Modules over a PID

Let R be a principal ideal domain. A module M over R is said to be *finitely generated* if there is a finite subset of M such that every element of M is an R-linear combination of elements in this set; that is, in the terminology used for vector spaces, the set spans M.

Theorem 1 (Stacked Basis Theorem for Finitely Generated Modules over a PID)**.** *Let R be a principal ideal domain. Let M be a free module of rank m and let M' be a submodule of M. Then*

a. *M' is free of rank n, $0 \le n \le m$.*

b. *If M' is not 0, then there exists a basis $\{e_1, \dots, e_m\}$ of M and non-zero elements $a_1, \dots, a_n$ of R such that $\{a_1e_1, \dots, a_ne_n\}$ is a basis for M'. Further the a_i satisfy $a_i \mid a_{i+1}$ for $1 \le i < n$.*

c. *The elements a_i are uniquely determined up to multiplication by units.*

Remark 2. Let N be a finitely generated R-module with generating set having m elements. Then there is a surjective homomorphism $S : R^m \longrightarrow N$ given by sending the basis elements to the m generating elements. Let $M' = \ker S$. The Stacked Basis Theorem implies that there exists a nice choice of bases so that the matrix for the inclusion map of $\ker S = M' \approx R^n$ into $M = R^m$ with respect to these bases only has non-zero entries on the diagonal, namely the a_i.

Definition 3. Let R be a principal ideal domain. A matrix $A \in R^{m\times n}$ is said to be in *Smith Normal Form* if all entries off the diagonal are zero, and if $a_{11}, \dots, a_{k,k}$ are all the non-zero entries, then $a_{i,i} \mid a_{i+1,i+1}$ for $1 \le i < k$.

Proposition 4. *Let R be a PID and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_\ell \subseteq \cdots$ be a chain of ideals of R. Then there exists an integer n_0 such that $I_j = I_{n_0}$ for all $j \ge n_0$.*

Proof. Let $I = \bigcup_{j\ge1} I_j$. Let $a, b \in I$, say $a \in I_i$ and $b \in I_j$. Given any pair of integers $1 \le i, j$, then either $I_i \subseteq I_j$ if $i < j$ or $I_j \subseteq I_i$ if $j < i$. Then both a and b lie in one, say I_i, and so does their sum. It easily follows then that I is an ideal of R. As R is a PID, there exists a $d \in R$ so that $I = (d)$. But $d \in I_{n_0}$ for some n_0. Hence $(d) \subseteq I_{n_0} \subseteq I_j \subseteq I = (d)$ if $j \ge n_0$. Hence all are equal as asserted. □

Definition 5. A module M is called *noetherian* if for any sequence of submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \subseteq M_\ell \subseteq \cdots$ there exists an integer n_0 such that $M_j = M_{n_0}$ for all $j \ge n_0$.

A ring R is called *noetherian* if R considered as a module is noetherian.

This condition is also referred to as the *ascending chain condition*.

We've thus proved that a PID is a noetherian ring, that is, it contains no infinite proper ascending chains of ideals.

Now let $T : R^n \longrightarrow R^m$ be a homomorphism and assume $\mathcal{A}$ is a basis for R^n and $\mathcal{B}$ is a basis for R^m. Then the matrix of T with respect to these two bases is $[T]_{\mathcal{A},\mathcal{B}}$, an $m \times n$ matrix. Via the interpretation of Theorem 1 as given in Remark 2, we ask the more general question:

Question 6. Given any homomorphism $T : R^n \longrightarrow R^m$ do there exists bases $\mathcal{A}'$ and $\mathcal{B}'$ so that $[T]_{\mathcal{A}',\mathcal{B}'}$ is in Smith Normal Form?

An equivalent version for matrices is the following:

Question 7. Let $A \in R^{m\times n}$. Is A equivalent to a matrix $B \in R^{m\times n}$ in Smith Normal Form? That is, do there exist invertible matrices $Q \in R^{m\times m}$ and $P \in R^{n\times n}$ so that $B = QAP$ is in Smith Normal Form?

For a PID we now show how to solve the general problem which will in particular solve the case for the inclusion map of Theorem 1. For $a, b \in R$, not both 0, there exist $r, s \in R$ such that $ra + sb = d$ for $d = \gcd(a, b)$. Since $d \mid a$ and $d \mid b$, $a' = a/d$ and $b' = b/d$ are elements of R and $ra' + sb' = 1$. Hence we have an invertible matrix

$$\begin{bmatrix} r & s \\ -b' & a' \end{bmatrix}.$$

Further note that

$$\begin{bmatrix} r & s \\ -b' & a' \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}.$$

In case $a \mid b$, $1 \cdot a + 0 \cdot b = a$, then the matrix is actually an elementary matrix

$$\begin{bmatrix} 1 & 0 \\ -b' & 1 \end{bmatrix}.$$

For a euclidean ring (e.g., $\mathbb{Z}$ or $F[x]$) it is easy to see the first 2×2 matrix is the product of elementary matrices (just use the euclidean algorithm). However, for an arbitrary PID, this is not always the case. Using topological methods one can show that the invertible matrix

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

(of determinant 1) with entries in the ring $R = \mathbb{R}[x]/(1 - x^2 - y^2)$ (the ring of "polynomial functions on the unit circle") is not the product of elementary matrices.

Assume A is an $m \times n$ matrix which is not 0 and let $\ell(A)$ denote the gcd of all its entries. We give an argument to show that there is sequence of steps (essentially bounded by the total number of primes in the factorization of $\ell(A)$) to put the matrix in Smith Normal Form.

If A has all entries 0 in the first column, apply a column operation (right multiply by the appropriate elementary matrix) to place at least one non-zero element in the first column.

Let $A = \left[a_{ij}\right]$. Take $i < j$ and let $a = a_{i,1}$ and $b = a_{j,1}$. Construct the $m \times m$ matrix L which is the same as the identity matrix in all positions except for the $(i,i),(i,j),(j,i),(j,j)$ positions. Place the four entries of the above matrix in these positions (r in (i,i), s in (i,j), $-b'$ in (j,i) and a' in (j,j)). Then the multiplication LA will replace the $(i,1)$ entry by d and the $(j,1)$ entry by 0.

By applying this process $m-1$ times (for the pairs $(1,1)$, $(j,1)$, $j = m$ through 2), the first column of $L_2 \cdots L_m A$ will have a single non-zero entry d_1 in the $(1,1)$ position. This entry will be the gcd of the entries of the first column. Now $(d_1) \subseteq (\ell(A))$.

If d_1 divides all the entries in the first row, we can apply elementary column operations to remove those entries without disturbing the first column. This will yield a single non-zero entry d in the first row and first column.

If not, similarly applying column operations (multiplication on the right by the same type of matrices) can then make the first row have a single non-zero entry d_2 (the gcd of the entries in the first row of our modified matrix) and $(d_1) \subseteq (d_2) \subseteq (\ell(A))$.

Unfortunately, the operations from the right may have messed up the first column. However, we may repeat the process to fill the first column with 0 except for the $(1,1)$ entry, call it d_3. Again we have $(d_1) \subseteq (d_2) \subseteq (d_3) \subseteq (\ell(A))$. Repeating the process over and over again must ultimately stabilize by Proposition 4 as there are no infinite strictly ascending chains of ideals in a PID. Once $d_i = d_{i+1}$ we can clean out the remaining entries of the relevant row or column without disturbing the row/column we just finished cleaning (as we observed in the first step).

The d in the $(1,1)$ position is now the only non-zero entry in the first row and column. If this d divides all other entries in the matrix, great. If not, there is some entry it does not divide. Add that column to the first column and start over. Repeat the entrire procedure until the $(1,1)$ entry divides all other entries in the matrix. That entry is now our a_1 which we wanted to find.

Let A' be the $(m-1) \times (n-1)$ matrix obtained from A be removing the first row and column. Iterate the same procedure until the normal form has been constructed.

This proves the existence part of the following theorem.

Theorem 8 (Smith Normal Form for Matrices over a PID)**.** *Let R be a PID and let $M \in R^{m \times n}$ be a matrix. Then there exist invertible matrices $P \in R^{m \times m}$ and $Q \in R^{n \times n}$ so that $A = PMQ$ is in Smith Normal Form. The Smith Normal Form is unique up to multiplication of the diagonal elements by units. Equivalently, the chain of ideals $(a_{1,1}) \subseteq (a_{2,2}) \subseteq \cdots \subseteq (a_{k,k})$ associated to the non-zero elements $a_{i,i}$ on the diagonal is unique.*

Remark 9. This reduction process is extremely important for solving both mathematical and practical problems. It is implemented in most systems for doing computational

mathematics. Usually one even has the option of obtaining not only the Smith Normal Form, but also the matrices Q and P,

Lemma 10. *Let R be a ring and M_1, M_2 modules. Let $N_i \subseteq M_i$ be submodules. Then there is a natural isomorphism*

$$(M_1 \oplus M_2)/(N_1 \oplus N_2) \longrightarrow M_1/N_1 \oplus M_2/N_2 \ .$$

Proof. This is left as an exercise. □

Corollary 11. *If N is a finitely generated module over a PID R, then there exist non-units $a_1, \ldots, a_k \in R$ with $a_1 \mid a_2 \mid \cdots \mid a_k$ and an integer $l \geq 0$ such that*

$$M \approx R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k) \oplus R^l \ .$$

The integers k and l are uniquely determined by N. The a_i are unique up to multiplication by units.

Corollary 12. *If A is a finitely generated abelian group, then there exist integers $1 < n_1, n_2, \ldots, n_k$ and $l \geq 0$ with $n_1 \mid n_2 \mid \cdots \mid n_k$ such that*

$$A \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k} \oplus \mathbb{Z}^l \ .$$

The integers k, l, and n_i are uniquely determined by A.

Remark 13. The number of terms and the (a_i) are uniquely determined by the module, but the particular decomposition is not. For example, if p is a prime there are several ways to decompose $A = \mathbb{Z}_p \oplus \mathbb{Z}_p$ as an internal direct sum. Note that different bases for A considered as a vector space over $\mathbb{Z}_p$ may give different decompositions as a sum of two one-dimensional subspaces. How many different ways can this be done? However, in all cases there are exactly two summands, each isomorphic to $\mathbb{Z}_p$.

Definition 14. An R-module M is called *cyclic* if there exists an element $m \in M$ so that $M = Rm = \{ rm \mid r \in R \}$. The element m is a generator of M.

Lemma 15. *Let R be a commutative ring. Any cyclic module M is isomorphic to R/I for some ideal I of R. Conversely every R/I is a cyclic module.*

Proof. This follows via the First Isomorphism Theorem as the kernel of the surjective map $R \longrightarrow M$ given by $r \mapsto rm$ has kernel an ideal of R. The converse is clear. □

Proof. To prove Corollary 11 note that by Lemma 10, the Stacked Basis Theorem, and the discussion following it, we obtain an isomorphism of $N \approx M/\ker T$ as a sum of cyclic modules of the form $R/(b)$ for various $b \in R$. If b is a unit, the quotient is R/R, the zero module. Omit these terms. This leaves only the terms corresponding to non-units and 0 (the terms from $n+1$ to m, if any). Renumber the a_i to $a_1, a_2, \ldots, a_k$ and let $l = m - n$.

Corollary 12 is immediate from the first for the PID $\mathbb{Z}$. □

In all cases we've written the finitely generated module as a sum of cyclic modules. The cyclic modules are of two types: either R (a free module), or $R/(a)$ for some non-zero a. The second type are what are called *torsion* modules.

Definition 16. Let M be an R-module. An element $m \in M$ is called *torsion* if there exists a non-zero element $r \in R$ so that $rm = 0$. We let $\operatorname{tor}(M)$ denote the set of all torsion elements of M,

Lemma 17. *Let M be an R-module. If R is a commutative domain, then $\operatorname{tor}(M)$ is a submodule of M.*

Proof. This is left as a homework exercise. □

In general for M a module over a commutative domain R, one has a short exact sequence

$$0 \longrightarrow \operatorname{tor}(M) \longrightarrow M \longrightarrow M/\operatorname{tor}(M) \longrightarrow 0 \ .$$

For M finitely generated and R a PID, the result above shows that the sequence splits (not a natural map), and that the module $M/\operatorname{tor}(M)$ is a free R-module.

It is always true that $M/\operatorname{tor}(M)$ is a torsion-free module (see exercises). If a module over a PID is finitely generated and torsion free, Corollary 11 implies that it is in fact free. This statement may be false if the module is not finitely generated even if R is a PID (see Exercise 7).

Corollary 18. *Let R be a PID. Then every finitely generated torsion-free module M is free.*

Our main application of these ideas to linear algebra comes from the next conclusion.

Corollary 19. *Let V be a finite dimensional vector space over the field F and let $T : V \longrightarrow V$ be a linear transformation. Then V is an $F[x]$-module via $f \cdot v = f(T)(v)$ and there exist monic non-scalar polynomials $f_1, f_2, \ldots, f_k \in F[x]$ with $f_1 \mid f_2 \mid \cdots \mid f_k$ such that there is an $F[x]$-module isomorphism*

$$V \approx F[x]/(f_1) \oplus \cdots \oplus F[x]/(f_k) \ .$$

The f_i and k are unique.

Definition 20. The f_i that appear in the corollary are called the *invariant factors* of T.

Proof. Now $T \in \operatorname{End}_F(V) = \operatorname{Hom}_F(V, V)$ which has dimension $n^2 = (\dim V)^2$. Thus the set $\left\{ I, T, T^2, \ldots, T^{n^2} \right\}$ must be linearly dependent over F as it has $1 + n^2$ elements. Therefore there exists a non-zero polynomial $f \in F[x]$ of degree at most n^2, so that $f(T) = 0$. Thus V is a torsion $F[x]$-module with all elements of V annihilated by the single element f: $f \cdot v = f(T)(v) = 0$. Thus this corollary is a concequence of the first one.

Alternatively one can note that $F[x]$ has infinite dimension over F and as V is of finite dimension over F there can be no copies of $F[x]$ in the decomposition of the $F[x]$-module V. □

Definition 21. Let V be a finite dimensional vector space over the field F. Let $T \in \mathrm{End}_F(V) = \mathrm{Hom}_F(V,V)$ be a linear transformation. The unique non-zero monic generator of the ideal

$$\{\, f \in F[x] \mid f(T) = 0 \,\}$$

is called the *minimal polynomial* of T.

Note that the minimal polynomial of T must then be f_k since all other f_i divide the last one, and each annihilates its respective cyclic module.

Definition 22. A subspace $W \subseteq V$ is *T-invariant* if $T(w) \in W$ for all $w \in W$.

A T-invariant subspace $W \subseteq V$ is called *cyclic* (with respect to T) if there exists a vector $w_0 \in W$ such that $\left\{\, T^i(w_0) \;\middle|\; 0 \le i \,\right\}$ spans W. (That is, W is a cyclic $F[x]$-module.)

Another way to describe the result of the last corollary is the following: Let V_i be the image of the submodule $F[x]/(f_i)$ under the inverse of the isomorphism given in the corollary. Then there is a decomposition of V into an internal direct sum of subspaces $V_1, V_2, \ldots, V_k$ such that

(1) V_i is T-invariant,

(2) V_i is cyclic,

(3) T restricted to V_i has minimal polynomial f_i,

(4) $f_i \mid f_{i+1}$ for $1 \le i < k$.

It is easy to show (see exercises) that for $f \in F[x]$, a non-scalar monic polynomial, $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$, then $M = F[x]/(f)$ is an $F[x]$-module, a finite dimensional vector space over F and $\mathcal{B} = \left\{\, \overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}} \,\right\}$ is a basis over F. Here $\overline{g}$ denotes the image of g in M under the natural surjection $F[x] \longrightarrow M$. If $S:\ M \longrightarrow M$ denotes the linear transformation given by $S(\overline{g}) = \overline{x}\,\overline{g}$, then its matrix with respect to $\mathcal{B}$

$$C(f) = [\, S \,]_{\mathcal{B}}$$

is called the *companion matrix* of the polynomial f. In fact f is the minimal polynomial of S, and of $C(f)$.

An easy computation shows that the $n \times n$ compation matrix is

$$C(f) = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

Corollary 23 (Rational Canoncial Form)**.** *Let V be a finite dimensional vector space over a field and let $T \in \mathrm{End}_F(V) = \mathrm{Hom}_F(V,V)$. Then there exists a basis $\mathcal{B}$ and non-scalar monic polynomials $f_1, \ldots, f_k$ so that*

$$[T]_{\mathcal{B}} = \begin{bmatrix} C(f_1) & 0 & 0 & \cdots & 0 & 0 \\ 0 & C(f_2) & 0 & \cdots & 0 & 0 \\ 0 & 0 & C(f_3) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & C(f_{k-1}) & 0 \\ 0 & 0 & 0 & \cdots & 0 & C(f_k) \end{bmatrix}$$

and $f_i \mid f_{i+1}$ for $1 \leq i < k$. The integer k and the polynomials f_i are uniquely determined by T.

Let R be a commutative ring with ideals I and J such that $I + J = R$ (they are said to be *relatively prime* or *comaximal*). Applying the Chinese Remainder Theorem yields that $R/IJ \approx R/I \oplus R/J$ as R-modules. For a sum of cyclic modules, one can use this isomorphism to obtain fewer terms (in case the hypotheses are satisfied for some pair of ideals that appear) or one can use it to obtain more terms if one can factor one of the ideals into a product of relatively prime ideals. We now push the latter idea to the limit:

If we take a decomposition and write $a_i = \prod_{j=1}^{t} p_j^{e_{ij}}$ where p_j, $1 \leq j \leq t$ are all the primes that appear in the a_i, then

$$\begin{aligned} M &= \bigoplus_{i=1}^{k} R/(a_i) \\ &= \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{t} R/(p_j^{e_{ij}}) \\ &= \bigoplus_{j=1}^{t} \bigoplus_{i=1}^{k} R/(p_j^{e_{ij}}) \ ; \end{aligned}$$

that is, if we write M_p for the summand corresponding to a given prime p we have

$$M = \bigoplus_{j=1}^{t} M_{p_j} \ .$$

The component M_p is sometimes called the *primary* component of M for the prime p.

Definition 24. A module is called *indecomposable* if it cannot be written as the internal direct sum of two non-zero submodules.

Lemma 25. *Let R be a PID. Then R and $R/(p^n)$ for p a prime and $n \geq 1$ are the only cyclic indecomposable R-modules.*

Proof. The easy proof is left as an exercise. □

This lemma asserts then that no further decomposition of our module is possible.

Definition 26. The $p_j^{e_{ij}}$ that appear in the decomposition are called the *elementary divisors* of T.

We now study a single cyclic module $R/(p^e)$ for $p \in F[x]$ a monic prime. Let's first consider the case where $p = x$. Then the minimal polynomial being x^e just means that the linear transformation S (= "multiplication by x") is nilpotent on the vector space $F[x]/(x^e)$. The companion matrix is just the $e \times e$ matrix with 1 in all positions just below the main diagonal:

$$C(x^e) = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

You may recall that you obtained this matrix for a nilpotent linear transformation in one of your early exercises.

We now look at another special case, $p = x - c$. However, we apply the preceding result to the transformation $S - cI$ which is nilpotent and has matrix $C(x^e)$. Henc S has matrix $cI + C(x^e)$ using the same basis as in the previous case:

$$\begin{aligned} J_e(c) &= cI + C(x^e) \\ &= \begin{bmatrix} c & 0 & 0 & \cdots & 0 & 0 \\ 1 & c & 0 & \cdots & 0 & 0 \\ 0 & 1 & c & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c & 0 \\ 0 & 0 & 0 & \cdots & 1 & c \end{bmatrix}. \end{aligned}$$

We call the square matrix $J_e(c)$ a *basic Jordan block* of size e.

For a given primary component M_c (note name change), corresponding to the prime $p = x - c$, we can order the terms by non-increasing exponents:

$$M_c = F[x]/((x-c)^{\ell_1}) \oplus F[x]/((x-c)^{\ell_2}) \oplus \cdots \oplus F[x]/((x-c)^{\ell_s})$$

with $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_s$.

Then the linear transformation S ("multiplication by x") on M_c has matrix

$$J(c) = \begin{bmatrix} J_{\ell_1}(c) & 0 & 0 & \cdots & 0 & 0 \\ 0 & J_{\ell_2}(c) & 0 & \cdots & 0 & 0 \\ 0 & 0 & J_{\ell_3}(c) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & J_{\ell_{s-1}}(c) & 0 \\ 0 & 0 & 0 & \cdots & 0 & J_{\ell_s}(c) \end{bmatrix}.$$

Finally we obtain

Corollary 27 (Jordan Normal Form)**.** *Let V be a finite dimensional vector space over the field F and let $T \in \mathrm{End}_F(V) = \mathrm{Hom}_F(V,V)$. Assume that the minimal polynomial f of T is a product of linear polynomials. Let the factorization be $f = (x-c_1)^{n_1}(x-c_2)^{n_2}\cdots(x-c_k)^{n_k}$ with c_i distinct and $n_i > 0$. Then*

a. *There exist unique T-invariant subspaces V_i such that $V = \bigoplus_{i=1}^k V_i$ with the minimal polynomial of T restricted to V_i being $(x-c_i)^{n_i}$;*

b. *There exists a basis for V so that the matrix for T with respect to this basis has the form*

$$\begin{bmatrix} J(c_1) & 0 & 0 & \cdots & 0 & 0 \\ 0 & J(c_2) & 0 & \cdots & 0 & 0 \\ 0 & 0 & J(c_3) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & J(c_{k-1}) & 0 \\ 0 & 0 & 0 & \cdots & 0 & J(c_k) \end{bmatrix}.$$

The matrix is unique up to the order in which the Jordan blocks occur on the diagonal.

Proof. Although the first statement follows from our earlier discussion, a version exists for any factorization of the minimal polynomial into pairwise relatively prime factors. See the even more general version for finitely generated torsion modules over a PID in the exercises at the end.

The second part is immediate from the earlier discussion. □

Throughout the discussion, we've avoided proving the various uniqueness statements. See the exercises below for a proof in a sequence of steps.

Exercises

ModulesPID 1. A module is called *indecomposable* if it cannot be written as the internal direct sum of two non-zero submodules.

a. Show that if R is a commutative domain, then R is an indecomposable R-module.

b. Show that the only indecomposable modules cyclic modules over a PID are R and $R/(p^n)$ for p a prime and $n \geq 1$ an integer.

c. Show that $\mathbb{Q}$ is a $\mathbb{Z}$-module which is indecomposable but not finitely generated.

d. Let R be a commutative domain that is not a field. Let F be its field of fractions. Show that F is an indecomposable R-module which is not a finitely generated.

ModulesPID 2. A module is called *simple* if it is non-zero and the only proper submodules are 0 and M.

a. Show that if R is a commutative ring (with 1) and I is a maximal ideal, then R/I is a simple R-module. Conversely, show that every simple module is isomorphic to such a cyclic module.

b. If R is a PID, show that any simple module is isomorphic to $R/(p)$ for some prime p.

ModulesPID 3. Let R be a PID. Let $m = (r_1, \ldots, r_n) \in R^n$ and assume that $\gcd(r_1, \ldots, r_n) = 1$. Show that there exists a basis for R^n which contains this element. First observe that this is equivalent to finding a matrix $A \in R^{n \times n}$ with m as its first row (or column). Argue by induction on n. The case $n = 1$ is trivial, and for the case $n = 2$ use the 2×2 matrix on the second page. In general reduce to a smaller size matrix using an argument similar to that used in the first step of constructing the Smith Normal Form.

ModulesPID 4. Let R be a PID and let $T : R^n \longrightarrow R$ be a homomorphism. One then obtains a short exact sequence

$$0 \longrightarrow \ker T \longrightarrow R^n \longrightarrow \operatorname{im} T \longrightarrow 0 \ .$$

Show that this seqence splits: that $R^n = \ker T \oplus Rx$ for $x \in R^n$ for which $T(x) = d$, $(d) = \operatorname{im} T$. And further $\ker T$ is a free module of rank $n-1$. [Apply the preceding exercise.]

ModulesPID 5. Let M be a finitely generated torsion-free module over a commutative domain R. Let S be R with 0 removed. Let F be the field of fractions of R.

a. This part generalizes the construction of the field of fractions. Define an equivalence relation on $M \times S$ by $(m,s) \sim (n,t)$ if $tm = sn$. Show that this is an equivalence relation and let m/s be the equivalence class of (m,s). Let $\mathrm{Frac}(M) = \{\, m/s \mid m \in M, s \in S \,\}$.

b. Define addition and scalar multiplication by elements of F and show that $\mathrm{Frac}(M)$ is a finite dimensional vector space over F.

c. Show that $\theta(m) = m/1$ gives an injective homomorphism $\theta : M \longrightarrow \mathrm{Frac}(M)$.

d. Choose a basis for $\mathrm{Frac}(M)$ over F and a corresponding isomorphism $\mathrm{Frac}(M) \approx F^m$. Now $R^m \subseteq F^m$ in a natural way. Let γ be the composition of θ with this isomorphism. Let m_i, $1 \le i \le n$ be a finite set of generators of M over R. Write $\gamma(m_i) \in F^m$ as $(a_1(i)/b_1(i), \ldots, a_m(i)/b_m(i))$. Let b be the least common multiple of the denominators $b_j(i)$. Then $M \approx bM \approx \gamma(bM) \subseteq R^m$.

e. Assume now that R is a PID. Apply the result of the preceding problem to conclude that M is a free module.

ModulesPID 6. Let R be a commutative ring. Let $I \subseteq R$ be an ideal. If $I \neq 0$ is free as an R-module, show that I is a principal ideal.

ModulesPID 7. a. Show that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module. Show that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

b. Let R be a commutative domain that is not a field. Let F be its field of fractions. Show that F is not a finitely generated R-module. Show that F is not a free R-module.

ModulesPID 8. Let R be a principal ideal domain (PID). Let m, n be positive integers and let $A \in R^{m \times n}$, the set of $m \times n$ matrices with entries in R. Define $\ell(A)$ to be the ideal of R generated by the entries of A (that is, the set of all R-linear combinations of entries the a_{ij} of A).

a. If $B \in R^{p \times m}$, show that $\ell(BA) \subseteq \ell(B) \cap \ell(A)$. Similarly if $C \in R^{n \times q}$, $\ell(AC) \subseteq \ell(A) \cap \ell(C)$.

b. In case $P \in R^{m \times m}$ and $Q \in R^{n \times n}$ have inverses, conclude that $\ell(PAQ) = \ell(A)$. That is, $\ell(B)$ gives the same value for any matrix B which is equivalent to A.

c. A matrix $A \in R^{m \times n}$ is said to be in *Smith Normal Form* if the only non-zero entries of A are on the diagonal, say $a_1, \ldots, a_k$ with $a_i \mid a_{i+1}$ for $1 \le i < k$. Compute $\ell(A)$ for A in Smith Normal Form (SNF).

d. If $b_1, b_2 \in R$ are arbitrary non-zero elements, let A be the matrix

$$\begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}.$$

Using row and column operations (as described earlier), put this matrix in Smith Normal Form

$$\begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} .$$

(You should be able to do this with 3 operations.) Describe a_1 and a_2 in terms of b_1 and b_2. Show that $b_1 b_2 = a_1 a_2$. Do not use determinants.

e. Let $b_1, \ldots, b_k$ be arbitrary non-zero elements of R and let A be the $k \times k$ matrix with these as its diagonal entries. Indicate how by repeatedly applying the previous part, the SNF of A can be determined. Note that each step of your procedure should always give a diagonal matrix with the same product (i.e., the determinant) of diagonal entries. What is a_1? What is a_n? Give a formula for a_i in terms of the prime factorizations of the b_i. [Hint: Phrase correctly and this will be easy!]

Remark: The following theorem can be proven:
If R is a PID and $A \in R^{m \times n}$ is non-zero, there exists a unique matrix B in SNF which is equivalent to A. (As usual for statements about a PID, we ignore multiplication by units.)

ModulesPID 9. Let $T \in \mathrm{End}_F(V) = \mathrm{Hom}_F(V, V)$ for V a finite dimensional vector space over F.

a. Give a formula for the last invariant factor of T in terms of the elementary divisors of T. This should be a very nice description.

b. Determine all of the invariant factors of T in terms of the elementary divisors of T. Give a formula for the number of invariant factors in terms of the elementary divisors.

c. Determine the elementary divisors in terms of the invariant factors. Give a formula for the total number in the list as an easy to describe sum over the invariant factors.

ModulesPID 10. Let R be a commutative ring and let M be an R-module. An element $m \in M$ is called a *torsion* element if there exists a non-zero element $r \in R$ such that $rm = 0$. Let $\mathrm{tor}(M)$ denote the set of torsion elements in M. Assume now and for the rest of the problem, that R is a domain (i.e., if $ab = 0$ for elements $a, b \in R$, then either $a = 0$ or $b = 0$).

a. Show that $\mathrm{tor}(M)$ is a submodule of M (i.e., is non-empty and closed under addition and scalar multiplication by arbitrary elements of R).

b. For M_1 and M_2 R-modules, determine $\mathrm{tor}(M_1 \oplus M_2)$.

c. If $N_1 \subseteq M_1$ is a submodule and $N_2 \subseteq M_2$ is a submodule, give an explicit isomorphim $(M_1 \oplus M_2)/(N_1 \oplus N_2) \longrightarrow M_1/N_1 \oplus M_2/N_2$ with details of proof. Compute $(M_1 \oplus M_2)/\mathrm{tor}(M_1 \oplus M_2)$.

d. Let $M = R^m$, the direct sum of m copies of R. What is $\mathrm{tor}(M)$?

e. Consider the quotient module $M/\mathrm{tor}(M)$. Show that it contains no non-zero torsion elements.

f. If R is a commutative ring and $a \in R$ is non-zero, compute $\mathrm{tor}(R/(a))$.

ModulesPID 11. Give an example of a ring R and module M with $\mathrm{tor}(M)$ not a submodule.

ModulesPID 12. Let M be a finitely generated torsion module over a PID R. Let $\mathrm{Ann}(M) = \{ r \in R \mid rm = 0 \ \forall m \in M \}$ be the annihilator of M.

a. Show that $\mathrm{Ann}(M)$ is a non-zero ideal of R.

b. If $(r) = \mathrm{Ann}(M)$ and $r = ab$ for $\gcd(a, b) = 1$, show that $M = M_a \oplus M_b$ for $M_s = \{ m \in M \mid sm = 0 \}$.

c. Let $p \in R$ be a prime. By abuse of notation, we write

$$M_p = \left\{ m \in M \;\middle|\; p^k m = 0 \text{ for some } k > 0 \right\} .$$

Show that $M = \bigoplus_p M_p$ gives a unique decomposition into a finite sum where each component M_p is annihilated by some (finite) power of the prime p.

ModulesPID 13. Let R be a PID and M a finitely generated R-module with $\mathrm{Ann}(M) = (p^n)$ (such as one of the components in the last part of the preceding exercise). Let $F = R/(p)$, a field.

a. For each i, $0 \le i < n$, show that $p^i M = \left\{ p^i m \;\middle|\; m \in M \right\}$ is a submodule of M with $p^{i+1}M \subset p^i M$. Show that $p^i M/p^{i+1}M$ is a vector space over the field F.

b. Show the the number of cyclic summands of M is uniquely determined by M and equal to $\dim_F M/pM$.

c. Give a formula for the number of summands in M which are of the form $R/(p^j)$ for a fixed $j \ge 1$. The formula should involve the numbers $\dim_F p^i M/p^{i+1}M$. Conclude that the number of such terms is uniquely determined by M.

d. Show that if $N \approx M$, then the integers determined above for M are equal to the ones for N obtained by the same procedure.

ModulesPID 14. Let R be a commutative ring with 1. Let M be a finitely generated free R-module, say $M \approx R^n$. Let $I \subseteq R$ be a maximal ideal and let $F = R/I$, a field.

a. Let IM be the set of all finite sums of elements of the form im for $i \in I$ and $m \in M$. This is a submodule of M. Show that M/IM is a finite dimensional vector space over the field F. How is $\dim_F M/IM$ related to the integer n? Prove your statement. Conclude that n only depends on M, and not on the basis.

b. If J were a different maximal ideal, let $K = R/J$. How are $\dim_F M/IM$ and $\dim_K M/JM$ related?

ModulesPID 15. Let F be a field and let $f \in F[x]$ be a monic polynomial not equal to 1: $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$. Then $M = F[x]/(f)$ is an $F[x]$-module and a finite dimensional vector space over F. For $g \in F[x]$ write $\overline{g}$ for the image of g in M under the natural surjection $F[x] \longrightarrow M$. Let $\mathcal{B} = \left\{ \overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}} \right\}$. Prove the $\mathcal{B}$ is an ordered basis of M. Let $S: M \longrightarrow M$ be the linear transformation given by $S(\overline{g}) = \overline{x}\,\overline{g}$. Compute the matrix of S with respect to $\mathcal{B}$. This matrix, $C(f)$, is called the *companion matrix* of the polynomial f. Prove that f is the minimal polynomial of S, and of $C(f)$.

ModulesPID 16. a. Let F be a field and let $R = F[x]$. Consider the exact sequence

$$R^2 \xrightarrow{S} R^2 \longrightarrow M \longrightarrow 0$$

where S is given by left multiplication by the diagonal matrix A

$$\begin{bmatrix} x-a & 0 \\ 0 & x-b \end{bmatrix}.$$

where $a \neq b$ are different elements of F. Then

$$\begin{aligned} M &\approx \operatorname{coker} S \\ &\approx (R \oplus R)/((x-a),(x-b)) \\ &\approx R/(x-a) \oplus R/(x-b) \end{aligned}$$

as R-modules and

$$\approx F \oplus F$$

as a vector space over F. As an $F[x]$ module, x acts as multiplication by a on the first factor and multiplication by b on the second factor (i.e., M is the sum of two cyclic modules). The Chinese Remainder Theorem shows that in fact M is a cyclic module. Verify this two differet ways:
(1) Apply the preceding problem to the matrix A and argue as above;
(2) Apply the Chinese Remainder theorem directly.
In both cases give an F-basis for the two-dimensional vector space M and give the matrix of the linear transformation "multiplication by x" on M.

b. If $M = R/(f_1) \oplus F/(f_2)$ is the direct sum of two arbitrary non-zero cyclic R-modules, explicitly give
(1) M as a direct sum of two cyclic R-modules $R/(a_1) \oplus R/(a_2)$ with $a_1 \mid a_2$;
(2) take the union of an F-basis for $R/(a_1)$ and one for $R/(a_2)$ and give the matrix for the linear transformation "multiplication by x" with respect to this basis.

ModulesPID 17. A module M is called *noetherian* if for any sequence of submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \subseteq M_\ell \subseteq \cdots$ there exists an integer n_0 such that $M_j = M_{n_0}$ for all $j \geq n_0$.

A module M satisfies the *maximum condition* if every non-empty collection of submodules contains a maximal element. A submodule N in the collection is *maximal* if no other module in the collection contains it strictly.

Prove that for a module M the following three statements are equivalent:

(1) M is noetherian;

(2) M satisfies the maximum condition;

(3) Every submodule of M is finitely generated.

To prove (1) implies (2) try to construct an ascending sequence of submodules. For (2) implies (3), consider the collection of finitely generated submodules of M. For (3) implies (1) consider the generators of the union of the ascending chain of submodules.

ModulesPID 18. A ring R is called *noetherian* if R considered as a module is noetherian. Show the if R is noetherian, then so is R^n for all $n \geq 1$. Given an induction argument using the surjective projection map $\pi_n : R^n \longrightarrow R$ on the last coordinate.

ModulesPID 19. Let

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be a short exact sequence of R-modules. Show that M_2 is noetherian if an only if M_1 and M_3 are noetherian.

ModulesPID 20. Show that a finite direct sum of noetherian modules is noetherian.

ModulesPID 21. Show that a module over a noetherian ring is noetherian if and only if it is finitely generated.

ModulesPID 22. Let M be a finitely generated noetherian module. Then M is a direct sum of a finite number of indecomposable modules. Argue as follows: Unless M is indecomposable, it must be possible to write it as $M = M_1 \oplus M_2$ for some non-zero indecomposable submodule M_1, with M_2 not 0. For if not, one can construct an infinite strictly increasing ascending chain of submodules. Next consider the collection of all submodules N of M with $M = N \oplus N'$ and N a finite sum of indecomposables. Pick a maximal element and argue that it must equal M.

ModulesPID 23. Let M be a finitely generated torsion-free module over a commutative domain R. Let I be a maximal ideal of R, and let $F = R/I$.

a. Show that M/IM is a finite dimensional vector space over the field F. Give an example to show that it is not necessarily true that M is a free module.

b. If J were a different maximal ideal, let $K = R/J$. How are $\dim_F M/IM$ and $\dim_K M/JM$ related? Give an example to show that these numbers need not be equal.

ModulesPID 24. Let V be a finite dimensional vector space with proper subspace W (i.e., $W \neq 0, V$). Let $T: V \longrightarrow V$ be a linear transformation having W as an invariant subspace. Let h be the minimal polynomial of T, h_1 the minimal polynomial of T restricted to W, and h_2 the minimal polynomial of the linear transformation T induces on the quotient V/W.

a. Show that $h_1|h$ and $h_2|h$.

b. Show $h|h_1h_2$.

c. If h_1 and h_2 are relatively prime, show that $h = h_1h_2$.

d. Give an example to show that the result of the previous part is false if h_1 and h_2 are not relatively prime.

ModulesPID 25. Let $T: V \longrightarrow V$ be a linear transformation on the finite dimensional vector space over the field F. An element $c \in F$ is called a *characteristic value* (*eigenvalue*) of T if there exists a non-zero vector $v \in V$ such that $T(v) = cv$. The vector v is called a *characteristic vector* (*eigenvector*) associated to c.

a. If $c_1, \ldots, c_k$ are distinct characteristic values of T with associated characteristic vectors v_i, show that the set $\{ v_1, \ldots, v_k \}$ is a linearly independent set.

b. Let $V_i = \ker(c_iI - T)$. Showthat $V_1 + \cdots + V_k$ is a direct sum. The subspace V_i is called the *characteristic subspaces* associated to the characteristic value c_i.

c. If $\dim V = n$ and T has n distinct characteristic values, show that there exists a basis $\mathcal{B}$ for V such that $[T]_{\mathcal{B}}$ is diagonal.

ModulesPID 26. Let $M = \{ f(x) \in \mathbb{Q}[x] \mid f(n) \in \mathbb{Z} \text{ for all } n \in \mathbb{Z} \}$ (i.e., the polynomials with rational coefficients which take on integral values at all the integers). Show that M is a free module (of infinite rank) over $\mathbb{Z}$ by proving that the set of binomial coefficient polynomials $\left\{ \binom{x}{k} \;\middle|\; k \geq 0 \right\}$ is a basis for M.

The Notes for the course *Math 4330, Honors Linear Algebra* at Cornell University have been developed over the last ten years or so mainly by the following (in chronological order):

Gerhard O. Michler

R. Keith Dennis

Martin Kassabov

W. Frank Moore

and

Yuri Berest.

Most sections have been revised so many times the original author may no longer recognize it. The intent is to provide a modern treatement of linear algebra using consistent terminology and notation. Some sections are written simply to provide a central source of information such as those on "Useful Definitions", "Subobjects", and "Universal Mapping Properties" rather than as a chapter as one might find in a traditional textbook. Additionally there are sections whose intent is to provide proofs of some results which are not given in the lectures, but rather provide them as part of a more thorough development of a tangential topic (e.g., Zorn's Lemma to develop cardinal numbers and the existence of bases and dimension in the general case).

A large number of challenging exercises from many different sources have been included. Although most should be readily solvable by students who have mastered the material, a few even more challenging ones still remain.

Much still remains to be done. Corrections and suggestions for additional exercises, topics and supplements are always welcome.