<u>Honors Algebra 4, MATH 371 Winter 2010</u>

Assignment 5

Due Wednesday, March 17 at 08:35

For the problems 1–7, we fix a principal ideal domain R.

1. Let M be any R-module.

   (a) For $m \in M$, the *annhilator of* m *in* R is defined to be

   $$\operatorname{ann}_R(m) := \{r \in R \ : \ rm = 0\}.$$

   Prove that $\operatorname{ann}_R(m)$ is an ideal of R.

   (b) We say that $m \in M$ is *torsion* if $\operatorname{ann}_R(m) \neq 0$ and we define the *torsion submodule of* M to be

   $$\operatorname{Tor}(M) := \{m \in M \ : \ \operatorname{ann}_R(m) \neq 0\}.$$

   We say that an R-module N is *torsion free* if $\operatorname{Tor}(N) = 0$. Prove that $\operatorname{Tor}(M)$ really is a submodule of M and that the quotient $M/\operatorname{Tor}(M)$ is torsion free.

2. Let M be any submodule of a free module R^n. Show that M is itself a free module, of rank at most n as follows:

   (a) Let $\pi_i : M \to R$ be the composition of the inclusion $M \hookrightarrow R^n$ with projection $R^n \to R$ on to the ith factor; it is an R-module homomorphism. If $\pi_1(M) = 0$, show that M is a submodule of R^{n-1} in a natural way.

   (b) If $\pi_1(M) \neq 0$ then it is an ideal of R, necessarily principal, say $\pi_1(M) = (d)$. For $m \in M$ with $\pi_1(m) = d$, show that $M \simeq Rm \oplus \ker \pi_1$ and that $\ker \pi_1$ is naturally a submodule of a free module of rank $n - 1$

   (c) Conclude by induction on n.

3. Prove that any finitely generated and torsion free R-module M is a submodule of a free module, and hence free as follows:

   (a) Let $\{m_1, \ldots, m_s\}$ be a minimal set of generators of M, and let M_i be the submodule of M generated by $\{m_1, \ldots, m_i\}$. Show that M_1 a free R-module.

   (b) Let $j \geq 1$ be the greatest integer such that M_j is free. If $j = s$ we are done. Otherwise, M_{j+1} is not free so there exists a relation

   $$x m_{j+1} + \sum_{1 \leq i \leq j} r_i m_i = 0$$

   with $x \in R$ nonzero. Show that multiplication by x on M_{j+1} is an R-module homomorphism whose image is contained in a free R-module.

   (c) Show that the kernel of multiplication by x is zero, and deduce that M_{j+1} is free after all. Conclude that M is free.

4. Prove that the short exact sequence

$$0 \longrightarrow \mathrm{Tor}(M) \longrightarrow M \longrightarrow M/\,\mathrm{Tor}(M) \longrightarrow 0$$

splits, so $M \simeq (M/\,\mathrm{Tor}(M)) \oplus \mathrm{Tor}(M)$ is the direct sum of its torsion submodule and a free module. Show that this decomposition of M as a direct sum of a torsion module and a free module is unique.

5. Let T be a *torsion* R-module, i.e. the inclusion $\mathrm{Tor}(R) \hookrightarrow T$ is an isomorphism. For each nonzero (principal) ideal $(r) \subseteq R$, we define the (r)*-primary submodule of* T to be

$$T_{(r)} := \{t \in T \ : \ r^n t = 0 \text{ for some } n \geq 0\}.$$

   (a) Show that $T_{(r)}$ is a submodule of T that depends only on the ideal (r) (and not on a specific choice of generator for this ideal).

   (b) If $r, s \in R$ have $gcd(r,s) = 1$, show that $T_{(r)} \cap T_{(s)} = 0$. Conclude that for such r, s we have $T_{(rs)} \simeq T_{(r)} \oplus T_{(s)}$. Hint: use the fact that for any nonnegative integers n, m, there exist $u, v \in R$ with $ur^n + vs^m = 1$.

   (c) Prove that there is a canonical isomorphism of R-modules

$$T \simeq \bigoplus_p T_p$$

   where p ranges over the distinct prime ideals of R.

6. Let p be a prime ideal of R and T_p a finitely generated, nonzero p-primary R-module.

   (a) Show that any quotient or sub-module of T_p is again p-primary and finitely generated (be careful for finite generation of submodules!)

   (b) Let $\mathrm{ann}(T_p) := \{r \in R \ : \ rt = 0 \text{ for all } t \in T_p\}$ be the *annihilator of* T_p *in* R. Prove that $\mathrm{ann}(T_p)$ is a proper ideal of R, and is equal to p^N for some positive integer N.

   (c) Suppose $\{t_1, \ldots, t_s\}$ is a set of generators for T_p as an R-module. Show that there exists a set of s generators $\{y_1, \ldots, y_s\}$ of T_p with

$$\mathrm{ann}_R(y_1) = \mathrm{ann}_R(T_p) = p^N$$

   (d) Let $\langle y_1 \rangle$ be the R-submodule of T_p generated by y_1 and set $T'_p := T_p/\langle y_1 \rangle$; it is again a finitely generated p-primary R-module. Suppose $y' \in T'_p$ has $\mathrm{ann}_R(y') = p^m$ for some positive integer m. Show that $m \leq N$ and that there exists $y \in T_p$ projecting to y' with $\mathrm{ann}_R(y) = p^m$.

   (e) Prove that there exist integers positive $m_1 \leq m_2 \leq \ldots \leq m_s$ with $\mathrm{ann}_R(T_p) = p^{m_s}$ and an isomorphism of R-modules

$$T_p \simeq R/p^{m_1} \oplus R/p^{m_2} \oplus \cdots \oplus R/p^{m_s} \tag{1}$$

   as follows: Fix a minimal set of generators $\{y_1, \ldots, y_s\}$ of T_p and proceed by induction on s.

i. By (6c), we may assume $\operatorname{ann}_R(y_1) = \operatorname{ann}_R(T_p)$. If $s = 1$ conclude.

ii. If $s > 1$, consider the short exact sequence of R-modules

$$0 \longrightarrow \langle y_1 \rangle \longrightarrow T_p \longrightarrow T_p' \longrightarrow 0 \tag{2}$$

Using the induction hypothesis and part (6d) to appropriately lift generators of the direct summands occurring in the decomposition of T_p' as in (1), show that this sequence is split, and conclude as desired.

(f) Show that the m_i as in (1) are uniquely determined by T_p. Hint: for each $j \geq 0$, consider the R-module $p^j T_p / p^{j+1} T_p$. Show that this is a vector space over the field R/p and compute its dimension.

You have just proved:

Theorem 1 (Structure theorem for finitely generated modules over a PID: Primary decomposition)**.** *Let R be a principal ideal domain and M a finitely generated R-module. Then there exist direct sum decompositions*

$$R \simeq F \oplus T \quad \textit{and} \quad T \simeq \bigoplus_p T_p$$

where F is a free R-module of finite rank, T is a torsion R-module and T_p is a p-primary torsion R-module. Here, F, T, T_p are each uniquely determined by M. Furthermore, for each p there exist integers $0 < m_1 \leq, \dots, \leq m_s$ and a direct sum decomposition

$$T_p \simeq R/p^{m_1} \oplus \cdots \oplus R/p^{m_s}$$

with s the minimal number of generators of T_p and $p_s^m = \operatorname{ann}_R(T_p)$. The integers $\{m_i\}$ are uniquely determined by M.

7. Now prove:

Corollary 1 (Structure theorem for finitely generated modules over a PID: Invariant factor decomposition)**.** *Let R be a principal ideal domain and M a finitely generated R-module. Then there exists a direct sum decomposition*

$$M \simeq F \oplus T$$

with F a free module and $T = \operatorname{Tor}(M)$ the torsion submodule of M. Moreover, there exists a nonnegative integer d and nonzero elements $a_1, a_2, \dots, a_m$ of R which are not units and which satisfy the divisibility relations

$$a_1 | a_2 | \cdots | a_m$$

such that there is a canonical isomorphism of R-modules

$$T \simeq R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_d).$$

The ideals (a_i) are uniquely determined by T (and hence by M); they are called the invariant factors *of M.*

Hint: Use Theorem 6 and the Chinese Remainder Theorem.

8. Now let F be a field and V a finite dimensional F-vector space equipped with a linear transformation $A : V \to V$. We consider V as an $F[X]$-module via

$$(a_0 + a_1 X + \cdots + a_n X^n)v := a_0 v + a_1 Av + \cdots + a_n A^n v,$$

where A^i denotes the composition of A with itself i-times. Since $F[X]$ is a PID, the structure theorems for V as an $F[X]$-module that you proved above apply.

(a) Let (a_i) for $i = 1, \dots, d$ be the invariant factors of V. Show that each a_i may be taken to be a monic polynomial, and that with this normalization the a_i's are uniquely determined by V and A (not just up to units).

(b) Let

$$g := b_0 + b_1 X + \cdots + X^k \in F[X]$$

be any monic polynomial and consider the finite-dimensional F-vector space

$$V_g := F[X]/(g).$$

Multiplication by X gives a linear transformation of V_g, which we denote by m_X. Show that the matrix of m_X with respect to the basis $1, X, X^2, \cdots, X^{k-1}$ of V_g is the *companion matrix* of g, given by the $k \times k$ matrix over F

$$C_g := \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -b_0 \\ 1 & 0 & \cdots & \cdots & \cdots & -b_1 \\ 0 & 1 & \cdots & \cdots & \cdots & -b_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -b_{k-1} \end{pmatrix}$$

(c) Prove that there exists a basis of V with respect to which the matrix of A is in *rational canonical form*, i.e. has the block form

$$\begin{pmatrix} C_{a_1} & & & \\ & C_{a_2} & & \\ & & \ddots & \\ & & & C_{a_d} \end{pmatrix} \tag{3}$$

Hint: First observe that V is a torsion $F[X]$-module. Now use the invariant factor form of the structure theorem for modules over a PID and part (8b).

(d) Prove that any square matrix M over F is similar to a matrix in rational canonical form; i.e. there exists an invertible matrix P such that $P^{-1}MP$ has the form (3), and show moreover that P and this rational canonical form of M are uniquely determined by M. Conclude that two $n \times n$ matrices over F are similar if and only if they have the same rational canonical form.