whose first coordinates generate this submodule of R. Show that any element of M can be written as an R-linear combination of $m_1, m_2, \ldots, m_k$ plus an element of M whose first coordinate is 0. Prove that $M \cap R^{n-1}$ is a submodule of R^{n-1} where R^{n-1} is the set of elements of R^n with first coordinate 0 and then use induction on n.

The following set of exercises outlines a proof of Theorem 5 in the special case where R is a Euclidean Domain using a matrix argument involving row and column operations. This applies in particular to the cases $R = \mathbb{Z}$ and $R = F[x]$ of interest in the applications and is computationally useful.

Let R be a Euclidean Domain and let M be an R-module.

16. Prove that M is finitely generated if and only if there is a surjective R-homomorphism $\varphi : R^n \to M$ for some integer n (this is true for any ring R).

Suppose $\varphi : R^n \to M$ is a surjective R-module homomorphism. By Exercise 15, $\ker \varphi$ is finitely generated. If $x_1, x_2, \ldots, x_n$ is a basis for R^n and $y_1, \ldots, y_m$ are generators for $\ker \varphi$ we have

$$y_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \quad i = 1, 2, \ldots, m$$

with coefficients $a_{ij} \in R$. It follows that the homomorphism φ (hence the module structure of M) is determined by the choice of generators for R^n and the matrix $A = (a_{ij})$. Such a matrix A will be called a *relations matrix*.

17. **(a)** Show that interchanging x_i and x_j in the basis for R^n interchanges the i^{th} column with the j^{th} column in the corresponding relations matrix.

(b) Show that, for any $a \in R$, replacing the element x_j by $x_j - ax_i$ in the basis for R^n gives another basis for R^n and that the corresponding relations matrix for this basis is the same as the original relations matrix except that a times the j^{th} column has been added to the i^{th} column. [Note that $\cdots + a_i x_i + \cdots + a_j x_j + \cdots = \cdots + (a_i + aa_j)x_i + \cdots + a_j(x_j - ax_i) + \ldots$.]

18. **(a)** Show that interchanging the generators y_i and y_j interchanges the i^{th} row with the j^{th} row in the relations matrix.

(b) Show that, for any $a \in R$, replacing the element y_j by $y_j - ay_i$ gives another set of generators for $\ker \varphi$ and that the corresponding relations matrix for this choice of generators is the same as the original relations matrix except that $-a$ times the i^{th} row has been added to the j^{th} row.

19. By the previous two exercises we may perform elementary row and column operations on a given relations matrix by choosing different generators for R^n and $\ker \varphi$. If all relation matrices are the zero matrix then $\ker \varphi = 0$ and $M \cong R^n$. Otherwise let a_1 be the (nonzero) g.c.d. (recall R is a Euclidean Domain) of all the entries in a fixed initial relations matrix for M.

(a) Prove that by elementary row and column operations we may assume a_1 occurs in a relations matrix of the form

$$\begin{pmatrix} a_1 & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

where a_1 divides a_{ij}, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$.

(b) Prove that there is a relations matrix of the form

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

where a_1 divides all the entries.

(c) Let a_2 be a g.c.d. of all the entries except the element a_1 in the relations matrix in (b). Prove that there is a relations matrix of the form

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

where a_1 divides a_2 and a_2 divides all the other entries of the matrix.

(d) Prove that there is a relations matrix of the form $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ where D is a diagonal matrix with nonzero entries $a_1, a_2, \dots, a_k$, $k \leq n$, satisfying

$$a_1 \mid a_2 \mid \cdots \mid a_k.$$

Conclude that

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k) \oplus R^{n-k}.$$

If n is not the minimal number of generators required for M then some of the initial elements $a_1, a_2, \dots$ above will be units, so the corresponding direct summands above will be 0. If we remove these irrelevant factors we have produced the invariant factors of the module M. Further, the image of the new generators for R^n corresponding to the direct summands above will then be a set of R-generators for the cyclic submodules of M in its invariant factor decomposition (note that the image in M of the generators corresponding to factors with a_i a unit will be 0). The *column* operations performed in the relations matrix reduction correspond to changing the basis used for R^n as described in Exercise 17:

(a) Interchanging the i^{th} column with the j^{th} column corresponds to interchanging the i^{th} and j^{th} elements in the basis for R^n.

(b) For any $a \in R$, adding a times the j^{th} column to the i^{th} column corresponds to subtracting a times the i^{th} basis element from the j^{th} basis element.

Keeping track of the column operations performed and changing the initial choice of generators for M in the same way therefore gives a set of R-generators for the cyclic submodules of M in its invariant factor decomposition.

This process is quite fast computationally once an initial set of generators for M and initial relations matrix are determined. The element a_1 is determined using the Euclidean Algorithm as the g.c.d. of the elements in the initial relations matrix. Using the row and column operations we can obtain the appropriate linear combination of the entries to produce this g.c.d. in the (1,1)-position of a new relations matrix. One then subtracts the appropriate multiple of the first column and first row to obtain a matrix as in Exercise 19(b), then iterates this process. Some examples of this procedure in a special case are given at the end of the following section.

20. Let R be an integral domain with quotient field F and let M be any R-module. Prove that the rank of M equals the dimension of the vector space $F \otimes_R M$ over F.

21. Prove that a finitely generated module over a P.I.D. is projective if and only if it is free.

22. Let R be a P.I.D. that is not a field. Prove that no finitely generated R-module is injective. [Use Exercise 4, Section 10.5 to consider torsion and free modules separately.]

12.2 THE RATIONAL CANONICAL FORM

We now apply our results on finitely generated modules in the special case where the P.I.D. is the ring $F[x]$ of polynomials in x with coefficients in a field F.

Let V be a finite dimensional vector space over F of dimension n and let T be a fixed linear transformation of V (i.e., from V to itself). As we saw in Chapter 10 we can consider V as an $F[x]$-module where the element x acts on V as the linear transformation T (and so any polynomial in x acts on V as the same polynomial in T). Since V has finite dimension over F by assumption, it is by definition finitely generated as an F-module, hence certainly finitely generated as an $F[x]$-module, so the classification theorems of the preceding section apply.

Any nonzero free $F[x]$-module (being isomorphic to a direct sum of copies of $F[x]$) is an infinite dimensional vector space over F, so if V has finite dimension over F then it must in fact be a torsion $F[x]$-module (i.e., its free rank is 0). It follows from the Fundamental Theorem that then V is isomorphic as an $F[x]$-module to the direct sum of cyclic, torsion $F[x]$-modules. We shall see that this decomposition of V will allow us to choose a basis for V with respect to which the matrix representation for the linear transformation T is in a specific simple form. When we use the invariant factor decomposition of V we obtain the *rational canonical form* for the matrix for T, which we analyze in this section. When we use the elementary divisor decomposition (and when F contains all the eigenvalues of T) we obtain the *Jordan canonical form*, considered in the following section and mentioned earlier as the matrix representing T which is as close to being a diagonal matrix as possible. The uniqueness portion of the Fundamental Theorem ensures that the rational and Jordan canonical forms are unique (which is why they are referred to as *canonical*).

One important use of these canonical forms is to classify the distinct linear transformations of V. In particular they allow us to determine when two matrices represent the same linear transformation, i.e., when two given $n \times n$ matrices are similar.

Note that this will be another instance where the structure of the space being acted upon (the invariant factor decomposition of V for example) is used to obtain significant information on the algebraic objects (in this case the linear transformations) which are acting. This will be considered in the case of *groups* acting on vector spaces in Chapter 18 (and goes under the name of Representation Theory of Groups).

Before describing the rational canonical form in detail we first introduce some linear algebra.

Definition.

(1) An element λ of F is called an *eigenvalue* of the linear transformation T if there is a nonzero vector $v \in V$ such that $T(v) = \lambda v$. In this situation v is called an *eigenvector* of T with corresponding eigenvalue λ.