Honors Algebra 4, MATH 371 Winter 2010

Assignment 5 Solutions

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.

   Solution: It is clear that $\operatorname{ann}_R(m)$ is closed under R-multiplication. If $r, s \in \operatorname{ann}_R(m)$ then $(r+s)m = rm + sm = 0$ so $\operatorname{ann}_R(M)$ is closed under addition as well, and is hence an ideal.

   (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.

   Solution: Suppose $m, n \in \operatorname{Tor}(M)$ and that $r, s \in R \setminus \{0\}$ are elements of $\operatorname{ann}_R(m)$ and $\operatorname{ann}_R(n)$, respectively. Then rs is nonzero as R is a domain and $rs \in \operatorname{ann}_R(um + n)$ for any $u \in R$. Thus, $\operatorname{Tor}(M)$ is a submodule of M. Suppose $m \in M$ and let $\overline{m}$ be the image of m in $M/\operatorname{Tor}(M)$. If $\overline{m}$ is torsion, there exists $r \in R \setminus \{0\}$ such that $r\overline{m} = 0$, or equivalently $rm \in \operatorname{Tor}(M)$. Thus, there exists $s \in R \setminus \{0\}$ such that $srm = 0$ so since $sr \neq 0$ we conclude that $m \in \operatorname{Tor}(M)$ and hence $\overline{m} = 0$.

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.

   Solution: The projection $R^n \to R$ on to the ith factor clearly has kernel isomorphic to R^{n-1}. Thus, if $\pi_1(M) = 0$ then $M = \ker(\pi_1) \subseteq R^{n-1}$.

   (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 $n - 1$.

   Solution: Let $x \in M$ be arbitrary. By assumption, $\pi_1(x) = rd$ for some $r \in R$ and hence $\pi_1(x - rm) = 0$. Thus, $x = rm + (x - rm)$ is in $Rm + \ker \pi_1$. This sum is nesessarily direct, since if $\pi_1(rm) = rd = 0$ then $r = 0$. Now $\ker \pi_1$ is a submodule of R^{n-1} in a natural way as in part (2a).

   (c) Conclude by induction on n.

   Solution: The base case is $n = 1$: then M is an ideal of R and hence is equal to Rd for some $d \in R$, which is a free R-module of rank at most 1 as R is a domain. Assuming

that the statement holds for $n-1$, if M is a submodule of R^n then by (2b) we have $M = Rm \oplus \ker \pi_1$. Necessarily Rm is a free rank 1 R-module and by the induction hypothesis, $\ker \pi_1 \subseteq R^{n-1}$ is also free over R of rank at most $n-1$.

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.

   Solution: The map $R \to M_1$ given by $1 \mapsto m_1$ is a surjective map of R-modules. It is injective as $M_1 \subseteq M$ is torsion free.

   (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

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

   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.

   Solution: It is obvious that multiplication by x is an R-module homomorphism. It's image is contained in M_j (since $xm_{j+1} \in M_j$), which is a free R-module by hypothesis.

   (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.

   Solution: This kernel is zero since M is torsion-free. Thus, M_{j+1} is isomorphic to the image of multiplication by x, which is a submodule of the free R-module M_j and is hence free by the previous problem. By our choice of j, this is a contradiction to our assumption that $j < s$ and hence M itself must be free.

4. Let M be a finitely generated R-module. Prove that the short exact sequence

   $$0 \longrightarrow \operatorname{Tor}(M) \longrightarrow M \longrightarrow M/\operatorname{Tor}(M) \longrightarrow 0$$

   splits, so $M \simeq (M/\operatorname{Tor}(M)) \oplus \operatorname{Tor}(M)$ 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 up to isomorphism.

   Solution: By the previous problem, $M/\operatorname{Tor}(M)$ is finitely generated and torsio-free so is a free R-module. The desired splitting then comes from the universal mapping property of free R-modules. Now if T is any torsion module and F is any free module, then the torsion submodule of $M := T \oplus F$ is clearly T, and $M/T \simeq F$. This gives the desired uniqueness up to isomorphism.

5. Let T be a *torsion* R-module, i.e. the inclusion $\operatorname{Tor}(T) \hookrightarrow T$ 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).

Solution: If $t, s \in T_{(r)}$ then $r^n t = 0$ and $r^m s = 0$ for some $m, n \geq 0$. It follows that $r^{m+n}(ut + s) = 0$ for any $u \in R$ so $T_{(r)}$ is an R-submodule of T. Since $r^n t = 0$ if and only if $ur^n t = 0$ for any unit $u \in R^\times$, it follows immediately that $T_{(r)}$ depends only on the ideal (r) .

(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 $ur^n + vs^m = 1$.

Solution: Let $t \in T_{(r)} \cap T_{(s)}$ and suppose that $r^n t = 0$ and $s^m t = 0$. Since (r^n, s^m) is the unit ideal, there exist $u, v \in R$ such that $ur^n + vs^m = 1$ and hence

$$t = (ur^n + vs^m)t = u(r^n t) + v(s^m t) = 0 + 0 = 0.$$

Now the natural map $T_{(r)} \oplus T_{(s)} \to T_{(rs)}$ sending (t, t') to $t + t'$ is surjective since if $(rs)^n t = 0$ then choosing $u, v \in R$ with $ur^n + vs^n = 1$ we have $t = ur^n t + vs^n t$ and $ur^n t \in T_{(s)}$ while $vs^n t \in T_{(r)}$. This map has kernel $T_{(r)} \cap T_{(s)} = 0$ so is an isomorphism.

(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.

Solution: For each p, we have a canonical inclusion $T_p \hookrightarrow T$, which gives a canonical mapping

$$\varphi : \bigoplus_p T_p \to T.$$

By (5b), we see that φ is injective. If $t \in T$ then $\mathrm{ann}_R(t)$ is a principal ideal of R, say generated by (d). If $d = \pi_1^{e_1} \cdots \pi_k^{e_k}$ is the prime factorization of d in R and $p_i = (\pi_i)$ the prime ideal corresponding to π_i, the an easy induction argument using (5b) shows that t is in the image of the restriction of φ to the submodule $\oplus_{i=1}^k T_{p_i}$ of $\bigoplus_p T_p$. It follows that φ is surjective as well, hence an isomorphism.

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!)

Solution: Clearly any quotient of a finitely generated module is again finitely generated, as the images of the generators are a generating set. Since R is a PID, it is noetherian and any submodule of a finitely generated R-module is again finitely generated (proof?). That any quotient or submodule of a p-primary module is p-primary is obvious.

(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.

Solution: Let $t \in T_p$ and suppose $\mathrm{ann}_R(t) = (r)$ for some $r \in R$. If π is a principal generator of p, we know that $\pi^n t = 0$ for some n which without loss of generality we can

assume is minimal with this property. Then π^n is a multiple of r, so we must have that $r = \pi^d u$ for a unit u and some $d \leq n$. We conclude that $\mathrm{ann}_R(t) = p^n$. By definition, $\mathrm{ann}(T_p)$ is equal to the intersection

$$\bigcap_{t \in T_p} \mathrm{ann}_R(t),$$

and hence has the form p^N for some N. It is a proper ideal since T_p is nonzero, and for $t \in T_p$ nonzero $\mathrm{ann}_R(t)$ is a proper ideal.

(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

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

Solution: We have seen that $\mathrm{ann}_R(t_i) = p^{n_i}$ for some integers n_i, and hence that these ideals form a chain. It follows that $\mathrm{ann}(T_p)$, which is the intersection of the $\mathrm{ann}_R(t_i)$, coincides with $\mathrm{ann}_R(t_i)$ for some i (specificaly, for any value of i with maximal n_i). By reordering the t_i's if need be, we conclude as desired.

(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 $\mathrm{ann}_R(y) = p^m$.

Solution: That $m \leq N$ is clear. Let x be any lift of y' to T_p, so $p^m x \in \langle y_1 \rangle$, say $p^m x = r y_1$. Then $p^{N-m} r y_1 = p^N x = 0$ so we conclude that $p^m | r$, say $r = p^m z$. Then $y := x - z y_1$ lifts y' and is killed by p^m. We conclude that $\mathrm{ann}_R(y) = p^d$ for some $d \leq m$. But since p^d then kills y', we must have $d = m$.

(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 $\mathrm{ann}_R(y_1) = \mathrm{ann}_R(T_p)$. If $s = 1$ conclude.
Solution: If $s = 1$, the map $R \to T_p$ sending r to $r y_1$ is surjective with kernel $\mathrm{ann}_R(y_1) = p^{m_1}$.

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.

Solution: Since the images of $y_2, \ldots, y_s$ generate T_p' as an R-module, the induction hypothesis implies that we have an isomorphism

$$T_p' \simeq R/p^{m_2} \oplus R/p^{m_3} \oplus \cdots \oplus R/p^{m_s}.$$

Choose $z_i \in T_p'$ mapping to a generator of the submodule R/p^{m_i} in the above direct sum decomposition, and let x_i be any lift of z_i to T_p satisfying $\mathrm{ann}_R(x_i) = p^{m_i}$; this is possible by (6d). Consider the R-linear mapping $T_p' \to T_p$ sending z_i to x_i. This is well-defined by our choice of x_i and gives a splitting of (2). We conclude as desired, since $\langle y_1 \rangle \simeq R/p^{m_1}$.

(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.

Solution: The dimension d_j of the $\mathbf{F}_p$-vector space $p^j T_p/p^{j+1}T_p$ is easily seen to be equal to the number of m_i which are greater than j. It is not hard to see that the m_i can be recovered from the d_j, and hence are uniquely determined by T_p as this is obviously true of the d_j.

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 $0 < m_1 \leq, \ldots, \leq m_s$ 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 $p_s^m = \mathrm{ann}_R(T_p)$. 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 $T = \mathrm{Tor}(M)$ the torsion submodule of M. Moreover, there exists a nonnegative integer d and nonzero elements $a_1, a_2, \ldots, a_m$ 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.

Solution: By the previous exercise, we have decompositions

$$R \simeq F \oplus T \quad \text{and} \quad T \simeq \bigoplus_{i=1}^{k} T_{p_i}$$

with F free and T torsion and uniquely determined by M up to isomorphism. For each i, we have

$$T_{p_i} \simeq R/p_i^{m_1(i)} \oplus \cdots \oplus R/p_i^{m_{s_i}(i)}$$

with s_i and

$$m_1(i) \leq m_2(i) \leq \cdots \leq m_{s_i}(i)$$

uniquely determined by T_{p_i} and hence by M. Let $m = \max_i\{s_i\}$ and define $a_{m-j} \in R$ to be any generator of the principal ideal

$$\prod_{i=1}^{k} p_i^{m_{s_i-j}(i)}$$

where we put $m_{s_i-j}(i) = 0$ if $s_i - j < 0$. Then $a_1|a_2|\cdots|a_m$ and the ideals (a_i) are uniquely determined by M as this is true of the $m_j(i)$.

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

$$(a_0 + a_1X + \cdots + a_nX^n)v := a_0v + a_1Av + \cdots + a_nA^nv,$$

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 $i = 1, \ldots, d$ 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).

   Solution: Since the units of $F[X]$ are just $F^\times$, any nonzero ideal of $F[X]$ has a unique generator which is monic.

   (b) Let

$$g := b_0 + b_1X + \cdots + X^k \in F[X]$$

   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

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

Solution: Obvious, using the identity

$$X \cdot X^{k-1} = X^k = -b_0 - b_1 X - \cdots - b_{k-1} X^{k-1}.$$

(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).

Solution: Since A satisfies its characteristic polynomial by Cayley-Hamilton, this characteristic polynomial annhihilates V as an $F[X]$-module. We deduce that V is torsion and hence isomorphic to $F[X]/(a_1) \oplus \cdots \oplus F[X]/(a_d)$ for $a_1, \cdots, a_d$ the invariant factors of V, normalized to be monic. Let B_i be the basis of $F[X]/(a_i)$ given by $1, X, X^2, \ldots, X^{\deg a_i - 1}$ and let B be the basis of V corresponding to the union of the B_i. Then the matrix of A with respect to B is easily seen to be as above, by 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.

Solution: Two matrices are similar if and only if there is a change of basis bringing one matrix to the other. It therefore follows from (3) that there is a change of basis matrix bringing M into rational canonical form. Clearly this rational canonical form is uniquely determined by M, as it is uniquely determined by the invariant factors of F^n as an $F[X]$-module via M. If M and M' are similar, then F^n as an $F[X]$ module via M is isomorphic to F^n as an $F[X]$ module via M', so the invariant factors are the same. The converse is clear from the above.