Reading: Dummit–Foote Ch 12.1–12.2 (up to page 479).

Summary of definitions and main results

Definitions we've covered: Torsion submodule, rank of a module, free rank, invariant factors, elementary divisors, characteristic polynomial, minimal polynomial, companion matrix, rational canonical form

Main results: Fundamental theorem for finitely generated modules over a PID (invariant factor form and elementary divisor form), matrices are classified up to conjugacy by their rational canonical forms

Warm-Up Questions

1. Which of the following rings are PIDs? Let $\mathbb{F}$ denote a field.

   $\mathbb{F}$, $\mathbb{F}[x]$, $\mathbb{F}[x,y]$, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}\oplus\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[x]$, $M_n(\mathbb{F})$, division ring, quotient of a PID

2. Let R be a ring.
   (a) Prove that if R is an integral domain, then for any R–module M the *torsion submodule*
   $$\text{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some } r \in R, r \neq 0\}$$
   is indeed an R–subdmoule of M.
   (b) Show by example that if R is not an integral domain, there may be R–modules M for which $\text{Tor}(M)$ is not a submodule.
   (c) Prove that if $\phi : M \to N$ is a map of R–modules, then $\phi(\text{Tor}(M)) \subseteq \text{Tor}(N)$.

3. Compute the torsion submodules of the following:
   (a) A finite abelian group G (as a $\mathbb{Z}$–module)
   (b) $\mathbb{Z}/5\mathbb{Z}$ as a $\mathbb{Z}$–module, and as a $\mathbb{Z}/5\mathbb{Z}$–module
   (c) The $\mathbb{Z}$–modules $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}/\mathbb{Z}$, and $\mathbb{R}/\mathbb{Z}$
   (d) A vector space V over a field $\mathbb{F}$
   (e) A free R–module F

4. Let R be an integral domain.
   (a) Let N be an R–module. Show that if its annihilator $\text{Ann}(N)$ is nonzero, then N is a torsion module.
   (b) Is the converse true? If N is torsion, must its annihilator be nonzero?
   (c) What if N is finitely generated and torsion, then must its annihilator be nonzero?

5. Suppose that R is a PID and M a finitely generated R–module with invariant factors $a_1, \ldots, a_m$. Show that the annihilator of $\text{Tor}(M)$ is the ideal generated by a_m.

6. Why is it reasonable to only discuss torsion and linear independence in R–modules when R is a domain? In what ways would these definitions behave badly if R had zero divisors or if R were noncommutative?

7. Suppose R is an integral domain and that $A = \{m_1, \ldots, m_n\}$ is a linearly independent subset of an R–module M. Prove or disprove: the submodule $RA \cong R^n$ is free on the basis A. In other words, a finite set is linearly independent iff it is the basis for a free submodule of M.

8. Let R be an integral domain. Let $\{m_1, m_2, \ldots, m_n\}$ be a generating set for an R–module M. Prove that any linearly independent set in M must have n or fewer elements. Conclude that the *rank* is well-defined for a finitely generated module over an integral domain. *Hint:* Use the method in Dummit–Foote 12.1 Proposition 3.

9. Let R be an integral domain. Suppose that $\mathbb{F}$ is a field containing R. Show that any linearly independent set $\{m_1, \ldots, m_n\}$ in an R–module M will yield a linearly independent set of vectors $\{1 \otimes m_1, \ldots, 1 \otimes m_n\}$ in the $\mathbb{F}$–vector space $\mathbb{F} \otimes_R M$. Conclude that the rank(M)=$\dim_{\mathbb{F}}(\mathbb{F} \otimes_R M)$.
   Remark: When R is an integral domain, it is always possible to construct a field $\mathbb{F}$ containing R (its *field of fractions*). The dimension $\dim_{\mathbb{F}}(\mathbb{F} \otimes_R M)$ is sometimes taken as the definition of the rank of M.

10. Let R be an integral domain.
    (a) Conclude from Exercise 8 that any set of $(n+1)$ elements in R^n are linearly dependent, and therefore that R^n has rank n.
    (b) Prove that any torsion R–module has rank zero.
    (c) Show that for any R–module M, rank(M)=rank($M/\text{Tor}(M)$).

11. Let R be an integral domain. Suppose S and T are both finite linearly independent sets of an R–module M, and that each is maximal in the sense that adding any additional element of M would yield a linearly dependent set. Show that S and T must have the same cardinality.

12. Find the invariant factors and elementary divisors of the finitely generated abelian group

$$M \cong \mathbb{Z}^{12} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{9\mathbb{Z}} \oplus \frac{\mathbb{Z}}{5\mathbb{Z}} \oplus \frac{\mathbb{Z}}{18\mathbb{Z}} \oplus \frac{\mathbb{Z}}{15\mathbb{Z}}.$$

13. (a) Show that the ideal $I = \langle x, y \rangle \subseteq R = \mathbb{Q}[x, y]$ is a finitely generated, torsion-free R–module, but not a free R–module. What is the rank of I?
    (b) In contrast, what can you say about finitely generated torsion-free modules over a PID?

14. **(Linear algebra review.)**
    (a) Consider a linear map $A : V \to V$, $\dim(V) = n$ (equivalently, of an $n \times n$ matrix A). Show that the following are equivalent. If A satisfies any of these conditions, it is called *singular*.
        1. A has a nontrivial kernel
        2. rank$(A) < n$
        3. A is not invertible
        4. The columns of A are linearly dependent
        5. The rows of A are linearly dependent
        6. $\det(A) = 0$
        7. $\lambda = 0$ is an eigenvalue of A
    (b) Let T be a linear transformation on a finite-dimensional $\mathbb{F}$-vector space V. Show that the following are equivalent
        1. λ is an eigenvalue of T
        2. $(\lambda I - T)$ is singular
        3. λ is a root of the characteristic polynomial of T
    (c) 1. Define what it means for two matrices to be *conjugate* (or *similar*)
        2. What is the conjugacy class of the zero matrix? The identity matrix? A scalar matrix?
        3. Explain why two matrices are conjugate if and only if they represent the same linear map with respect to different bases.
        4. Show that conjugate matrices have the same determinant.
        5. Show that $(ABA^{-1})^n = AB^nA^{-1}$.
    .

15. Let $A : V \to V$ be a linearly transformation on a finite dimensional vector space V.

(a) Suppose A is given by a *block diagonal matrix*, that is, a matrix with square matrices $\mathbf{A}_i$ (its *blocks*) on the diagonal:

$$A = \begin{bmatrix} \mathbf{A}_1 & 0 & \cdots & 0 \\ 0 & \mathbf{A}_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{A}_n \end{bmatrix}$$

$$\left(\text{eg.} \begin{bmatrix} 1 & 2 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 6 & 4 \end{bmatrix} \text{ has } \mathbf{A}_1 = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \text{ and } \mathbf{A}_2 = \begin{bmatrix} 4 & 2 \\ 6 & 4 \end{bmatrix} \right.$$

$$\left. \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 5 & 0 \\ 0 & 3 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} \text{ has } \mathbf{A}_1 = \begin{bmatrix} 1 \end{bmatrix}, \quad \mathbf{A}_2 = \begin{bmatrix} 2 & 5 \\ 3 & 4 \end{bmatrix} \text{ and } \mathbf{A}_3 = \begin{bmatrix} 4 \end{bmatrix} \right)$$

Explain how the blocks of A correspond to a decomposition of V into a direct sum of subspaces $V = V_1 \oplus \cdots \oplus V_n$ where each V_i is invariant under the action of A. (The matrix A is sometimes called the *direct sum* of its blocks $A = \mathbf{A}_1 \oplus \mathbf{A}_2 \oplus \cdots \oplus \mathbf{A}_n$.)

(b) Conversely, explain why, if V decomposes into a direct sum of subspaces that are invariant under A, then the corresponding matrix for A will be block diagonal. (What are the sizes of the blocks?)

(c) Observe that $\text{Trace}(A) = \text{Trace}(\mathbf{A}_1) + \cdots + \text{Trace}(\mathbf{A}_n)$, and $\text{Det}(A) = \text{Det}(\mathbf{A}_1) \cdots \text{Det}(\mathbf{A}_n)$.

(d) What is the product of two block diagonal matrices (assuming blocks of the same sizes)?

16. (a) Let A be an $n \times n$ matrix. Show that A satisfies its minimal polynomial (ie, $m_A(A)$ is the zero matrix), and that it is the smallest-degree polynomial that vanishes on A.

(b) Let T be a linear map. Show that $m_T(A) = 0$ for any matrix representation A of T, and that the minimal polynomial $m_T(x)$ is the smallest-degree polynomial with this property.

(c) Show that the matrix $\begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix}$ satisfies the polynomial $x^2 - x - 2$. Conclude that this polynomial must be in the ideal $\langle m_T(x) \rangle$ and therefore a multiple of the minimal polynomial $m_T(x)$. What are the possibilities for $m_T(x)$?

17. Suppose that V is an $\mathbb{F}[x]$–module that is n dimensional over the field $\mathbb{F}$. Let T be the linear map on V given by multiplication by x.

(a) What does the dimension of V imply about the possible degrees of the invariant factors $a_1(x)$, $a_2(x)$, $\ldots, a_m(x)$?

(b) Show in particular that the minimal polynomial of T has degree at most n.

(c) If $m_T(x)$ has degree exactly n, what does this tell you about the invariant-factor decomposition of V?

(d) Conversely, suppose that V is a cyclic $\mathbb{F}[x]$–module. What can you conclude about the minimal polynomial of T?

18. What is the characteristic polynomial of a companion matrix $\mathcal{C}_{a(x)}$?

19. A linear map $L : V \to V$ is called *nilpotent* if $L^k = 0$ for some positive $k \in \mathbb{Z}$. Show that the following $n \times n$ matrices $J_{0,n}$ are nilpotent, and find the minimal k such that $J_{0,n}^k = 0$.

$$J_{0,1} = \begin{bmatrix} 0 \end{bmatrix} \qquad J_{0,2} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad J_{0,3} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \qquad J_{0,4} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$J_{0,n} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} \qquad \begin{bmatrix} J_{0,2} & 0 & 0 \\ 0 & J_{0,2} & 0 \\ 0 & 0 & J_{0,3} \end{bmatrix} \text{ (here 0 denotes the zero matrix).}$$

20. Find the characteristic polynomial and the minimal polynomials of the following matrices.

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \quad \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

21. Let A be an $n \times n$ square matrix and B the $2n \times 2n$ block diagonal matrix $\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$. Let $c_A(x)$ and $m_A(x)$ be the characteristic and minimal polynomials of A. What are the characteristic and minimal polynomials of B? Observe in particular that the minimal polynomial of B can have degree at most n.

22. Prove that the minimal polynomial of

$$A = \begin{bmatrix} \mathbf{A}_1 & 0 & \cdots & 0 \\ 0 & \mathbf{A}_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{A}_n \end{bmatrix}$$

is the least common multiple of the minimal polynomial of the blocks $\mathbf{A}_i$.

23. Prove that conjugate matrices have the same characteristic polynomial and the same minimal polynomial.

24. Let $\mathbb{F}$ be a field and all matrices taken over $\mathbb{F}$.
   (a) Show that 2×2 matrices are conjugate iff they have the same characteristic polynomial.
   (b) Show that 3×3 matrices are conjugate iff they have the same characteristic and minimal polynomials.
   (c) Write down two nonconjugate 4×4 matrices with the same minimal and characteristic polynomials.