Advanced Algebra II

MODULES OVER PRINCIPAL IDEAL DOMAIN

In order to prove the uniqueness of the decomposition and also another description by *invariant factors*. We need to work more.

Lemma 0.1. *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 $f : M(p) \cong N(p)$.*

Proof. The proof are straightforward. We leave it to the readers. □

Lemma 0.2. *Let $r = \prod_{i=1,...,k} p_i^{n_i}$. Then*

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

Proof. The is a generalization of Chinese Remainder Theorem. Just copy the proof then we are done. □

Theorem 0.3. *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*.

Proof. We have seen the existence of decomposition into elementary divisors. By the similar method as we did in finitely generated abelian groups, one can construct the invariant factors out of elementary divisors. Thus it suffices to prove uniqueness for both cases.

For a fix prime p, we consider $M[p]$. It's a vector space over $R/(p)$ and $d_1 := \dim_{R/(p)} M[p]$ measure the number of elementary divisor of order p^n. We next consider $pM[p]$ and define $d_2 := \dim_{R/(p)} pM[p]$. Then d_2 measure the number of elementary divisor of order p^n with $n \geq 2$. Inductively, we define $d_k := \dim_{R/(p)} p^{k-1} M[p]$ which measure the number of elementary divisor of order p^n with $n \geq k$. The point is that these d_k are uniquely determined by M. It's easy to see that M

has $d_k - d_{k+1}$ elementary divisor (p^k), and this is uniquely determined by M. □

Corollary 0.4 (Jordan canonical form)**.** *Let A be a $n \times n$ matrix over a field k. Suppose that it satisfies a polynomial (in particular, characteristic polynomial or minimal polynomial) which splits into linear factors. Then A has Jordan canonical form.*

Proof. We view A as a linear transformation on a n-dimensional vector space V over k. Then V can be viewed as a $k[x]$-module by $f(x)v := f(A)v$. It's well-known that $k[x]$ is a principal ideal domain. It's clear that V is a torsion module since A satisfies a polynomial. Thus $V = \sum V(x - \lambda)$, or even V decomposes into cyclic submodule of order $(x - \lambda_i)^{k_i}$. It's easy to check that submodule of V is a vector subspace. And one can pick a basis in a cyclic submodule so that the matrix is represented as a Jordan block. □

Corollary 0.5 (fundamental theorem of finitely generated abelian group)**.**