Math 554 Uniqueness of Invariant Factors April 2, 2010 Heinzer

Let M be a finitely generated module over a principal ideal domain D. As discussed in Jacobson, if M is generated by elements $x_1, \ldots, x_n$ and if $D^{(n)}$ denotes the free D-module with ordered basis $(e_1, \ldots, e_n)$, then there exists a surjective D-module homomorphism $\eta : D^{(n)} \to M$ defined by setting $\eta(e_i) = x_i$, $i = 1, \ldots, n$. Let $K = \ker \eta$. Associated to each element $e \in D^{(n)}$ there is a unique coset $e + K = \{e + k \mid k \in K\}$ of K in $D^{(n)}$. The collection of all such cosets is denoted $D^{(n)}/K$ and is given the structure of a D-module in a natural way. The elements of M are identified with the cosets $e + K$, and $M \cong D^{(n)}/K$. If $f_1, \ldots, f_m$ generate the submodule K, then $f_i = \sum_{j=1}^{n} a_{ij} e_j$ for $1 \leq i \leq m$ and the matrix $A = (a_{ij}) \in D^{m \times n}$ is called the *relations matrix* for M with respect to the ordered set of generators $(f_1, \ldots, f_m)$ in terms of the ordered basis $(e_1, \ldots, e_n)$. Jacobson proves that for invertible matrices $Q \in D^{m \times m}$ and $P \in D^{n \times n}$ the matrix $A' = QAP^{-1}$ is also a relations matrix for M. Jacobson also proves in Theorem 3.8 that A is equivalent to a matrix which has the "diagonal" form $\operatorname{diag}\{d_1, d_2, \ldots, d_r, 0, \ldots 0\}$, where the $d_i \neq 0$ and $d_i | d_j$ if $i \leq j$. A matrix equivalent to A having this diagonal form is called a *normal form* for A. The diagonal elements of a normal form are called *invariant factors* of A. In Theorem 3.9 Jacobson gives formulas for the invariant factors of the matrix $A \in D^{m \times n}$ and proves their uniqueness up to units of D.

Assume now that M is a finitely generated torsion module M over the principal ideal domain D. Using that a relation matrix for M is equivalent to a diagonal matrix, we obtain a representation for M as a direct sum of cyclic D-modules

$$M \;=\; Dz_1 \;\oplus \cdots \oplus\; Dz_n,$$

where $\operatorname{ann} z_i = (d_i)$ for each i and $(d_1) \supseteq (d_2) \supseteq \cdots \supseteq (d_n)$ are nonzero proper ideals of D that are called the *invariant factors* of M. If D is the polynomial ring $F[x]$, where F is a field, then the ideals (d_i) are generated by monic polynomials and these monic polynomials are called the invariant factors of M. If $D = \mathbb{Z}$, then the ideals (d_i) are generated by positive integers and these positive integers are called the invariant factors of M. We want to prove uniqueness of these invariant factors. To prove this directly amounts to proving the following: suppose m and n are positive integers and $(a_1) \supseteq (a_2) \supseteq \cdots \supseteq (a_n)$

and $(b_1) \supseteq (b_2) \supseteq \cdots \supseteq (b_m)$ are nonzero proper ideals of the principal ideal domain D such that

$$D/(a_1) \oplus \cdots \oplus D/(a_n) = M = D/(b_1) \oplus \cdots \oplus D/(b_m),$$

then $m = n$ and $(a_i) = (b_i)$ for $i = 1, \ldots, n$. It is easy to see that $\operatorname{ann} M = (a_n)$ and $\operatorname{ann} M = (b_m)$. Hence $(a_n) = (b_m)$.

Let (p) be a maximal ideal of D. Then

$$p(D/(a_1)) \oplus \cdots \oplus p(D/(a_n)) = pM = p(D/(b_1)) \oplus \cdots \oplus p(D/(b_m)).$$

Moreover

(1) $p(D/(a_i) = ((p) + (a_i))/(a_i) = D/(a_i)$, if a_i is not a multiple of p, and

(2) $p(D/(a_i) = (p)/(a_i)$, if a_i is a multiple of p.

Thus if a_i is a multiple of p, then $\frac{D/(a_i)}{p(D/(a_i)} \cong D/(p)$, while if a_i is not a multiple of p, then $\frac{D/(a_i)}{p(D/(a_i)} = 0$. A similar statement holds with respect to the b_i.

The quotient module M/pM is annihilated by (p) and hence is a vector space over the field $D/(p)$. Moreover, direct sums behave well with respect to this quotient, so if a_1 is a multiple of p, then each a_i is a multiple of p and M/pM is an n-dimensional vector space over $D/(p)$. It is now easy to see that $m = n$, for by symmetry we may assume $n \geq m$. Let (p) be a maximal ideal such that a_1 is a multiple of p. Then M/pM is n-dimensional as a vector space over $D/(p)$. Considering the direct sum of the $D/(b_i)$, it follows that $m = n$ and b_1 is a multiple of p. Letting p vary over all maximal ideals of D, it follows that each prime p that divides a_1 also divides b_1. By symmetry, a_1 and b_1 are contained in exactly the same maximal ideals of D.

To show that $(a_1) = (b_1)$ we have to work a little harder. In addition to M/pM, we consider $p^sM/p^{s+1}M$ for s a positive integer. We have

$$p^s(D/(a_1)) \oplus \cdots \oplus p^s(D/(a_n)) = p^sM = p^s(D/(b_1)) \oplus \cdots \oplus p^s(D/(b_m)),$$

and likewise for p^{s+1} Moreover

(1) $p^{s+1}(D/(a_i)) = \frac{(p^{s+1})+(a_i)}{(a_i)} = \frac{(p^s)+(a_i)}{(a_i)}$, if a_i is not a multiple of p^{s+1}, and

(2) $p^{s+1}(D/(a_i)) = \frac{(p^{s+1})}{(a_i)}$, if a_i is a multiple of p^{s+1}.

Thus if a_i is a multiple of p^{s+1}, then the quotient module

$$\frac{p^s(D/(a_i)}{p^{s+1}(D/(a_i)} \cong D/(p),$$

while if a_i is not a multiple of p^{s+1}, then this quotient module is zero. A similar statement holds with respect to the b_i. It follows that a_1 is a multiple of p^{s+1} if and only if b_1 is a multiple of p^{s+1} for each maximal ideal (p) of D and each nonnegative integer s. Therefore $(a_1) = (b_1)$.

Thus if a_i is a multiple of p^{s+1}, then the quotient module

$$p^s(D/(a_i))/p^{s+1}(D/(a_i)) \cong D/(p),$$

while if a_i is not a multiple of p^{s+1}, then this quotient module is zero. A similar statement holds with respect to the b_i. It follows that a_1 is a multiple of p^{s+1} if and only if b_1 is a multiple of p^{s+1} for each maximal ideal (p) of D and each nonnegative integer s. Therefore $(a_1) = (b_1)$.

To show that $(a_i) = (b_i)$ we modify the argument above as follows: we have already seen that $n = m$. Observe that a_i is a multiple of p^{s+1} if and only if $p^sM/p^{s+1}M$ has dimension at least $n - i + 1$ as a vector space over $D/(p)$ if and only if b_i is a multiple of p^{s+1}. Therefore $(a_i) = (b_i)$ for $i = 1, \ldots, n$.

Let me now make some comments on the elementary divisors of a finitely generated torsion module M over a principal ideal domain D. Exercise 1 from Section 3.9 in Jacobson gives a nice illustration of elementary divisors. Let me use x instead of λ for the indeterminate. Then $D = \mathbb{R}[x]$ and M is the direct sum of cyclic D-modules whose order ideals are generated by the polynomials

$$(x-1)^3, \quad (x^2+1)^2, \quad (x-1)(x^2+1)^4, \quad (x+2)(x^2+1)^2.$$

Thus

$$M \;=\; \frac{D}{(x-1)^3} \;\oplus\; \frac{D}{(x^2+1)^2} \;\oplus\; \frac{D}{(x-1)(x^2+1)^4} \;\oplus\; \frac{D}{((x+2)(x^2+1)^2}.$$

To obtain the primary decomposition of M, we write

$$\frac{D}{(x-1)(x^2+1)^4} \;\cong\; \frac{D}{(x-1)} \;\oplus\; \frac{D}{(x^2+1)^4}$$

and

$$\frac{D}{(x+2)(x^2+1)^2} \cong \frac{D}{(x+2)} \oplus \frac{D}{(x^2+1)^2}.$$

Thus M has 3 primary components, the one associated to $(x+2)$ is $D/(x+2)$, the one associated to $(x-1)$ is $D/(x-1) \oplus D/(x-1)^3$ and the one associated to (x^2+1) is

$$\frac{D}{(x^2+1)^2} \oplus \frac{D}{(x^2+1)^2} \oplus \frac{D}{(x^2+1)^4}.$$

The elementary divisors of M are the ideals

$$(x+2), \quad (x-1), \quad (x-1)^3, \quad (x^2+1)^2, \quad (x^2+1)^2, \quad (x^2+1)^4.$$

It is now easy to read off the invariant factors of M from its elementary divisors. The invariant factors of M are

$$(x^2+1)^2, \qquad (x-1)(x^2+1)^2, \qquad (x+2)(x-1)^3(x^2+1)^4.$$

I suggest you try the following questions/exercises concerning subgroups and submodules.

Let p be a prime integer and let $M = \mathbb{Z}/(p) \oplus \mathbb{Z}/(p^2)$.

(1) How many cyclic subgroups of order p^2 does M have ?

(2) Prove that every cyclic subgroup of M of order p^2 is a direct summand of M.

(3) How many subgroups of order p does M have ?

(4) Among the subgroups of M of order p, how many are direct summands of M ?

(5) How many subgroups of order p does the group $\mathbb{Z}/(p) \oplus \mathbb{Z}/(p^2) \oplus \mathbb{Z}/(p^3)$ have ?

Let $F = \mathbb{Z}/p\mathbb{Z}$ be the finite field with p elements and consider the $F[x]$-module $V = F[x]/(x^2) \oplus F[x]/(x^3)$.

(1) How many $F[x]$-submodules with p elements does V have?

(2) How many cyclic $F[x]$-submodules with p^2 elements does V have?

(3) How many noncyclic $F[x]$-submodules with p^2 elements does V have?

(4) Among the cyclic $F[x]$-submodules of V with p^2 elements, how many are direct summands of V ?

(5) How many cyclic $F[x]$-submodules with p^3 elements does V have ?