$. x is a primitive element of $\mathbb{Z}$-module $\mathbb{Z}^3$ as $\gcd(2, 4, 3) = 1$. Now $x = 2e_1 + 4e_2 + 3e_3 = 2y_1 + 3e_3$, where $y_1 = e_1 + 2e_2$, a primitive element of $\mathbb{Z}^3$. Since $y_1 \in \langle e_1, e_2 \rangle$, we can find $x_2 \in \langle e_1, e_2 \rangle$ so that $\langle y_1, x_2 \rangle = \langle e_1, e_2 \rangle$. Since $y_1 = e_1 + 2e_2$ ($a = 1$, $b = 2 \Rightarrow c = 1$, $d = -1$), by the above argument, $x_2 = -e_1 - e_2$. Thus, $\{y_1, x_2, e_3\}$ is a basis of $\mathbb{Z}^3$. Now $x = 2y_1 + 3e_3 \in \langle y_1, e_3 \rangle$, and x is primitive we have $x_1 = -y_1 - e_3$ ($a = 2$, $b = 3$, $c = 1$, $d = -1$) and $\langle x, x_1 \rangle = \langle y_1, e_3 \rangle$. Hence, $\{x, x_1, x_2\}$ is a required basis of $\mathbb{Z}^3$.

LECTURE – V

Proposition 0.15. *Let M be a module over a division ring D of finite rank n and let $X = \{x_1, \ldots, x_n\}$ be a subset of $M \setminus \{0\}$.*

(*i*) *If X is a linearly independent set, then X is a basis of M.*
(*ii*) *If X generates M, then X is a basis of M.*

Proof. (*i*) Since $\operatorname{rank}_D(M) = n$, the set X is a maximal linearly independent subset of M. Hence, X is a basis of M.

(*ii*) Let $Y = \{y_1, \ldots, y_k\}$ be a maximal linearly independent subset of X. The set Y is nonempty since every nonzero element of M is linearly independent. We now claim that $Y = X$. Suppose on the contrary that there is $y \in X \setminus Y$. Then $Y \cup \{y\}$ is a linearly dependent set, and so for some $r, r_1, \ldots, r_k \in R$, $ry + r_1y_1 + \cdots + r_ky_k = 0$. If $r = 0$, then $r_1, \ldots, r_k$ are all zero, and so $Y \cup \{y\}$ is linearly independent set. This contradicts that Y is a maximal linearly independent subset of X. Thus, $r \neq 0$ and $y = \sum_{i=1}^{k}(-r^{-1}r_i)y_i \in \langle Y\rangle$. Therefore, $X \subseteq \langle Y\rangle$ and $M = \langle Y\rangle$. But then $\operatorname{rank}_D(M) = k$, a contradiction.

Proposition 0.15(*i*) may not be true for finitely generated free modules over PIDs.

Example 0.16. Let $M = \mathbb{Z} \oplus \mathbb{Z}$ be a free $\mathbb{Z}$-module of rank 2. Then $\{(2, 0), (0, 1)\}$ is a linearly independent subset of M and it does not generate M as $(1, 0) \neq r(2, 0) + s(0, 1)$ for any $r, s \in \mathbb{Z}$.

However, statement (*ii*) of Proposition 0.15 is valid for such modules.

Proposition 0.17. *Let R be a PID and let M be a finitely generated free R-module of rank n. If $X = \{x_1, \ldots, x_n\} \subseteq M \setminus \{0\}$, and X generates M, then X is a basis.*

Proof. Let $\{e_1, \ldots, e_n\}$ be a standard basis of R^n. Then there is an R-module homomorphism $f\colon R^n \to M$ such that $f(e_i) = x_i$ for

$i = 1, \ldots, n$. Since $M = \langle X \rangle$, f is actually a R-module epimorphism. Thus, there is a short exact sequence $0 \longrightarrow K \longrightarrow R^n \xrightarrow{f} M \longrightarrow 0$ with $\ker f = K$. Since M is free, $R^n \simeq M \oplus K$. By Theorem 0.2, K is a free R-module and $\operatorname{rank}_R(K) \leq n$. Therefore, $n = \operatorname{rank}_R(R^n) = \operatorname{rank}_R(M) + \operatorname{rank}_R(K)$. Hence, $\operatorname{rank}_R(K) = 0$, and $K = \{0\}$. Thus, f is an isomorphism, and X is a basis of M.

LECTURE – VI

Theorem 0.18. **(Invariant factor theorem for submodules)** *Let R be a PID, let M be a free R-module and let N be a submodule of M of finite rank n. Then there is a basis B of M, a subset $\{x_1, \ldots, x_n\}$ of B and nonzero elements $r_1, \ldots, r_n$ of R such that $\{r_1x_1, \ldots, r_nx_n\}$ is a basis of N and for each i, r_i divides r_{i+1}.*

Proof not required.

Theorem 0.19. *Let M be a nonzero finitely generated module over a PID R. If $\mu(M) = n$, then M is a direct sum of cyclic submodules:*

$$M = Rx_1 \oplus \cdots \oplus Rx_n$$

such that $Ann(x_i) \supseteq Ann(x_{i+1})$ for $i = 1, \ldots, n-1$, with $Ann(x_1) \neq R$ and $Ann(x_n) = Ann(M)$.

Proof. Let $M = \langle u_1, \ldots, u_n \rangle$ and let $f\colon R^n \to M$ be defined by $f(a_1, \ldots, a_n) = \sum_{i=1}^n a_iu_i$. Then, f is an R-module epimorphism. If $K = \ker f$, then K is a free submodule of rank m and $m \leq n$ (Theorem 0.2). Choose a basis $\{y_1, \ldots, y_n\}$ of R^n and nonzero elements $r_1, \ldots, r_m$ of R such that $\{r_1y_1, \ldots, r_my_m\}$ is a basis of K and for each i, $r_i | r_{i+1}$ (Theorem 0.18). If for each i, $x_i = f(y_i)$, then $\{x_1, \ldots, x_n\}$

generates M. Since for any $x \in M$ there is $y \in R^n$ such that $f(y) = x$ and since $y = \sum_{i=1}^{n} a_i y_i$ for some $a_1, \ldots, a_n \in R$, so $x = \sum_{i=1}^{n} a_i x_i$.

Next, we show that $M = Rx_1 \oplus \cdots \oplus Rx_n$. Suppose that $\sum_{i=1}^{n} a_i x_i = 0$, $a_i \in R$. Then $\sum_{i=1}^{n} a_i y_i \in K$, and so $\sum_{i=1}^{n} a_i y_i = \sum_{j=1}^{m} b_j r_j y_j$, for some $b_1, \ldots, b_m \in R$. Since $\{y_1, \ldots, y_n\}$ is a basis of R^n, so $a_i = b_i r_i$ for $i = 1, \ldots, m$ and $a_i = 0$ for $i = m+1, \ldots, n$. Now for $i = 1, \ldots, m$, $a_i x_i = f(a_i y_i) = f(b_i r_i y_i) = 0$, as $r_i y_i \in K$. Hence, $a_i x_i = 0$ for all i and $M = Rx_1 \oplus \cdots \oplus Rx_n$.

If $a \in \operatorname{Ann}(x_i)$, then $ax_i = 0$, and so $f(ay_i) = 0$, that is, $ay_i \in K$. If $i > m$, then $ay_i \in K$ implies that $a = 0$. Thus for $i > m$, $\operatorname{Ann}(x_i) = \{0\}$. If $i \leq m$, then $ay_i \in K$ implies that $ay_i = \sum_{j=1}^{m} b_j r_j y_j$, for some $b_1, \ldots, b_m \in R$, and so $a = b_i r_i$, that is, $r_i | a$. Thus, $\operatorname{Ann}(x_i) \subseteq \langle r_i \rangle$. Since $r_i x_i = r_i f(y_i) = f(r_i y_i) = 0$, so $r_i \in \operatorname{Ann}(x_i)$. Therefore, $\operatorname{Ann}(x_i) = \langle r_i \rangle$. Since for each i, $r_i | r_{i+1}$, so $\operatorname{Ann}(x_i) \supseteq \operatorname{Ann}(x_{i+1})$.

Finally, if $m < n$, then M has a torsion free element, and so $\operatorname{Ann}(x_n) = \{0\} = \operatorname{Ann}(M)$. If $m = n$, then M is a torsion module and $r_i | r_n$ for all i, and so $r_n M = \{0\}$. Thus, $\operatorname{Ann}(x_n) = \langle r_n \rangle = \operatorname{Ann}(M)$.

Now $\operatorname{Ann}(x_1) \neq R$, because otherwise $Rx_1 = 0$ and $\mu(M) < n$.

LECTURE – VII

Corollary 0.20. *If M is a finitely generated module over a PID R, then $M = T(M) \oplus F$, where F is a free module of finite rank.*

Proof. By Theorem 0.19, $M = Rx_1 \oplus \cdots \oplus Rx_n$ with $\operatorname{Ann}(x_i) \supseteq \operatorname{Ann}(x_{i+1})$ for $i = 1, \ldots, n-1$. Let k be the least positive integer such that $\operatorname{Ann}(x_{k+1}) = \{0\}$. Then $\operatorname{Ann}(x_{k+1}) = \cdots = \operatorname{Ann}(x_n) = \{0\}$, and so $x_{k+1}, \ldots, x_n$ are torsion free elements in M. Therefore, $F = Rx_{k+1} \oplus \cdots \oplus Rx_n$ is a free R-module of rank $n-k$. Let $T = Rx_1 \oplus \cdots \oplus Rx_k$.

Then $M = T \oplus F$ and we claim that $T(M) = T$. Since $\mathrm{Ann}\,(x_1) \supseteq \mathrm{Ann}\,(x_i)$ for $i = 1, \ldots, k$ and R is a PID, so if $\mathrm{Ann}\,(x_k) = \langle a \rangle$, then $ax = 0$ for all $x \in T$. Thus, $T \subseteq T(M)$. Conversely, if $x \in T(M)$, then $x = y + z$, for some $y \in T$ and $z \in F$. Let $r \in R \setminus \{0\}$ such that $rx = 0$. Then $ry + rz = 0$. Since $M = T \oplus F$, so $rz = 0$. But F is torsion free, and so $z = 0$.

The cyclic decomposition is, in general, not unique. If M is a free R-module of rank n, where R is a PID, and if $\{x_1, \ldots, x_n\}$ is a basis of M, then $M = Rx_1 \oplus \cdots \oplus Rx_n$. So every basis will give a different cyclic decomposition.

Proposition 0.21. *Let R be a PID and let M and N be finitely generated R-modules. Then M and N are isomorphic modules if and only if $T(M)$ and $T(N)$ are isomorphic and $\mathit{rank}_R(M/T(M)) = \mathit{rank}_R(N/T(N))$.*

Proof. If $f\colon M \to N$ is an R-module isomorphism, then for $x \in M$ with $rx = 0$, and $r \in R \setminus \{0\}$, we have $rf(x) = f(rx) = 0$, and so $f(x) \in T(N)$. Therefore, $f(T(M)) \subseteq T(N)$. Similarly, for f^{-1}, we have $f^{-1}(T(N)) \subseteq T(M)$. Hence, $f(T(M)) = T(N)$, and $f|_{T(M)}\colon T(M) \to T(N)$ is an R-module isomorphism. If $\eta\colon N \to N/T(N)$ is the canonical R-module epimorphism, then $\eta \circ f\colon M \to N/T(N)$ is an R-module epimorphism and $\ker(\eta \circ f) = T(M)$. Therefore, $M/T(M) \simeq N/T(N)$, and so $\mathrm{rank}_R(M/T(M)) = \mathrm{rank}_R(N/T(N))$.

Conversely, if $\mathrm{rank}_R(M/T(M)) = \mathrm{rank}_R(N/T(N))$, then $M/T(M) \cong N/T(N)$ and so $M \cong T(M) \oplus M/T(M) \cong T(N) \oplus N/T(N) \cong N$.

LECTURE – VIII

DEFINITION: If M is a finitely generated torsion module over a PID R and $M = Rx_1 \oplus \cdots \oplus Rx_m$ with $R \neq \mathrm{Ann}\,(x_1) \supseteq \cdots \supseteq \mathrm{Ann}\,(x_m) \neq \{0\}$, then the chain of annihilator ideals is called the **chain of invariant ideals** of M. If $\mathrm{Ann}\,(x_i) = \langle r_i \rangle$ for all i, then generators $r_1, \ldots, r_m$ are such that $r_i | r_{i+1}$ for $i = 1, \ldots, m-1$, called the **invariant factors** of M.

There is another decomposition of a torsion module over a PID using the prime factorization property of a PID.

DEFINITION: Let R be an integral domain and let M be an R-module. If p is a prime in R, then a p**-primary component** of M is

$$M_p = \{\, x \in M \mid p^n x = 0 \text{ for some } n \in \mathbb{N} \,\}.$$

Verify that M_p is a submodule of M. If $M = M_p$, then M is called a p**-primary module**. We say that M is **primary** if $M = M_p$ for some prime p.

THEOREM 0.22. *A finitely generated torsion module over a PID is a direct sum of primary submodules.*

Proof. Let R be a PID and let M be a finitely generated torsion R-module. If $M = \langle y_1, \ldots, y_n \rangle$, then as M is torsion, $\mathrm{Ann}\,(y_i) = \langle a_i \rangle$ for each i, and so $a_1 \cdots a_n$ is a nonzero element of $\mathrm{Ann}\,(M)$. Let $\mathrm{Ann}\,(M) = \langle r \rangle$ and $r = up_1^{k_1} \cdots p_l^{k_l}$ be the unique factorization of r into a product of nonassociate primes $p_1, \ldots, p_l$ with u a unit in R. Let

$$M_{p_i} = \{\, x \in M \mid p_i^n x = 0 \text{ for some } n \in \mathbb{N} \,\}.$$

If $x \in M_{p_i}$ and $x \neq 0$, then $\mathrm{Ann}\,(x) = \langle p_i^k \rangle$ for some $k \in \mathbb{Z}^+$. Since $\mathrm{Ann}\,(M) \subseteq \mathrm{Ann}\,(x)$, so $p_i^k | r$, and so $k \leq k_i$. Therefore, $M_{p_i} = \{ x \in M \mid p_i^{k_i} x = 0 \}$. Now we will prove that $M = M_{p_1} \oplus \cdots \oplus M_{p_l}$. If $q_i = r/p_i^{k_i}$, then $\gcd(q_1, \ldots, q_l) = 1$, and so $b_1 q_1 + \cdots + b_l q_l = 1$ for some $b_1, \ldots, b_l \in R$. Therefore, $x = x_1 + \cdots + x_l$, where $x_i = b_i q_i x \in M_{p_i}$. Thus, $M = M_{p_1} + \cdots + M_{p_l}$. Let $x_1 + \cdots + x_l = 0$, where each $x_i \in M_{p_i}$. If $x_j \neq 0$ for some j, then $q_j(x_1 + \cdots + x_l) = 0$ implies that $q_j x_j = 0$. Since $\gcd(p_j^{k_j}, q_j) = 1$, so $a p_j^{k_j} + b q_j = 1$, for some $a, b \in R$. Therefore, $x_j = (a p_j^{k_j} + b q_j) x_j = 0$. Hence, $M = M_{p_1} \oplus \cdots \oplus M_{p_l}$.

LECTURE – IX

Theorem 0.23. *A finitely generated torsion module over a PID is a direct sum of primary cyclic submodules.*

Proof. Let R be a PID and let M be a finitely generated torsion R-module. By Theorem 0.22, $M = M_{p_1} \oplus \cdots \oplus M_{p_l}$, a direct sum of primary submodules. Now for $i = 1, \ldots, l$, by Theorem 0.19, it follows that $M_{p_i} = R x_{i1} \oplus \cdots \oplus R x_{in_i}$ such that $R \neq \mathrm{Ann}\,(x_{i1}) \supseteq \cdots \supseteq \mathrm{Ann}\,(x_{in_i}) \neq \{0\}$. Hence, $M = \oplus_{i=1}^{l} M_{p_i} = \oplus_{i=1}^{l} \oplus_{j=1}^{n_i} R x_{ij}$.

Note that in the proof of Theorem 0.23 if we let $\mathrm{Ann}\,(x_{ij}) = \langle p_i^{e_{ij}} \rangle$ for $j = 1, \ldots, n_i$ and $i = 1, \ldots, l$, then we have $e_{i1} \leq \cdots \leq e_{in_i}$. The set of primes $\{ p_i^{e_{ij}} \mid j = 1, \ldots, n_i,\ i = 1, \ldots, l \}$ are called the set of **elementary divisors** of M.

Let M be a module over a PID R. An element $a \in M$ is said to have **order** r if $\mathrm{Ann}\,(a) = \langle r \rangle$. The element r is unique up to multiplication by a unit. If a is of order r then the cyclic submodule Ra generated by a is said to be cyclic of order r. Note that $a \in M$ has order 0 if and only if $Ra \simeq R$, that is, Ra is a free R-module of rank one. Also a is of order 1 ($\in R$) if and only if $a = 0$.

Now we can combine all these results together to obtain the following fundamental theorem for a finitely generated module over a PID.

THEOREM 0.24. *Let M be a finitely generated module over a PID R.*
(i) M is the direct sum of a free module F of finite rank and a finite number of cyclic torsion modules. The torsion summands, if any, are of orders $r_1, \ldots, r_l$, where $r_1, \ldots, r_l$ are nonzero elements of R such that $r_i | r_{i+1}$ for $i = 1, \ldots, l-1$. The rank of F and the list of ideals $\langle r_1 \rangle, \ldots, \langle r_l \rangle$ are uniquely determined by M.
(ii) M is the direct sum of a free submodule E of finite rank and a finite number of cyclic torsion modules, if any, of orders $p_1^{e_1}, \ldots, p_k^{e_k}$, where $p_1, \ldots, p_k$ are primes in R (not necessarily distinct) and $e_1, \ldots, e_k$ are positive integers (not necessarily distinct). The rank of E and the list of ideals $\langle p_1^{e_1} \rangle, \ldots, \langle p_k^{e_k} \rangle$ are uniquely determined by M.

That's all in UNIT-III students. I shall be coming back to you soon with the fourth and the final unit.

Take care and stay safe