The constructive approach to mathematics has recently enjoyed a renaissance. This was caused largely by the appearance of Bishop's *Foundations of Constructive Analysis*, but also by the proliferation of powerful computers, which stimulated the development of constructive algebra for implementation purposes. In this book, the authors present the fundamental structures of modern algebra from a constructive point of view. Beginning with basic notions, the authors proceed to treat PID's, field theory (including Galois theory), factorization of polynomials, Noetherian rings, valuation theory, and Dedekind domains.

Mines / Richman / Ruitenburg A Course in Constructive Algebra

Ray Mines
Fred Richman
Wim Ruitenburg

A Course in Constructive Algebra

Chapter V. Principal Ideal Domains

1. DIAGONALIZING MATRICES

The theory of modules over a principal ideal domain is closely related to the theory of vector spaces over a field and is almost identical to the theory of abelian groups, which are modules over the integers. The analogue of a finite-dimensional vector space is a finitely presented module over a principal ideal domain. A finitely presented module is given by matrix. In this section we prove some basic facts about matrices over a principal ideal domain.

An $m \times n$ matrix $A = (a_{ij})$ is **diagonal** if $a_{ij} = 0$ whenever $i \neq j$. Two $m \times n$ matrices A and B are **equivalent** if there is an invertible $m \times m$ matrix C, and an invertible $n \times n$ matrix D, such that $A = CBD$.

1.1 LEMMA. *Each matrix over a principal ideal domain is equivalent to a diagonal matrix.*

PROOF. The key is the construction of certain invertible 2×2 matrices. If $sa + tb = d \neq 0$ is the GCD of a and b, then for all u,v there are w,x such that

$$\begin{bmatrix} a & b \\ u & v \end{bmatrix} \cdot \begin{bmatrix} s & -b/d \\ t & a/d \end{bmatrix} = \begin{bmatrix} d & 0 \\ w & x \end{bmatrix}.$$

Moreover, the right hand factor is invertible since its determinant is 1. Similarly, if a and b are in a column, we multiply on the left as follows.

$$\begin{bmatrix} s & t \\ -b/d & a/d \end{bmatrix} \cdot \begin{bmatrix} a & u \\ b & v \end{bmatrix} = \begin{bmatrix} d & w \\ 0 & x \end{bmatrix}.$$

Thus if a and b are entries in the same row (column) of a matrix B, we can multiply B on the right (left) by an invertible matrix leaving d in the position occupied by a, and 0 in the position occupied by b, and fixing the entries not in the rows or columns of a or b.

We shall operate on a given matrix A by left and right multiplication by invertible matrices to obtain a diagonal matrix. If $A = 0$ we are done. Otherwise, by row and column interchanges, we can bring a nonzero element a_1 to the upper left hand corner. By a sequence of right multiplications

by invertible matrices we can replace a_1 by a_2, the GCD of all elements in the first row, leaving zeros in the remaining places in the first row. Similarly, by left multiplications, we can replace a_2 by a_3, the GCD of all elements now in the first column, leaving zeros in the rest of the first column. Continue by replacing a_3 by a_4, the GCD of all elements now in the first row, and so on. In this manner we generate a sequence $(a_1),(a_2),\ldots$ of principal ideals such that $a_{i+1} | a_i$ for each i. Hence, for some n, we have $a_n | a_{n+1}$. But that means that a_n is a GCD of the elements in the first row (or column), while the remaining elements in the first column (or row) are zero. Hence, by elementary row or column operations, we can clear both the first row and the first column, making all elements in the first row and column zero, except for the corner. By induction on the size of the matrix, we can diagonalize A. □

A matrix $A = (a_{ij})$ is in **Smith normal form** if it is diagonal and $a_{ii} | a_{i+1,i+1}$ for each i.

1.2 THEOREM. *Each matrix over a principal ideal domain is equivalent to a matrix in Smith normal form.*

PROOF. By Lemma 1.1 we may assume that we are given a diagonal matrix. Let a,b be diagonal elements and $d = sa + tb$ be the GCD of a and b. Then

$$\begin{bmatrix} s & t \\ -b/d & a/d \end{bmatrix} \cdot \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} 1 & -tb/d \\ 1 & sa/d \end{bmatrix} = \begin{bmatrix} d & 0 \\ 0 & ab/d \end{bmatrix}.$$

Repeated application of this observation allows us to convert our diagonal matrix to a diagonal matrix with the property that the corner element divides all the remaining elements. Then, by induction on the size of A, we obtain a matrix in Smith normal form. □

We want to show that each matrix is equivalent to an essentially unique matrix in Smith normal form. Given a matrix A, define $\Delta_i(A)$ to be the ideal generated by the determinants of all $i \times i$ submatrices of A.

1.3 LEMMA. *Let A and B be equivalent $m \times n$ matrices over a GCD-domain R. Then $\Delta_i(A) = \Delta_i(B)$ for all i.*

PROOF. It suffices to show that if C is an invertible $m \times m$ matrix, then $\Delta_i(CA) = \Delta_i(A)$. The rows of CA are linear combinations of the rows of A. Hence the determinants of $i \times i$ submatrices of CA are linear combinations of the determinants of $i \times i$ submatrices of A. So $\Delta_i(A) \supseteq \Delta_i(CA)$. Since C is invertible, we also have $\Delta_i(CA) \supseteq$

$\Delta_i(C^{-1}CA) = \Delta_i(A)$. So $\Delta_i(CA) = \Delta_i(A)$. □

1.4 THEOREM. *Two $m \times n$ matrices in Smith normal form over a GCD-domain are equivalent if and only if corresponding elements are associates.*

PROOF. Let $D = (d_{ij})$ be a matrix in Smith normal form. We easily verify that $\Delta_1(D) = (d_{11})$, and $\Delta_i(D)\cdot(d_{i+1,i+1}) = \Delta_{i+1}(D)$ for each $i \leq m-1$. So the diagonal elements of D are determined, up to a unit, by the ideals $\Delta_i(D)$. By Lemma 1.3 this implies that if two matrices in Smith normal form are equivalent, then their elements are associates. □

EXERCISES

1. Find a matrix in Smith normal form, over $\mathbb{Z}$, that is equivalent to the matrix
$$\begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6. \\ 7 & 8 & 9 \end{matrix}$$
2. A **valuation ring** is a commutative ring R such that for any two elements a and b in R, either $(a) \subseteq (b)$ or $(b) \subseteq (a)$. Show that each matrix over a valuation ring is equivalent to a matrix in Smith normal form.
3. Show that a square matrix over $\mathbb{Z}$ is invertible if and only if it is a product of elementary matrices.
4. Show that a square matrix over $\mathbb{Z}$ has determinant 1 if and only if it is a product of elementary matrices corresponding to elementary operations of type (iii).

   Hint: $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}\cdot\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$

2. FINITELY PRESENTED MODULES

Let M be a module over a commutative ring R. A **finite presentation** of M is a triple $(M, (x_1,\ldots,x_n), A)$ where $x_1,\ldots,x_n$ is a finite set of generators of M, and A is an $m \times n$ matrix of elements of R whose rows generate the module of relations among the x's. Thus for each element $(\alpha_1,\ldots,\alpha_n) \in R^n$ we have $\alpha_1x_1 + \cdots + \alpha_nx_n = 0$ if and only if $(\alpha_1,\ldots,\alpha_n) = vA$ for some $v \in R^m$. We may identify a finitely presented module with its finite presentation.

The matrix A contains all the information about the structure of the module M. Given M, the matrix A depends on the choice of generators

$x_1,\ldots,x_n$ and on the choice of generators for the module of relations. If $M \cong R/(r_1) \oplus \cdots \oplus R/(r_n)$, then we can get a diagonal matrix A for M; conversely, if we can get a diagonal matrix A for M, then we have exhibited M as a direct sum of cyclic modules. Thus it behooves us to examine how to pass from one matrix for M to another.

Let $(M, (x_1,\ldots,x_n), A)$ be a finitely presented R-module. Then $(M, (x_1,\ldots,x_n), B)$ is a finitely presented R-module if and only if the rows of B generate the same submodule of R^n as the rows of A; this happens if $B = FA$ for some invertible $m \times m$ matrix F. What happens to the matrix A of relations of a finitely presented module $(M, (x_1,\ldots,x_n), A)$ when we change the generators $x_1,\ldots,x_n$?

2.1 THEOREM. *Let $(M, (x_1,\ldots,x_n), A)$ be a finitely presented module over a commutative ring R, and let E be an $n \times n$ invertible matrix over R. Then $(M, (x_1,\ldots,x_n), A) = (M, (x_1,\ldots,x_n)E^t, AE^{-1})$.*

PROOF. Let $(y_1,\ldots,y_n)^t = E(x_1,\ldots,x_n)^t$. Clearly $y_1,\ldots,y_n$ generate M. Moreover the following are equivalent.

$$(r_1,\ldots,r_n)E^{-1}(y_1,\ldots,y_n)^t = (r_1,\ldots,r_n)(x_1,\ldots,x_n)^t = 0$$
$$(r_1,\ldots,r_n) = (s_1,\ldots,s_m)A \text{ for some } (s_1,\ldots,s_m)$$
$$(r_1,\ldots,r_n)E^{-1} = (s_1,\ldots,s_m)(AE^{-1}).$$

Hence the module of relations among $y_1,\ldots,y_n$ is generated by the rows of AE^{-1}. □

2.2 COROLLARY. *Let A be an $m \times n$ matrix over a commutative ring R, and let $(M, (x_1,\ldots,x_n), A)$ be a finitely presented R-module. Let E be an $n \times n$ invertible matrix over R, and F an $m \times m$ invertible matrix over R. Then $(M, (x_1,\ldots,x_n), A) = (M, (x_1,\ldots,x_n)E^t, FAE^{-1})$.*

PROOF. As the rows of FAE^{-1} have the same span as those of AE^{-1}, the corollary is an immediate consequence of 2.1. □

2.3 THEOREM (Structure Theorem). *Let M be a finitely presented module over a principal ideal domain R. Then there exist principal ideals $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ such that M is isomorphic to the direct sum $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$.*

PROOF. Let $(M, (x_1,\ldots,x_n), A)$ be a finite presentation of M. By Theorem 1.4 there exist invertible matrices E and F such that $D = FAE^{-1}$ is

a diagonal matrix in Smith normal form. By Corollary 2.2 we have

$$(M, (x_1,\dots,x_n), A) = (M, (x_1,\dots,x_n)E^t, D).$$

If $(y_1,\dots,y_n) = (x_1,\dots,x_n)E^t$, then $M = Ry_1 \oplus \cdots \oplus Ry_n$, and $Ry_i \cong R/I_i$ where $I_i = (d_{ii})$. □

The decomposition in Theorem 2.3 is essentially unique over an arbitrary commutative ring.

2.4 THEOREM. *Let R be a commutative ring, $m \le n$ positive integers, and $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$ and $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_n$ ideals of R. Suppose M is an R-module that is isomorphic to $\Sigma_{i=1}^m R/I_i$ and to $\Sigma_{j=1}^n R/J_j$. Then*

(a) $J_1 = J_2 = \cdots = J_{n-m} = R$.

(b) $I_i = J_{n-m+i}$ *for* $i = 1,\dots,m$.

PROOF. To prove (a) it suffices to show that if $m < n$, then $J_1 = R$. Let $S = R/J_1$. Then

$$S^n = \Sigma_{j=1}^n R/(J_j + J_1) \cong M/(J_1M) \cong \Sigma_{i=1}^m R/(I_i + J_1)$$

as S-modules. We can map S^m onto $\Sigma_{i=1}^m R/(I_i + J_1)$, so $S = 0$ by (II.7.5).

As (a) holds we may assume that $m = n$. To prove (b) it suffices, by symmetry, to show that $I_k \subseteq J_k$ for $k = 1,\dots,n$. Let $x \in I_k$. Then

$$\Sigma_{j=1}^n R/(J_j:x) \cong xM \cong \Sigma_{i=k+1}^n R/(I_i:x)$$

where $(K:x) = \{r \in R : rx \in K\}$. Applying (a) to xM we get $(J_1:x) = (J_2:x) = \cdots = (J_k:x) = R$. Thus $x \in J_k$. □

EXERCISES

1. Show that a finitely presented abelian group is a direct sum of a finite number of infinite cyclic and finite cyclic groups.
2. Give a Brouwerian example of a cyclic group that is neither finite nor infinite.
3. Show that if an $m \times n$ matrix over a commutative ring R has a left inverse, and $m < n$, then $R = 0$.
4. Let H be a detachable subgroup of a free abelian group (free $\mathbb{Z}$-module) on a discrete set. Show that for each h in H there exists x in H such that $h \in \langle x\rangle$ and $H/\langle x\rangle$ is a detachable subgroup of a free abelian group on a discrete set.

5. Use Exercise 4 to show that a detachable subgroup of a free abelian group on a countable discrete set is a free abelian group on a countable discrete set. (Construct generators x_i for H inductively so that $H/\langle x_1,\dots,x_{n-1}\rangle$ is a detachable subgroup of a free abelian group on a countable discrete set for each $n \ge 1$.)

3. TORSION MODULES, p-COMPONENTS, ELEMENTARY DIVISORS

Let M be a module over a discrete integral domain R. The **torsion submodule** $\tau(M)$ of M is defined to be $\{m \in M : am = 0 \text{ for some } a \neq 0\}$. We easily see that $\tau(M)$ is a submodule of M. If $\tau(M) = M$, then we say that M is a **torsion** module. If d is a nonzero element of R, and $dM = 0$, then we say that M is **bounded** by d.

3.1 THEOREM. *Let M be a finitely presented module over a principal ideal domain R. Then $\tau(M)$ is a finitely presented detachable submodule of M, and $M \cong \tau(M) \oplus R^n$ for some n. Moreover $\{d \in R : d\tau(M) = 0\}$ is a nonzero principal ideal.*

PROOF. By Theorem 2.3 there exist principal ideals $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$ such that M is isomorphic to the direct sum $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_m$. If $I_k = 0$ for all k, then the conclusions are clear. Otherwise choose k such that $I_k \neq 0$ and $I_i = 0$ for $i > k$. Then $\tau(M) \cong R/I_1 \oplus \cdots \oplus R/I_k$ and $M \cong \tau(M) \oplus R^{m-k}$. Moreover $I_k = \{d \in R : d\tau(M) = 0\}$. □

Let M be a module over a commutative ring R, and let $d \in R$. Then the **d-component** of M is defined by $M_d = \{m \in M : d^k m = 0 \text{ for some } k\}$. We easily verify that M_d is a submodule of M. Observe that $M_a + M_b \subseteq M_{ab}$ for all $a,b \in R$ and $M_{(a^n)} = M_a$ for all $n > 0$.

3.2 LEMMA. *Let M be a module over a commutative ring R. Let a and b be strongly relatively prime elements of R. Then $M_{ab} = M_a \oplus M_b$, and, if M is finitely generated, the projection of M_{ab} onto M_a is realized by multiplication by an element of R. The module M_{ab} is cyclic if and only if the submodules M_a and M_b are cyclic.*

PROOF. To show that $M_{ab} = M_a \oplus M_b$, it suffices to show that $K = K_a \oplus K_b$ for each finitely generated submodule of M_{ab}, so we may assume that M is finitely generated. Then $a^k b^k M_{ab} = 0$ for some positive integer k.

There exist s and t in R such that $sa^k + tb^k = 1$. Let $\pi_a = tb^k$ and $\pi_b = sa^k$. Then

(i) $\pi_a M_{ab} \subseteq M_a$ and $\pi_b M_{ab} \subseteq M_b$,

(ii) $\pi_a M_b = 0$ and $\pi_b M_a = 0$,

(iii) $\pi_a x = x$ for $x \in M_b$ and $\pi_b x = x$ for $x \in M_a$,

so $M_{ab} = M_a \oplus M_b$ and multiplication by π_a gives the projection of M_{ab} onto M_a.

If $M_{ab} = Rx$, then M_a is generated by $\pi_a x$, and M_b is generated by $\pi_b x$. Conversely suppose $M_a = Ry$ and $M_b = Rz$, and let $x = y + z$. Then $y = \pi_a x \in Rx$ and $z = \pi_b x \in Rx$, so $M_{ab} = Rx$. □

3.3 THEOREM. *Let M be a module over a commutative ring. Let $a = p(1)^{e(1)} \cdots p(m)^{e(m)}$, where the $p(i)$ are pairwise strongly relatively prime. Then $M_a = M_{p(1)} \oplus \cdots \oplus M_{p(m)}$, and, if M is finitely generated, the projection of M_a onto $M_{p(i)}$ is realized by multiplication by an element of the ring.*

PROOF. Apply Lemma 3.2 repeatedly. □

If p is a prime in a discrete integral domain R, then an R-module M is said to be **p-primary** if $M_p = M$. If $dM = 0$ for some nonzero element of R which is a product of powers of strongly relatively prime primes, then we can decompose M into a direct sum of primary submodules by (3.3).

3.4 THEOREM. *Let R be a PID, and p a prime in R. If M is a finitely presented p-primary R-module, then M is isomorphic to a finite direct sum of R-modules, each of the form $R/(p^n)$ for some $n > 0$.*

PROOF. By the structure theorem (2.3), M is isomorphic to a finite direct sum of R-modules, each of the form R/I for some principal ideal I. As M is p-primary, each I contains a positive power of p. If $p^m \in I = (a)$, then $p^m = ab$. Because p is a prime, we can write $a = up^n$ where u is a unit; so $I = (p^n)$. □

The powers of p occurring in (3.5) are called the **elementary divisors** of M. If M can be written as a direct sum of primary submodules, then the elementary divisors of M are the elementary divisors of the various primary submodules of M.

EXERCISES

1. Find the primary components of the abelian group $\mathbb{Z}/12\mathbb{Z}$.
2. Let R be a Bézout domain and p a prime in R. Show that $R/(p^m)$ is a valuation ring. Prove Theorem 3.4 for R a Bézout domain.

4. LINEAR TRANSFORMATIONS

Let V be a finite dimensional vector space over a discrete field k, and let $T : V \to V$ be a linear transformation. We can make the vector space V into a module over $k[X]$ by defining $Xv = T(v)$ for each $v \in V$. By the Cayley-Hamilton theorem, the $k[X]$-module V is bounded (by the characteristic polynomial of T). We shall show that the $k[X]$-module V is finitely presented.

4.1 LEMMA. *Let V be a vector space over a discrete field k with basis $u_1,\ldots,u_n$, and $T : V \to V$ a linear transformation such that $T(u_i) = \Sigma\, a_{ji}u_j$. Let $e_1,\ldots,e_n$ be a basis for $k[X]^n$, and let $\varphi : k[X]^n \to V$ take $\Sigma\, f_i(X)e_i$ to $\Sigma\, f_i(T)u_i$. Define $d_i \in k[X]^n$ by*

$$d_i = Xe_i - \Sigma_{j=1}^n a_{ji}e_j.$$

Then $\ker \varphi$ is a free $F[X]$-module with basis $d_1,\ldots,d_n$.

PROOF. Obviously $d_1,\ldots,d_n \in \ker \varphi$. Suppose $g_1e_1 + \cdots + g_ne_n \in \ker \varphi$, where $g_i \in k[X]$. Using the relations $Xe_i = d_i + \Sigma_{j=1}^n a_{ji}e_j$, we can write

$$g_1e_1 + \cdots + g_ne_n = h_1d_1 + \cdots + h_nd_n + b_1e_1 + \cdots + b_ne_n,$$

where $b_i \in k$. So $b_1e_1 + \cdots + b_ne_n \in \ker \varphi$. Since $u_1,\ldots,u_n$ is a basis of V as vector space over k, this implies that each $b_i = 0$. Hence $d_1,\ldots,d_n$ generate $\ker \varphi$.

If $h_1d_1 + \cdots + h_nd_n = 0$, then $\Sigma_{i=1}^n h_iXe_i = \Sigma_{i=1}^n \Sigma_{j=1}^n h_ia_{ji}e_j$. If some $h_i \neq 0$, then we may assume that the degree of h_1 is maximal among the degrees of $h_1,\ldots,h_n$. But $h_1X = \Sigma_{i=1}^n h_ia_{1i}$, so $h_1 = 0$. Thus $d_1,\ldots,d_n$ are linearly independent. □

By (2.3) the $k[X]$-module V can be written as $V = C_1 \oplus \cdots \oplus C_s$, where the C_i are cyclic $k[X]$-modules, isomorphic to $k[X]/(f_i)$ for nonzero monic polynomials f_i, with f_i dividing f_{i+1} for $i = 1,\ldots,s-1$. The polynomial f_s generates the ideal $\{g \in k[X] : gV = 0\} = \{g \in k[X] : g(T) = 0\}$, and is called the **minimal polynomial** of T. By the Cayley-Hamilton theorem, the