matrix is 1. It follows from Corollary M.3.8 that the right hand is equal to the determinant of A

M.3.5. Prove a cofactor expansion by columns: For fixed j,

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \det(A_{i,j}).$$

M.3.6. Prove Cramer’s rule: If A is an invertible n–by–n matrix over R, and $b \in R^n$, then the unique solution to the matrix equation $Ax = b$ is given by

$$x_j = \det(A)^{-1} \det(\tilde{A}_j),$$

where $\tilde{A}_j$ is the matrix obtained by replacing the j–th column of A by b.

M.4. Finitely generated Modules over a PID, part I

In this section, and the following section, we will determine the structure of finitely generated modules over a principal ideal domain. We begin in this section by considering finitely generated free modules.

The following simple lemma is valid for modules over any ring with identity; it should go in an earlier section:

Lemma M.4.1. *Let R be any ring with multiplicative identity. If an R–module is finitely generated and free, then any basis of M is finite.*

Proof. Suppose that M is an R–module with a (possibly infinite) basis B and a finite generating set S. Each element of S is a linear combination of finitely many elements of B. Since S is finite, it is contained in the span of a finite subset B_0 of B. But then $M = \text{span}(S) \subseteq \text{span}(\text{span}(B_0)) = \text{span}(B_0)$. So B_0 spans M. But no proper subset of a basis can be spanning. (If $b \in B \setminus B_0$, then b can be written as an R–linear combination of elements of B_0, $b - \sum a_j b_j = 0$, contradicting the linear independence of B.) Therefore, $B = B_0$. ■

Let R be a commutative ring with identity element, and let M denote an R–module. Represent elements of the R–module M^n by n–by–1 matrices (row “vectors”) with entries in M. For any n–by–s matrix C with entries in R, right multiplication by C gives an

R–module homomorphism from M^n to M^s. Namely, if $C = (c_{i,j})$, then

$$[v_1, \dots, v_n]\, C = \left[\sum_i c_{i,1} v_i, \dots, \sum_i c_{i,s} v_i\right].$$

If B is an s–by–t matrix over R, then the homomorphism implemented by CB is the composition of the homomorphism implemented by C and the homomorphism implemented by B,

$$[v_1, \dots, v_n]\, CB = ([v_1, \dots, v_n]\, C)B,$$

as follows by a familiar computation. If $\{v_1, \dots, v_n\}$ is linearly independent over R and $[v_1, \dots, v_n]\, C = 0$, then C is the zero matrix. See Exercise M.4.1

Let us show next that any two bases of a finitely generated free R–module have the same cardinality. (The argument requires only that R is a commutative ring with identity element and relies on determinants, so it ought to be moved the the section on determinants.)

Lemma M.4.2. *Let R be a commutative ring with identity element. Any two bases of a finitely generated free R–module have the same cardinality.*

Proof. We already know that any basis of a finitely generated R module is finite. Suppose that an R module M has a basis $\{v_1, \dots, v_n\}$ and a spanning set $\{w_1, \dots, w_m\}$. We will show that $m \geq n$.

Each w_j has a unique expression as an R–linear combination of the basis elements v_j,

$$w_j = a_{1,j} v_1 + a_{2,j} v_2 + \cdots + a_{n,j} v_n.$$

Let A denote the n–by–m matrix $A = (a_{i,j})$. The m relations above can be written as a single matrix equation:

$$[v_1, \dots, v_n]A = [w_1, \dots, w_m]. \tag{M.4.1}$$

Since $\{w_1, \dots, w_m\}$ spans M, we can also write each v_j as an R–linear combinations of the elements w_i,

$$v_j = b_{1,j} w_1 + b_{2,j} w_2 + \cdots + b_{n,j} w_n.$$

Let B denote the m–by–n matrix $B = (b_{i,j})$. The n relations above can be written as a single matrix equation:

$$[w_1, \dots, w_m]B = [v_1, \dots, v_n]. \tag{M.4.2}$$

Combining (M.4.1) and (M.4.2), we have

$$[v_1, \dots, v_n]AB = [w_1, \dots, w_m]B = [v_1, \dots, v_n],$$

or

$$[v_1, \dots, v_n](AB - E_n) = 0,$$

where E_n denotes the n–by–n identity matrix. Because of the linear independence of the v_j, we must have $AB = E_n$. Now, if $m < n$, we augment A by appending $n - m$ columns of zeros to obtain an n–by–n matrix A'. Likewise, we augment B by adding $n - m$ rows of zeros to obtain an n–by–n matrix B'. We have $A'B' = AB = E_n$. Taking determinants, we obtain $1 = \det(E_n) = \det(A'B) = \det(A')\det(B')$. But $\det(A') = 0$, since the matrix A' has a column of zeros. This contradiction shows that $m \geq n$.

In particular, any two basis have the same cardinality. ■

Definition M.4.3. Let R be a commutative ring with identity element. The *rank* of a finitely generated free R–module is the cardinality of any basis.

Remark M.4.4. The zero module over R is free of rank zero. The empty set is a basis. This is not just a convention; it follows from the definitions.

For the rest of this section, R denotes a principal ideal domain.

Lemma M.4.5. *Let F be a finitely generated free module over a principal idea domain R. Any submodule N of F is free, with* $\operatorname{rank}(N) \leq \operatorname{rank}(F)$.

Proof. We prove this by induction on the rank n of F. A submodule (ideal) of R has the form Rd, since R is a PID. If $d \neq 0$, then the one element set $\{d\}$ is a basis of Rd. If $d = 0$, then the ideal is the zero ideal, hence free of rank 0. This verifies the case $n = 1$.

Suppose that F has rank $n > 1$ and that for any free R module F' of rank less than n and for any submodule N' of F', N' is free, and $\operatorname{rank}(N') \leq \operatorname{rank}(F')$.

Let $\{f_1, \dots, f_n\}$ be a basis of F, put $F' = \operatorname{span}(\{f_1, \dots, f_{n-1}\}$, and $N' = N \cap F'$. By the induction hypothesis, N' is free with rank $\leq n-1$. Let $\{h_1, \dots, h_k\}$ be a basis of N'. (If $N' = \{0\}$, then $k = 0$.)

Every element $x \in F$ has a unique expansion $x = \sum_{i=1}^{n} \alpha_i(x) f_i$. The map $x \mapsto \alpha_n(x)$ is an R–module homomorphism from F to R.

If $\alpha_n(N) = \{0\}$, then $N = N'$, and N is free of rank $\leq n-1$. Otherwise, the image of N under this map is a nonzero ideal of R, so of the form dR for some nonzero $d \in R$. Choose $h_{k+1} \in N$ such that $\alpha_n(h_{k+1}) = d$.

I claim that $\{h_1, \dots, h_k, h_{k+1}\}$ is a basis of N.

If $x \in N$, then $\alpha_n(x) = rd$ for some $r \in R$. Then $y = x - rh_{k+1}$ satisfies $\alpha_n(y) = 0$. Therefore, $y \in N \cap F' = N'$. It follows that y is in the span of $\{h_1, \dots, h_k\}$ and thus, x is in the span of $\{h_1, \dots, h_k, h_{k+1}\}$.

Now suppose $\sum_{j=1}^{k+1} \beta_j h_j = 0$ for some $\beta_j \in R$. Observe that $\alpha_n(h_j) = 0$ for $j \leq k$. Therefore,

$$0 = \alpha_n(\sum_{j=1}^{k+1} \beta_j h_j) = \alpha_n(\beta_{k+1}h_{k+1}) = \beta_{k+1}d.$$

It follows that $\beta_{k+1} = 0$. But $\{h_1, \dots, h_k\}$ is linearly independent over R, so all the remaining β_j are zero as well. This completes the proof. ■

Corollary M.4.6. *If M is a finitely generated module over a principal ideal domain, then every submodule of M is finitely generated.*

Proof. Suppose that M has a finite spanning set $x_1, \dots, x_n$. Then M is the homomorphic image of a free R–module of rank n. Namely consider a free R module F with basis $\{f_1, \dots, f_n\}$. Define an R–module homomorphism from F onto M by $\varphi(\sum_i r_i f_i) = \sum_i r_i x_i$. Let A be a submodule of M and let $N = \varphi^{-1}(A)$. According to Lemma M.4.5, N is free of rank $\leq n$. The image under φ of a basis of N is a spanning set of A, of cardinality no more than n. ■

Our next goal is to obtain a more refined version of the previous lemma. Recall that if N is an s dimensional subspace of an n–dimensional vector space F, then there is a basis $\{v_1, \dots, v_n\}$ of F such that $\{v_1, \dots, v_s\}$ is a basis of of N. For modules over a principal ideal domain, the analogous statement is the following: If F is a free R–module of rank n and N is a submodule of rank s, then there exists a basis $\{v_1, \dots, v_n\}$ of F, and there exist elements $d_1, d_2, \dots, d_s$ of R, such that d_i divides d_j if $i \leq j$ and $\{d_1v_1, \dots, d_sv_s\}$ is a basis of N.

The key to this is the following statement about diagonalization of rectangular matrices over R. Say that a (not necessarily square) matrix $A = (a_{i,j})$ is *diagonal* if $a_{i,j} = 0$ unless $i = j$. If A is m–by–n

and $k = \min\{m, n\}$, write $A = \operatorname{diag}(d_1, d_2, \dots, d_k)$ if A is diagonal and $a_{i,i} = d_i$ for $1 \le i \le k$.

Proposition M.4.7. *Let A be an m–by–n matrix over R. Then there exist invertible matrices $P \in \operatorname{Mat}_m(R)$ and $Q \in \operatorname{Mat}_n(R)$ such that $PAQ = \operatorname{diag}(d_1, d_2, \dots, d_s, 0, \dots, 0)$, where d_i divides d_j for $i \le j$.*

Diagonalization of the matrix A is accomplished by a version of Gaussian elimination (row and column reduction). For the sake of completeness, we will discuss the diagonalization process for matrices over an arbitrary principal ideal domain. However, we also want to pay particular attention to the case that R is a Euclidean domain, for two reasons. First, in applications we will be interested exclusively in the case that R is Euclidean. Second, if R is Euclidean, Gaussian elimination is a constructive process, assuming that Euclidean division with remainder is constructive. (For a general PID, the diagonalization process follows an “algorithm,” but there is a non-constructive step in the process.)

Let us review the elementary row and column operations of Gaussian elimination, and their implementation by pre– or post–mulitplication by elementary invertible matrices.

The first type of elementary row operation replaces some row a_i of A by that row plus a multiple of another row a_j, leaving all other rows unchanged. The operation of replacing a_i by $a_i + \beta a_j$ is implemented by multiplication on the left by the m–by-m matrix $E + \beta E_{i,j}$, where E is the m–by-m identity matrix, and $E_{i,j}$ is the matrix unit with a 1 in the (i, j) position. $E + \beta E_{i,j}$ is invertible in $\operatorname{Mat}_m(R)$ with inverse $E - \beta E_{i,j}$.

For example, for $m = 4$,

$$E + \beta E_{2,4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & \beta \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The second type of elementary row operation replaces some row a_i with γa_i, where γ is a unit in R. This operation is implemented by multiplication on the left by the m–by-m diagonal matrix $D(i, \gamma)$ whose diagonal entries are all 1 except for the i–th entry, which is γ. $D(i, \gamma)$ is invertible in $\operatorname{Mat}_m(R)$ with inverse $D(i, \gamma^{-1})$.

For example, for $m = 4$,

$$D(3, \gamma) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The third type of elementary row operation interchanges two rows. The operation of interchanging the i–th and j–th rows is implemented by multiplication on the left by the m–by-m permutation matrix $P_{i,j}$ corresponding to the transposition (i, j). $P_{i,j}$ is its own inverse in $\mathrm{Mat}_m(R)$.

For example, for $m = 4$,

$$P_{2,4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

When we work over an arbitrary PID R, we require one more type of row operation. In this fourth type of row operation, each of two rows is simultaneously replaced by linear combinations of the two rows. Thus a_i is replaced by $\alpha a_i + \beta a_j$, while a_j is replaced by $\gamma a_i + \delta a_j$. We require that this operation be invertible, which is the case precisely when the matrix $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ is invertible in $\mathrm{Mat}_2(R)$. Consider the m–by–m matrix $U(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}; i, j)$ that coincides with the identity matrix except for the 2–by–2 submatrix in the i–th and j–th rows and i–th and j–th columns, which is equal to $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$. For example, when $m = 4$,

$$U(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}; 2, 4) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \alpha & 0 & \beta \\ 0 & 0 & 1 & 0 \\ 0 & \gamma & 0 & \delta \end{bmatrix}.$$

The matrix $U(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}; i, j)$ is invertible with inverse $U(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}^{-1}; i, j)$. Left multiplication by $U(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}; i, j)$ implements the fourth type of elementary row operation.

Elementary column operations are analogous to elementary row operations. They are implemented by right multiplication by invertible n–by–n matrices.

We say that two matrices are *row–equivalent* if one is transormed into the other by a sequence of elementary row operations; likewise, two matrices are *column–equivalent* if one is transormed into the other by a sequence of elementary column operations. Two matrices are *equivalent* if one is transformed into the other by a sequence of elementary row and column operations.

We need a way to measure the size of a nonzero element of R. If R is a Euclidean domain, we can use the Euclidean function d. If R is non-Euclidean, we need another measure of size. Since R is a unique factorization domain, each nonzero element a can be factored as $a = up_1p_2 \cdots p_\ell$. where u is a unit and the p_i's are irreducibles. The number ℓ of irreducibles appearing in such a factorization is uniquely determined. We define the *length* of a to be ℓ. For a a nonzero element of R, define

$$|a| = \begin{cases} d(a) & \text{if } R \text{ is Euclidean with Euclidean function } d. \\ \text{length}(a) & \text{if } R \text{ is not Euclidean.} \end{cases}$$

Lemma M.4.8.

(a) *$|ab| \geq \max\{|a|, |b|\}$.*

(b) *$|a| = |b|$ if a and b are associates.*

(c) *If $|a| \leq |b|$ and a does not divide b, then any greatest common divisor δ of a and b satisfies $|\delta| < |a|$.*

Proof. Exercise M.4.2 ■

In the following discussion, when we say that a is smaller than b, we mean that $|a| \leq |b|$; when we say that a is strictly smaller than b, we mean that $|a| < |b|$.

Lemma M.4.9. *Suppose that A has nonzero entry α in the $(1, 1)$ position and another nonzero entry β in the first row or first column, with $|\alpha| \leq |\beta|$.*

(a) *If α divides β, then A is equivalent to a matrix A' with $(1, 1)$ entry equal to α, such that A' has more zero entries in its first row and first column than does A.*

(b) *If α does not divide β, then A is equivalent to a matrix A' whose $(1, 1)$ entry is nonzero and strictly smaller than α.*

Proof. We can suppose that the nonzero entry β is in the first column of A, in the $(i, 1)$ position. If α divides β, then a row operation of the first type gives a matrix A' with a zero in the $(i, 1)$ position, and with the other entries in the first row and column the same as those of A.

If α does not divide β then any greatest common δ of α and β satsfies $|\delta| < |\alpha|$, by the previous lemma. There exist $s, t \in R$ such that $\delta = s\alpha + t\beta$. Consider the matrix $\begin{bmatrix} s & t \\ -\beta/\delta & \alpha/\delta \end{bmatrix}$. This matrix has determinant equal to 1, so it is invertible in $\mathrm{Mat}_2(R)$. Notice that $\begin{bmatrix} s & t \\ -\beta/\delta & \alpha/\delta \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \delta \\ 0 \end{bmatrix}$. It follows that

$$A' = U(\begin{bmatrix} s & t \\ -\beta/\delta & \alpha/\delta \end{bmatrix}; 1, i)A$$

has $(1, 1)$ entry equal to δ.

The case that the nonzero entry β is in the first row is handled similarly, with column operations rather than row operations. ■

Remark M.4.10. The proof of this lemma is non-constructive, because in general there is no constructive way to find s and t satisfying $s\alpha + t\beta = \delta$. However, if R is a Euclidean domain, we have an alternative constructive proof. If α divides β, proceed as before. Otherwise, write $\beta = q\alpha + r$ where $d(r) < d(\alpha)$. A row operation of the first type gives a matrix with r in the $(i, 1)$ position. Then interchanging the first and i–th rows yields a matrix with r in the $(1, 1)$ position. Since $d(r) < d(\alpha)$, we are done.

Proof of Proposition M.4.7. If A is the zero matrix, there is nothing to do. Otherwise, we proceed as follows:

Step 1. There is a nonzero entry of minimum size. By row and column permutations, we can put this entry of minimum size in the $(1, 1)$ position. Denote the $(1, 1)$ entry of the matrix by α. According to Lemma M.4.9, if there is a nonzero entry in the first row or column which is not divisible by α, then A is equivalent to a matrix whose nonzero entry of least degree is strictly smaller than α. If necessary, move the entry of minimum size to the $(1, 1)$ position by row and column permutations.

Since the size of the $(1, 1)$ entry cannot be reduced indefinitely, after some number of row or column operations which reduce the size of the $(1, 1)$ entry, we have to reach a matrix whose $(1, 1)$ entry divides all other entries in the first row and column. Then by row and column operations of the first type, we obtain a block diagonal matrix

$$\begin{bmatrix} \epsilon & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \boxed{B'} & \\ 0 & & & \end{bmatrix}.$$

Step 2. We wish to obtain such a block diagonal matrix as in Step 1 in which the $(1,1)$ entry divides all the other matrix entries. If ϵ no longer has minimum size among nonzero entries, then apply row and column interchanges to move an entry of minimum size to the $(1,1)$ position. If ϵ is of minimum size, but some entry of B' is not divisible by ϵ, replace the first row of the large matrix by the sum of the first row and the row containing the offending entry. This gives a matrix with ϵ in the $(1,1)$ position and at least one entry not divisible by ϵ in the first row. In either case, repeating Step 1 will give a new block diagonal matrix whose $(1,1)$ entry is smaller than ϵ.

Again, the size of the $(1,1)$ entry cannot be reduced indefinitely, so after some number of repetitions, we obtain a block diagonal matrix

$$\begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \boxed{B} & \\ 0 & & & \end{bmatrix}.$$

whose $(1,1)$ entry d_1 divides all the other matrix entries.

Step 3. By an appropriate inductive hypothesis, B is equivalent to a diagonal matrix $\text{diag}(d_2, \dots, d_r, 0, \dots, 0)$, with d_i dividing d_j if $2 \le i \le j$. The row and column operations effecting this equivalence do not change the first row or first column of the larger matrix, nor do they change the divisibility of all entries by d_1. Thus A is equivalent to a diagonal matrix with the required divisibility properties. ■

Recall that any two bases of a finite dimensional vector space are related by an invertible change of basis matrix. The same is true for bases of free modules over a commutative ring with identity. Suppose that $\{v_1, \dots, v_n\}$ is a basis of the free module F. Let $(w_1, \dots, w_n)$ be another sequence of n module elements. Each w_j has a unique expression as an R–linear combination of the basis elements v_i,

$$w_j = \sum_i c_{i,j} v_i.$$

Let C denote the matrix $C = (c_{i,j})$. We can write the n equations above as the single matrix equation:

$$[v_1, \dots, v_n]\, C = [w_1, \dots, w_m]. \tag{M.4.3}$$

Lemma M.4.11. *In the situation described above, $\{w_1, \dots, w_n\}$ is a basis of F if, and only if, C is invertible in* $\mathrm{Mat}_n(R)$.

Proof. If $\{w_1, \dots, w_n\}$ is a basis, we can also write each v_j as an R–linear combinations of the w_i's,

$$v_j = \sum_k d_{i,j} w_i.$$

Let D denote the matrix $D = (d_{i,j})$. We can write the n previous equations as the single matrix equation:

$$[w_1, \dots, w_m]\, D = [v_1, \dots, v_n]. \tag{M.4.4}$$

Combining (M.4.4) and (M.4.3), we obtain

$$[v_1, \dots, v_n] = [v_1, \dots, v_n]\, CD.$$

Using the linear independence of $\{v_1, \dots, v_n\}$, as in the proof of Lemma M.4.2, we conclude that $CD = E_n$, the n–by–n identity matrix. Thus C has a right inverse in $\mathrm{Mat}_n(R)$. It follows from this that $\det(C)$ is a unit in R, and, therefore, C is invertible in $\mathrm{Mat}_n(R)$, by Corollary M.3.16.

Conversely, suppose that C is invertible in $\mathrm{Mat}_n(R)$ with inverse C^{-1}. Then

$$[v_1, \dots, v_n] = [w_1, \dots, w_n] C^{-1}.$$

This shows that $\{v_1, \dots, v_n\}$ is contained in the R–span of $\{w_1, \dots, w_n\}$, so the latter set spans F.

Finally, suppose $\sum_j \alpha_j w_j = 0$. Then

$$0 = [w_1, \dots, w_n] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = [v_1, \dots, v_n]\, C \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

By the linear independence of the v_k we have $C \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$. But then

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = C^{-1} C \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0.$$ ■

We can now combine Proposition M.4.7 and Lemma M.4.11 to obtain our main result about bases of free R–modules and their submodules:

Theorem M.4.12. *If F is a free R–module of rank n and N is a submodule of rank s, then there exists a basis $\{v_1, \dots, v_n\}$ of F, and there exist elements $d_1, d_2, \dots, d_s$ of R, such that d_i divides d_j if $i \le j$ and $\{d_1 v_1, \dots, d_s v_s\}$ is a basis of N.*

Proof. We already know that N is a free module. Let $\{f_1, \dots, f_n\}$ be a basis of F and $\{e_1, \dots, e_s\}$ a basis of N. Expand each e_j in terms of the f_i's,

$$e_j = \sum_i a_{i,j} f_i.$$

We can rewrite this as

$$[e_1, \dots, e_s] = [f_1, \dots, f_n]A, \tag{M.4.5}$$

where A denotes the n–by–s matrix $A = (a_{i,j})$. According to Proposition M.4.7, there exist invertible matrices $P \in \mathrm{Mat}_n(R)$ and $Q \in \mathrm{Mat}_s(R)$ such that $A' = PAQ$ is diagonal,

$$A' = PAQ = \mathrm{diag}(d_1, d_2, \dots, d_s).$$

We will see below that all the d_j are necessarily nonzero. Again, according to Proposition M.4.7, P and Q can be chosen so that d_i divides d_j whenever $i \le j$. We rewrite (M.4.5) as

$$[e_1, \dots, e_s]Q = [f_1, \dots, f_n]P^{-1}A'. \tag{M.4.6}$$

According to Lemma M.4.11, if we define $\{v_1, \dots, v_n\}$ by

$$[v_1, \dots, v_n] = [f_1, \dots, f_n]P^{-1}$$

and $\{w_1, \dots, w_s\}$ by

$$[w_1, \dots, w_s] = [e_1, \dots, e_s]Q,$$

then $\{v_1, \dots, v_n\}$ is a basis of F and $\{w_1, \dots, w_s\}$ is a basis of N. By Equation (M.4.6), we have

$$[w_1, \dots, w_s] = [v_1, \dots, v_n]A' = [d_1 v_1, \dots, d_s v_s].$$

In particular, d_j is nonzero for all j, since $\{d_1 v_1, \dots, d_s v_s\}$ is a basis of N. ■

Exercises M.4

M.4.1. Let R be a commutative ring with identity element and let M be a module over R.

(a) Let A and B be matrices over R of size n–by–s and s–by–t respectively. Show that for $[v_1, \dots, v_n] \in M^n$,

$$[v_1, \dots, v_n](AB) = ([v_1, \dots, v_n]A)B.$$

(b) Show that if $\{v_1, \dots, v_n\}$ is linearly independent subset of M, and $[v_1, \dots, v_n]A = 0$, then $A = 0$.

M.4.2. Prove Lemma M.4.8

M.5. Finitely generated Modules over a PID, part II.

Consider a finitely generated module M over a principal ideal domain R. Let $x_1, \dots, x_n$ be a set of generators of minimal cardinality. Then M is the homomorphic image of a free R–module of rank n. Namely consider a free R module F with basis $\{f_1, \dots, f_n\}$. Define an R–module homomorphism from F onto M by $\varphi(\sum_i r_i f_i) = \sum_i r_i x_i$. Let N denote the kernel of φ. According to Theorem M.4.12, N is free of rank $s \le n$, and there exists a basis $\{v_1, \dots, v_n\}$ of F and nonzero elements $d_1, \dots, d_s$ of R such that $\{d_1 v_1, \dots, d_s v_s\}$ is a basis of N and d_i divides d_j for $i \le j$. Therefore

$$M \cong F/N = (Rv_1 \oplus \cdots \oplus Rv_n)/(Rd_1 v_1 \oplus \cdots \oplus Rd_s v_s)$$

Lemma M.5.1. *Let $A_1, \dots, A_n$ be R–modules and $B_i \subseteq A_i$ submodules. Then*

$$(A_1 \oplus \cdots \oplus A_n)/(B_1 \oplus \cdots \oplus B_n) \cong A_1/B_1 \oplus \cdots \oplus A_n/B_n.$$

Proof. Consider the homomorphism of $A_1 \oplus \cdots \oplus A_n$ onto $A_1/B_1 \oplus \cdots \oplus A_n/B_n$ defined by $(a_1, \dots, a_n) \mapsto (a_1 + B_1, \cdots, a_n + B_n)$. The kernel of this map is $B_1 \oplus \cdots \oplus B_n \subseteq A_1 \oplus \cdots \oplus A_n$, so by the isomorphism theorem for modules,

$$(A_1 \oplus \cdots \oplus A_n)/(B_1 \oplus \cdots \oplus B_n) \cong A_1/B_1 \oplus \cdots \oplus A_n/B_n.$$

■

Observe also that $Rv_i/Rd_i v_i \cong R/(d_i)$, since

$$r \mapsto rv_i + Rd_i v_i$$

is a surjective R–module homomorphism with kernel (d_i). Applying Lemma M.5.1 and this observation to the situation described above gives

$$\begin{aligned} M \cong & Rv_1/Rd_1 v_1 \oplus \cdots \oplus Rv_s/Rd_s v_s \oplus Rv_{s+1} \cdots \oplus Rv_n \\ & \cong R/(d_1) \oplus \cdots \oplus R/(d_s) \oplus R^{n-s}. \end{aligned}$$

If some d_i were invertible, then $R/(d_i)$ would be the zero module, so could be dropped from the direct sum. But this would display M as generated by fewer than n elements, contradicting the minimality of n.

We have proved the existence part of the following fundamental theorem:

Theorem M.5.2. *(Structure Theorem for Finitely Generated Modules over a PID: Invariant Factor Form) Let R be a principal ideal domain, and let M be a (nonzero) finitely generated module over R.*

(a) *M is a direct sum of cyclic modules,*

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_s) \oplus R^k,$$

where the a_i are nonzero, nonunit elements of R, and a_i divides a_j for $i \geq j$.

(b) *The decomposition in part (a) is unique, in the following sense: Suppose*

$$M \cong R/(b_1) \oplus R/(b_2) \oplus \cdots \oplus R/(b_t) \oplus R^\ell,$$

where the b_i are nonzero, nonunit elements of R, and b_i divides b_j for $i \geq j$. Then $s = t$, $\ell = k$ and $(a_i) = (b_i)$ for all i.

Remark M.5.3. For convenience, the order of the ring elements has been reversed with respect to Theorem M.4.12. In that theorem, we stipulated that d_i divides d_j for $i \leq j$, whereas here we have that a_i divides a_j for $i \geq j$.

Before addressing the uniqueness statement in the theorem, we wish to introduce the notions of annihilators and torsion.

Suppose that R is an integral domain (not necessarily a PID) and M is an R–module.

For $x \in M$, define the annihilator of x in R to be

$$\text{ann}(x) = \{r \in R : rx = 0\}.$$

Then ann(x) is an ideal in R and ann$(x) \underset{\neq}{\subset} R$. See Exercise M.5.1.

An element $x \in M$ is called a *torsion element* if ann$(x) \neq \{0\}$, that is, there exists a nonzero $r \in R$ such that $rx = 0$.

If $x, y \in M$ are two torsion elements then $sx + ty$ is also a torsion element for any $s, t \in R$. In fact, if r_1 is a nonzero element of R such that $r_1x = 0$ and r_2 is a nonzero element of R such that $r_2y = 0$, then $r_1r_2 \neq 0$ and $r_1r_2(sx + ty) = 0$. It follows that the set of torsion elements of M is a submodule, called the *torsion submodule*, and denoted by M_{tor}. We say that M is a *torsion module* if $M = M_{\text{tor}}$. We say that M is *torsion free* if $M_{\text{tor}} = \{0\}$. One can check that M/M_{tor} is torsion free. See Exercise M.5.3

Example M.5.4. Let G be a finite abelian group. Then G is a finitely generated torsion module over $\mathbb{Z}$. In fact, every abelian group is a $\mathbb{Z}$–module by Example M.1.8. G is finitely generated since it is finite. Moreover, G is a torsion module, since every element is of finite order; that is, for every $a \in G$, there is an $n \in \mathbb{Z}$ such that $na = 0$.

Example M.5.5. Let V be a finite dimensional vector space over a field K. Let $T \in \text{End}_K(V)$. Recall from Example M.1.10 that V becomes a $K[x]$–module with $(\sum_i \alpha_i x^i)v = \sum_i \alpha_i T^i(v)$ for each polynomial $\sum_i \alpha_i x^i \in K[x]$ and each $v \in V$. V is finitely generated over $K[x]$ because a basis over K is a finite generating set over $K[x]$. Moreover, V is a torsion module over $K[x]$ for the following reason: Let n denote the dimension of V. Given $v \in V$, the set of $n+1$ elements $\{v, T(v), T^2(v), T^3(v), \dots, T^n(v)\}$ is not linearly independent over K, so there exist elements $\alpha_0, \alpha_1, \dots, \alpha_n$ of K, not all zero, such that $\alpha_0 v + \alpha_1 T(v) + \cdots + \alpha_n T^n(v) = 0$. Thus $\sum_i \alpha_i x^i \neq 0$ and $(\sum_i \alpha_i x^i)v = \sum_i \alpha_i T^i(v) = 0$. This means that v is a torsion element. We have shown that V is a finitely generated torsion module over $K[x]$.

If $S \subseteq M$ is any subset, we define the annihilator of S to be $\text{ann}(S) = \{r \in R : rx = 0 \text{ for all } x \in S\} = \bigcap_{x \in S} \text{ann}(x)$. Note that $\text{ann}(S)$ is an ideal, and $\text{ann}(S) = \text{ann}(RS)$, the annihilator of the submodule generated by S. See Exercise M.5.2

Consider a torsion module M over R. If S is a *finite* subset of M then $\text{ann}(S) = \text{ann}(RS)$ is a nonzero ideal of R; in fact, if $S = \{x_1, \dots, x_n\}$ and for each i, r_i is a nonzero element of R such that $r_i x_i = 0$, then $\prod_i r_i$ is a nonzero element of $\text{ann}(S)$. If M is a finitely generated torsion module, it follows that $\text{ann}(M)$ is a nonzero ideal of R.

For the remainder of this section, R again denotes a principal idea domain and M denotes a (nonzero) finitely generated module over R.

For $x \in M_{\text{tor}}$, any generator of the ideal $\text{ann}(x)$ is called a *period* of x. If $a \in R$ is a period of $x \in M$, then $Rx \cong R/\text{ann}(x) = R/(a)$.

According to xxx, any submodule of M is finitely generated If A is a torsion submodule of M, any generator of $\mathrm{ann}(A)$ is a called a *period* of A.

The period of an element x, or of a submodule A, is not unique, but any two periods of of x (or of A) are associates.

Lemma M.5.6. *Let M be a finitely generated module over a principal ideal domain R.*

(a) *If $M = A \oplus B$, where A is a torsion submodule, and B is free, then $A = M_{\mathrm{tor}}$.*

(b) *M has a direct sum decomposition $M = M_{\mathrm{tor}} \oplus B$, where B is free. The rank of B in any such decomposition is uniquely determined.*

(c) *M is a free module if, and only if, M is torsion free.*

Proof. We leave part (a) as an exercise. See Exercise M.5.4. According to the existence part of Theorem M.5.2, M has a direct sum decomposition $M = A \oplus B$, where A is a torsion submodule, and B is free. By part (a), $A = M_{\mathrm{tor}}$. Consequently, $B \cong M/M_{\mathrm{tor}}$, so the rank of B is determined. This proves part (b).

For part (c), note that any free module is torsion free. On the other hand, if M is torsion free, then by the decomposition of part (b), M is free. ■

Lemma M.5.7. *Let $x \in M$, let $\mathrm{ann}(x) = (a)$, and let $p \in R$ be irreducible.*

(a) *If p divides a, then $Rx/pRx \cong R/(p)$.*

(b) *If p does not divide a, then $pRx = Rx$.*

Proof. Consider the module homomoprhism of R onto Rx, $r \mapsto r\,x$, which has kernel (a). If p divides a, then $(p) \supseteq (a)$, and the image of (p) in Rx is pRx. Hence by Proposition M.2.8, $R/(p) \cong Rx/pRx$. If p does not divide a, then p and a are relatively prime. Hence there exist $s, t \in R$ such that $sp + ta = 1$. Therefore, for all $r \in R$, $r\,x = 1rx = psrx + tarx = psrx$. It follws that $Rx = pRx$. ■

Lemma M.5.8. *Suppose $p \in R$ is irreducible and $pM = \{0\}$. Then M is a vector space over $R/(p)$. Moreover, if $\varphi : M \longrightarrow \overline{M}$ is* *a surjective R–module homomorphism, then $\overline{M}$ is an $R/(p)$–vector space as well, and φ is $R/(p)$–linear.*

Proof. Let $\psi : R \longrightarrow \mathrm{End}(M)$ denote the homomorphism corresponding to the R–module structure of M, $\psi(r)(m) = rm$. Since $pM = \{0\}$, $pR \subseteq \ker(\psi)$. By Proposition 6.3.9, ψ factors through $R/(p)$; that is, there is a homomorphism $\tilde{\psi} : R/(p) \longrightarrow \mathrm{End}(M)$ such that $\psi = \tilde{\psi} \circ \pi$, where $\pi : R \longrightarrow R/(p)$ is the quotient map. Hence M is a vector space over the field $R/(p)$. The action of $R/(p)$ on M is given by

$$(r + (p))x = \tilde{\psi}(r + (p))(x) = \psi(r)(x) = rx.$$

Suppose that $\varphi : M \longrightarrow \overline{M}$ is a surjective R–module homomorphism. For $x \in M$, $p\varphi(x) = \varphi(px) = 0$. Thus $p\overline{M} = p\varphi(M) = \{0\}$, and $\overline{M}$ is a also an $R/(p)$–vector space. Moreover,

$$\varphi((r + (p))x) = \varphi(rx) = r\varphi(x) = (r + (p))\varphi(x),$$

so φ is $R/(p)$–linear. ■

We are now ready for the proof of uniqueness in Theorem M.5.2.

Proof of Uniqueness in Theorem M.5.2 Suppose that M has two direct sum decompositions:

$$M = A_0 \oplus A_1 \oplus A_2 \oplus \cdots \oplus A_s,$$

where

- A_0 is free,
- for $i \geq 1$, $A_i \cong R/(a_i)$, and
- the ring elements a_i are nonzero and noninvertible, and a_i divides a_j for $i \geq j$;

and also

$$M = B_0 \oplus B_1 \oplus B_2 \oplus \cdots \oplus B_t,$$

where

- B_0 is free,
- for $i \geq 1$, $B_i \cong R/(b_i)$, and
- the ring elements b_i are nonzero and noninvertible, and b_i divides b_j for $i \geq j$;

We have to show that $\mathrm{rank}(A_0) = \mathrm{rank}(B_0)$, $s = t$, and $(a_i) = (b_i)$ for all $i \geq 1$.

By Lemma M.5.6 , we have

$$M_{\mathrm{tor}} = A_1 \oplus \cdots \oplus A_s = B_1 \oplus B_2 \oplus \cdots \oplus B_t.$$

Hence $A_0 \cong M/M_{\text{tor}} \cong B_0$. By uniqueness of rank (Lemma M.4.2), $\text{rank}(A_0) = \text{rank}(B_0)$.

It now suffices to prove that the two decompositions of M_{tor} are essentially the same, so we may assume that $M = M_{\text{tor}}$ for the rest of the proof.

Note that a_1 and b_1 are periods of M. So we can assume $a_1 = b_1 = m$.

We proceed by induction on the length of m, that is, the number of irreducibles (with multiplicity) occuring in an irreducible factorization of m. If this number is one, then m is irreducible, and all of the b_i and a_j are associates of m. In this case, we have only to show that $s = t$. Since $mM = \{0\}$, by Lemma M.5.8, M is an $R/(m)$–vector space; moreover, the first direct sum decomposition gives $M \cong (R/(m))^s$ and the second gives $M \cong (R/(m))^t$ as $R/(m)$–vector spaces. It follows that $s = t$ by uniqueness of dimension.

We assume now that the length of m is greater than one and that the uniqueness assertion holds for all finitely generated torsion modules with a period of smaller length.

Let p be an irreducible in R. Then $a \mapsto pa$ is a module endomorphism of M that maps each A_i into itself. According to Lemma M.5.7, if p divides a_i then $A_i/pA_i \cong R/(p)$, but if p is relatively prime to a_i, then $A_i/pA_i = \{0\}$.

We have

$$\begin{aligned} M/pM &\cong (A_1 \oplus A_2 \oplus \cdots \oplus A_s)/(pA_1 \oplus pA_2 \oplus \cdots \oplus pA_s) \\ &\cong A_1/pA_1 \oplus A_2/pA_2 \oplus \cdots \oplus A_s/pA_s \cong (R/(p))^k, \end{aligned}$$

where k is the number of a_i such that p divides a_i.

Since $p(M/pM) = \{0\}$, according to Lemma M.5.8, all the R–modules in view here are actually $R/(p)$–vector spaces and the isomorphisms are $R/(p)$–linear. It follows that the number k is the dimension of M/pM as an $R/(p)$–vector space. Applying the same considerations to the other direct sum decomposition, we obtain that the number of b_i divisible by p is also equal to $\dim_{R/(p)}(M/pM)$.

If p is an irreducible dividing a_s, then p divides exactly s of the b_i. Hence $s \le t$. Reversing the role of the two decompositions, we get $t \le s$. Thus the number of direct summands in the two decompositions is the same.

Fix an irreducible p dividing a_s. Then p must divide b_s as well. Let k' be the last index such that $a_{k'}/p$ is not a unit.

Then pA_j is cyclic of period a_j/p for $j \le k'$, while $pA_j = \{0\}$ for $j > k'$, and $pM = pA_1 \oplus \cdots \oplus pA_{k'}$. Likewise, let k'' be the last index such that $b_{k''}/p$ is not a unit. Then pB_j is cyclic of period b_j/p for $j \le k''$, while $pB_j = \{0\}$ for $j > k''$, and $pM = pB_1 \oplus \cdots \oplus pB_{k''}$.

Applying the induction hypothesis to pM (which has period m/p) gives $k' = k''$ and $(a_i/p) = (b_i/p)$ for all $i \leq k'$. It follows that $(a_i) = (b_i)$ for all $i \leq k'$. But for $k' < i \leq s$, we have $(a_i) = (b_i) = (p)$. ■

The elements a_i appearing in the direct sum decomposition of the Structure Theorem are called the *invariant factors* of M. They are determined only up to multiplication by units.

Corollary M.5.9. *Let R be a principal ideal domain, and let M be a (nonzero) finitely generated torsion module over R. Suppose that there exists an irreducible p in R and a natural number n such that $p^n M = \{0\}$.*

(a) *There exist natural numbers $s_1 \geq s_2 \cdots \geq s_k$ such that*
$$M \cong R/(p^{s_1}) \otimes R/(p^{s_2}) \otimes \cdots \otimes R/(p^{s_k}).$$

(b) *The sequence of exponents in part (b) is unique. That is, if $t_1 \geq t_2 \geq \cdots \geq t_\ell$, and*
$$M \cong R/(p^{t_1}) \otimes R/(p^{t_2}) \otimes \cdots \otimes R/(p^{t_\ell}).$$
then $k = \ell$ and $t_i = s_i$ for all i.

Proof. This is just the special case of the theorem for a module whose period is a power of an irreducible. ■

For each irreducible p , define
$$M[p] = \{x \in M : p^j x = 0 \text{ for some } j\}.$$

It is straightforward to check that $M[p]$ is a submodule of M. If p and p' are associates, then $M[p] = M[p']$. Note that $p^r x = 0$ for $x \in M[p]$, where p^r is the largest power of p dividing the period m of M. See Exercise M.5.6. $M[p] = \{0\}$ if p does not divide m.

We will show that M is the (internal) direct sum of the submodules $M[p]$ for p appearing in an irreducible factorization of m.

Theorem M.5.10. *(Primary decomposition theorem) Let M be a finitely generated torsion module over a principal ideal domain R, let m be a period of M with irreducible factorization $m = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$. Then*
$$M \cong M[p_1] \oplus \cdots \oplus M[p_k].$$

Proof. For each index i let $f_i = m/p_i^{m_i}$; that is, f_i is the product of all the irreducible factors of m that are relatively prime to p_i. For all $x \in M$, we have $f_i x \in M[p_i]$, because $p_i^{m_i}(f_i x) = mx = 0$. Furthermore, if $x \in M[p_j]$ for some $j \neq i$, then $f_i x = 0$, because $p_j^{m_j}$ divides f_i.

The greatest common divisor of $\{f_1, \dots, f_s\}$ is 1. Therefore, there exist $t_1, \dots, t_s$ in R such that $t_1 f_1 + \cdots + t_s f_s = 1$. Hence for any $x \in M$, $x = 1x = t_1 f_1 x + \cdots + t_s f_s x \in M[p_1] + M[p_2] + \cdots + M[p_s]$. Thus $G = M[p_1] + \cdots + M[p_s]$.

Suppose that $x_j \in M[p_j]$ for $1 \leq j \leq s$ and $\sum_j x_j = 0$. Fix an index i. Since $f_i x_j = 0$ for $j \neq i$, we have

$$0 = f_i(\sum_j x_j) = \sum_j f_i x_j = f_i x_i.$$

Because f_i is relatively prime to the period of each nonzero element of $M[p_i]$, it follows that $x_i = 0$. Thus by Proposition M.1.28 $M = M[p_1] \oplus \cdots \oplus M[p_s]$. ■

Corollary M.5.11. *Let $y \in M$ and write $y = y_1 + y_2 + \cdots + y_s$, where $y_j \in M[p_j]$ for each j. Then $y_j \in Ry$.*

Proof. If f_j and t_j are as in the proof of the theorem, then $y_j = f_j t_j y$. ■

Lemma M.5.12. *Suppose a finitely generated torsion module M over a principal ideal domain R is an internal direct sum of a collection $\{C_i\}$ of cyclic submodules, each having period a power of a prime. Then for each irreducible p, the sum of those C_i that are annihilated by a power of p is equal to $M[p]$.*

Proof. Let $p_1, p_2, \dots, p_s$ be a list of the irreducibles appearing in an irreducible factorization of a period m of M.

Denote by $A[p_j]$ the sum of those C_i that are annihilated by a power of p_j. Then $A[p_j] \subseteq M[p_j]$ and M is the internal direct product of the submodules $A[p_j]$. Since M is also the internal direct product of the submodules $M[p_j]$, it follows that $A[p_j] = M[p_j]$ for all j. ■

Theorem M.5.13. *(Structure Theorem for Finitely Generated Torsion Modules over a PID, Elementary Divisor Form) Let R be a principal ideal domain, and let M be a (nonzero) finitely generated torsion module over R. Then M isomorphic to a direct sum of cyclic submodules, each having period a power of an irreducible,*

$$M \cong \bigoplus_j \bigoplus_i R/(p_j^{n_{i,j}})$$

The number of direct summands, and the annihilator ideals $(p_j^{n_{i,j}})$ of the direct summands are uniquely determined (up to order).

Proof. For existence, first decompose M as the direct sum of its primary components:

$$M \cong M[p_1] \oplus \cdots \oplus M[p_k]$$

using Theorem M.5.10, and then apply Corollary M.5.9 to each of the primary components.

For uniqueness, suppose that $\{C_i : 1 \leq i \leq K\}$ and $\{D_i : 1 \leq i \leq L\}$ are two families of cyclic submodules of M, each with period a power of an irreducible, such that $M = C_1 \oplus \cdots \oplus C_K$ and $M = D_1 \oplus \cdots \oplus D_L$.

Let m be a period of M with irreducible factorization $m = p_1^{m_1} \cdots p_s^{m_s}$. Then for each of the cyclic submodules in the two families has period a power of one of the irreducibles $p_1, \dots, p_s$. Group the two families accordingly:

$$\{C_i\} = \bigcup_{p_j} \{C_i^{p_j} : 1 \leq i \leq K(p_j)\}, \quad \text{and}$$
$$\{D_i\} = \bigcup_{p_j} \{D_i^{p_j} : 1 \leq i \leq L(p_j)\},$$

where the periods of $C_i^{p_j}$ and $C_i^{p_j}$ are powers of p_j. It follows from the previous lemma that for each j,

$$\bigoplus_{i=1}^{K(p_j)} C_i^{p_j} = \bigoplus_{i=1}^{L(p_j)} D_i^{p_j} = M[p_j].$$

Corollary M.5.9 implies that $K(p_j) = L(p_j)$ and the annihilator ideals of the submodules $C_i^{p_j}$ agree with those of the submodules $D_i^{p_j}$ up to order.

It follows that $K = L$ and that the list of annihilator ideals of the submodules C_i agree with the list of annihilator ideals of the submodules D_i, up to order. ■

The periods $p_j^{n_{i,j}}$ of the direct summands in the decomposition described in Theorem M.5.13 are called the*elementary divisors* of M. They are determined up to multiplication by units.

Example M.5.14. Let

$$f(x) = x^5 - 9x^4 + 32x^3 - 56x^2 + 48x - 16$$

and

$$g(x) = x^{10}-6x^9+16x^8-30x^7+46x^6-54x^5+52x^4-42x^3+25x^2-12x+4.$$

Their irreducible factorizations in $\mathbb{Q}[x]$ are

$$f(x) = (x-2)^4(x-1)$$

and

$$g(x) = (x-2)^2(x-1)^2\left(x^2+1\right)^3.$$

Let M denote the $Q[x]$–module $M = \mathbb{Q}[x]/(f) \oplus \mathbb{Q}[x]/(g)$. Then

$$\begin{aligned} M &\cong \mathbb{Q}[x]/((x-2)^4) \oplus \mathbb{Q}[x]/((x-1)) \\ &\quad \oplus \mathbb{Q}[x]/((x-2)^2) \oplus \mathbb{Q}[x]/((x-1)^2) \oplus \mathbb{Q}[x]/((x^2+1)^3) \end{aligned}$$

The elementary divisors of M are $(x-2)^4, (x-2)^2, (x-1)^2, (x-1)$, and $(x^2+1)^3$. Regrouping the direct summands gives:

$$\begin{aligned} M &\cong \left(\mathbb{Q}[x]/((x-2)^4) \oplus \mathbb{Q}[x]/((x-1)^2) \oplus \mathbb{Q}[x]/((x^2+1)^3)\right) \\ &\oplus \left(\mathbb{Q}[x]/((x-2)^2) \oplus \mathbb{Q}[x]/((x-1))\right) \\ &\cong \mathbb{Q}[x]/((x-2)^4(x-1)^2\left(x^2+1\right)^2) \oplus \mathbb{Q}[x]/((x-2)^2(x-1)). \end{aligned}$$

The invariant factors of M are $(x-2)^4(x-1)^2\left(x^2+1\right)^3$ and $(x-2)^2(x-1)$.

Exercises M.5

M.5.1. Let M be a module over an integral domain R. For an nonzero element $x \in M$, show that $\operatorname{ann}(x)$ is an ideal of R and $\operatorname{ann}(x) \underset{\neq}{\subset} R$.

M.5.2. Let R be an integral domain, M an R–module and S a subset of R. Show that $\operatorname{ann}(S)$ is an ideal of R and $\operatorname{ann}(S) = \operatorname{ann}(RS)$.

M.5.3. Let M be a module over an integral domain R. Show that M/M_{tor} is torsion free

M.5.4. Let M be a module over an integral domain R. Suppose that $M = A \oplus B$, where A is a torsion submodule and B is free. Show that $A = M_{\text{tor}}$.

M.5.5. Let M be a finitely generated torsion module over a PID R. Let p and p' be two associated irreducibles of R; i.e. $p = up'$ where u is a unit. Show that $M[p] = M[p']$.

M.5.6. Let M be a finitely generated torsion module over a PID R. Let m be a period of M with irreducible factorization $m = p_1^{m_1} \cdots p_s^{m_s}$. Show that for each i and for all $x \in M[p_i]$, $p_i^{m_i} x = 0$.

M.6. Rational canonical form

In this section we apply the theory of finitely generated modules of a principal ideal domain to study the structure of a linear transformation of a finite dimensional vector space.

If T is a linear transformation of a finite dimensional vector space V over a field K, then V has a $K[x]$–module structure determined by $f(x)v = f(T)v$ for $f(x) \in K[x]$ and $v \in V$. Since V is finitely generated as a K–module, it is finitely generated as a $K[x]$–module. Moreover, V is a torsion module over $K[x]$. In fact, if V is n–dimensional, then $\text{End}_K(V)$ is an n^2–dimensional vector space over K, so the $n^2 + 1$ linear transformations $\text{id}, T, T^2, \dots, T^{n^2}$ are not linearly independent. Therefore, there exist $\alpha_0, \dots, \alpha_{n^2}$ such that $\sum_{j=0}^{n^2} \alpha_j T^j = 0$ in $\text{End}_K(V)$. But this means that the polynomial $\sum_{j=0}^{n^2} \alpha_j x^j$ is in the annihilator of V in $K[x]$.

A $K[x]$–submodule of V is a vector subspace V_1 that is invariant under T, $Tv \in V_1$ for all $v \in V_1$. If $(x_1, \dots, x_n)$ is an ordered basis of V such that the first k basis elements form a basis of V_1, then the matrix of T with respect to this basis has the block triangular form:

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}.$$

If $V = V_1 \oplus V_2$ where both V_1 and V_2 are invariant under T, and $(x_1, \dots, x_n)$ is an ordered basis of V such that the first k elements constitute a basis of V_1 and the remaining elements constitute a basis of V_2, then the matrix of T with respect to this basis has the block diagonal form:

$$\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}.$$

If V is the direct sum of several T–invariant subspaces,

$$V = V_1 \oplus \cdots \oplus V_s,$$