Chapter 12

Modules

Be wise! Generalize!

Piccayune Sentinel

1. THE DEFINITION OF A MODULE

Let R be a commutative ring. An *R-module V* is an abelian group with law of composition written $+$, together with a scalar multiplication $R \times V \longrightarrow V$, written $r, v \rightsquigarrow rv$, which satisfies these axioms:

$$\text{(1.1)}\quad \begin{array}{ll} \text{(i)} & 1v = v, \\ \text{(ii)} & (rs)v = r(sv), \\ \text{(iii)} & (r+s)v = rv + sv, \\ \text{(iv)} & r(v+v') = rv + rv', \end{array}$$

for all $r, s \in R$ and $v, v' \in V$. Notice that these are precisely the axioms for a vector space. An F-module is just an F-vector space, when F is a field. So modules are the natural generalizations of vector spaces to rings. But the fact that elements of a ring needn't be invertible makes modules more complicated.

The most obvious examples are the modules R^n of *R-vectors*, that is, row or column vectors with entries in the ring. The laws of composition for R-vectors are the same as for vectors with entries in a field:

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{bmatrix} \quad \text{and} \quad r\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ra_1 \\ \vdots \\ ra_n \end{bmatrix}$$

The modules thus defined are called *free modules*. But when R is not a field, it is no longer true that these are the only modules. There will be modules which are not isomorphic to any free module, though they are spanned by a finite set.

Let us examine the concept of module in the case that R is the ring of integers $\mathbb{Z}$. Any abelian group V, its law of composition written additively, can be made into a module over $\mathbb{Z}$ in exactly one way, by the rules

$$nv = v + \cdots + v = \text{“}n \text{ times } v\text{”}$$

and $(-n)v = -(nv)$, for any positive integer n. These rules are forced on us by axioms (1.1), starting with $1v = v$, and they do make V into a $\mathbb{Z}$-module; in other words, the axioms (1.1) hold. This is intuitively very plausible. To make a formal proof, we would go back to Peano's axioms. Conversely, any $\mathbb{Z}$-module has the structure of an abelian group, given by forgetting about its scalar multiplication. Thus

(1.2) *abelian group and $\mathbb{Z}$-module are equivalent concepts.*

We must use additive notation in the abelian group in order to make this correspondence seem natural.

The ring of integers provides us with examples to show that modules over a ring need not be free. No finite abelian group except the zero group is isomorphic to a free module $\mathbb{Z}^n$, because $\mathbb{Z}^n$ is infinite if $n > 0$ and $\mathbb{Z}^0 = 0$.

The remainder of this section extends some of our basic terminology to modules. A *submodule* of an R-module V is a nonempty subset which is closed under addition and scalar multiplication. We have seen submodules in one case before, namely ideals.

(1.3) **Proposition.** The submodules of the R-module R^1 are the ideals of R.

Proof. By definition, an ideal is a subset of R which is closed under addition and under multiplication by elements of R. □

The definition of *homomorphism* of R-modules copies that of linear transformation of vector spaces. A homomorphism $\varphi\colon V \longrightarrow W$ of R-modules is a map which is compatible with the laws of composition

(1.4) $$\varphi(v + v') = \varphi(v) + \varphi(v') \quad \text{and} \quad \varphi(rv) = r\varphi(v),$$

for all $v, v' \in V$ and $r \in R$. A bijective homomorphism is called an *isomorphism*. The *kernel* of a homomorphism $\varphi\colon V \longrightarrow W$ is a submodule of V, and the *image* of φ is a submodule of W.

The proof given for vector spaces [Chapter 4 (2.1)] shows that every homomorphism $\varphi\colon R^m \longrightarrow R^n$ of free modules is left multiplication by a matrix whose entries are in R.

We also need to extend the concept of quotient group to modules. Let R be a ring, and let W be a submodule of an R-module V. The quotient V/W is the additive group of cosets [Chapter 2 (9.5)] $\overline{v} = v + W$. It is made into an R-module by the rule

$$r\overline{v} = \overline{rv}. \tag{1.5}$$

We have made such constructions several times before. The facts we will need are collected together below.

(1.6) **Proposition.**

(a) The rule (1.5) is well-defined, and it makes $\overline{V} = V/W$ into an R-module.

(b) The canonical map $\pi\colon V \longrightarrow \overline{V}$ sending $v \rightsquigarrow \overline{v}$ is a surjective homomorphism of R-modules, and its kernel is W.

(c) *Mapping property:* Let $f\colon V \longrightarrow V'$ be a homomorphism of R-modules whose kernel contains W. There is a unique homomorphism: $\overline{f}\colon \overline{V} \longrightarrow V'$ such that $f = \overline{f}\pi$.

(d) *First Isomorphism Theorem:* If $\ker f = W$, then $\overline{f}$ is an isomorphism from $\overline{V}$ to the image of f.

(e) *Correspondence Theorem:* There is a bijective correspondence between submodules $\overline{S}$ of $\overline{V}$ and submodules S of V which contain W, defined by $S = \pi^{-1}(\overline{S})$ and $\overline{S} = \pi(S)$. If S and $\overline{S}$ are corresponding modules, then V/S is isomorphic to $\overline{V}/\overline{S}$.

We already know the analogous facts for groups and normal subgroups. All that remains to be checked in each part is that scalar multiplication is well-defined, satisfies the axioms for a module, and is compatible with the maps. These verifications follow the pattern set previously. □

2. MATRICES, FREE MODULES, AND BASES

Matrices with entries in a ring can be manipulated in the same way as matrices with entries in a field. That is, the operations of matrix addition and multiplication are defined as in Chapter 1, and they satisfy similar rules. A matrix with entries in a ring R is often called an *R-matrix.*

Let us ask which R-matrices are invertible. The *determinant* of an $n \times n$ R-matrix $A = (a_{ij})$ can be computed by any of the old rules. It is convenient to use the complete expansion [Chapter 1 (4.12)], because it exhibits the determinant as a polynomial in the n^2 matrix entries. So we write

$$\det A = \sum_{p} \pm\, a_{1p(1)} \cdots a_{np(n)}, \tag{2.1}$$

the sum being over all permutations of the set $\{\mathbf{1},\ldots,\mathbf{n}\}$, and the symbol ± standing for the sign of the permutation. Evaluating this formula on an R-matrix, we obtain an element of R. The usual rules for determinant apply, in particular

$$\det AB = (\det A)(\det B).$$

We have proved this rule when the matrix entries are in a field [Chapter 1 (3.16)], and we will discuss the reason that such formulas carry over to rings in the next section. Let us assume for now that they do carry over.

If A has a multiplicative inverse A^{-1} with entries in R, then

$$(\det A)(\det A^{-1}) = \det I = 1.$$

This shows that the determinant of an invertible R-matrix is a *unit* of the ring. Conversely, let A be an R-matrix whose determinant δ is a unit. Then we can find its inverse by Cramer's Rule: $\delta I = A(\operatorname{adj} A)$, where the adjoint matrix is calculated from A by taking determinants of minors [Chapter 1 (5.4)]. This rule also holds in any ring. So if δ is a unit, we can solve for A^{-1} in R as

$$A^{-1} = \delta^{-1}(\operatorname{adj} A).$$

(2.2) **Corollary.** The invertible $n \times n$ matrices A with entries in R are those matrices whose determinant is a unit. They form a group

$$GL_n(R) = \{\text{invertible } n \times n \ R\text{-matrices}\},$$

called the *general linear group over R*. □

The fact that the determinant of an invertible matrix must be a unit is a strong condition on the matrix when R has few units. For instance, if R is the ring of integers, the determinant must be ± 1. Most integer matrices are invertible real matrices, so they are in $GL_n(\mathbb{R})$. But unless the determinant ± 1, the entries of the inverse matrix won't be integers, so the inverses will not be in $GL_n(\mathbb{Z})$. Nevertheless, there are always reasonably many invertible matrices if $n > 1$, because the elementary matrices

$$I + ae_{ij} = \begin{bmatrix} 1 & & a \\ & \ddots & \\ & & 1 \end{bmatrix}, \quad i \neq j, \quad a \in R,$$

have determinant 1. These matrices generate a good-sized group. The other elementary matrices, the transposition matrices and the matrices

$$\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & u & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}, \quad u \quad \text{a unit in } R,$$

are also invertible.

We now return to the discussion of modules over a ring R. The concepts of basis and independence (Chapter 3, Section 3) can be carried over from vector spaces to modules without change: An ordered set $(v_1, \ldots, v_k)$ of elements of a module V is said to *generate* (or *span*) V if every $v \in V$ is a linear combination:

$$(2.3) \qquad v = r_1 v_1 + \cdots + r_k v_k, \quad \text{with } r_i \in R.$$

In that case the elements v_i are called *generators*. A module V is said to be *finitely generated* if there exists a finite set of generators. Most of the modules we study will be finitely generated. A $\mathbb{Z}$-module V is finitely generated if and only if it is a finitely generated abelian group in the sense of Chapter 6, Section 8.

We saw in Section 1 that modules needn't be isomorphic to any of the modules R^k. However, a given module may happen to be, and if so, it is called a *free module* too. Thus a finitely generated module V is free if there is an isomorphism

$$\varphi: R^n \xrightarrow{\sim} V.$$

For instance, lattices in $\mathbb{R}^2$ are free $\mathbb{Z}$-modules, whereas finite, nonzero abelian groups are not free. A free $\mathbb{Z}$-module is also called a *free abelian group*. Free modules form an important and natural class, and we will study them first. We will study general modules beginning in Section 5.

Following the definitions for vector spaces, we call a set of elements $(v_1, \ldots, v_n)$ of a module V *independent* if no nontrivial linear combination is zero, that is, if the following condition holds:

$$(2.4) \qquad \textit{If } r_1 v_1 + \cdots + r_n v_n = 0, \textit{ with } r_i \in R, \textit{ then } r_i = 0 \text{ for } i = 1, \ldots, n.$$

The set is a *basis* if it is both independent and a generating set. The *standard basis* $\mathbf{E} = (e_1, \ldots, e_k)$ is a basis of R^k. Exactly as with vector spaces, $(v_1, \ldots, v_k)$ is a basis if every $v \in V$ is a linear combination (2.3) in a unique way.

We may also speak of linear combinations and linear independence of infinite sets, using the terminology of Chapter 3, Section 5.

Let us denote the ordered set $(v_1, \ldots, v_n)$ by $\mathbf{B}$, as in Chapter 3, Section 3. Then multiplication by $\mathbf{B}$,

$$\mathbf{B}X = (v_1, \ldots, v_n) \begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix} = v_1 x_1 + \cdots + v_n x_n,$$

defines a homomorphism of modules

$$(2.5) \qquad \mu: R^n \longrightarrow V.$$

This homomorphism is surjective if and only if the set $(v_1, \ldots, v_n)$ generates V, and injective if and only if it is independent. Thus it is bijective if and only if $\mathbf{B}$ is a basis of V, in which case V is a free module. So a module V has a basis if and only if it is free. Most modules have no bases.

Computation with bases of free R-modules can be done in much the same way as with bases of vector spaces, using matrices with entries in R. In particular, we can speak of the *coordinate vector* of an element $v \in V$, with respect to a basis $\mathbf{B} = (v_1, \ldots, v_n)$. It is the unique column vector $X \in R^n$ such that

$$v = \mathbf{B}X = v_1 x_1 + \cdots + v_n x_n.$$

If two bases $\mathbf{B} = (v_1, \ldots, v_n)$ and $\mathbf{B}' = (v_1', \ldots, v_r')$ for the same free module V are given, then the matrix of change of basis is obtained as in Chapter 3, Section 4 by writing the elements v_j of the first basis as linear combinations of the second basis: $\mathbf{B} = \mathbf{B}'P$, or

$$v_j = \sum_{i=1}^{t} v_i' p_{ij}. \tag{2.6}$$

As with vector spaces, any two bases of the same free module over a nonzero ring have the same cardinality, provided that R is not the zero ring. Thus $n = r$ in the above bases. This can be proved by considering the inverse matrix $Q = (q_{ij})$ which is obtained by writing $\mathbf{B}'$ in terms of $\mathbf{B}$: $\mathbf{B}' = \mathbf{B}Q$. Then

$$\mathbf{B} = \mathbf{B}'P = \mathbf{B}QP.$$

Since $\mathbf{B}$ is a basis, there is only one way to write v_j as a linear combination of $(v_1, \ldots, v_n)$, and that is $v_j = 1v_j$, or $\mathbf{B} = \mathbf{B}I$. Therefore $QP = I$, and similarly $PQ = I$: The matrix of change of basis is an invertible R-matrix.

Now P is an $r \times n$ matrix, and Q is a $n \times r$ matrix. Suppose that $r > n$. Then we make P and Q square by adding zeros:

$$\left[\begin{array}{c|c} P & 0 \end{array}\right] \left[\begin{array}{c} Q \\ \hline 0 \end{array}\right] = I.$$

This does not change the product PQ. But the determinants of these square matrices are zero, so they are not invertible, because $R \neq 0$. This shows that $r = n$, as claimed.

It is a startling fact that there exist *noncommutative* rings R for which the modules R^n for $n = 1, 2, 3, \ldots$ are all isomorphic (see miscellaneous exercise 6). Determinants do not work well unless the matrix entries commute.

Unfortunately, most concepts relating to vector spaces have different names when used for modules over rings, and it is too late to change them. The number of elements of a basis for a free module V is called the *rank* of V, instead of the dimension.

As we have already remarked, every homomorphism $\varphi: R^n \longrightarrow R^m$ between column vectors is left multiplication by a matrix A. If $\varphi: V \longrightarrow W$ is a homomorphism of free R-modules with bases $\mathbf{B} = (v_1, \ldots, v_n)$ and $\mathbf{C} = (w_1, \ldots, w_m)$ respectively, then the *matrix* of the homomorphism is defined to be $A = (a_{ij})$, where

$$\varphi(v_j) = \sum_i w_i a_{ij} \tag{2.7}$$

as before [Chapter 4 (2.3)]. A change of the bases $\mathbf{B}, \mathbf{C}$ by invertible R-matrices P, Q changes the matrix of φ to $A' = QAP^{-1}$ [Chapter 4 (2.7)].

3. THE PRINCIPLE OF PERMANENCE OF IDENTITIES

In this section, we address the following question: Why do the properties of matrices with entries in a field continue to hold when the entries are in an arbitrary ring? Briefly, the reason is that they are *identities*, which means that they hold when the matrix entries are replaced by variables. To be more precise, assume we want to prove some identity such as the multiplicative property of the determinant, $(\det A)(\det B) = \det(AB)$, or Cramer's Rule. Suppose that we have already checked the identity for matrices with complex entries. We don't want to do the work again, and anyhow we may have used special properties of $\mathbb{C}$, such as the field axioms, the fact that every complex polynomial has a root, or the fact that $\mathbb{C}$ has characteristic zero, to check the identity there. We did use special properties to prove the identities mentioned, so the proofs we gave will not work for rings. We are now going to show how to deduce such identities for all rings from the same identities for the complex numbers.

The principle is very general, but in order to focus attention, let us concentrate on the identity $(\det A)(\det B) = \det(AB)$. We begin by replacing the matrix entries with variables. So we consider the same identity

$$(\det X)(\det Y) = \det(XY),$$

where X and Y denote $n \times n$ matrices with variable entries. Then we can substitute elements in any ring R for these variables. Formally, the substitution is defined in terms of the ring of integer polynomials $\mathbb{Z}[\{x_{ij}\}, \{y_{k\ell}\}]$ in $2n^2$ variable matrix entries. There is a unique homomorphism from the ring of integers to any ring R [Chapter 10 (3.9)]. Given matrices $A = (a_{ij})$, $B = (b_{k\ell})$ with entries in R, there is a homomorphism

$$(3.1) \qquad \mathbb{Z}[\{x_{ij}\}, \{y_{k\ell}\}] \longrightarrow R,$$

the substitution homomorphism, which sends $x_{ij} \rightsquigarrow a_{ij}$ and $y_{k\ell} \rightsquigarrow b_{k\ell}$ [Chapter 10 (3.4)]. Our variable matrices have entries in the polynomial ring, and it is natural to say that the homomorphism sends $X \rightsquigarrow A$ and $Y \rightsquigarrow B$, meaning that the entries of $X = (x_{ij})$ are mapped to the entries of $A = (a_{ij})$ and so on, by the map.

The general principle we have in mind is this: Suppose we want to prove an identity, all of whose terms are polynomials with integer coefficients in the matrix entries. Then the terms are compatible with ring homomorphisms: For example, if a homomorphism $\varphi: R \longrightarrow R'$ sends $A \rightsquigarrow A'$ and $B \rightsquigarrow B'$, then it sends $\det A \rightsquigarrow \det A'$. To see this, note that the complete expansion of the determinant is

$$\det A = \sum_{p} \pm a_{1p(1)} \cdots a_{np(n)},$$

the summation being over all permutations p. Since φ is a homomorphism,

$$\varphi(\det A) = \sum_p \pm \varphi(a_{1p(1)} \cdots a_{np(n)}) = \sum \pm a_{1p(1)}' \cdots a_{np(n)}' = \det A'.$$

Obviously, this is a general principle. Consequently, if our identity holds for the R-matrices A, B, then it also holds for the R'-matrices A', B'.

Now for every pair of matrices A, B, we have the homomorphism (3.1) which sends $X \rightsquigarrow A$ and $Y \rightsquigarrow B$. We substitute $\mathbb{Z}$ $[\{x_{ij}\}, \{y_{ij}\}]$ for R and R for R' in the principle just described. We conclude that if the identity holds for the variable matrices X, Y in $\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}]$, then it holds for every pair of matrices in any ring R:

(3.2) *To prove our identity in general, we need only prove it for the variable matrices X, Y in the ring $\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}]$.*

To prove it for variable matrices, we consider the ring of integers as a subring of the field of complex numbers, noting the inclusion of polynomial rings

$$\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}] \subset \mathbb{C}[\{x_{ij}\}, \{y_{ij}\}].$$

We may as well check our identity in the bigger ring. Now by hypothesis, our identity is equivalent to the equality of certain polynomials in the variables $\{x_{ij}\}, \{y_{ij}\}, \ldots$. Let us write the identity as $f(x_{ij}, y_{kl}) = 0$. The symbol f may stand for several polynomials.

We now consider the polynomial *function* corresponding to the polynomial $f(x_{ij}, y_{kl})$, call it $\tilde{f}(x_{ij}, y_{kl})$. If the identity has been proved for all complex matrices, then it follows that $\tilde{f}(x_{ij}, y_{kl})$ is the zero function. We apply the fact [Chapter 10 (3.8)] that a polynomial is determined by the function it defines to conclude that $f(x_{ij}, y_{ij}) = 0$, and we are done.

It is possible to formalize the above discussion and to prove a precise theorem concerning the validity of identities in an arbitrary ring. However, even mathematicians occasionally feel that it isn't worthwhile making a precise formulation—that it is easier to consider each case as it comes along. This is one of those occasions.

4. DIAGONALIZATION OF INTEGER MATRICES

In this section we discuss simplification of an $m \times n$ integer matrix $A = (a_{ij})$ by a succession of elementary operations. We will apply this procedure later to classify abelian groups. The same method will work for matrices with entries in a Euclidean domain and, with some modification, for matrices with entries in a principal ideal domain.

The best results are obtained if we allow both row and column operations together. So we allow these operations:

(4.1)

(i) add an integer multiple of one row to another, or add an integer multiple of one column to another;

(ii) interchange two rows or two columns;

(iii) multiply a row or a column by a unit.

Of course, the units in $\mathbb{Z}$ are ± 1. Any such operation can be made by multiplying A on the left or right by a suitable elementary integer matrix. The result of a sequence of these operations will have the form

(4.2)
$$A' = QAP^{-1},$$

where $Q \in GL_m(\mathbb{Z})$ and $P^{-1} \in GL_n(\mathbb{Z})$ are products of elementary integer matrices. Needless to say, we could drop the inverse symbol from P. We put it there because we will want to interpret the operation as a change of basis.

Over a *field*, any matrix can be brought into the block form

$$A' = \begin{bmatrix} I & \\ & 0 \end{bmatrix}$$

by such operations [Chapter 4 (2.9)]. We can not hope for such a result when working with integers. We can't even do it for 1 × 1 matrices. But we can diagonalize:

(4.3) **Theorem.** Let A be an $m \times n$ integer matrix. There exist products Q, P of elementary integer matrices as above, so that $A' = QAP^{-1}$ is diagonal:

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{bmatrix} & \\ & 0 \end{bmatrix}$$

where the diagonal entries d_i are nonnegative and where each diagonal entry divides the next: $d_1 | d_2$, $d_2 | d_3, \ldots$.

Proof. The strategy is to perform a sequence of operations so as to end up with a matrix

(4.4)
$$\begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \begin{bmatrix} & B & \end{bmatrix} & \\ 0 & & & \end{bmatrix}$$

in which d_1 divides every entry of B. When this is done, we work on B. The process is based on repeated division with remainder. We will describe a systematic method, though using this method is usually not the quickest way to proceed.

We may assume $A \neq 0$.

Step 1: By permuting rows and columns, move a nonzero entry with smallest absolute value to the upper left corner. Multiply the first row by -1 if necessary, so that this upper left entry a_{11} becomes positive.

We now try to clear out the first row and column. Whenever an operation produces a nonzero entry in the matrix whose absolute value is smaller than $|a_{11}|$, we go back to Step 1 and start the whole process over. This is likely to spoil the work we have done to clear out matrix entries. However, progress is being made because the size of a_{11} is reduced every time. We will not have to return to Step 1 infinitely often.

Step 2: Choose a nonzero entry a_{i1} in the first column, with $i > 1$, and divide by a_{11}:

$$a_{i1} = a_{11}q + r,$$

where $0 \leq r < a_{11}$. Subtract q times (row 1) from (row i). This changes a_{i1} to r.

If $r \neq 0$, we go back to Step 1. If $r = 0$, we have produced a zero in the first column. Finitely many repetitions of Steps 1 and 2 result in a matrix in which $a_{i1} = 0$ for all $i > 1$. Similarly, we may use the analogue of Step 2 for column operations to clear out the first row, eventually ending up with a matrix in which the only nonzero entry in the first row and column is a_{11}, as required by (4.3). However, a_{11} may not yet divide every entry of the matrix B (4.4).

Step 3: Assume that a_{11} is the only nonzero entry in the first row and column, but that some entry b of B is not divisible by a_{11}. Add the column of A which contains b to column 1. This produces an entry b in the first column.

We go back to Step 2. Division with remainder will now produce a smaller matrix entry, sending us back to Step 1. A finite sequence of these steps will produce a matrix of the form (4.4), allowing us to proceed by induction. □

(4.5) **Example.** We do not follow the systematic method:

$$A = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \xrightarrow[\text{oper}]{\text{column}} \begin{bmatrix} 1 & -1 \\ 3 & 2 \end{bmatrix} \xrightarrow[\text{oper}]{\text{column}} \begin{bmatrix} 1 & \\ 3 & 5 \end{bmatrix} \xrightarrow[\text{oper}]{\text{row}} \begin{bmatrix} 1 & \\ & 5 \end{bmatrix} = A'.$$

Here

$$Q = \begin{bmatrix} 1 & \\ -3 & 1 \end{bmatrix} \quad \text{and} \quad P^{-1} = \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Note that the key ingredient in this proof is the division algorithm. The same proof will work when $\mathbb{Z}$ is replaced by any Euclidean domain.

(4.6) **Theorem.** Let R be a Euclidean domain, for instance a polynomial ring $F[t]$ in one variable over a field. Let A be an $m \times n$ matrix with entries in R. There are products Q, P of elementary R-matrices such that $A' = QAP^{-1}$ is diagonal and such that each diagonal entry of A' divides the next: $d_1 \mid d_2 \mid d_3 \mid \ldots$. If $R = F[t]$, we can normalize by requiring the polynomials d_i to be monic. □

(4.7) **Example.** Diagonalization of a matrix of polynomials:

$$A = \begin{bmatrix} t^2-3t+2 & t-2 \\ (t-1)^3 & t^2-3t+2 \end{bmatrix} \xrightarrow[\text{oper}]{\text{row}} \begin{bmatrix} t^2-3t+2 & t-2 \\ (t-1)^2 & 0 \end{bmatrix} \xrightarrow[\text{oper}]{\text{row}} \begin{bmatrix} -t+1 & t-2 \\ (t-1)^2 & 0 \end{bmatrix} \xrightarrow[\text{oper}]{\text{column}}$$

$$\begin{bmatrix} -1 & t-2 \\ (t-1)^2 & 0 \end{bmatrix} \xrightarrow[\text{oper}]{\text{column}} \begin{bmatrix} -1 & 0 \\ (t-1)^2 & (t-1)^2(t-2) \end{bmatrix} \xrightarrow[\text{oper}]{\text{row}} \begin{bmatrix} 1 & \\ & (t-1)^2(t-2) \end{bmatrix} = A'.$$

In both examples, we ended up with 1 in the upper left corner. This isn't surprising. The matrix entries will often have greatest common divisor 1.

The diagonalization of integer matrices can be used to describe homomorphisms between free abelian groups. As we have already remarked (2.8), a *homomorphism φ: $V \longrightarrow W$ of free abelian groups is described by a matrix*, once bases for V and W are chosen. A change of bases in V, W by invertible integer matrices P, Q changes A to $A' = QAP^{-1}$. So we have proved the following theorem:

(4.8) **Theorem.** Let φ: $V \longrightarrow W$ be a homomorphism of free abelian groups. There exist bases of V and W such that the matrix of the homomorphism has the diagonal form (4.3). □

In the rest of this section, we will investigate the meaning of this theorem for two auxiliary groups associated to a homomorphism: its kernel and its image.

Let φ: $\mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ be left multiplication by the $m \times n$ integer matrix A. The kernel of φ is the subgroup of $\mathbb{Z}^n$ of integer solutions of the system of linear equations

$$AX = 0. \tag{4.9}$$

These solutions can be read off immediately when the matrix is diagonal: In order for X to solve the diagonal system $d_1x_1 = 0, \ldots, d_nx_n = 0$, we must have $x_i = 0$ unless $d_i = 0$, and if $d_i = 0$, then x_i can be arbitrary.

To solve (4.9) in general, we may diagonalize A, say to $A' = QAP^{-1}$, where Q, P are products of elementary integer matrices. We make the change of variable $X' = PX$ and solve the diagonal system

$$A'X' = QAP^{-1}X' = 0.$$

Since Q is invertible, the system of equations $QAX = 0$ has the same solutions as the system $AX = 0$. So the solutions of the original system are $X = P^{-1}X'$.

Next, let us examine the image of φ: $\mathbb{Z}^n \longrightarrow \mathbb{Z}^m$, the map defined by multiplication by the integer matrix A as before. We can describe this image as the set of vectors $B \in \mathbb{Z}^m$ such that the system of integer equations $AX = B$ has an integer solution. We will often denote this image by $A\mathbb{Z}^n$. Multiplication by A sends the basis vectors $e_1,\ldots,e_n \in \mathbb{Z}^n$ to the columns

$$(4.10) \qquad A_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \ldots, A_n = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix}$$

of A, so the image is the set of integer linear combinations of these columns. In other words, the columns generate the image.

We can turn this description around, starting with an arbitrary *subgroup* S of the free abelian group $\mathbb{Z}^m$ which is given to us explicitly by a set of generators $A_1,\ldots,A_n \in \mathbb{Z}^m$. Let A be the matrix whose columns are A_i. Then S is the image of left multiplication by A. This interpretation of S as the image of a homomorphism tells us the meaning of left and right multiplication by invertible integer matrices Q and P^{-1}: Left multiplication by Q corresponds to a change of basis in the module $\mathbb{Z}^m$, the range of the map. Its effect is to multiply each of the generators A_i by Q. On the other hand, right multiplication by P^{-1} represents a change of basis in the domain $\mathbb{Z}^n$. This changes the generating set of S. For example, adding r times column 1 to column 2 changes A_2 to $A_2' = A_2 + rA_1$ and leaves the other generators unchanged. Combining these observations with diagonalization results in the following theorem:

(4.11) **Theorem.** Let S be a subgroup of a free abelian group W of rank m. There is a basis $(w_1,\ldots,w_m)$ of W and a basis $(u_1,\ldots,u_n)$ of S with the following properties: (i) $n \leq m$, (ii) for each $j \leq n$ there is a positive integer d_j such that $u_j = d_j w_j$, and (iii) $d_1 \mid d_2 \mid d_3 \ldots$.

(4.12) **Corollary.** Every subgroup of a free abelian group of rank m is free, and its rank is at most m. □

Proof of Theorem (4.11). Roughly speaking, we need only choose a basis $\mathbf{B} = (w_1,\ldots,w_m)$ for W and a set of generators $(u_1,\ldots u_n)$ for S, to obtain an $m \times n$ matrix A which represents S as above. The diagonalization theorem gives us a diagonal matrix $A' = QAP^{-1}$ representing S with respect to a new basis $\mathbf{B}' = (w_1',\ldots,w_p')$ and new generating set $(u_1',\ldots,u_n')$. Then $u_j' = d_j w_j'$. We drop the primes to obtain the basis and generating set required. This completes the proof except for three points.

First, we may have $n > m$, that is, there may be more columns than rows. But if so, then since A' is diagonal, its jth column is zero for each $j > m$; hence the corresponding generator u_j is zero too. The zero element is useless as a generator, so we throw it out. For the same reason, we may throw out a generator u_j whenever $d_j = 0$. After we do this, all d_j will be positive, and we will have $n \leq m$.

Notice that if S is the zero subgroup, we will end up throwing out all the generators. As with vector spaces, we must adopt the convention that the empty set generates the zero module, or else make a special mention of this exceptional case in the statement of the theorem.

Next, we verify that if the basis and generating set are chosen so that $d_i > 0$ and $n \leq m$, then $(u_1, \ldots, u_n)$ is a basis of S. Since it generates S, what has to be proved is that $(u_1, \ldots, u_n)$ is independent. We rewrite a linear relation $r_1u_1 + \cdots + r_nu_n = 0$ in the form $r_1d_1w_1 + \cdots + r_nd_nw_n = 0$. Since $(w_1, \ldots, w_m)$ is a basis, $r_id_i = 0$ for each i, and since $d_i > 0$, $r_i = 0$.

The final point is more serious: We need a finite set of generators of S to get started. How do we know that there is such a set? It is a fact that every subgroup of a finitely generated abelian group is itself finitely generated. We will prove this in Section 5. For the moment, the theorem is proved only with the additional hypothesis that S is finitely generated. The hypothesis that W is finitely generated can not be removed. □

Theorem (4.11) is quite explicit. Let S be the subgroup of $\mathbb{Z}^m$ generated by the columns of a matrix A, and suppose that $A' = QAP^{-1}$ is diagonal. To display S in the form asserted in the theorem, we rewrite this equation in the form

$$Q^{-1}A' = AP^{-1}, \tag{4.13}$$

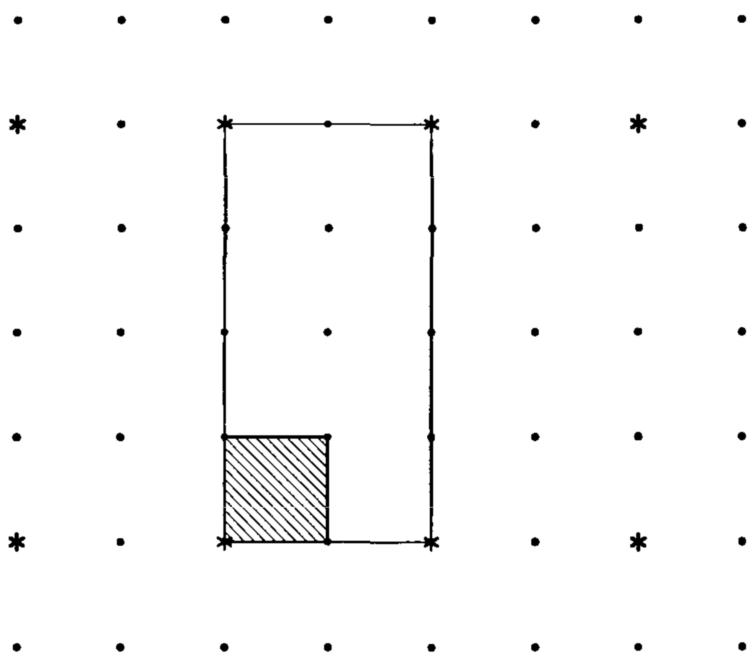
and we interpret it as follows: The columns of the matrix AP^{-1} form our new set of generators for S. Since the matrix A' is diagonal, (4.13) tells us that the new generators are multiples of the columns of Q^{-1}. We change the basis of $\mathbb{Z}^m$ from the standard basis to the basis made up of the columns of Q^{-1}. The matrix of this change of basis is Q [see Chapter 3 (4.21)]. Then the new generators are multiples of the new basis elements.

For instance, let S be the lattice in $\mathbb{R}^2$ generated by the two columns of the matrix A of Example (4.5): Then

$$Q^{-1}A' = \begin{bmatrix} 1 & \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & \\ & 5 \end{bmatrix} = \begin{bmatrix} 1 & \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = AP^{-1}. \tag{4.14}$$

The new basis of $\mathbb{Z}^2$ is $(w_1', w_2') = \left(\begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} \\ 1 \end{bmatrix}\right)$, and the new generators of S are $(u_1', u_2') = (u_1, u_2)P^{-1} = (w_1', 5w_2')$.

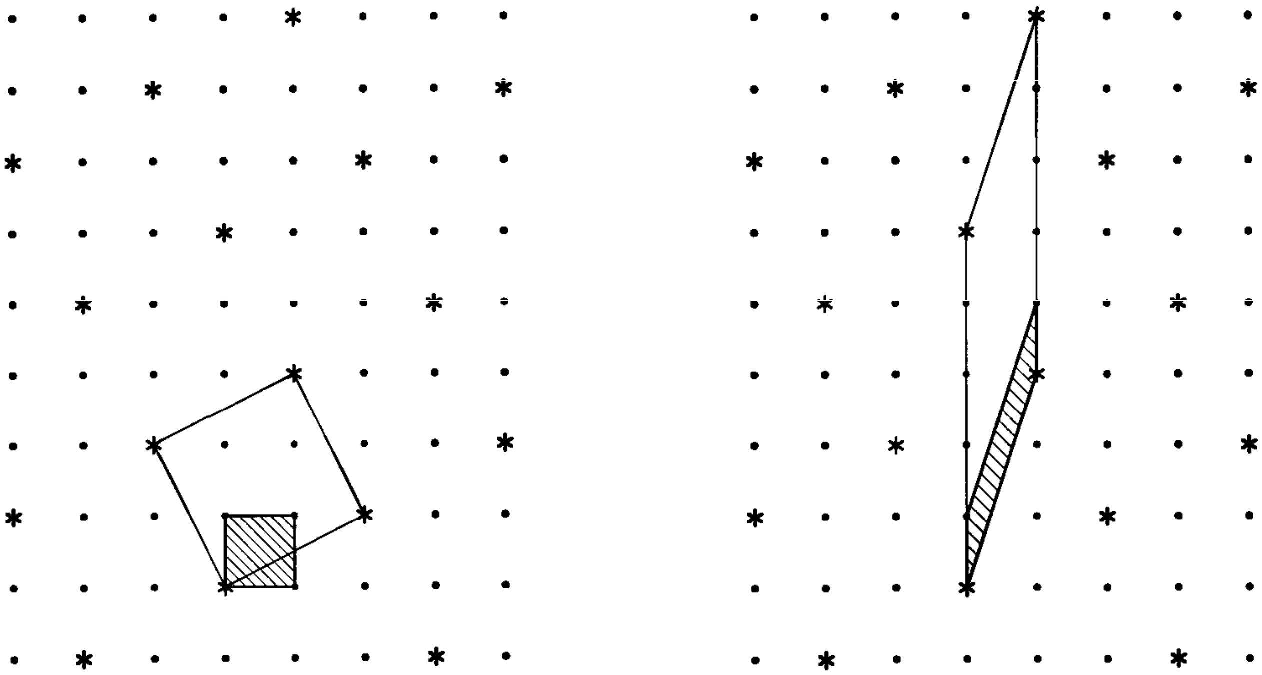
Theorem (4.3) is striking when it is used to describe the relative position of a sublattice S in a lattice L. To illustrate this, it will be enough to consider plane lattices. The theorem asserts that there are bases (v_1, v_2) and (w_1, w_2) of L and S such that the coordinate vectors of w_j with respect to the basis (v_1, v_2) are diagonal. Let us refer the lattice L back to $\mathbb{Z}^2 \subset \mathbb{R}^2$ by means of the basis (v_1, v_2). Then the equations $w_i = d_iv_i$ show that S looks like this figure, in which we have taken $d_1 = 2$ and $d_2 = 4$:



(4.15) **Figure.** $S = *$, matrix $\begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$.

Notice the fact, which we have asserted before [Chapter 11 (10.10)], that the index $[L{:}S]$ is the ratio of the areas of the parallelograms spanned by bases. This is evident when the bases are in such a relative position.

In practice, when the lattices L and S are given to us in $\mathbb{R}^2$ at the start, the change of basis required to get such "commensurable" bases of L and S leads to rather long and thin parallelograms, as is shown below for Example (4.14).



(4.16) **Figure.** Diagonalization, applied to a sublattice.

5. GENERATORS AND RELATIONS FOR MODULES

In this section we turn our attention to modules which are not free. We will show how to describe a large class of modules by means of matrices called *presentation matrices*. We will then apply the diagonalization procedure to these matrices to the study of abelian groups.

As an example to keep in mind, we may consider an abelian group or $\mathbb{Z}$-module V which is generated by three elements (v_1, v_2, v_3). We suppose that these generators are subject to the relations

$$\begin{aligned} 3v_1 + 2v_2 + v_3 &= 0 \\ 8v_1 + 4v_2 + 2v_3 &= 0 \\ 7v_1 + 6v_2 + 2v_3 &= 0 \\ 9v_1 + 6v_2 + v_3 &= 0. \end{aligned} \tag{5.1}$$

The information describing this module is summed up in the matrix

$$A = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix}, \tag{5.2}$$

whose columns are the coefficients of the relations (5.1):

$$(v_1, v_2, v_3)A = (0,0,0,0).$$

As usual, scalars appear on the right side in this matrix product. It is this method of describing a module which we plan to formalize.

If $(v_1, , \ldots, v_m)$ are elements of an R-module V, equations of the form

$$a_1v_1 + \cdots + a_mv_m = 0, \quad a_i \in R, \tag{5.3}$$

are called *relations* among thc elements. Of course, when we refer to (5.3) as a relation, we mean that the formal expression is a relation: If we evaluate it in V, we get $0 = 0$. Since the relation is determined by the R-vector $(a_1, \ldots, a_m)^t$, we will refer to this vector as a *relation vector*, meaning that (5.3) is true in V. By a *complete set of relations* we mean a set of relation vectors such that every relation vector is a linear combination of this set. It is clear that a matrix such as (5.2) will not describe the module V completely, unless its columns form a complete set of relations.

The concept of a complete set of relations can be confusing. It becomes much clearer when we work with homomorphisms of free modules rather than directly with the relations or the relation vectors. Let an $m \times n$ matrix A with entries in a ring R be given. As we know, left multiplication by this matrix is a homomorphism of R-modules

$$\varphi: R^n \longrightarrow R^m. \tag{5.4}$$

In addition to the kernel and image, which we described in the last section when $R = \mathbb{Z}$, there is another important auxiliary module associated with a homomorphism $\varphi\colon W \longrightarrow W'$ of R-modules, called its *cokernel*. The cokernel of φ is defined to be the quotient module

$$W'/(\operatorname{im} \varphi). \tag{5.5}$$

If we denote the image of left multiplication by A by AR^n, the cokernel of (5.4) is R^m/AR^n. This cokernel is said to be *presented* by the matrix A. More generally, we will call any isomorphism

$$\sigma\colon R^m/AR^n \xrightarrow{\sim} V \tag{5.6}$$

a *presentation* of a module V, and we say that the matrix A is a *presentation matrix* for V if there is such an isomorphism.

For example, the cyclic group $\mathbb{Z}/(5)$ is presented as a $\mathbb{Z}$-module by the 1×1 integer matrix $[5]$. As another example, let V be the $\mathbb{Z}$-module presented by the matrix $\begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$. The columns of this matrix are the relation vectors, so V is generated by two elements v_1, v_2 with the relations $2v_1 + v_2 = -v_1 + 2v_2 = 0$. We may solve the first relation, obtaining $v_2 = -2v_1$. This allows us to eliminate the second generator. Substitution into the second relation gives $-5v_1 = 0$. So V can also be generated by a single generator v_1, with the single relation $5v_1 = 0$. This shows that V is isomorphic to $\mathbb{Z}/(5)$. This 2×2 matrix also presents the cyclic group $\mathbb{Z}/(5)$.

We will now describe a theoretical method of finding a presentation of a given module V. To carry out this method in practice, the module would have to be given in a very explicit way. Our first step is to choose a set of generators $(v_1, \ldots, v_m)$. So V must be finitely generated for us to get started. These generators provide us with a surjective homomorphism

$$f\colon R^m \longrightarrow V, \tag{5.7}$$

sending the column vector $X = (x_1, \ldots, x_m)$ to $v_1x_1 + \cdots + v_mx_m$. The elements of the kernel of f are the relation vectors. Let us denote this kernel by W. By the First Isomorphism Theorem, V is isomorphic to R^m/W.

We repeat the procedure, choosing a set of generators $(w_1, \ldots, w_n)$ for W, and we use these generators to define a surjective homomorphism

$$g\colon R^n \longrightarrow W \tag{5.8}$$

as before. Since W is a submodule of R^m, composition of the homomorphism g with the inclusion $W \subset R^m$ gives us a homomorphism

$$\varphi\colon R^n \longrightarrow R^m. \tag{5.9}$$

This homomorphism is left multiplication by a matrix A. By construction, W is the image of φ, which is AR^n, so $R^m/AR^n = R^m/W \approx V$. Therefore, A is a presentation matrix for V.

The columns of the matrix A are our chosen generators for the module W of relations:

$$w_1 = \begin{bmatrix} a_{11} \\ \cdot \\ \cdot \\ \cdot \\ a_{m1} \end{bmatrix}, \ldots, w_n = \begin{bmatrix} a_{1n} \\ \cdot \\ \cdot \\ \cdot \\ a_{mn} \end{bmatrix}.$$

Since they generate W, these columns form a complete set of relations among the generators $(v_1, \ldots, v_m)$ of the module V. Since the columns are relation vectors,

$$(v_1, \ldots, v_m)A = 0. \tag{5.10}$$

Thus the presentation matrix A for a module V is determined by

(5.11)

(i) a set of generators for V, and

(ii) a complete set of relations among these generators.

We have let one point slip by in this description. In order to have a finite set of generators for the module of relations W, this module must be finitely generated. This does not look like a satisfactory hypothesis, because the relationship of our original module V with W is unclear. We don't mind assuming that V is finitely generated, but it isn't good to impose hypotheses on a module which arises in the course of some auxiliary construction. We will need to examine this point more closely [see (5.16)]. But except for this point, we can now speak of generators and relations for a finitely generated R-module V.

Since the presentation matrix depends on the choices (5.11), many matrices present the same module, or isomorphic modules. Here are some rules for manipulating a matrix A without changing the isomorphism class of the module it presents:

(5.12) **Proposition.** Let A be an $m \times n$ presentation matrix for a module V. The following matrices A' present the same module V:

(i) $A' = QAP^{-1}$, where $Q \in GL_m(R)$ and $P \in GL_n(R)$;

(ii) A' is obtained by deleting a column of zeros;

(iii) the jth column of A is e_i, and A' is obtained from A by deleting the ith row and jth column.

Proof.

(i) The module R^m/AR^n is isomorphic to V. Since the change of A to QAP^{-1} corresponds to a change of basis in R^m and R^n, the isomorphism class of the quotient module does not change.

(ii) A column of zeros corresponds to the trivial relation, which can be omitted.

(iii) Suppose that the jth column of the matrix A is e_i. The corresponding relation is $v_i = 0$. So it holds in the module V, and therefore v_i can be left out of the generating set $(v_1,\ldots,v_m)$. Doing so changes the matrix A by deleting the ith row and jth column. □

It may be possible to simplify a matrix quite a lot by these rules. For instance, our original example of the integer matrix (5.2) reduces as follows:

$$A = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 2 & 1 & 6 \\ 0 & 0 & 2 & 4 \\ 1 & 2 & 2 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 1 & 6 \\ 0 & 2 & 4 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 1 & 6 \\ -4 & 0 & -8 \end{bmatrix} \longrightarrow$$

$$\longrightarrow [-4 \quad -8] \longrightarrow [-4 \quad 0] \longrightarrow [4].$$

Thus A presents the abelian group $\mathbb{Z}/(4)$.

By definition, an $m \times n$ matrix presents a module by means of m generators and n relations. But as we see from this example, the number of generators and the number of relations depend on choices. They are not uniquely determined by the module.

Consider two more examples: The 2×1 matrix $\begin{bmatrix} 4 \\ 0 \end{bmatrix}$ presents an abelian group V by means of two generators (v_1, v_2) and one relation $4v_1 = 0$. We can not simplify this matrix. The group which it presents is isomorphic to the product group $\mathbb{Z}/(4) \times \mathbb{Z}$. On the other hand, the matrix $[4 \quad 0]$ presents a group with one generator v_1 and two relations, the second of which is the trivial relation. This group is $\mathbb{Z}/(4)$.

We will now discuss the problem of finite generation of the module of relations. For modules over a nasty ring, this module needn't be finitely generated, even though V is. Fortunately this problem does not occur with the rings we have been studying, as we will now show.

(5.13) **Proposition.** The following conditions on an R-module V are equivalent:

(i) Every submodule W of V is finitely generated;

(ii) *ascending chain condition:* There is no infinite strictly increasing chain $W_1 < W_2 < \ldots$ of submodules of V.

Proof. Assume that V satisfies the ascending chain condition, and let W be a submodule of V. We select a set $w_1, w_2, \ldots, w_k$ of generators of W in the following way: If $W = 0$, then W is generated by the empty set. If not, we start with a nonzero element $w_1 \in W$. To continue, assume that $w_1,\ldots, w_i$ have been chosen, and let W_i be the submodule generated by these elements. If W_i is a proper submodule of W, let w_{i+1} be an element of W which is not contained in W_i. Then $W_1 < W_2 < \ldots$. Since V satisfies the ascending chain condition, this chain of submodules can not be continued indefinitely. Therefore some W_k is equal to W. Then $(w_1,\ldots, w_k)$ generates W. The converse follows the proof of Theorem (2.10) of Chapter 11. Assume that every submodule of V is finitely generated, and let $W_1 \subset W_2 \subset \dots$ be an infinite increasing chain of submodules of V. Let U denote the union of these submodules. Then U is a submodule [see Chapter 11 (2.11)]; hence it is finitely generated. Let $u_1, \dots u_r$ be generators for U. Each u_ν is in one of the modules W_i, and since the chain is increasing, there is an i such that all of the generators are in W_i. Then the module U they generate is also in W_i, and we have $U \subset W_i \subset W_{i+1} \subset U$. This shows that $U = W_i = W_{i+1}$ and that the chain is not strictly increasing. □

(5.14) **Lemma.**

(a) Let $\varphi\colon V \longrightarrow W$ be a homomorphism of R-modules. If the kernel and the image of φ are finitely generated modules, so is V. If V is finitely generated and if φ is surjective, then W is finitely generated. More precisely, suppose that $(v_1, \dots, v_n)$ generates V and that φ is surjective. Then $(\varphi(v_1), \dots, \varphi(v_n))$ generates W.

(b) Let W be a submodule of an R-module V. If both W and V/W are finitely generated, so is V. If V is finitely generated, so is V/W.

Proof. For the first assertion of (a), we follow the proof of the dimension formula for linear transformations [Chapter 4 (1.5)], choosing a set of generators $(u_1, \dots u_k)$ for $\ker \varphi$ and a set of generators $(w_1, \dots, w_m)$ for $\operatorname{im} \varphi$. We also choose elements $v_i \in V$ such that $\varphi(v_i) = w_i$. Then we claim that the set $(u_1, \dots, u_k; v_1, \dots, v_m)$ generates V. Let $v \in V$ be arbitrary. Then $\varphi(v)$ is a linear combination of $(w_1, \dots, w_m)$, say $\varphi(v) = a_1 w_1 + \cdots + a_m w_m$. Let $v' = a_1 v_1 + \cdots + a_m v_m$. Then $\varphi(v') = \varphi(v)$. Hence $v - v' \in \ker \varphi$, so $v - v'$ is a linear combination of $(u_1, \dots, u_k)$, say $v - v' = b_1 u_1 + \cdots + b_k u_k$. Therefore $v = a_1 v_1 + \cdots + a_m v_m + b_1 u_1 + \cdots + b_k u_k$. This shows that the set $(u_1, \dots, u_k; v_1, \dots, v_m)$ generates V, as required. The proof of the second assertion of (a) is easy. Part (b) follows from part (a) by a consideration of the canonical homomorphism $\pi\colon V \longrightarrow V/W$. □

(5.15) **Definition.** A ring R is called *noetherian* if every ideal of R is finitely generated.

Principal ideal domains are obviously noetherian, so the rings $\mathbb{Z}$, $\mathbb{Z}[i]$, and $F[x]$ (F a field) are noetherian.

(5.16) **Corollary.** Let R be a noetherian ring. Every proper ideal I of R is contained in a maximal ideal.

Proof. If I is not maximal itself, then it is properly contained in a proper ideal I_2, and if I_2 is not maximal, it is properly contained in a proper ideal I_3, and so on. By the ascending chain condition (5.13), the chain $I = I_1 < I_2 < I_3 \dots$ must be finite. Therefore I_k is maximal for some k. □

The relevance of the notion of noetherian ring to our problem is shown by the following proposition:

(5.17) **Proposition.** Let V be a finitely generated module over a noetherian ring R. Then every submodule of V is finitely generated.

Proof. It suffices to prove the proposition in the case that $V = R^m$. For assume that we have proved that the submodules of R^m are finitely generated, for all m. Let V be a finitely generated R-module. Then there is a surjective map $\varphi\colon R^m \longrightarrow V$. Given a submodule S of V, let $L = \varphi^{-1}(S)$. Then L is a submodule of the module R^m, and hence L is finitely generated. Also, the map $L \longrightarrow S$ is surjective. Hence S is finitely generated (5.14).

To prove the proposition when $V = R^m$, we use induction on m. A submodule of R is the same as an ideal of R (1.3). Thus the noetherian hypothesis on R tells us that the proposition holds for $V = R^m$ when $m = 1$. Suppose $m > 1$. We consider the projection

$$\pi\colon R^m \longrightarrow R^{m-1}$$

given by dropping the last entry: $\pi(a_1,\ldots,a_m) = (a_1,\ldots,a_{m-1})$. Its kernel is $\{(0,\ldots,0,a_m)\} \approx R$. Let $W \subset R^m$ be a submodule, and let $\varphi\colon W \longrightarrow R^{m-1}$ be the restriction of π to W. The image $\varphi(W)$ is finitely generated, by induction. Also, $\ker\varphi = (W \cap \ker\pi)$ is a submodule of $\ker\pi \approx R$, so it is finitely generated too. By Lemma (5.14), W is finitely generated, as required. □

This proposition completes the proof of Theorem (4.11).

Since principal ideal domains are noetherian, submodules of finitely generated modules over these rings are finitely generated. But in fact, most of the rings which we have been studying are noetherian. This follows from another of Hilbert's famous theorems:

(5.18) **Theorem.** *Hilbert Basis Theorem:* If a ring R is noetherian, then so is the polynomial ring $R[x]$.

The Hilbert Basis Theorem shows by induction that the polynomial ring $R[x_1,\ldots,x_n]$ in several variables over a noetherian ring R is noetherian, hence that the rings $\mathbb{Z}[x_1,\ldots,x_n]$ and $F[x_1,\ldots,x_n]$ (F a field) are noetherian. Also, quotients of noetherian rings are noetherian:

(5.19) **Proposition.** Let R be a noetherian ring, and let I be an ideal of R. The quotient ring $\overline{R} = R/I$ is noetherian.

Proof. Let $\overline{J}$ be an ideal of $\overline{R}$, and let $J = \pi^{-1}(\overline{J})$ be the corresponding ideal of R, where $\pi\colon R \longrightarrow \overline{R}$ is the canonical map. Then J is finitely generated, say by $(a_1,\ldots,a_m)$. It follows that the finite set $(\overline{a}_1,\ldots,\overline{a}_m)$ generates $\overline{J}$(5.14). □

Combining this proposition with the Hilbert Basis Theorem gives the following result:

(5.20) **Corollary.** Any ring which is a quotient of a polynomial ring over the integers or over a field is noetherian. □

Proof of the Hilbert Basis Theorem. Assume that R is noetherian, and let I be an ideal of the polynomial ring $R[x]$. We must show that a finite set of polynomials suffices to generate this ideal.

Let's warm up by reviewing the case that R is a field. In that case, we may choose a nonzero polynomial $f \in I$ of lowest degree, say

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \quad a_n \neq 0, \tag{5.21}$$

and prove that it generates the ideal as follows: Let

$$g(x) = b_m x^m + \cdots + b_1 x + b_0, \quad b_m \neq 0, \tag{5.22}$$

be a nonzero element of I. Then the degree m of g is at least n. We use induction on m. The polynomial

$$g(x) - (b_m/a_n)x^{m-n}f(x) = g_1(x) \tag{5.23}$$

is an element of I of degree $< m$. By induction, g_1 is divisible by f; hence g is divisible by f.

Formula (5.23) is the first step in the division with remainder of g by f. The method does not extend directly to arbitrary rings, because division with remainder requires that the leading coefficient of f be a unit. More precisely, in order to form the expression (5.23) we need to know that a_n divides b_m in the ring R, and there is no reason for this to be true. We will need more generators.

Let us denote by A the set of leading coefficients of all the polynomials in I, together with the zero element of R.

(5.24) **Lemma.** The set A of leading coefficients of the polynomials in an ideal of $R[x]$, together with 0, forms an ideal of R.

Proof. If $\alpha = a_n$ is the leading coefficient of f, then $r\alpha$ is the leading coefficient of rf, unless by chance $r\alpha = 0$. In both cases, $r\alpha \in A$. Next, let $\alpha = a_n$ be the leading coefficient of f, and let $\beta = b_m$ be the leading coefficient of g, where, say, $m \geq n$. Then α is also the leading coefficient of $x^{m-n}f$. Hence the coefficient of x^m in the polynomial $h = x^{m-n}f + g$ is $\alpha + \beta$. This is the leading coefficient of h unless it is zero, and in either case, $\alpha + \beta \in A$. □

We return to the proof of the Hilbert Basis Theorem. According to the lemma, the set A is an ideal of the noetherian ring R, so there exists a finite set of generators, say $(\alpha_1, \ldots, \alpha_k)$, for this ideal. We choose for each i, $1 \leq i \leq k$, a polynomial

$f_i \in I$ with leading coefficient α_i, and we multiply these polynomials by powers of x as necessary, so that their degrees become equal to some common integer n.

The set of polynomials $(f_1,\dots,f_k)$ obtained in this way will allow us to adapt the induction step (5.23), but it will probably not generate I. We have little chance of finding a polynomial of degree $<n$ in the ideal $(f_1,\dots,f_k)$. So we must add some elements of low degree to get generators for our ideal. The following lemma is easy, and we omit its proof:

(5.25) **Lemma.** Let P_n denote the set of polynomials in $R[x]$ which have degree $< n$, together with zero, and let $S_n = I \cap P_n$. Then S_n is an R-submodule of the R-module P_n.

The R-module P_n is generated by the monomials $1, x,\dots, x^{n-1}$, so it is finitely generated. Since R is noetherian, we may use Lemma (5.25) and Proposition (5.17) to conclude that there is a finite set $(h_1,\dots,h_s)$ of elements which generates S_n as an R-module. We claim that the combined set $(f_1,\dots,f_k; h_1,\dots,h_s)$ generates I.

Denote by J the ideal generated by this set. By construction, $J \subset I$. We need to prove the opposite inclusion, and we use induction on the degree of an element $g \in I$. We denote this degree by m. If $m < n$, then $g \in S_n$, and therefore g is a linear combination of $(h_1,\dots,h_s)$, with coefficients in R. So $g \in J$ in that case. Assume that $m \geq n$, and let the leading coefficient of g be $b = b_m$. Then b is in the ideal A of leading coefficients, so it is a linear combination of the generators of that ideal, say $b = r_1\alpha_1 + \cdots + r_k\alpha_k$. Remembering that α_i is the leading coefficient of f_i, we see that the polynomial

$$p = x^{m-n}(\sum_i r_i f_i)$$

has the same leading coefficient and the same degree as g, and it is in J. So $g_1 = g - p$ has degree less than m. By induction, $g_1 \in J$, and hence $g \in J$. □

6. THE STRUCTURE THEOREM FOR ABELIAN GROUPS

The Structure Theorem for abelian groups asserts that a finitely generated abelian group V is a direct sum of cyclic groups. The work of the proof has already been done. We know that there exists a diagonal presentation matrix for V, and what remains for us to do is to interpret the meaning of this diagonal matrix for the group.

We first need to extend the concept of direct sum from vector spaces to arbitrary modules. The definition is the same. Let $W_1,\dots,W_k$ be submodules of a module V. Their *sum* is the submodule which they generate. It consists of all sums

$$(6.1) \qquad W_1 + \cdots + W_k = \{v \in V \mid v = w_1+\cdots+w_k, \quad \text{with } w_i \in W_i\}.$$

The verification that this is a submodule is routine, and it is the same as for sums of subspaces of a vector space. We say that V is the *direct sum* of the submodules W_i if

(6.2)

(i) they *generate*: $V = W_1 + \cdots + W_k$;

(ii) they are *independent*: If $w_1 + \cdots + w_k = 0$, with $w_i \in W_i$, then $w_i = 0$ for each i.

Thus V is the direct sum of the submodules W_i if every element $v \in V$ can be written uniquely in the form $v = w_1 + \cdots + w_k$, with $w_i \in W_i$. As with vector spaces, two submodules W_1, W_2 are independent if and only if $W_1 \cap W_2 = 0$ [see Chapter 3 (6.5)].

The symbol $\oplus$ is used to denote direct sums as before. So the notation

$$V = W_1 \oplus \cdots \oplus W_k \tag{6.3}$$

means that V is the direct sum of the submodules W_i.

(6.4) **Theorem.** *Structure Theorem for abelian groups:* Let V be a finitely generated abelian group. Then V is a direct sum of finite cyclic subgroups $C_{d_1}, \dots, C_{d_k}$ and a free abelian group L:

$$V = C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L,$$

where the order d_i of C_{d_i} is greater than 1, and $d_1 \,|\, d_2 \,|\, d_3 \dots$.

We will use additive notation for the law of composition in the cyclic group here. So C_n is generated by one element v, with one relation $nv = 0$. Thus C_n is isomorphic to $\mathbb{Z}/(n)$. The isomorphism $\mathbb{Z}/(n) \longrightarrow C_n$ sends the residue of an integer r to rv.

Proof of the theorem. We choose a presentation matrix A for V, determined by a set of generators and a complete set of relations. We can do this because V is finitely generated and because $\mathbb{Z}$ is a noetherian ring (see Section 5). By Proposition (5.12), the matrix A may be replaced by QAP^{-1}, where Q and P are invertible. Therefore we may assume that A is diagonal, that the diagonal entries are nonzero, and that each diagonal entry divides the next. Moreover, we can drop any column of zeros, and any row and column in which the diagonal entry is 1 (5.12). So we may assume that the diagonal entries d_i are not 0 or 1. The matrix A will then have the shape

$$\left[\begin{array}{cccc} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_k \\ \hline & & 0 & \end{array}\right]. \tag{6.5}$$

It will therefore be an $m \times k$ matrix, where $k \leq m$. The meaning of this in terms of generators and relations for our module is that V is generated by m elements

$v_1,\dots,v_m$, and that

(6.6) $$d_1v_1 = 0,\ d_2v_2 = 0,\dots,d_kv_k = 0$$

forms a complete set of relations among these generators.

For $j = 1,\dots,k$, let us denote by C_j the cyclic subgroup generated by v_j. Let L be the subgroup generated by the remaining generators $v_{k+1},\dots,v_m$. Since the columns of (6.5) are a complete set of relations, there is no relation involving these last $m - k$ generators. Therefore L is a free abelian group of rank $m - k$. We now verify that $V = C_1 \oplus \cdots \oplus C_k \oplus L$ and that C_j is a cyclic group of order d_j. First, since V is generated by the v_i and since each of the v_i is included in one of the summands, it is clear that V is the sum of these subgroups. Next, suppose that we have a relation, say

$$z_1 + \cdots + z_k + w = 0,$$

where $z_j \in C_j$ and $w \in L$. Since C_j is the cyclic group generated by v_j, we can write $z_j = r_jv_j$ for some integer r_j. Similarly, we may write $w = r_{k+1}v_{k+1} + \cdots + r_mv_m$ for some integers r_j. Then the relation has the form

$$r_1v_1 + \cdots + r_mv_m = 0.$$

Since the columns of (6.5) form a complete set of relations, the vector $(r_1,\dots,r_m)^t$ is a linear combination of these columns. So $r_j = 0$ if $j > k$, which implies that $w = 0$. In addition, r_j must be divisible by d_j if $j \le k$, say $r_j = d_js_j$. Then $z_j = s_jd_jv_j = 0$. Thus the relation was trivial, and this shows that the subgroups are independent. It also shows that the order of the cyclic group C_j is d_j. So we have $V = C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L$, as required. □

A finite abelian group is finitely generated, so as stated above the Structure Theorem decomposes a finite abelian group into a direct sum of finite cyclic groups, in which the order of each summand divides the next. The free abelian summand is zero in this case. It is sometimes convenient to decompose the cyclic groups further, into cyclic groups of prime power order. This decomposition is based on Proposition (8.4) of Chapter 2, which we restate here:

(6.7) Let r, s be relatively prime integers. The cyclic group C_{mn} of order rs is the direct sum of cyclic subgroups of orders r and s. □

Combining this lemma with the Structure Theorem yields the following:

(6.8) **Corollary.** *Structure Theorem, alternate form:* Every finitely generated abelian group is a direct sum of cyclic groups of prime power orders and of a free abelian group. □

It is natural to ask whether the orders of the cyclic subgroups which decompose a given finite abelian group are uniquely determined by the group. If the order of V

is a product of distinct primes, there is no problem. For example, if the order is 30, then V must be isomorphic to $C_2 \oplus C_3 \oplus C_5$. But can the same group be both $C_2 \oplus C_2 \oplus C_4$ and $C_4 \oplus C_4$? It is not difficult to show that this is impossible by counting elements of orders 1 or 2. The group $C_4 \oplus C_4$ contains four such elements, while $C_2 \oplus C_2 \oplus C_4$ contains eight. This counting method will always work.

(6.9) **Theorem.** *Uniqueness for the Structure Theorem:*

(a) Suppose that a finite abelian group V is a direct sum of cyclic groups $C_{d_1} \oplus \cdots \oplus C_{d_k}$ where $d_1 | d_2 | \ldots$. The integers d_j are determined by the group V.

(b) The same is true if the decomposition is into prime power orders, that is, if each d_j is the power of a prime.

We leave the proof as an exercise. □

The counting of elements is simplified notationally by representing a direct sum as a product. Let R be a ring. The *direct product* of R-modules $W_1, \ldots, W_k$ is the product set $W_1 \times \cdots \times W_k$ of k-tuples:

$$(6.10) \qquad W_1 \times \cdots \times W_k = \{(w_1, \ldots, w_k) \,|\, w_i \in W_i\}.$$

It is made into a module by vector addition and scalar multiplication:

$$(w_1, \ldots, w_k) + (w_1', \ldots, w_k') = (w_1 + w_1', \ldots, w_k + w_k'), \quad r(w_1, \ldots, w_k) = (rw_1, \ldots, rw_k).$$

Verification of the axioms for a module is routine.

Direct products and direct sums are isomorphic, as the following proposition shows:

(6.11) **Proposition.** Let $W_1, \ldots, W_k$ be submodules of an R-module V.

(a) The map σ: $W_1 \times \cdots \times W_k \longrightarrow V$ defined by

$$\sigma(w_1, \ldots, w_k) = w_1 + \cdots + w_k$$

is a homomorphism of R-modules, and its image is the sum $W_1 + \cdots + W_k$.

(b) The homomorphism σ is an isomorphism if and only if V is the direct sum of the submodules W_i.

We have seen similar arguments several times before, so we omit the proof. Note that the second part of the proposition is analogous to the statement that the map (2.5) $R^k \longrightarrow V$ defined by a set $(v_1, \ldots v_k)$ is bijective if and only if this set is a basis. □

Since a cyclic group C_d of order d is isomorphic to the standard cyclic group $\mathbb{Z}/(d)$, we can use Proposition (6.11) to restate the Structure Theorem as follows:

(6.12) **Theorem.** *Product version of the Structure Theorem:* Every finitely generated abelian group V is isomorphic to a direct product of cyclic groups

$$\mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_k) \times \mathbb{Z}^r,$$

where d_i, r are integers. There is a decomposition in which each d_i divides the next and one in which each d_i is a prime power. □

This classification of abelian groups carries over to Euclidean domains without essential change. Since a Euclidean domain R is noetherian, any finitely generated R-module V has a presentation matrix (5.6), and by the diagonalization theorem (4.6) there is a presentation matrix A which is diagonal.

To carry along the analogy with abelian groups, we define a *cyclic R-module* V to be one which is generated by a single element v. This is equivalent with saying that V is isomorphic to a quotient module R/I, where I is the ideal of R elements α such that $\alpha v = 0$. Namely, the map $\varphi: R \longrightarrow V$ sending $r \rightsquigarrow rv$ is a surjective homomorphism of modules because v generates V, and the kernel of φ, the module of relations, is a submodule of R, an ideal I (1.3). So V is isomorphic to R/I by the First Isomorphism Theorem. Conversely, if $R/I \longrightarrow V$ is an isomorphism, the image of 1 will generate V. If R is a Euclidean domain, then the ideal I will be principal, so V will be isomorphic to $R/(\alpha)$ for some $\alpha \in R$. In this case the module of relations will also be generated by a single element.

Proceeding as in the case of abelian groups, one proves the following theorem:

(6.13) **Theorem.** *Structure Theorem for modules over Euclidean domains:*

(a) Let V be a finitely generated module over a Euclidean domain R. Then V is a direct sum of cyclic modules C_j and a free module L. Equivalently, there is an isomorphism

$$\varphi: V \longrightarrow R/(d_1) \times \cdots \times R/(d_k) \times R^r$$

of V with a direct product of cyclic modules $R/(d_i)$ and a free module R^r, where r is nonnegative, the elements $d_1, \ldots d_k$ are not units and not zero, and d_i divides d_{i+1} for each $i = 1, \ldots, k - 1$.

(b) The same assertion as (*a*), except that the condition that d_i divides d_{i+1} is replaced by this: Each d_i is a power of a prime element of R. Thus V is isomorphic to a product of the form

$$R/(p_1{}^{e_1}) \times \cdots \times R/(p_n{}^{e_n}) \times R^r,$$

with repetitions of primes allowed. □

For example, consider the $F[t]$-*module* V presented by the matrix A of Example (4.7). According to (5.12), it is also presented by the diagonal matrix

$$A' = \begin{bmatrix} 1 & \\ & (t-1)^2(t-2) \end{bmatrix},$$

and we can drop the first row and column from this matrix (5.12). So V is presented by the 1×1 matrix $[g]$, where $g(t) = (t-1)^2(t-2)$. This means that V is a cyclic module, isomorphic to $F[t]/(g)$. Since g has two relatively prime factors, V can be further decomposed. It is isomorphic to the direct product of two cyclic modules

$$(6.14) \qquad V \approx F[t]/(g) \approx [F[t]/(t-1)^2] \times [F[t]/(t-2)]. \ \square$$

With slightly more work, Theorem (6.13) can be extended to modules over any principal ideal domain. It is also true that the prime powers occurring in (b) are unique up to unit factors. A substitute for the counting argument which proves Theorem (6.9) must be found to prove this fact. We will not carry out the proof.

7. APPLICATION TO LINEAR OPERATORS

In this section we apply the theory developed in the last section in a novel way to linear operators on vector spaces over a field. This application provides a good example of the way "proof analysis" can lead to new results in mathematics. The method developed first for abelian groups is extended formally to modules over Euclidean domains. Then it is applied to a concrete new situation in which the ring is a polynomial ring. This was not the historical development. The theories for abelian groups and for linear operators were developed independently and were tied together later. But it is striking that the two cases, abelian groups and linear operators, can be formally analogous and yet end up looking so different when the same theory is applied to them.

The key observation which allows us to proceed is that if we are given a linear operator

$$(7.1) \qquad T: V \longrightarrow V$$

on a vector space over a field F, then we can use this operator to make V into a module over the polynomial ring $F[t]$. To do so, we have to define multiplication of a vector v by a polynomial $f(t) = a_nt^n + \cdots + a_1t + a_0$. We set

$$(7.2) \qquad f(t)v = a_nT^n(v) + a_{n-1}T^{n-1}(v) + \cdots + a_1T(v) + a_0v.$$

The right side can be written as $[f(T)](v)$, where $f(T)$ denotes the linear operator $a_nT^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0I$ obtained by substituting T for t. The brackets have been added only for clarity. With this notation, we obtain the formulas

$$(7.3) \qquad tv = T(v) \quad \text{and} \quad f(t)v = [f(T)](v).$$

The fact that rule (7.2) makes V into an $F[t]$-module is easy to verify. The formulas (7.3) may appear tautological. They raise the question of why we need a new symbol t. But remember that $f(t)$ is a formal polynomial, while $f(T)$ denotes a certain linear operator.

Conversely, let V be an $F[t]$-module. Then scalar multiplication of elements of V by a polynomial $f(t)$ is defined. In particular, we are given a rule for multiplying by the constant polynomials, the elements of F. If we keep the rule for multiplying by constants but forget for the moment about multiplication by nonconstant polynomials, then the axioms (1.1) show that V becomes a vector space over F. Next, we can multiply elements of V by the polynomial t. Let us denote the operation of multiplication by t on V as T. Thus T is the map

$$(7.4) \qquad T\colon V \longrightarrow V, \quad \text{defined by } T(v) = tv.$$

This map is a *linear operator* on V, when it is considered as a vector space over F. For $t(v + v') = tv + tv'$ by the distributive law (1.1), and hence $T(v + v') = T(v) + T(v')$. And if $c \in F$, then $tcv = ctv$ by the associative law (1.1) and the commutative law in $F[t]$; hence $T(cv) = cT(v)$. So an $F[t]$-module V provides us with a linear operator on a vector space.

The operations we have described, going from linear operators to modules and back, are inverses of each other:

(7.5) *Linear operator on an F-vector space and $F[t]$-module are equivalent concepts.*

We will want to apply this observation to finite-dimensional vector spaces, but let us note in passing the linear operator which corresponds to the free $F[t]$-module $F[t]$ of rank 1. We know that $F[t]$ is infinite-dimensional when it is considered as a vector space over F. The monomials $(1, t, t^2, \ldots)$ form a basis, and we can use this basis to identify $F[t]$ with the space Z of infinite F-vectors, as in Chapter 10 (2.8):

$$Z = \{(a_0, a_1, a_2, \ldots) \mid a_i \in F \text{ and only finitely many } a_i \text{ are nonzero}\}.$$

Multiplication by t on $F[t]$ corresponds to the *shift operator* T:

$$(a_0, a_1, a_2, \ldots) \rightsquigarrow (0, a_0, a_1, a_2, \ldots).$$

Thus, up to isomorphism, the free $F[t]$-module of rank 1 corresponds to the shift operator on the space Z.

We now begin our application to linear operators. Given a linear operator T on a vector space V over F, we may also view V as an $F[t]$-module. Let us suppose that V is finite-dimensional as a vector space, say of dimension n. Then it is certainly finitely generated as a module, and hence it has a presentation matrix. There is some danger of confusion here because there are two matrices around: the presentation matrix for the module V, and the matrix of the linear operator T. The presentation matrix is an $r \times s$ matrix with polynomial entries, where r is the number of chosen generators for the module and s is the number of relations. On the other hand, the matrix of the linear operator is an $n \times n$ matrix whose entries are scalars, where n is the dimension of V as a vector space. Both matrices contain the information needed to describe the module and the linear operator.

Regarding V as an $F[t]$-module, we can apply Theorem (6.13) to conclude that V is a direct sum of cyclic submodules, say

$$V = W_1 \oplus \cdots \oplus W_k,$$

where W_i is isomorphic to $F[t]/(p_i^{e_i})$, $p_i(t)$ being an irreducible polynomial in $F[t]$. There is no free summand, because we are assuming that V is finite-dimensional.

We have two tasks: to interpret the meaning of the direct sum decomposition for the linear operator T, and to describe the linear operator when the module is cyclic. It will not be surprising that the direct sum decomposition gives us a block decomposition of the matrix of T, when a suitable basis is chosen. The reason is that each of the subspaces W_i is T-invariant, because W_i is an $F[t]$-submodule. Multiplication by t carries W_i to itself, and t operates on V as the linear operator T. We choose bases $\mathbf{B}_i$ for the subspaces W_i. Then the matrix of T with respect to the basis $\mathbf{B} = (\mathbf{B}_1, \ldots, \mathbf{B}_k)$ has the desired block form [Chapter 4 (3.8)].

Next, let W be a cyclic $F[t]$-module. Then W is generated as a *module* by a single element w; in other words, every element of W can be written in the form

$$g(t)w = b_r t^r w + \cdots + b_1 t w + b_0 w,$$

where $g(t) = b_r t^r + \cdots + b_1 t + b_0 \in F[t]$. This implies that the elements $w, tw, t^2 w, \ldots$ span W as a vector space. In terms of the linear operator, W is spanned by the vectors $w, T(w), T^2(w), \ldots$.

Various relations between properties of an $F[t]$-module and the corresponding linear operator are summed up in the table below.

(7.6) **Dictionary.**

multiplication by t	operation of T
free module of rank 1	shift operator
cyclic module generated by v	vector space spanned by $v, T(v), T^2(v), \ldots$
submodule	T-invariant subspace
direct sum of submodules	direct sum of T-invariant subspaces
$F[t]$-module	*Linear operator T*

Let us now compute the matrix of a linear operator T on a vector space which corresponds to a cyclic $F[t]$-module. Since every ideal of $F[t]$ is principal, such a module will be isomorphic to a module of the form

$$W = F[t]/(f), \tag{7.7}$$

where $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ is a polynomial in $F[t]$. Let us use the symbol w_0 to denote the residue of 1 in W. This is our chosen generator for the module. Then the relation $fw_0 = 0$ holds, and f generates the module of relations.

The elements $w_0, tw_0, \ldots, t^{n-1}w_0$ form a basis for $F[t]/(f)$ [see Chapter 10 (5.7)]. Let us denote this basis by $w_i = t^i w_0$. Then

$$tw_0 = w_1, \quad tw_1 = w_2, \ldots, \quad tw_{n-2} = w_{n-1},$$

and also $fw_0 = 0$. This last relation can be rewritten using the others in order to determine the action of t on w_{n-1}:

$$(t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0)w_0 = tw_{n-1} + a_{n-1}w_{n-1} + \cdots + a_1 w_1 + a_0 w_0 = 0.$$

Since T acts as multiplication by t, we have

$$T(w_0) = w_1, \quad T(w_1) = w_2, \ldots, \quad T(w_{n-2}) = w_{n-1},$$

and

$$T(w_{n-1}) = -a_{n-1}w_{n-1} - \cdots - a_1 w_1 - a_0 w_0.$$

This determines the matrix of T. It has the form illustrated below for various values of n:

$$(7.8) \qquad [-a_0], \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{bmatrix}, \ldots, \begin{bmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & \vdots \\ & & \ddots & \ddots & \vdots \\ & & & \cdot\; 0 & \vdots \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

(7.9) **Theorem.** Let T be a linear operator on a finite-dimensional vector space V over a field F. There is a basis for V with respect to which the matrix of T is made up of blocks of the type (7.8). □

Such a form for the matrix of a linear operator is called a *rational canonical form*. It isn't particularly nice, but it is the best form available for an arbitrary field.

For example, the module (6.14) is a direct sum of two modules. Its rational canonical form is

$$(7.10) \qquad \left[\begin{array}{cc|c} & -1 & \\ 1 & 2 & \\ \hline & & 2 \end{array}\right].$$

We now consider more carefully the case that F is the field of complex numbers. Every irreducible polynomial in $\mathbb{C}[t]$ is linear, $p(t) = t - \alpha$, so according to Theorem (6.12), every finite-dimensional $\mathbb{C}[t]$-module is a direct sum of submodules isomorphic to ones of the form

$$(7.11) \qquad W = \mathbb{C}[t]/(t - \alpha)^n.$$

We let w_0 denote the residue of 1 in W as before, but we make a different choice of basis for W this time, setting $w_i = (t-\alpha)^i w_0$. Then

$$(t-\alpha)w_0 = w_1, \quad (t-\alpha)w_1 = w_2, \ldots, \quad (t-\alpha)w_{n-2} = w_{n-1}, \quad \text{and } (t-\alpha)w_{n-1} = 0.$$

We replace t by T and solve, obtaining

$$Tw_i = w_{i+1} + \alpha w_i,$$

for $i = 0, \ldots, n - 2$, and

$$Tw_{n-1} = \alpha w_{n-1}.$$

The matrix of T has the form

$$(7.12)\qquad [\alpha], \begin{bmatrix} \alpha & 0 \\ 1 & \alpha \end{bmatrix}, \begin{bmatrix} \alpha & 0 & 0 \\ 1 & \alpha & 0 \\ 0 & 1 & \alpha \end{bmatrix}, \ldots, \begin{bmatrix} \alpha & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \alpha \end{bmatrix}.$$

These matrices are called *Jordan blocks*. Thus we obtain the following theorem:

(7.13) **Theorem.** Let $T: V \longrightarrow V$ be a linear operator on a finite-dimensional complex vector space. There is a basis of V such that the matrix of T with respect to this basis is made up of Jordan blocks. □

Such a matrix is said to be in *Jordan form*, or to be a *Jordan matrix*. Note that it is lower triangular, so the diagonal entries are its eigenvalues. Jordan form is much nicer than rational canonical form.

It is not hard to show that every Jordan block has a unique eigenvector.

Given any square complex matrix A, the theorem asserts that PAP^{-1} is in Jordan form for some invertible matrix P. We often refer to PAP^{-1} as "the Jordan form for A." It is unique up to permutation of the blocks, because the terms in the direct sum decomposition are unique, though we have not proved this.

The Jordan form of the module (6.14) is made up of two Jordan blocks:

$$(7.14)\qquad \left[\begin{array}{cc|c} 1 & & \\ 1 & 1 & \\ \hline & & 2 \end{array}\right].$$

One important application of Jordan form is to the explicit solution of systems of a first-order linear differential equation

$$(7.15)\qquad \frac{dX}{dt} = AX.$$

As we saw in Chapter 4 (7.11), the problem of solving this equation reduces easily to solving the equation $\dfrac{dX}{dt} = \tilde{A}X$, where $\tilde{A} = PAP^{-1}$ is any similar matrix. So provided that we can determine the Jordan form $\tilde{A}$ of the given matrix A, it is enough to solve the resulting system. This in turn reduces to the case of a single Jordan block. One example of a 2 × 2 Jordan block was computed in Chapter 4 (8.18).

The solutions for an arbitrary $k \times k$ Jordan block A can be determined by computing the matrix exponential. We denote by N the $k \times k$ matrix obtained by substituting $\alpha = 0$ into (7.12). Then $N^k = 0$. Hence

$$e^{Nt} = I + Nt/1! + \cdots + N^{k-1}t^{k-1}/(k-1)!.$$

This is a lower triangular matrix which is constant on diagonal bands and whose entries on the ith diagonal band below the diagonal are $t^i/i!$. Since N and αI

commute,

$$e^{At} = e^{\alpha t}e^{Nt} = e^{\alpha t}(I + Nt/1! + \cdots + N^{k-1}t^{k-1}/(k-1)!).$$

Thus if A is the matrix

$$A = \begin{bmatrix} 3 & & \\ 1 & 3 & \\ & 1 & 3 \end{bmatrix},$$

then

$$e^{At} = \begin{bmatrix} e^{3t} & & \\ & e^{3t} & \\ & & e^{3t} \end{bmatrix}\begin{bmatrix} 1 & & \\ t & 1 & \\ \frac{1}{2}t^2 & t & 1 \end{bmatrix} = \begin{bmatrix} e^{3t} & & \\ te^{3t} & e^{3t} & \\ \frac{1}{2}t^2e^{3t} & te^{3t} & e^{3t} \end{bmatrix}.$$

Theorem (8.14) of Chapter 4 tells us that the columns of this matrix form a basis for the space of solutions of the differential equation (7.15).

Computing the Jordan form of a given matrix requires finding the roots of its characteristic polynomial $p(t)$. If the roots $\alpha_1, \ldots, \alpha_n$ are distinct, the Jordan form is diagonal:

$$\begin{bmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_k \end{bmatrix}.$$

Suppose that the root $\alpha_1 = \alpha$ is an r-fold root of $p(t)$. Then there are various possibilities for the part of the Jordan matrix with diagonal entries α. Here are the possibilities for small r:

$$r = 1\colon [\alpha]; \quad r = 2\colon \begin{bmatrix} \alpha & \\ 1 & \alpha \end{bmatrix}, \left[\begin{array}{c|c} \alpha & \\ \hline & \alpha \end{array}\right];$$

$$r = 3\colon \begin{bmatrix} \alpha & & \\ 1 & \alpha & \\ & 1 & \alpha \end{bmatrix}, \left[\begin{array}{cc|c} \alpha & & \\ 1 & \alpha & \\ \hline & & \alpha \end{array}\right], \left[\begin{array}{c|c|c} \alpha & & \\ \hline & \alpha & \\ \hline & & \alpha \end{array}\right];$$

$$r = 4\colon \begin{bmatrix} \alpha & & & \\ 1 & \alpha & & \\ & 1 & \alpha & \\ & & 1 & \alpha \end{bmatrix}, \left[\begin{array}{ccc|c} \alpha & & & \\ 1 & \alpha & & \\ & 1 & \alpha & \\ \hline & & & \alpha \end{array}\right], \left[\begin{array}{cc|cc} \alpha & & & \\ 1 & \alpha & & \\ \hline & & \alpha & \\ & & 1 & \alpha \end{array}\right], \left[\begin{array}{cc|c|c} \alpha & & & \\ 1 & \alpha & & \\ \hline & & \alpha & \\ \hline & & & \alpha \end{array}\right],$$

$$\left[\begin{array}{c|c|c|c} \alpha & & & \\ \hline & \alpha & & \\ \hline & & \alpha & \\ \hline & & & \alpha \end{array}\right].$$

They can be distinguished by computing eigenvectors of certain operators related to T. The space of solutions to the system of equations

$$(A - \alpha I)x = 0$$

is the space of eigenvectors of A with eigenvalue α. One can solve this system explicitly, given A and α. If $r = 4$, the dimensions of the solution space in the five cases shown above are $1, 2, 2, 3, 4$ respectively, because one eigenvector is associated to each block. So this dimension distinguishes all cases except the second and third. These remaining two cases can be distinguished by the matrix $(A - \alpha I)^2$. It is zero in case three and not zero in case two.

It can be shown that the dimensions of the null spaces of the operators $(A - \alpha I)^\nu$, $\nu = 1, 2, \ldots, r/2$, distinguish the Jordan forms in all cases.

8. FREE MODULES OVER POLYNOMIAL RINGS

The structures of modules over a ring become increasingly complicated with increasing complication of the ring. It is even difficult to determine whether or not an explicitly presented module is free. In this section we describe, without proof, a theorem which characterizes free modules over polynomial rings. This theorem was proved by Quillen and Suslin in 1976.

Let $R = \mathbb{C}[x_1, \ldots, x_k]$ be the polynomial ring in k variables, and let V be a finitely generated R-module. We choose a presentation matrix A for the module. The entries of A will be polynomials $a_{ij}(x)$, and if A is an $m \times n$ matrix, then V is isomorphic to the cokernel R^m/AR^n of multiplication by A on R-vectors. We can evaluate the matrix entries $a_{ij}(x)$ at any point $p = (p_1, \ldots\, p_k)$ of $\mathbb{C}^k$, obtaining a complex matrix $A(p)$ whose i, j-entry is $a_{ij}(p)$.

(8.1) **Theorem.** Let V be a finitely generated module over the polynomial ring $\mathbb{C}[x_1, \ldots, x_k]$, and let A be an $m \times n$ presentation matrix for V. Denote by $A(p)$ the evaluation of A at a point $p \in \mathbb{C}^k$. Then V is a free module of rank r if and only if $A(p)$ has rank $m - r$ for every point p. □

The proof of this theorem requires background which we don't have. However, we can easily see how to use it to determine whether or not a given module is free. For example, consider the polynomial ring in two variables: $R = \mathbb{C}[x, y]$. Let V be the module presented by the 4×2 matrix

$$A = \begin{bmatrix} 1 & x \\ y & x+3 \\ x & y \\ x^2 & y^2 \end{bmatrix}. \tag{8.2}$$

So V has four generators and two relations. Let p be a point $(a, b) \in \mathbb{C}^2$. The two columns of the matrix A_p are

$$v_1 = (1, b, a, a^2)^t, \quad v_2 = (a, a+3, b, b^2)^t.$$

It is not hard to show that these two vectors are linearly independent for every choice of a, b, from which it follows that the rank of $A(p)$ is 2 for every point (a, b). For suppose that the vectors are dependent: $v_2 = cv_1$, or vice versa. Then the first coordinates show that $v_2 = av_1$, hence

$$a+3 = ab, \quad b = a^2, \quad b^2 = a^3. \tag{8.3}$$

These equations have no common solutions. By Theorem (8.1), V is a free module of rank 2.

We can get an intuitive understanding for this theorem by considering the vector space $V_p = \mathbb{C}^m/A(p)\,\mathbb{C}^n$ which is presented by the complex matrix $A(p)$. It is natural to think of this vector space as a kind of "evaluation of the module V at the point p," and it can be shown that V_p is essentially independent of the choice of the presentation matrix. Therefore we can use the module V to associate a vector space V_p to every point $p \in \mathbb{C}^k$. If we imagine moving the point p about, then the vector space V_p will vary in a continuous way, providing that its dimension does not jump around. This is because the matrix $A(p)$ presenting V_p depends continuously on p. Families of vector spaces of constant dimension, parametrized by a topological space, are called *vector bundles*. The module is free if and only if the family of vector spaces V_p forms a vector bundle.

> *"Par une déformation coutumière aux mathématiciens,*
> *je me'en tenais au point de vue trop restreint.*
>
> Jean-Louis Verdier

EXERCISES

1. The Definition of a Module

1. Let R be a ring, considered as an R-module. Determine all module homomorphisms $\varphi: R \longrightarrow R$.
2. Let W be a submodule of an R-module V. Prove that the additive inverse of an element of W is in W.
3. Let $\varphi: V \longrightarrow W$ be a homomorphism of modules over a ring R, and let V', W' be submodules of V, W respectively. Prove that $\varphi(V')$ is a submodule of W and that $\varphi^{-1}(W')$ is a submodule of V.
4. (a) Let V be an abelian group. Prove that if V has a structure of $\mathbb{Q}$-module with its given law of composition as addition, then this structure is uniquely determined.
   (b) Prove that no finite abelian group has a $\mathbb{Q}$-module structure.
5. Let $R = \mathbb{Z}[\alpha]$, where α is an algebraic integer. Prove that for any integer m, R/mR is finite, and determine its order.

6. A module is called *simple* if it is not the zero module and if it has no proper submodule.
   (a) Prove that any simple module is isomorphic to R/M, where M is a maximal ideal.
   (b) Prove *Schur's Lemma:* Let $\varphi: S \longrightarrow S'$ be a homomorphism of simple modules. Then either φ is zero, or else it is an isomorphism.
7. The *annihilator* of an R-module V is the set $I = \{r \in R \mid rV = 0\}$.
   (a) Prove that I is an ideal of R.
   (b) What is the annihilator of the $\mathbb{Z}$-module $\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4)$? of the $\mathbb{Z}$-module $\mathbb{Z}$?
8. Let R be a ring and V an R-module. Let E be the set of *endomorphisms* of V, meaning the set of homomorphisms from V to itself. Prove that E is a noncommutative ring, with composition of functions as multiplication and with addition defined by $[\varphi + \psi](m) = \varphi(m) + \psi(m)$.
9. Prove that the ring of endomorphisms of a simple module is a field.
10. Determine the ring of endomorphisms of the R-module (a) R and (b) R/I, where I is an ideal.
11. Let $W \subset V \subset U$ be R-modules.
    (a) Describe natural homomorphisms which relate the three quotient modules U/W, U/V, and V/W.
    (b) Prove the *Third Isomorphism Theorem:* $U/V \approx (U/W)/(V/W)$.
12. Let V, W be submodules of a module U.
    (a) Prove that $V \cap W$ and $V + W$ are submodules.
    (b) Prove the *Second Isomorphism Theorem:* $(V + W)/W$ is isomorphic to $V/(V \cap W)$.
13. Let V be an R-module, defined as in (1.1). If the ring R is not commutative, it is not a good idea to define $vr = rv$. Explain.

2. Matrices, Free Modules, and Bases

1. Let $R = \mathbb{C}[x, y]$, and let M be the ideal of R generated by the two elements (x, y). Prove or disprove: M is a free R-module.
2. Let A be an $n \times n$ matrix with coefficients in a ring R, let $\varphi: R^n \longrightarrow R^n$ be left multiplication by A, and let $d = \det A$. Prove or disprove: The image of φ is equal to dR^n.
3. Let I be an ideal of a ring R. Prove or disprove: If R/I is a free R-module, then $I = 0$.
4. Let R be a ring, and let V be a free R-module of finite rank. Prove or disprove:
   (a) Every set of generators contains a basis.
   (b) Every linearly independent set can be extended to a basis.
5. Let I be an ideal of a ring R. Prove that I is a free R-module if and only if it is a principal ideal, generated by an element α which is not a zero divisor in R.
6. Prove that a ring R such that every finitely generated R-module is free is either a field or the zero ring.
7. Let A be the matrix of a homomorphism $\varphi: \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ between free modules.
   (a) Prove that φ is injective if and only if the rank of A is n.
   (b) Prove that φ is surjective if and only if the greatest common divisor of the determinants of the $m \times m$ minors of A is 1.
8. Reconcile the definition of free abelian group given in Section 2 with that given in Chapter 6, Section 8.

3. The Principle of Permanence of Identities

1. In each case, decide whether or not the principle of permanence of identities allows the result to be carried over from the complex numbers to an arbitrary commutative ring.
   (a) the associative law for matrix multiplication
   (b) Cayley–Hamilton Theorem
   (c) Cramer's Rule
   (d) product rule, quotient rule, and chain rule for differentiation of polynomials
   (e) the fact that a polynomial of degree n has at most n roots
   (f) Taylor's expansion of a polynomial
2. Does the principle of permanence of identities show that $\det AB = \det A \det B$ when the entries of the matrices are in a noncommutative ring R?
3. In some cases, it may be convenient to verify an identity only for the real numbers. Does this suffice?
4. Let R be a ring, and let A be a 3×3 R-matrix in $SO_3(R)$, that is, such that $A^tA = I$ and $\det A = 1$. Does the principle of permanence of identities show that A has an eigenvector in R^3 with eigenvalue 1?

4. Diagonalization of Integer Matrices

1. Reduce each matrix below to diagonal form by integer row and column operations.
   (a) $\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}$ (b) $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ (c) $\begin{bmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{bmatrix}$
   (d) In the first case, let $V = \mathbb{Z}^2$ and let $L = AV$. Draw the sublattice L, and find commensurable bases of V and L.
2. Let A be a matrix whose entries are in the polynomial ring $F[t]$, and let A' be obtained from A by polynomial row and column operations. Relate $\det A$ to $\det A'$.
3. Determine integer matrices P^{-1}, Q which diagonalize the matrix $A = \begin{bmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{bmatrix}$.
4. Let $d_1, d_2, \ldots$ be the integers referred to in Theorem (4.3).
   (a) Prove that d_1 is the greatest common divisor of the entries a_{ij} of A.
   (b) Prove that $d_1 d_2$ is the greatest common divisor of the determinants of the 2×2 minors of A.
   (c) State and prove an extension of (a) and (b) to d_i for arbitrary i.
5. Determine all integer solutions to the system of equations $AX = 0$, when $A = \begin{bmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{bmatrix}$.
6. Find a basis for the following submodules of $\mathbb{Z}^3$.
   (a) The module generated by $(1,0,-1)$, $(2,-3,1)$, $(0,3,1)$, $(3,1,5)$.
   (b) The module of solutions of the system of equations $x + 2y + 3z = 0$, $x + 4y + 9z = 0$.
7. Prove that the two matrices $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ and $\begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$ generate the group $SL_2(\mathbb{Z})$ of integer matrices with determinant 1.

8. Prove that the group $SL_n(\mathbb{Z})$ is generated by elementary integer matrices of the first type.

9. Let α, β, γ be complex numbers, and let $A = \{\ell\alpha + m\beta + n\gamma \mid \ell, m, n, \in \mathbb{Z}\}$ be the subgroup of $\mathbb{C}^+$ they generate. Under what conditions is A a lattice in $\mathbb{C}$?

10. Let $\varphi\colon \mathbb{Z}^k \longrightarrow \mathbb{Z}^k$ be a homomorphism given by multiplication by an integer matrix A. Show that the image of φ is of finite index if and only if A is nonsingular and that if so, then the index is equal to $|\det A|$.

11. **(a)** Let $A = (a_1, \ldots, a_n)^t$ be an integer column vector. Use row reduction to prove that there is a matrix $P \in GL_n(\mathbb{Z})$ such that $PA = (d, 0, \ldots, 0)^t$, where d is the greatest common divisor of $a_1, \ldots, a_n$.

(b) Prove that if $d = 1$, then A is the first column of a matrix of $M \in SL_n(\mathbb{Z})$.

5. Generators and Relations for Modules

1. In each case, identify the abelian group which has the given presentation matrix:

$$\begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}0\\5\end{bmatrix}, [2 \quad 0 \quad 0], \begin{bmatrix}1 & \\ 1 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & 1\\0 & 0\end{bmatrix}, \begin{bmatrix}2 & 3\\1 & 2\end{bmatrix}, \begin{bmatrix}2 & 4\\1 & 4\end{bmatrix}, \begin{bmatrix}4 & 6\\2 & 3\end{bmatrix}.$$

2. Find a ring R and an ideal I of R which is not finitely generated.

3. Prove that existence of factorizations holds in a noetherian integral domain.

4. Let $V \subset \mathbb{C}^n$ be the locus of zeros of an infinite set of polynomials $f_1, f_2, f_3, \ldots$. Prove that there is a finite subset of these polynomials whose zeros define the same locus.

5. Let S be a subset of $\mathbb{C}^n$. Prove that there is a finite set of polynomials $(f_1, \ldots, f_k)$ such that any polynomial which vanishes identically on S is a linear combination of this set, with polynomial coefficients.

6. Determine a presentation matrix for the ideal $(2, 1 + \delta)$ of $\mathbb{Z}[\delta]$, where $\delta = \sqrt{-5}$.

***7.** Let S be a subring of the ring $R = \mathbb{C}[t]$ which contains $\mathbb{C}$ and is not equal to $\mathbb{C}$. Prove that R is a finitely generated S-module.

8. Let A be the presentation matrix of a module V with respect to a set of generators $(v_1, \ldots, v_m)$. Let $(w_1, \ldots, w_r)$ be another set of elements of V, and write the elements in terms of the generators, say $w_i = \Sigma p_{ij} v_j$, $p_{ij} \in R$. Let $P = (p_{ij})$. Prove that the block matrix $\left[\begin{array}{c|c} A & -P \\ \hline 0 & I \end{array}\right]$ is a presentation matrix for V with respect to the set of generators $(v_1, \ldots, v_m; w_1, \ldots, w_r)$.

***9.** With the notation of the previous problem, suppose that $(w_1, \ldots, w_r)$ is also a set of generators of V and that B is a presentation matrix for V with respect to this set of generators. Say that $v_i = \Sigma q_{ij} w_j$ is an expression of the generators v_i in terms of the w_j.

(a) Prove that the block matrix $M = \left[\begin{array}{c|c|c|c} A & -P & I & 0 \\ \hline 0 & I & -Q & B \end{array}\right]$ presents V with respect to the generators $(v_1, \ldots, v_m; w_1, \ldots, w_r)$.

(b) Show that M can be reduced to A and to B by a sequence of operations of the form (5.12).

10. Using 9, show that any presentation matrix of a module can be transformed to any other by a sequence of operations (5.12) and their inverses.

6. The Structure Theorem for Abelian Groups

1. Find a direct sum of cyclic groups which is isomorphic to the abelian group presented by the matrix $\begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix}$.
2. Write the group generated by x, y, with the relation $3x + 4y = 0$ as a direct sum of cyclic groups.
3. Find an isomorphic direct product of cyclic groups, when V is the abelian group generated by x, y, z, with the given relations.
   (a) $3x + 2y + 8z = 0,\ 2x + 4z = 0$
   (b) $x + y = 0,\ 2x = 0,\ 4x + 2z = 0,\ 4x + 2y + 2z = 0$
   (c) $2x + y = 0,\ x - y + 3z = 0$
   (d) $2x - 4y = 0, \quad 2x + 2y + z = 0$
   (e) $7x + 5y + 2z = 0,\ 3x + 3y = 0,\ 13x + 11y + 2z = 0$
4. Determine the number of isomorphism classes of abelian groups of order 400.
5. Classify finitely generated modules over each ring.
   (a) $\mathbb{Z}/(4)$ (b) $\mathbb{Z}/(6)$ (c) $\mathbb{Z}/n\mathbb{Z}$.
6. Let R be a ring, and let V be an R-module, presented by a diagonal $m \times n$ matrix A: $V \approx R^m/AR^n$. Let $(v_1, \ldots, v_m)$ be the corresponding generators of V, and let d_i be the diagonal entries of A. Prove that V is isomorphic to a direct product of the modules $R/(d_i)$.
7. Let V be the $\mathbb{Z}[i]$-module generated by elements v_1, v_2 with relations $(1 + i)v_1 + (2 - i)v_2 = 0, \quad 3v_1 + 5iv_2 = 0$. Write this module as a direct sum of cyclic modules.
8. Let $W_1, \ldots, W_k$ be submodules of an R-module V such that $V = \Sigma W_i$. Assume that $W_1 \cap W_2 = 0,\ (W_1 + W_2) \cap W_3 = 0, \ldots, (W_1 + W_2 + \cdots + W_{k-1}) \cap W_k = 0$. Prove that V is the direct sum of the modules $W_1, \ldots, W_k$.
9. Prove the following.
   (a) The number of elements of $\mathbb{Z}/(p^e)$ whose order divides p^ν is p^ν if $\nu \leq e$, and is p^e if $\nu \geq e$.
   (b) Let $W_1, \ldots, W_k$ be finite abelian groups, and let u_j denote the number of elements of W_j whose order divides a given integer q. Then the number of elements of the product group $V = W_1 \times \cdots \times W_k$ whose order divides q is $u_1 \cdots u_k$.
   (c) With the above notation, assume that W_j is a cyclic group of prime power order $d_j = p^{e_j}$. Let r_1 be the number of d_j equal to a given prime p, let r_2 be the number of d_j equal to p^2, and so on. Then the number of elements of V whose order divides p^ν is p^{s_ν}, where $s_1 = r_1 + \cdots + r_k$, $s_2 = r_1 + 2r_2 + \cdots + 2r_k$, $s_3 = r_1 + 2r_2 + 3r_3 + \cdots + 3r_k$, and so on.
   (d) Theorem (6.9).

7. Application to Linear Operators

1. Let T be a linear operator whose matrix is $\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$. Is the corresponding $\mathbb{C}[t]$-module cyclic?

2. Determine the Jordan form of the matrix $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$.

3. Prove that $\begin{bmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 1 \end{bmatrix}$ is an idempotent matrix, and find its Jordan form.

4. Let V be a complex vector space of dimension 5, and let T be a linear operator on V which has characteristic polynomial $(t - \alpha)^5$. Suppose that the rank of the operator $T - \alpha I$ is 2. What are the possible Jordan forms for T?

5. Find all possible Jordan forms for a matrix whose characteristic polynomial is $(t + 2)^2(t - 5)^3$.

6. What is the Jordan form of a matrix whose characteristic polynomial is $(t - 2)^2(t - 5)^3$ and such that the space of eigenvectors with eigenvalue 2 is one-dimensional, while the space of eigenvectors with eigenvalue 5 is two-dimensional?

7. **(a)** Prove that a Jordan block has a one-dimensional space of eigenvectors.
   (b) Prove that, conversely, if the eigenvectors of a complex matrix A are multiples of a single vector, then the Jordan form for A consists of one block.

8. Determine all invariant subspaces of a linear operator whose Jordan form consists of one block.

9. In each case, solve the differential equation $dX/dt = AX$ when A is the Jordan block given.

   (a) $\begin{bmatrix} 2 & \\ 1 & 2 \end{bmatrix}$ **(b)** $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ **(c)** $\begin{bmatrix} 1 & & \\ 1 & 1 & \\ & 1 & 1 \end{bmatrix}$

10. Solve the differential equation $dX/dt = AX$ when A is **(a)** the matrix (7.14), **(b)** the matrix (7.10), **(c)** the matrix of problem 2, **(d)** the matrix of problem 3.

11. Prove or disprove: Two complex $n \times n$ matrices A, B are similar if and only if they have the same Jordan form.

12. Show that every complex $n \times n$ matrix is similar to a matrix of the form $D + N$, where D is diagonal, N is nilpotent, and $DN = ND$.

13. Let $R = F[x]$ be the polynomial ring in one variable over a field F, and let V be the R-module generated by an element v which satisfies the relation $(x^3 + 3x + 2)v = 0$. Choose a basis for V as F-vector space, and find the matrix of the operator multiplication by t with respect to this basis.

14. Let V be an $F[t]$-module, and let $\mathbf{B} = (v_1, \ldots, v_n)$ be a basis for V, as F-vector space. Let B be the matrix of T with respect to this basis. Prove that $A = tI - B$ is a presentation matrix for the module.

15. Let $p(t)$ be a polynomial over a field F. Prove that there exists an $n \times n$ matrix with entries in F whose characteristic polynomial is $p(t)$.

16. Prove or disprove: A complex matrix A such that $A^2 = A$ is diagonalizable.

17. Let A be a complex $n \times n$ matrix such that $A^k = I$ for some n. Prove that the Jordan form for A is diagonal.

18. Prove the Cayley–Hamilton Theorem, that if $p(t)$ is the characteristic polynomial of an $n \times n$ matrix A, then $p(A) = 0$.

19. The *minimal polynomial* $m(t)$ of a linear operator T on a complex vector space V is the polynomial of lowest degree such that $m(T) = 0$.

(a) Prove that the minimal polynomial divides the characteristic polynomial.

(b) Prove that every root of the characteristic polynomial $p(t)$ is also a root of the minimal polynomial $m(t)$.

(c) Prove that T is diagonalizable if and only if $m(t)$ has no multiple root.

20. Find all possible Jordan forms for 8×8 matrices whose minimal polynomial is $x^2(x-1)^3$.

21. Prove or disprove: A complex matrix A is similar to its transpose.

22. Classify linear operators on a finitely generated $F[t]$-module, dropping the assumption that the module is finite-dimensional as a vector space.

23. Prove that the ranks of $(A - \alpha I)^\nu$ distinguish all Jordan forms, and hence that the Jordan form depends only on the operator and not on the basis.

24. Show that the following concepts are equivalent:

(i) R-module, where $R = \mathbb{Z}[i]$;

(ii) abelian group V, together with a homomorphism φ: $V \longrightarrow V$ such that $\varphi \circ \varphi = -\text{identity}$.

25. Let $F = \mathbb{F}_p$. For which prime integers p does the additive group F^1 have a structure of $\mathbb{Z}[i]$-module? How about F^2?

26. Classify finitely generated modules over the ring $\mathbb{C}[\epsilon]$, where $\epsilon^2 = 0$.

8. Free Modules over Polynomial Rings

1. Determine whether or not the modules over $\mathbb{C}[x,y]$ presented by the following matrices are free.

(a) $\begin{bmatrix} x^2+1 & x \\ x^2y+x+y & xy+1 \end{bmatrix}$ (b) $\begin{bmatrix} xy-1 \\ x^2-y^2 \\ y \end{bmatrix}$ (c) $\begin{bmatrix} x-1 & x \\ y & y+1 \\ x & y \\ x^2 & 2y \end{bmatrix}$

2. Prove that the module presented by (8.2) is free by exhibiting a basis.

3. Following the model of the polynomial ring in one variable, describe modules over the ring $\mathbb{C}[x,y]$ in terms of real vector spaces with additional structure.

4. Let R be a ring and V an R-module. Let I be an ideal of R, and let IV be the set of finite sums $\Sigma s_i v_i$, where $s_i \in I$ and $v_i \in V$.

(a) Show how to make V/IV into an R/I-module.

(b) Let A be a presentation matrix for V, and let $\bar{A}$ denote its residue in R/I. Prove that $\bar{A}$ is a presentation matrix for V/IV.

(c) Show why the module V_p defined in the text is essentially independent of the presentation matrix.

***5.** Using exercise 9 of Section 5, prove the easy half of the theorem of Quillen and Suslin: If V is free, then the rank of $A(p)$ is constant.

6. Let $R = \mathbb{Z}[\sqrt{-5}]$, and let V be the module presented by the matrix $A = \begin{bmatrix} 2 \\ 1+\delta \end{bmatrix}$.

(a) Prove that the residue of A has rank 1 for every prime ideal P of R.

(b) Prove that V is not free.

Miscellaneous Problems

1. Let G be a lattice group, and let g be a rotation in G. Let $\overline{g}$ be the associated element of the point group $\overline{G}$. Prove that there is a basis for $\mathbb{R}^2$, not necessarily an orthonormal basis, such that the matrix of $\overline{g}$ with respect to this basis is in $GL_2(\mathbb{Z})$.

***2.** (a) Let α be a complex number, and let $\mathbb{Z}[\alpha]$ be the subring of $\mathbb{C}$ generated by α. Prove that α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a finitely generated abelian group.

(b) Prove that if α, β are algebraic integers, then the subring $\mathbb{Z}[\alpha, \beta]$ of $\mathbb{C}$ which they generate is a finitely generated abelian group.

(c) Prove that the algebraic integers form a subring of $\mathbb{C}$.

***3.** *Pick's Theorem:* Let Δ be the plane region bounded by a polygon whose vertices are at integer lattice points. Let I be the set of lattice points in the interior of Δ and B the set of lattice points on the boundary of Δ. If p is a lattice point, let $r(p)$ denote the fraction of 2π of the angle subtended by Δ at p. So $r(p) = 0$ if $p \notin \Delta$, $r(p) = 1$ if p is an interior point of Δ, $r(p) = \frac{1}{2}$ if p is on an edge, and so on.

(a) Prove that the area of Δ is $\sum_p r(p)$.

(b) Prove that the area is $|I| + \frac{1}{2}(|B| - 2)$ if Δ has a single connected boundary curve.

4. Prove that the integer orthogonal group $O_n(\mathbb{Z})$ is a finite group.

***5.** Consider the space $V = \mathbb{R}^k$ of column vectors as an inner product space, with the ordinary dot product $(v \cdot w) = v^t w$. Let L be a lattice in V, and define $L^* = \{w \mid (v \cdot w) \in \mathbb{Z} \text{ for all } v \in L\}$.

(a) Show that L^* is a lattice.

(b) Let $\mathbf{B} = (v_1, \ldots, v_k)$ be a lattice basis for L, and let $P = [\mathbf{B}]^{-1}$ be the matrix relating this basis of V to the standard basis $\mathbf{E}$. What is the matrix A of dot product with respect to the basis $\mathbf{B}$?

(c) Show that the columns of P form a lattice basis for L^*.

(d) Show that if A is an integer matrix, then $L \subset L^*$, and $[L^* : L] = |\det A|$.

6. Let V be a real vector space having a countably infinite basis $\{v_1, v_2, v_3, \ldots\}$, and let E be the ring of linear operators on V.

(a) Which infinite matrices represent linear operators on V?

(b) Describe how to compute the matrix of the composition of two linear operators in terms of the matrix of each of them.

(c) Consider the linear operators T, T' defined by the rules

$$T(v_{2n}) = v_n, \quad T(v_{2n-1}) = 0, \quad T'(v_{2n}) = 0, \quad T'(v_{2n-1}) = v_n, \quad n = 1, 2, 3, \ldots .$$

Write down their matrices.

(d) We can consider $E^1 = E$ as a module over the ring E, with scalar multiplication on the left side of a vector. Show that $\{T, T'\}$ is a basis of E^1 as E-module.

(e) Prove that the free E-modules E^k, $k = 1, 2, 3 \ldots$, are all isomorphic.

7. Prove that the group $\mathbb{Q}^+/\mathbb{Z}^+$ is not an infinite direct sum of cyclic groups.

8. Prove that the additive group $\mathbb{Q}^+$ of rational numbers is not a direct sum of two proper subgroups.

9. Prove that the multiplicative group $\mathbb{Q}^\times$ of rational numbers is isomorphic to the direct sum of a cyclic group of order 2 and a free abelian group with countably many generators.

10. Prove that two diagonalizable matrices are simultaneously diagonalizable, that is, that there is an invertible matrix P such that PAP^{-1} and PBP^{-1} are both diagonal, if and only if $AB = BA$.

***11.** Let A be a finite abelian group, and let $\varphi: A \longrightarrow \mathbb{C}^\times$ be a homomorphism which is not the trivial homomorphism ($\varphi(x) = 1$ for all x). Prove that $\sum_{a \in A} \varphi(a) = 0$.

12. Let A be an $m \times n$ matrix with coefficients in a ring R, and let $\varphi: R^n \longrightarrow R^m$ be left multiplication by A. Prove that the following are equivalent:

(i) φ is surjective;

(ii) the determinants of the $m \times m$ minors of A generate the unit ideal;

(iii) A has a right inverse, a matrix B with coefficients in R such that $AB = I$.

***13.** Let $(v_1, \ldots, v_m)$ be generators for an R-module V, and let J be an ideal of R. Define JV to be the set of all finite sums of products av, $a \in J$, $v \in V$.

(a) Show that if $JV = V$, there is an $n \times n$ matrix A with entries in J such that $(v_1, \ldots, v_m)(I - A) = 0$.

(b) With the notation of (a), show that $\det(I - A) = 1 + \alpha$, where $\alpha \in J$, and that $\det(I - A)$ annihilates V.

(c) An R-module V is called *faithful* if $rV = 0$ for $r \in R$ implies $r = 0$. Prove the *Nakayama Lemma:* Let V be a finitely generated, faithful R-module, and let J be an ideal of R. If $JV = V$, then $J = R$.

(d) Let V be a finitely generated R-module. Prove that if $MV = V$ for all maximal ideals M, then $V = 0$.

***14.** We can use a pair $x(t), y(t)$ of complex polynomials in t to define a complex path in $\mathbb{C}^2$, by sending $t \rightsquigarrow (x(t), y(t))$. They also define a homomorphism $\varphi: \mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$, by $f(x, y) \rightsquigarrow f(x(t), y(t))$. This exercise analyzes the relationship between the path and the homomorphism. Let's rule out the trivial case that $x(t), y(t)$ are both constant.

(a) Let S denote the image of φ. Prove that S is isomorphic to the quotient $\mathbb{C}[x, y]/(f)$, where $f(x, y)$ is an irreducible polynomial.

(b) Prove that t is the root of a monic polynomial with coefficients in S.

(c) Let V denote the variety of zeros of f in $\mathbb{C}^2$. Prove that for every point $(x_0, y_0) \in V$, there is a $t_0 \in \mathbb{C}$ such that $(x_0, y_0) = (x(t_0), y(t_0))$.