Advanced Algebra II

MODULES OVER PRINCIPAL IDEAL DOMAIN

Definition 0.1. *Let $M \in {}_R\mathfrak{M}$. For $x \in M$, we define the annihilator of x, denoted $A(x)$, to be $\{r \in R | rx = 0\}$.*
We can also define the annihilator of M, denoted $A(M)$, to be $\{r \in R | rx = 0, \forall x \in M\}$.

It's easy to check that $A(x)$ (resp. $A(M)$) is a left ideal (hence a submodule of R). By considering the sujective map $R \to Rx$, one has $R/A(x) \cong Rx$.

Let $M \in {}_R\mathfrak{M}$. For $x \in M$, we say that x is torsion if $A(x) \neq 0$.

Example 0.2. *If R is an integral domain, then the set of all torsion elements M_τ is a submodule, called torsion submodule. However, this is not true in general. For example, take $R = \mathbb{Z}_6, M = \mathbb{Z}_6$ as an R-module. One sees that $2, 3$ are torsion elements, but $5 = 2 + 3$ is not.*

Let M be a module over an integral domain. We say that M is a torsion module if $M = M_\tau$. And M is said to be a torsion-free module if $M_\tau = 0$.

Theorem 0.3. *A finitely generated torsion free module $M \in {}_R\mathfrak{M}$ over a principal ideal domain R is free.*

Proof. Let $X = \{x_1, ..., x_n\}$ be a spanning set of M. In X, we consider all independent subsets of X. There exists a maximal independent subset, say $S := \{x_1, ..., x_k\}$ and let F be the submodule generated by S. F is clearly a free module.

Thus for all x_i, $i > k$, one has

$$r_i x_i = \sum_{j=1}^{k} r_{ij} x_j \in F.$$

Let $r = \prod_{i>k}^{n} r_i$. It's clear that $rM < F$. Therefore, rM is a free module.

Lastly, we consider $f : M \to M$ by $f(x) = rx$. Since M is torsion free, $\mathrm{Ker} f = 0$. By the isomorphism theorem, one has

$$rM = \mathrm{Im} f \cong M/\mathrm{Ker} f = M.$$

In particular, M is free. □

Corollary 0.4. *Let M be a finitely generated module over a principal ideal domain R. Then $M = M_\tau \oplus F$, where F is a free submodule and $F \cong M/M_\tau$*

Proof. M/M_τ is a finitely generated module. We claim that it's a torsion-free module. Then by the Theorem, it's a free module. Hence the sequence $0 \to M_\tau \to M \to M/M_\tau \to 0$ splits. Indeed, $M \cong M_\tau \oplus M/M_\tau$. Let F be the image of the inclusion $\imath : M/M_\tau \to M$. The it's clear that F is free and $F \cong M/M_\tau$.

It suffices to prove that M/M_τ is torsion-free. For any $x + M_\tau$ such that $rx + M_\tau = 0$. Then $rx \in M_\tau$, therefore, there exists $s \in R$ such that $srx = (sr)x = 0$. In particular, $x \in M_\tau, x + M_\tau = M_\tau$. □

We have seen that a finitely generated module over principal ideal domain can be decomposed into "free part" and "torsion part". Our next goal is to analyze the torsion part.

Proposition 0.5. *Let R be a principal ideal domain and $p \in R$ a prime element.*

(1) *if $p^i x = 0$, then $A(x) = (p^j)$ for some $j \leq i$.*
(2) *if $A(x) = p^i$, then $p^j x \neq 0$ for $j < i$.*

Remark 0.6. *Let R be a principal ideal domain. Then $p \in R$ a prime element if and only if p is irreducible. Please note that the notion of prime and irreducible are not the same in general.*

Let R be a principal ideal domain and $M \in {}_R\mathfrak{M}$. An element $x \in M$ is said to be has order r if $A(x) = (r)$. We have the following further decomposition of torsion part.

Theorem 0.7. *Let M be a torsion module over a principal ideal domain R. For a prime $p \in R$, let $M(p) := \{x \in M | A(x) = p^n \text{ for some } n\}$.*

(1) *$M(p) < M$.*
(2) *$M = \oplus M(p)$.*
(3) *If M is finitely generated, then it's a finite direct sum.*

Proof. The first statement is easy.

The proof is basically the same as Chinese remainder theorem. For a fixed $x \in M$, with $A(x) = (r)$. Since R is a unique factorization domain, one can write $r = \prod_{i=1,\ldots,n} p_i^{a_i}$. Let $r_i := r/p_i^{a_i}$, then it's clear that $(r_1, ..., r_n) = 1$. In particular, there exist $s_1, ..., s_n \in R$ such that $\sum s_i r_i = 1$. Therefore,

$$x = \sum s_i r_i x.$$

Let $x_i := s_i r_i x$. Then $p_i^{a_i} x_i = r s_i x = 0$. Thus $x_i \in M(p)$. Hence we have seen that M is generated by $M(p)$.

Let $M(p)'$ be the submodule generated by $M(q)$ with $q \neq p$. It remains to show that the intersection of $M(p) \cap M(p)' = 0$ which is easy.

Lastly, if M is finitely generated. Then $A(M) = (r)$ for some r. Let $r = \prod_{i=1,\ldots,n} p_i^{a_i}$, then one can easily prove that $M = \oplus_{i=1,\ldots,n} M(p_i)$. □

Thus it suffices to work on the submodule $M(p)$. We need the following lemma taking care of element of maximal order.

Lemma 0.8. *Let M be a module over a principal ideal domain R such that $p^nM = 0$ and $p^{n-1}M \neq 0$. Let $x \in M$ be a element of orderp^n.*

(1) *If $M \neq Rx$, then there exist $y \in M$ such that $Rx \cap Ry = 0$.*
(2) *There is a submodule $N < M$ such that $M = Rx \oplus N$.*

Proof. If $M \neq Rx$, then there is $c \in MRx$. Consider $\{c, pc, ...p^nc = 0 \in Rx\}$. One can pick j such that $p^jc \in Rx$ but $p^{j-1}c \notin Rx$.

Let $p^jc = rx$. Factorize $r = r'p^k \in R$. Since

$$0 = p^nc = p^{n-j}rx = p^{n-j+k}r'x.$$

One has $n - j + k \geq n$, thus $k \geq j \geq 1$.

We consider $y = p^{j-1}c - r'p^{k-1}x \in M$. $y \neq 0$ since $p^{j-1}c \notin Rx$ and $py = 0$. If $Rx \cap Ry \neq 0$, then there is $s \in R$ such that $sy \in Rx$. Clearly, $(p, s) = 1$, thus $1 = p\alpha + s\beta$ for some $\alpha, \beta \in R$. It follows that $y = \beta sy \in Rx$, and therefore, $p^{j-1}c \in Rx$. This is a contradiction.

For the second statement, we consider $\mathcal{S} = \{N < M | N \cap Ra\} = 0\}$. If $M = Rx$ then nothing to prove. We may assume that $M \neq Rx$, hence $\mathcal{S} \neq \emptyset$. By Zorn's Lemma, there is a maximal element N. We claim that $M = Rx + N$ then we are done.

To this end, we consider M/N. Clearly, $p^nM/N = 0$ and $p^n(x+N) = 0$. It's not difficult to check that $x + N \in M/N$ has order p^n. If $M/N = R(a + N)$ then we are happy. Otherwise, apply (1) to M/N, there is $y \in M$ such that $y + N \notin R(x + N)$. Then one checks that $N + Ry \cap Rx = 0$ and thus contradicts to the maximality of N. □

Theorem 0.9. *Keep the notation as above. Let $M = M(p)$ be a finitely generated module. Then M is a direct sum of cyclic R-modules of order $p^{n_1}, ..., p^{n_k}$, where $n_1 \geq n_2 \geq .... \geq n_k \geq 1$.*

Proof. Let $x_1, ..., x_r$ be generators whose order are $p_{m_1}, ..., p^{m_r}$ respectively. Let $n_1 := \max\{m_i\}$. We may assume that $x_1 \in M$ is an element of order n_1. Then $M = Rx_1 \oplus N$. By induction, we are done. □

These $p_i^{n_j}$ are called the *elementary divisors*. In order to prove the uniqueness of the decomposition and also another description by *invariant factors*. We need to work more.

Lemma 0.10. *Let M, N be module over a principal ideal domain, $r \in R$ and $p \in R$ is prime.*

(1) *rM and $M[r] := \{x \in M | rx = 0\}$ are submodules.*
(2) *$M[p]$ is a vector space over $R/(p)$.*
(3) *$(R/(p^n))[p] \cong R/(p)$ and $p^m(R/(p^n)) \cong R/(p^{n-m})$ for $m < n$.*
(4) *If $M \cong \oplus M_i$, then $rM \cong \oplus rM_i$ and $M[r] \cong \oplus M_i[r]$.*
(5) *If $f : M \to N$ a ${}_R\mathfrak{M}$-isomorphism, then $f : M_\tau \cong N_\tau$, and $f : M(p) \cong N(p)$.*

Lemma 0.11. *Let* $r = \prod_{i=1,...,k} p_i^{n_i}$. *Then*

$$R/(r) \cong \oplus_{i=1,...,k} R/(p_i^{n_i}).$$

Theorem 0.12. *Let* M *be a finitely generated module over a principal ideal domain* R. *Then*

(1) M *is a direct sum of a free module* F *of finite rank and a finite number of cyclic torsion modules of order* $r_1, ..., r_m$ *respectively. Where* $r_1|r_2|...|r_m$. *And the rank of* F *and the list of ideals* $(r_1), ..., (r_m)$ *is unique.*

(2) M *is a direct sum of a free module* F *of finite rank and a finite number of cyclic torsion modules of order* $p_1^{a_1}, ..., p_k^{a_k}$ *respectively. And the rank of* F *and the list of ideals* $(p_1^{a_1}), ..., (p_k^{a_k})$ *is unique.*

The $r_1, ..., r_m$ are called *invariant factors.* And $p_1^{a_1}, ..., p_k^{a_k}$ are called *elementary divisors.*