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

$$A' = QAP^{-1}, \tag{4.2}$$

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: $d_1 \mid d_2$, $d_2 \mid d_3, \ldots$.

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

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

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: $d_1 | d_2 | d_3 | \dots$. 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 $\varphi: V \longrightarrow W$ 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 $\varphi: V \longrightarrow W$ 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 $\varphi: \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ 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 $d_1x_1 = 0, \dots, d_nx_n = 0$, 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 $\varphi: \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$, 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 $e_1,\dots,e_n \in \mathbb{Z}^n$ to the columns

$$A_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \dots, A_n = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} \tag{4.10}$$

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 $A_1,\dots,A_n \in \mathbb{Z}^m$. 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 $(w_1,\dots,w_m)$ of W and a basis $(u_1,\dots,u_n)$ of S with the following properties: (i) $n \le m$, (ii) for each $j \le n$ there is a positive integer d_j such that $u_j = d_j w_j$, and (iii) $d_1 \mid d_2 \mid d_3 \dots$.

(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 $\mathbf{B} = (w_1,\dots,w_m)$ for W and a set of generators $(u_1,\dots u_n)$ 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 $\mathbf{B}' = (w_1',\dots,w_p')$ and new generating set $(u_1',\dots,u_n')$. 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 $n \le m$.

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 $(u_1,\dots,u_n)$ is a basis of S. Since it generates S, what has to be proved is that $(u_1,\dots,u_n)$ 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 $(w_1,\dots,w_m)$ 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

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

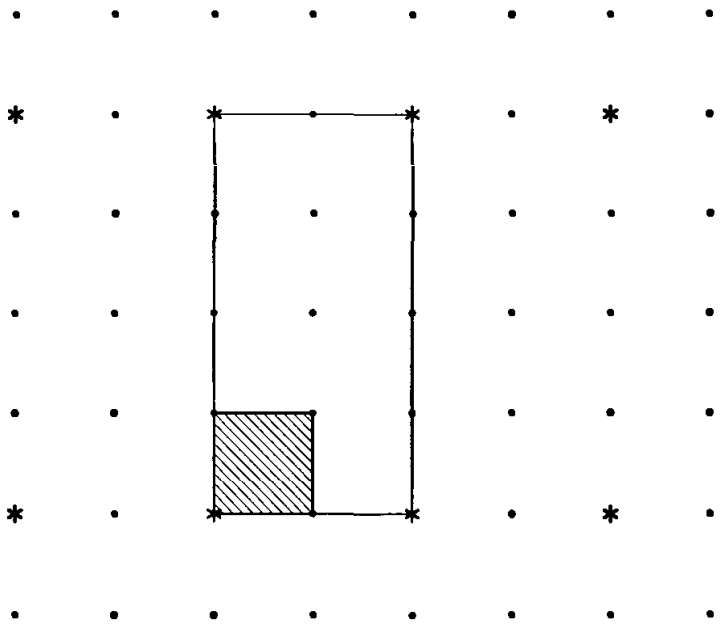
and we interpret it as follows: The columns of the matrix AP^{-1} form our new set of generators for S. Since the matrix A' is diagonal, (4.13) tells us that the new generators are multiples of the columns of Q^{-1}. We change the basis of $\mathbb{Z}^m$ from the standard basis to the basis made up of 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 $(u_1', u_2') = (u_1, u_2)P^{-1} = (w_1', 5w_2')$.

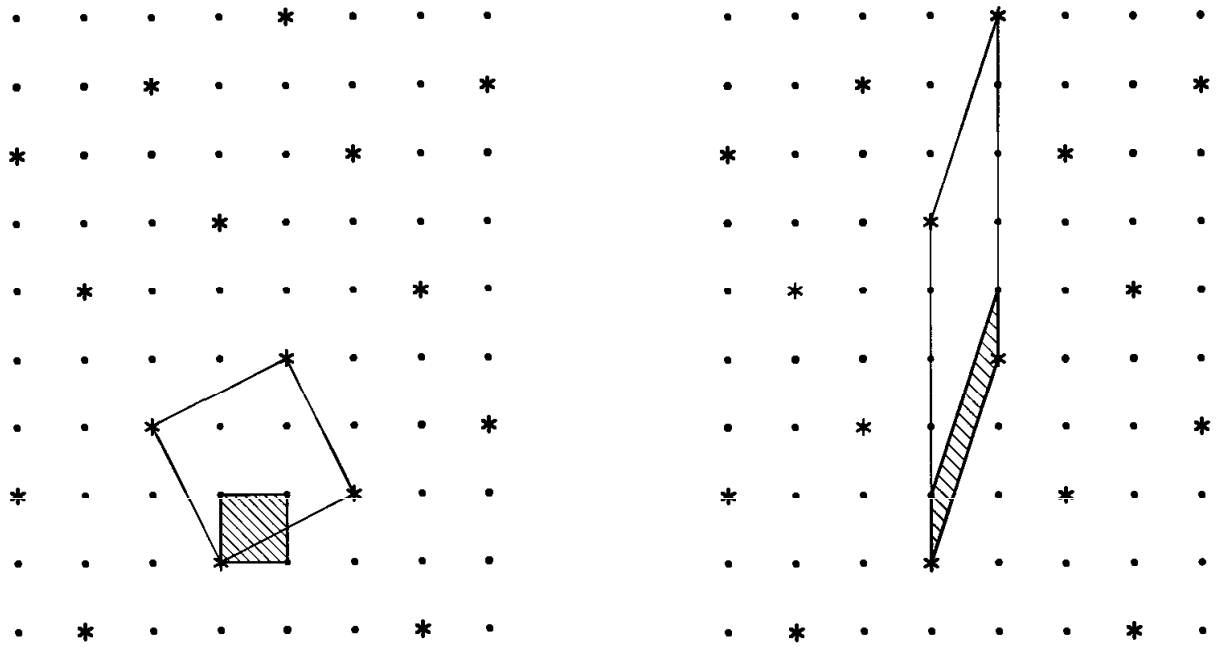
Theorem (4.3) is striking when it is used to describe the relative position of a sublattice S in a lattice L. To illustrate this, it will be enough to consider plane lattices. The theorem asserts that there are bases (v_1, v_2) and (w_1, w_2) of L and S such that the coordinate vectors of w_j with respect 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 the 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

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

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 $\varphi: W \longrightarrow W'$ of R-modules, called its *cokernel*. The cokernel of φ is defined to be the quotient module

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

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

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

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

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

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

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

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

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

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:

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

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 gen-

erating set $(v_1,\dots,v_m)$. 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 $W_1 < W_2 < \dots$ 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 $w_1, w_2,\dots, w_k$ 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 $w_1,\dots, w_i$ 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 $W_1 < W_2 < \dots$. 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 $(w_1,\dots, w_k)$ 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 φ: $V \longrightarrow W$ 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 π: $V \longrightarrow V/W$. □

(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: $\pi(a_1,\dots,a_m) = (a_1,\dots,a_{m-1})$. Its kernel is $\{(0,\dots,0,a_m)\} \approx R$. 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 $R[x_1,\dots,x_n]$ in several variables over a noetherian ring R is noetherian, hence that the rings $\mathbb{Z}[x_1,\dots,x_n]$ and $F[x_1,\dots,x_n]$ (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 $\bar{R} = R/I$ is noetherian.

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

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

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 $C_{d_1}, \ldots, C_{d_k}$ 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 $d_1 \mid d_2 \mid d_3 \ldots$.

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

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

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

$$d_1v_1 = 0,\ d_2v_2 = 0,\dots,\ d_kv_k = 0 \tag{6.6}$$

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:

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

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

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

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

$$T\colon V \longrightarrow V \tag{7.1}$$

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 $f(t) = a_n t^n + \cdots + a_1 t + a_0$. We set

$$f(t)v = a_n T^n(v) + a_{n-1} T^{n-1}(v) + \cdots + a_1 T(v) + a_0 v. \tag{7.2}$$

The right side can be written as $[f(T)](v)$, where $f(T)$ denotes the linear operator $a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0 I$ obtained by substituting T for t. The brackets have been added only for clarity. With this notation, we obtain the formulas

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

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