Lectures on Modules over Principal Ideal Domains

Parvati Shastri
Department of Mathematics
University of Mumbai

1 – 7 May 2014

Contents

1 Modules over Commutative Rings

1.1 Definition and examples of Modules

(Throughout these lectures, R denotes a commutative ring with identity, k denotes a field, V denotes a finite dimensional vector space over k and M denotes a module over R, unless otherwise stated.)

The notion of a module over a commutative ring is a generalization of the notion of a vector space over a field, where the scalars belong to a commutative ring. However, many basic results in the theory of vector spaces are no longer true for modules over a commutative ring, even when the ring is sufficiently nice, say for instance the ring of integers. Historically, the theory of modules has its origin in Number Theory and Linear Algebra. The word *module* seems to have occurred for the first time in Number Theory. We shall first give some formal definitions.

Definition 1.1 *A triple $(M, +, .)$, where $(M, +)$ is an abelian group and $. : R \times M \to M$ is a map (called scalar multiplication) satisfying the following conditions, is called a module over R (or an R-module):*

(i) $a.(m + m') = a.m + a.m'$ *for all* $m, m' \in M, a \in R$,

(ii) $(a + b).m = a.m + b.m$ *for all* $a, b \in R, m \in M$,

(iii) $a.(b.m) = (ab).m$ *for all* $m \in M, a, b \in R$,

(iv) $1.m = m$ *for all* $m \in M$.

As usual, we shall now onwards, write am for $a.m$

Definition 1.2 *A sub group N of M is called a sub module of M, if it is closed under scalar multiplication induced from M; i.e., if the following condition is satisfied:*
For all $a \in R$ and $m \in N$, $am \in N$.

If N is a sub module of M, then the quotient group M/N has the natural structure of a module over R, with the scalar multiplication defined as follows:
$a.\overline{m} = \overline{am}$ for all $\overline{m} \in M/N$ and $a \in R$.
We call M/N (with this scalar multiplication) the quotient module (of M by N).
The corresponding notion of a linear map between vector spaces, is called a *homomorphism* of modules.

Definition 1.3 *Let M, M' be modules over R. A function*

$$f : M \to M'$$

is called a homomorphism (of modules), if the following conditions are satisfied:

(i) f is a group homomorphism; i.e., $f(m_1 + m_2) = f(m_1) + f(m_2)$ for all $m_1, m_2 \in M$.

(ii) f preserves scalar multiplication; i.e., $f(am) = af(m)$ for all $a \in R$ and $m \in M$.

A bijective homomorphism is called an isomorphism. A homomorphism (respectively, isomorphism) of M into (respectively onto) itself is called an endomorphism (respectively automorphism) of M.

Example 1.4

1. *A vector space is a module over a field.*
2. *Any ideal in R is a module over R. In particular, R is a module over itself.*

3. *Abelian group and $\mathbb{Z}-$module are one and the same. So any abelian group is a $\mathbb{Z}$- module.*

4. *If $(M_i)_{i\in I}$ is a family of modules over R, then so are the direct product $\prod_{i\in I} M_i$ and the direct sum $\bigoplus_{i\in I} M_i$. Note that $\bigoplus_{i\in I} M_i$ is a sub module of $\prod_{i\in I} M_i$ and the two are equal, if (and only if) I is finite.*

5. *For any R-modules M, N the set $\mathrm{Hom}_R(M,N)$ forms an R- module in an obvious way: given $f, g \in \mathrm{Hom}_R(M,N)$ and $a \in R$ we have $(f+g)(x) = f(x)+g(x); (af)(x) = af(x),\ \forall\ x \in M$.*

6. *Let $\mathfrak{a}$ be an ideal of R and M be an R-module. Let $\mathfrak{a}M$ be the set of all finite linear combinations of elements of M with coefficients in $\mathfrak{a}$. Then $\mathfrak{a}M$ is a sub module of M.*

The following are routine exercises which the student should do just once.

Exercise 1.5 1. *If $f : M \to M'$ is an isomorphism of $R-$modules, prove that $f^{-1} : M' \to M$ is also a homomorphism of R- modules.*

2. *Prove that the natural map $\eta : M \to M/N$ is an R- module homomorphism.*

3. *Define the following terms in the context of modules over a commutative ring: Set of generators, linearly independent set, finite generation, basis, kernel, image and co-kernel of a homomorphism.*

4. *Consider R as a module over itself. Prove that a singleton set $\{x\}$ is linearly independent if and only if x is not a zero divisor in R.*

5. *State and prove the fundamental homomorphism theorems for modules.*

We shall now illustrate several basic results on vector spaces that *fail* for modules over commutative rings, in general.

1. *Every vector space has a basis.* This is no longer true for modules over a commutative ring. For instance, if G is a finite abelian group, then it is a $\mathbb{Z}-$module, as remarked earlier. But there does not exist any $\mathbb{Z}$-linearly independent element in G.

2. *Any linearly independent subset of a vector space V can be completed to a basis of V.* This is not true for modules in general. For instance, $\{2\}$ is a linearly independent subset of $\mathbb{Z}$ which can not be extended to a basis of $\mathbb{Z}$ as a module over itself. In fact if $n \neq 0 \in \mathbb{Z}$, then the set $\{2, n\}$ is linearly dependent (prove it). In fact, show that any two elements of $\mathbb{Z}$ are linearly dependent.

3. For a subset S of a vector space, the following statements are equivalent:

   (i) S is maximal linearly independent set.

   (ii) S is minimal system of generators.

   (iii) S is a basis.

   This is no more true for modules in general. You can take $\mathbb{Z}$ as module over itself and try to produce counter example. In fact neither (i) implies (ii) nor (ii) implies (i). Nor (i) or (ii) imply (iii). However, (iii) does imply (i) and (ii).

1.2 Free modules and bases

Definition 1.6 *An $R-$module M is said to be free, if there exists a basis for M.*

Example 1.7 *(i) Any vector space over a field is free.*

(ii) Any ring R is a free module over itself, with a basis consisting of a single element $\{1\}$. In fact, $\{u\}$ is a basis of R as module over itself, if and only if u is a unit of R.

(iii) If $(M_i)_{i\in I}$ is a family of free modules over R, then $\bigoplus_{i\in I} M_i$ is also a free module over R. In particular, R^n is free over R with the standard basis $\{e_1, e_2, \cdots, e_n\}$, where $e_i = (0, 0, \cdots 1, 0, \cdots, 0)$; i.e., the i^{th} co-ordinate of e_i is 1 and all other co-ordinates are zero.

(iv) Let R be an integral domain. Then an ideal in R is free if and only if it is a principal ideal.

Remark 1.8

(i) Free modules are like vector spaces. But as you can easily see, even when M is free, 2 and 3 above may fail.

(ii) A sub module of a free module need not be free.

(iii) If an ideal $\mathfrak{a}$ of R is free as an $R-$module, then $\mathfrak{a}$ is a principal ideal. A principal ideal $\mathfrak{a}$ is free if it is generated by a non zero divisor. In particular, if R is an integral domain, then an ideal is free if and only if it is principal.

Proposition 1.9 *If M is a finitely generated free module, then the cardinality of any basis of M is finite. More over, any two bases have the same cardinality.*

Proof: Let $\{v_1, v_2, \cdots, v_n\}$ be a set of generators for M. Let $B := \{e_i : i \in I\}$ be a basis of M. Then each v_j is a finite linear combination of the e_i's. Let S be the set of all the e_i's that occur with non zero coefficients, in the expression for $v_j = \sum_{i\in I} \alpha_i e_i$, for $1 \leq j \leq n$. Clearly $S \subset B$, S is finite and generates M. We claim $S = I$. For, suppose that $e \in B \setminus S$. Then e is a linear combination of elements of S. This is a contradiction to the fact that elements of B are linearly independent. Thus $S = B$ and hence I is finite. So the first part of the theorem follows. Let now, $\{v_1, v_2, \cdots, v_n\}$ and $\{u_1, u_2, \cdots, u_m\}$ be any two bases of M. Then, $v_i = \sum_{j=1}^{m} a_{ji} u_j$ for all $1 \leq i \leq n$ and $u_j = \sum_{i=1}^{n} b_{ij} v_i$. Let $A = [a_{ij}]$ and $B = [b_{ij}]$. Clearly, $A \in M(m \times n, R)$ and $B \in M(n \times m, R)$. Also, $AB = I_m$ and $BA = I_n$. Without loss of generality, suppose that $n < m$. Let $A_1, B_1 \in M(m, R)$ be defined by,

$$A_1 = [A|O] \text{ and } B_1 = \begin{bmatrix} B \\ O \end{bmatrix},$$

where O denotes a zero matrix of appropriate size. Then $A_1 B_1 = AB = I_m$. Therefore, $\det A_1$ and $\det B_1$ are units. Clearly this implies there can not be a row or column of zeroes, in B_1, A_1 respectively. Therefore $n \geq m$. By symmetry, $m \geq n$. Therefore $m = n$.
Alternate proof: We reduce the problem to the case of a vector space as follows. There exists a maximal ideal $\mathfrak{m}$ in R. Then $R^n \cong R^m$ implies $\mathfrak{m}R^n \cong \mathfrak{m}R^m$. This implies $R^n/\mathfrak{m}R^n \cong R^m/\mathfrak{m}R^m$. But $R^r/\mathfrak{m}R^r$ is a vector space of dimension r over the field $R/\mathfrak{m}$ (Prove it!). The same argument holds for free modules with an infinite basis, as well.

Remark 1.10 *There exist non commutative rings R for which $R^n \cong R^m$ for any $m, n \in N$ (see exercise III, 24).*

Definition 1.11 *Let M be a finitely generated free R-module. Then the cardinality of any basis of M is called the rank of M.*

Remark 1.12 *Let R be an integral domain and k be the field of fractions of R. Then $R^n \subset k^n$ and spans the vector space k^n over k. If $R^n \cong R^m$, then we can extend the isomorphism (because it is defined on a set of n linearly independent elements), to an isomorphism of $k^n \to k^m$. This is impossible unless $m = n$. Thus in the case of integral domains, this argument gives another way of defining rank of a free module. In fact, if R is an integral domain and M is a free module over R, we can define the rank of any sub module N of M to be the dimension of the vector space spanned by N in k^n, although N may not be free.*

Exercise 1.13 *(Do not use the proposition above for doing this exercise.) Let R be an integral domain. Let M be free R-module. Prove that any two maximal linearly independent subsets of M have the same cardinality. What is this cardinality?*

2 Modules over a Principal Ideal Domain

2.1 Review of principal ideal domains

Recall that an integral domain R is said to be a Euclidean domain if there exists a function $\delta : R \setminus \{0\} \to \mathbb{N} \cup \{o\}$ such that division algorithm holds with respect to δ. That is, given $a \neq 0$ and $b \in R$, there exist q and $r \in R$ such that $b = aq + r$, either $r = 0$ or $\delta(r) < \delta(a)$. It is an easily proved theorem that every Euclidean domain is a PID. For example, the ring of rational integers is a Euclidean domain with the usual absolute value as the Euclidean function. A polynomial ring in one variable over a field k is Euclidean with the degree of a polynomial as the Euclidean function. The ring of Gaussian integers, $\mathbb{Z}[\sqrt{-1}]$ and the ring of Eisenstein integers, $\mathbb{Z}[\omega]$, (where ω is primitive cube root of unity) are also Euclidean domains, with respect the usual absolute value. However, not all PID's are Euclidean domains. For instance, the ring $\mathbb{Z}[\alpha] := \{a + b\alpha \in \mathbb{C} : a, b \in \mathbb{Z}\}$ where $\alpha = \frac{1+\sqrt{-19}}{2}$ is a PID but not a Euclidean domain (See for instance [D-F] for a proof).

Recall how one proves that in a PID, every non zero element is written as a product of irreducible elements. In fact, we have, $a|b$ if and only if $(b) \subset (a)$. Since, every ascending chain of ideals of a PID, terminates, the result follows.

Exercise 2.1

1. *If R is a PID, prove that every ascending chain of ideals of R terminates.*
2. *Prove that any nonempty family of ideals in R has a maximal element.*

Exercise 2.2 *Let R be a PID. Let $a, b \in R$. Then prove that the gcd of a, b is a linear combination of a, b. That is, if $d =$ gcd of a, b, then there exist $x, y \in R$ such that $d = xa + yb$.*

2.2 Structure of finitely generated modules over a PID: Cyclic Decomposition

From now on, R denotes a PID, unless otherwise stated.

Theorem 2.3 *Let R be a PID and M be a finitely generated free module over R, of rank n. Then every submodule of M is also free of rank $\leq n$.*

Proof: Let $\{e_1, e_2, \cdots, e_n\}$ be a basis of M so that $M \cong R^n$. We prove the theorem by induction on n. If $n = 1$, then $M \cong R$. Since R is a PID, every ideal (submodule of R) is free of rank ≤ 1. So the theorem holds for $n = 1$. Assume the theorem to be true for all modules of rank $\leq n-1$. Let N be a submodule of M. If $N = \{0\}$, there is nothing to prove. Suppose $N \neq \{0\}$. Consider the projection maps $\pi_i : M = R^n \to R$ for $1 \leq i \leq n$. Then $\ker \pi_i$ is a module over R of rank $n - 1$. Since $N \neq \{0\}$, $\pi_i(N) \neq \{0\}$ for some i. Therefore $\pi_i(N)$ is non zero ideal in R. Thus it is free of rank 1. Also, $\ker \pi_i \cap N$ is a submodule of $\ker \pi_i$. By induction hypothesis, rank of $\ker \pi_i \cap N$ is $\leq n - 1$. Let α be a generator for $\pi_i(N)$ and $v \in N$ be any element such that $\pi_i(v) = \alpha$. It is an easy exercise to show that $N = \ker \pi_i \cap N \oplus vR$. If $\{v_1, v_2, \cdots v_m\}$ is a basis of $\ker \pi_i \cap N$, then $\{v_1, v_2 \cdots v_m, v = v_{m+1}\}$ is a basis of N. Hence rank of N equals $m + 1 \leq n$. This completes the proof of the theorem.

The following is a stronger version of the above theorem, which is crucial in the study of finitely generated modules over a PID.

Theorem 2.4 *(Structure Theorem) Let R be a PID and M be a finitely generated free module over R of rank n. Then the following are true.*

(a) If N is a submodule of M, then N is also finitely generated, free of rank r, with $0 \leq r \leq n$.

(b) If $N \neq \{0\}$, then there exists a basis $\{e_1, e_2, \cdots, e_n\}$ of M and non zero elements $a_1, a_2, \cdots, a_r \in R$ such that $\{a_1e_1, a_2e_2, \cdots, a_re_r\}$ is a basis of N and $a_i|a_{i+1}$ $\forall$ $1 \leq i \leq r - 1$.

Example 2.5 *Consider $M = \mathbb{Z} \times \mathbb{Z}$. This is a subgroup of R^2 and $\{(1,0),(0,1)\}$ is basis of M. Let N_1 be the submodule of M generated by $\{(2,0),(0,1)\}$ and N_2 be the submodule of M generated by $\{(1,0),(2,2)\}$. Draw the picture in the plane and mark the points of M, N_1, N_2. Prove that the standard basis is already is as asserted in the theorem, for the submodule N_1. But for N_2, you need to make a change of basis. For instance, $\{(1,0),(1,1)\}$ is another basis of $\mathbb{Z}^2$, for which, if we take $\alpha_1 = 1$, and $\alpha_2 = 2$, we get the statement of the theorem. What does it mean geometrically?)*

Proof: We have already proved part (a). We will prove part (b). The theorem is trivial for $N = \{0\}$. So we may assume that $N \neq \{0\}$. Consider the family

$$\mathcal{F} = \{T(N) : T \in \mathrm{Hom}_R(M, R)\}.$$

Each $T(N)$ is a submodule of R. That is to say, it is an ideal of R. But R is a PID. Now any nonempty family of ideals of a PID, has a maximal element and it is a principal ideal. Let (α) be a maximal element of $\mathcal{F}$. We claim that it is not the zero ideal. For proving this, note that M is free of rank n. Therefore $M \cong R^n$. Let π_j denote the j^{th} projection map. Since $N \neq \{0\}$, there exists $x = (x_1, x_2, \cdots, x_n) \in N$ such that $x_j \neq 0$ for some j. Clearly, for this j, $\pi_j(N) \neq 0$. This means $(\alpha) \neq (0)$.

By the definition of $\mathcal{F}$, it follows that there exists $T_0 \in \mathrm{Hom}_R(M, R)$ and an element $v \in N$ such that $T_0(v) = \alpha$. We claim that if $T \in \mathrm{Hom}_R(M, R)$, then α divides $T(v)$. For this, let $d = \gcd(\alpha, T(v))$. Since R is a PID, there exist $x, y \in R$ such that $d = x\alpha + yT(v)$. Since d divides α, we have $(\alpha) \subset (d)$. But $d = x\alpha + yT(v) = (xT_0 + yT)(v)$ and $(xT_0 + yT) \in \mathrm{Hom}_R(M, R)$. Therefore, by the choice of α, it follows that $d \in (alpha)$. Thus we must have $(d) = (\alpha)$ and hence α divides $T(v)$, for all $T \in \mathrm{Hom}_R(M, R)$.

In particular, this applies to the projection maps π_j. Thus α divides $\pi_j(v)$. Hence $v = (\alpha b_1, \alpha b_2, \cdots, \alpha b_n)$. Let $w = (b_1, b_2, \cdots, b_n)$ so that $v = \alpha w$. But then, $\alpha = T_0(v)\alpha T_0(w)$. Therefore, we get $T_0(w) = 1$. We claim:

1. $M = (\ker(T_0)) \oplus Rw$
2. $N = (N \cap \ker(T_0)) \oplus Rv$.

Proof of the claim is left as an exercise.

By [1] above, rank of $\ker T_0$ is $n - 1$.

Now, to complete the proof of (b), we use induction on the rank n of M. The case $n = 1$ is obvious, since R is a PID. So let $n > 1$ and assume the result to be true for all free modules of rank $< n$. Since $\ker T_0$ is a free module of rank $n-1$, by induction hypothesis there exists a basis $\{e_2, e_3, \cdots, e_n\}$ of $\ker T_0$ and elements $\alpha_2, \alpha_3, \cdots \alpha_r \in R$ such that $\{\alpha_2 e_2, \alpha_3 e_3, \cdots, \alpha_r e_r\}$ is a basis of $(\ker T_0) \cap N$ and $\alpha_i | \alpha_{i+1}$ for all $2 \leq i \leq r-1$. Let us take $\alpha = \alpha_1$ and $w = e_1$, where α and v are as in the discussion in the first part of the proof. It is now clear that $\{e_1, e_2, \cdots, e_n\}$ is a basis of M and $\{\alpha_1 e_1, \alpha_2 e_2, \cdots, \alpha_r e_r\}$ is a basis of N. We have to prove that α_1 divides α_2. Let $T \in \mathrm{Hom}_R(M, R)$ be defined by $T(e_1) = 1 = T(e_2)$ and $T(e_i) = 0$ for $i > 2$. Then $\alpha_1 = T(\alpha w) \in T(N)$. Thus $(\alpha) \subset T(N)$. By the maximality of (α), it follows that $T(N) = (\alpha_1)$. Since $\alpha_2 = T(\alpha_2 e_2)$, it follows that $\alpha_2 \in (\alpha_1)$. Clearly, this means α_1 divides α_2. The theorem is completely proved.

For further discussions, it is convenient to have the following definition.

Definition 2.6 *A module M over a commutative ring R is said to be cyclic, if it is generated by one element.*

Corollary 2.7 *Let R be a PID and let M be a finitely generated $R-$module. Then M is isomorphic to a finite direct sum of cyclic modules. More specifically, $M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n)$, where $(a_1) \supset (a_2) \supset \cdots \supset (a_n)$.*

Proof: Let M be generated by $\{x_1, x_2, \cdots, x_n\}$. Then, $\exists$ a surjective homomorphism $f : R^n \to M$. By the theorem, there exists a basis $\{e_1, e_2, \cdots, e_n\}$ of R^n and elements $\alpha_1, \alpha_2, \cdots, \alpha_m \in R$ such that

$\alpha_1 e_1, \alpha_2 e_2, \cdots, \alpha_m e_m\}$ is a basis of $\ker f$. Since $\mathbb{R}^n/\ker f \cong M$, the corollary follows by taking $\alpha_i = \{0\}$ for $n \geq i \geq m$.

Corollary 2.8 *Let R be a PID and $M \cong R/(a_1) \times R/(a_2) \cdots \times R/(a_n)$, where $(a_1) \supset (a_2) \supset \cdots \supset (a_n)$. Then M is free if and only if $(a_i) = (0)$ for all $1 \leq i \leq n$.*

Proof: Left as an exercise.

2.3 Equivalence of matrices over a PID

Definition 2.9 *Let R be a commutative ring. Two matrices $A, B \in M(m \times n, R)$ are said to be equivalent if there exist invertible matrices $P \in M(n, R), \mathbb{Q} \in M(m, R)$, such that $QAP^{-1} = B$.*

Clearly, this is an equivalence relation. It is an interesting problem to determine a particularly simple matrix in each equivalence class. If R is a field, then every matrix $A \in M(m \times n, R$ is equivalent to a matrix

$$\begin{bmatrix} 1 & 0 & \cdots & \cdot & \cdot & \cdots & 0 \\ 0 & 1 & \cdots & \cdot & \cdot & \cdots & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \cdot & \cdots & 1 & \cdot & \cdots & 0 \\ 0 & \cdot & \cdots & \cdot & 0 & \cdots & 0 \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdot & \cdots & \cdot & \cdot & \cdots & 0 \end{bmatrix}.$$

The situation is not so nice for arbitrary commutative rings. However, if R is a PID, we can show that every matrix $A \in M(m \times n, R)$ is equivalent to a matrix $[\alpha_{ij}]$, where $\alpha_{ll} = d_l$ for $1 \leq l \leq r$ and $\alpha_{ij} = 0$ for all i, j such that $(i, j) \neq (l, l), 1 \leq l \leq r$ and $d_l | d_{l+1}$ for all $1 \leq l \leq (r-1)$. First let us show, how the structure theorem can be used to prove this fact.

Theorem 2.10 *Let R be a PID. Then every matrix $A \in M(m \times n, R)$ is equivalent to a matrix*

$$\begin{bmatrix} d_1 & 0 & \cdots & \cdot & \cdot & \cdots & 0 \\ 0 & d_2 & \cdots & \cdot & \cdot & \cdots & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \cdot & \cdots & d_r & \cdot & \cdots & 0 \\ 0 & \cdot & \cdots & \cdot & 0 & \cdots & 0 \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdot & \cdots & \cdot & \cdot & \cdots & 0 \end{bmatrix}$$

with $d_i | d_{i+1}$ for $1 \leq i \leq r-1$.

Definition 2.11 *The matrix form obtained in the above proposition is called as Smith normal form or simply normal form of the given matrix over R.*

Proof: Let T_A denote the homomorphism : $R^n \to R^m$ given by left multiplication by A. Then $T_A(R^n)$ is a sub module of a free module of rank m. Therefore, by structure theorem there exists a basis $B' = \{e_1, e_2, \cdots, e_m\}$ of R^m and elements $d_1, d_2, \cdots, d_r \in R$ such that $\{d_1 e_1, d_2 e_2, \cdots, d_r e_r\}$ is a basis of $T_A(R^n)$. Let $f_i \in R^n, 1 \leq i \leq r$ be such that $T_A(f_i) = d_i e_i$ for $1 \leq i \leq r$ and N be the sub module of R^n generated by $\{f_1, f_2, \cdots, f_r\}$. Then $R^n = N \oplus \ker T_A$. Let $\{f_{r+1}, f_{r+2}, \cdots, f_n\}$ be any basis of $\ker T_A$. Then $B = \{f_1, f_2, \cdots, f_n\}$ is a basis of R^n. It is easy to see that the matrix of the linear transformation with

respect to the bases B and B' of R^n and R^m respectively, is of the required form. Equivalently, if P denote the matrix of the change of basis of R^n and Q denotes the matrix of change of basis of R^m, then QAP^{-1} is of the required form.

The proof of the structure theorem is existential. Therefore the above theorem is also so. It is possible to give a direct proof of the above theorem which is constructive and does not use the structure theorem. In fact, we can directly prove the above theorem on equivalence of matrices (which is constructive) and use it to derive the structure theorem. Let us do it now. For this, it is instructive to recall how this is done for matrices over a field. This is done by elementary row and column operations on matrices. This method can be applied to matrices over a Euclidean domain with some modification to matrices over a PID. First let us assume that R is a Euclidean domain. Let δ be a Euclidean function on R.

Step I: If A is the zero matrix, there is nothing to prove. Otherwise, by interchanging the rows and columns you can move an element of smallest size, as the $(1,1)^{\text{th}}$ element. That is to say, in the new matrix a_{11} is such that $\delta(a_{11})$ is the least. Now bring the first row, to the form $[a_{11}, 0, \cdots, 0]$ as follows. If all elements in the first row are multiples of a_{11}, subtract a suitable multiple of the first column from the j^{th} column for all j. Otherwise, suppose a_{1k} is not a multiple of a_{11}. Then, write $a_{1j} = qa_{11} + r$ where $\delta(r) < \delta(a_{11})$ and interchange the first column and the j^{th} column. Now repeat the process, until you get all zeroes in the first row, except the first one. You can do similar row operations on the first column to obtain a matrix of the form,

$$\begin{bmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ 0 & b_{22} & b_{23} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & b_{m1} & b_{m2} & \cdots & b_{mn} \end{bmatrix}.$$

Step II: Now, if all the b_{ij} are multiples of a_{11}, we do step I to the matrix $B = [b_{ij}]$. Suppose that not all b_{ij} are multiples of a_{11}. Say, b_{ij} is not a multiple of a_{11}. Then add the i^{th} row to the first row. Subtract a multiple of the first column from the j^{th} column, so that the ij^{th} entry is of smaller size than a_{11}. Now interchange the first and the j^{th} column and then the first and the i^{th} row. Repeat the first step to make all other entries in the first row and column zero. Since, each time we are reducing the size of the element, viz.; $\delta(*)$, (which is a positive integer), in a finite number of steps, we must get a matrix of the above type such that a_{11} divides b_{ij} for all $2 \leq i \leq m, 2 \leq j \leq n$.

Now apply step I and II to the matrix $B = [b_{ij}]$.

It remains to consider the case of a principal ideal domain. Here, we do not have the Euclidean function. We need to replace the Euclidean function, by suitable size function. For any $\alpha \neq 0$, we know that α can be uniquely expressed as product of primes. Define the length of an element $l(\alpha)$ to be the number of primes in its factorization. To be precise, if $\alpha = p_1 p_2 \cdots p_r$, ($p_i$'s are not necessarily distinct, we define $l(\alpha)$ to be r. Note that if α is a unit, $r = 0$ and so the length is 0. For proving the theorem for matrices over a PID, in addition to the elementary row and column operations (which sufficed in the case of Euclidean domains), we need to multiply on the left and right by matrices of the following type. $J := [a_{ij}]_{1 \leq i,j \leq n}$, with $a_{ii} = 1$ for all $i \geq 3$, $a_{ij} = 0$ for $i \neq j, \geq 3$ and the two by two matrix

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

is invertible. By interchanging rows and columns, as in the earlier case we can assume that $a_{11} \neq 0, l(a_{11}) \leq l(a_{ij})\ \forall\ i, j$. If a_{11} does not divide a_{1j} for some j, let $d = (a_{11}, a_{1j})$ be the gcd of a, b. Without loss of generality, we can assume that $j = 2$. Then $l(d) < l(a_{11})$. Since R is a PID, there exist $x, y \in R$ such that

$d = -xa_{11} + ya_{12}$. Let $s = a_{12}/d, t = a_{11}/d$. Then we have,

$$\begin{bmatrix} -t & s \\ y & -x \end{bmatrix} \begin{bmatrix} x & s \\ y & t \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus the matrix $\begin{bmatrix} x & s \\ y & t \end{bmatrix}$ is invertible. Now multiply A by the matrix J. In the resulting matrix, the first row is $[d, 0, a_{13}, \cdots, a_{1n}]$. The rest of the proof should be clear to the student by now. We leave it as an exercise.

Definition 2.12 *The elements which we obtained in the above theorem are called the invariant factors of A. They are uniquely determined, upto multiplication by units of R.*

Exercise 2.13 *Do some exercises based on $k[X], \mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. See Miscellaneous Exercises (Exercises V) for details.*

2.4 Presentation Matrices: generators and relations

Although every finitely generated module over a PID does not admit a basis, from the structure theorem, we can show that such a module can be given by a set of generators and a complete set of relations between these generators. In fact if M is generated by $\{x_1, x_2, \cdots, x_n\}$, then there exists a surjective homomorphism $f : R^n \to M$ given by $f(e_i) = x_i$, where $\{e_1, e_2, \cdots, e_n\}$ is the standard basis of R^n. Let $N = \ker f$. Then $\ker f \cong R^m$ for some m. Thus $M \cong R^n/f(R^m)$. Suppose $\{v_1, v_2, \cdots, v_m\}$ is a basis of $\ker f$, then clearly $f(v_i) = 0$ for $1 \leq i \leq m$ gives a complete system of relations between the generators of M. If $f(v_j) = \sum_{i=1}^{n} a_{ij}x_i$, then it is obvious that we can write these relations in the form of a matrix equation:

$$A[v_1, v_2, \cdots, v_n]^t = 0,$$

(though $\{v_1, v_2, \cdots, v_n\}$ is not a basis,) where $A = [a_{ij}]$ is the matrix of the coefficients of the relations $f(v_i) = 0$. The matrix A as obtained above is called a *presentation matrix* of M. There can be several presentation matrices for a given module M. Also it is easy to see that any $m \times n$ matrix defines a finitely generated module; viz., $T_A(R^n)$, where T_A is given by left multiplication by A.

Let us take an example to illustrate this. For simplicity we take $\mathbb{Z}$-modules. The case of a general PID will be left as a routine exercise. You are advised to do it on your own.

Exercise 2.14 *Based on $k[X], \mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$.*

Remark 2.15 *If R is Euclidean, every matrix can be reduced to a diagonal form through elementary row and column operations. (This is the same as saying every invertible matrix over a Euclidean domain is a product of elementary matrices.) However this is not true for arbitrary PID's. For instance, it is not true for the ring $\mathbb{Z}[\frac{-1+\sqrt{-19}}{2}]$ (cf. [COH]). Therefore the matrices Q, P as obtained in the above proposition can not be replaced by a product of elementary matrices, in general, if R is a PID, although it can always be done for Euclidean domains.*

Exercise 2.16 *Let R be a PID. If A is a presentation matrix for M and $M \cong R^n/A(R^m) \cong \oplus_{i=1}^{s} R/(a_i), (a_i) \neq (0)$, then prove that $(\det A) = (a_1 a_2 \cdots a_s)$.*

3 Classification of finitely generated modules over a PID

3.1 Finitely generated torsion modules

Definition 3.1 *Let R be a ring and M be an $R-$module. An element $m \in M$ is said to be a torsion element if there exists a non zero scalar $a \in R$ such that $am = 0$. A module M is said to be a torsion module, if every element of M is a torsion element. It is said to be torsion free, if $am = 0$ implies $a = 0$ or $m = 0$; i.e., there is no torsion element except zero. The set of all torsion elements of a module M is denoted by M_{tor}.*

Exercise 3.2

(i) Let R be an integral domain. Prove that the set of all torsion elements of M is a submodule of M.

(ii) Let R be an integral domain and let N be the submodule of M consisting of all torsion elements of M. Prove that M/N is torsion free.

(iii) Let R be an integral domain. Let M be a free module over R. Prove that the only torsion element of M is 0. (Thus, if R is an integral domain, M is free implies M is torsion free.)

(iv) Take $R = \mathbb{Z}$ and $M = \mathbb{Q}$. Then, prove that M is torsion free but not free.

(v) Prove that $\mathbb{Q}$ is not finitely generated as a module over $\mathbb{Z}$.

(vi) Prove or disprove: The group of all roots of unity in $\mathbb{C}$ is a torsion abelian group.

Proposition 3.3 *Let R be a PID and M be a finitely generated torsion free $R-$module. Then M is free.*

Proof: Apply Corollary (2.6).

Proposition 3.4 *Let M be a finitely generated module over a PID R. Then there exists a submodule N of M which is finitely generated free and $M = M_{tor} \bigoplus N$.*

Proof: M/M_{tor} is finitely generated torsion free and hence free. Let $\eta : M \to M/M_{\text{tor}}$ be the natural quotient map. Let $\{e_i : 1 \leq i \leq m\}$ be a basis of M/M_{tor} and $v_i \in M$ be such that $\eta(v_i) = e_i$. If N denotes the submodule of M spanned by $\{v_i : 1 \leq i \leq m\}$, then N is free and $M = N \oplus M_{\text{tor}}$.

Definition 3.5 *The rank of M is defined to be the rank of M/M_{tor}.*

Proposition 3.6 *Let R be a PID and M, N be two finitely generated modules over R. Then M and N are isomorphic if and only if they have the same rank and the torsion submodules are isomorphic; i.e., $M_{tor} \cong N_{tor}$.*

Proof: Exercise.

To complete the classification of finitely generated modules over a PID, we need to classify finitely generated torsion modules. This is what we shall do in the next two section.

3.2 Primary Decomposition of finitely generated torsion modules over a PID

Definition 3.7 *The set $\{\alpha \in R : \alpha M = \{0\}\}$ is called the annihilator of M and is denoted by $ann(M)$.*

Exercise 3.8

(a) Prove that $ann(M)$ is an ideal in R.

(b) Let R be a PID and M be a cyclic module over R. Then prove that $M \cong R/(\alpha)$ for some $\alpha \in R$.

(c) Prove that $ann(M) = (\alpha)$ if α is as in (b).

Definition 3.9 *Let p be a prime in R. A module M is said to be $p-$primary, if every element of M is annihilated by some power of p. Let p be a prime element of R. For any $R-$module M, let $M_p := \{v \in M : p^r v = 0\}$ for some $r \geq 1$. It is easy to see that M_p is a submodule of M. The submodule M_p is called the p-primary component of M.*

Exercise 3.10 *A cyclic module M is $p-$primary if and only if $ann(M)$ is equal to (p^r) for some $r \geq 1$.*

Proposition 3.11 *A cyclic torsion module over a PID is the direct sum of its $p-$primary submodules. To be more precise, let M be a cyclic torsion module over a PID R. Then, $M \cong \oplus_p M_p$ where p runs over the prime divisors of ann (M).*

Proof: Since M is cyclic, $M \cong R/(a)$, where (a) is the annihilator of M, by the above exercise. Let $(a) = \prod_{i=1}^{r} p_i^{n_i}$. By Chinese Remainder theorem, we have an isomorphism of rings

$$R/(a) \cong \prod_{i=1}^{r} R/(p_i^{n_i}).$$

Clearly this is also an isomorphism of $R-$modules. (Direct sum of finitely many modules is the same as the direct product.)

Corollary 3.12 *Let M be a finitely generated torsion module over a PID R. Then $M_p = \{0\}$ for almost all p and $M = \oplus_p M_p$, where p ranges over all primes in R.*

Proof: Exercise.

Proposition 3.13 *Let M be a finitely generated $p-$primary module. Then,*

$$M \cong \oplus_{i=1}^{r} R/p^{n_i},$$

where $n_i \leq n_{i+1}$ are positive integers. Moreover, the sequence $n_1 \leq n_2 \leq \cdots \leq n_r$ is uniquely determined.

Proof: The first part of the proposition follows from the structure theorem (You can also prove it directly. See exercise below.) Now to prove the uniqueness, it is enough to prove the following. If

$$M = \oplus_{i=1}^{r} \left[R/(p^i)\right]^{n_i}$$

and

$$N = \oplus_{i=1}^{s} \left[R/(p^i)\right]^{m_i}$$

are isomorphic, with $m_i \geq 0$ and $m_r, n_s \neq 0$, then $r = s$ and $n_i = m_i$ for all $1 \leq i \leq r$. As in the case of abelian groups, let us define the exponent of M to be the smallest power of p which annihilates M. It is clear that isomorphic modules will have the same exponent. Therefore, we must have $r = s$. We shall prove the result by induction on the exponent. So let

$$M = \oplus_{i=1}^{r} \left[R/(p^i)\right]^{n_i}$$

and

$$N = \oplus_{i=1}^{s} \left[R/(p^i)\right]^{m_i}.$$

If $r = 1$, then M and N are vector spaces over $R/(p)$. Comparing the dimension, we get $n_1 = m_1$. So the statement is true. So let $r \geq 2$. Then $pM \cong pN$ and the exponents of these modules is p^{r-1}. If any of the n_i, m_i were zero, then the same holds for pM and pN. By induction hypothesis $n_i = m_i$ for all $2 \leq i \leq r$. Now, if $\psi : M \cong N$ is an isomorphism, then $\psi(pM) = pN$. So ψ induces an isomorphism $M/pM \cong N/pN$. Since $M/pM \cong [R/(p)]^{\sum n_i}$ and $N/pN \cong [R/(p)]^{\sum m_i}$ we get $n_1 = m_1$ as well.

Definition 3.14 *Let M be a finitely generated torsion module. Then, by the above proposition*

$$M \cong \oplus_{i=1}^{m} M_{p_i}$$

where $M_{p_i} \cong \oplus_{j=1}^{n_i} R/(p_i)^{r_{ij}}$, r_{ij} being positive integers. These prime powers, $(p_i)^{r_{ij}}$, (which are uniquely determined) are called the elementary divisors of M.

Theorem 3.15 (Elementary Divisor Theorem) *Two finitely generated R-modules are isomorphic if and only if they have the same rank and same sequence of elementary divisors (counted with multiplicity).*

Proof: This is an easy corollary of the above proposition.

Exercise 3.16

(i) Find all abelian groups of order $32, 36, 200$.

(ii) Prove or disprove: $(\mathbb{Z}/8\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$.

(iii) $(\mathbb{Z}/16\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$.

Remark 3.17 *The Elementary Divisor Theorem has important applications in Algebraic Number Theory and Linear Algebra. In fact, let V be a finite dimensional vector space over a field k and let T be any linear transformation on V. Then V can be considered as a module over the polynomial ring $k[X]$ with scalar multiplication defined as follows: $f(X)v = T(v)$ for all $v \in V$ and $f(X) \in k[X]$. By applying Elementary Divisor Theorem to V as a module over $k[X]$, one can prove that there is a basis of V with respect to which the matrix of T has the Jordan canonical form, if k is algebraically closed (or under the weaker assumption that all the eigen values of T are in k).*

Remark 3.18 *One can have primary decomposition of any torsion module (not necessarily finitely generated) over a PID; i.e., the statement of the corollary 2.18 is true for any torsion module over R.*

Remark 3.19 *We have derived the primary decomposition of a torsion module from the structure theorem. However primary decomposition can be directly established (without the use of structure theorem). This in turn can be used to prove the structure theorem. See for instance, Lang, Algebra.*

3.3 Uniqueness of Cyclic Decomposition

In the previous section we have seen that every finitely generated module over a PID can be expressed as a direct sum of cyclic modules. We shall now show that such a decomposition is essentially unique.

Theorem 3.20 Invariance Theorem *Let R be a PID and let M be a finitely generated $R-$module. Then*

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n),$$

where $(a_1) \supset (a_2) \supset \cdots \supset (a_n)$, where $(a_1) \neq R$. More over the ideals (a_i) are uniquely determined.

proof: We have already proved that $M \cong \oplus_{i=1}^{r} R/(a_i)$ with $(a_i) \supset (a_{i+1})$. If for some $i, a_i = 0$, then $R/(a_i)$ is free of rank one. We know that the rank is uniquely determined. So number of zero ideals is the same in any decomposition. So to prove the uniqueness of the ideals, (a_i), we can assume that a_i's are nonzero. Clearly under these assumptions M is a torsion module. So the theorem will follow, if we prove it for torsion modules. We claim that the ideals as stated in the theorem are completely determined by the primary decomposition. In other words, if M is a torsion module and $M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$ is any cyclic decomposition, with $(a_i) \supset (a_{i+1})$, $(a_1) \neq R$, then the ideals (a_i) are uniquely determined. We shall do it by comparing it with the primary decomposition of M. Take a primary decomposition of each cyclic

factor, using Chinese Remainder Theorem and take their direct sum. We get a primary decomposition of M by collecting all the direct summands corresponding to each prime p, that divides the a_i's. Let $p_1, p_2, \cdots, p_r$ be the set of all primes that occur in the factorization of a_n. Since $a_i | a_{i+1}$ for all i, it follows that these are all the prime ideals that occur in the primary decomposition of M, that we obtained. That is to say, $M_p = \{0\}$ for $p \neq p_i$ for $1 \leq i \leq r$. Since primary decomposition is unique (upto isomorphism), the elementary divisors of M must be powers of these primes. Now, let us list the elementary divisors of M in the ascending order of the powers of these primes; i.e.,

$$\begin{array}{ccccc} p_1^{l_{11}} & p_1^{l_{12}} & p_1^{l_{13}} & \cdots & \cdots \\ p_2^{l_{21}} & p_2^{l_2 2} & p_2^{l_{23}} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_r^{l_{r1}} & p_r^{l_{r2}} & p_r^{l_{r3}} & \cdots & \cdots \end{array}$$

where $l_{ij} \leq l_{ik}$ if $j \leq k$. Each row here has finitely many entries. The conditions $a_i | a_{i+1}$ imply that a_m must be the product of the highest powers of the p_i's, a_{m-1} must be the product of the next highest powers of the remaining powers and so on. This proves that the ideals (a_i) are completely determined by the primary decomposition.

Remark 3.21 *In this course, we have shown that every finitely generated torsion module is a finite direct sum of cyclic modules and used this to show that every finitely generated torsion module has a primary decomposition. But it is possible to prove directly, that a finitely generated torsion module has a primary decomposition, without using the cyclic decomposition theorem. In fact, one can derive the cyclic decomposition theorem, using primary decomposition. Also, a direct proof of uniqueness of cyclic decomposition is possible on the same lines as the proof of uniqueness of primary decomposition. We leave this for self study.*

Definition 3.22 *The ideals (a_i) associated to the module M, which are unique by the above theorem, are called the invariant ideals of M.*

Theorem 3.23 *Let R be a PID and let M, N be finitely generated $R-$modules. Then M and N are isomorphic if and only if they have the same set of invariant ideals.*

Proof: Exercise.

4 Modules over $k[X]$ and Linear Operators

One of the main applications of the structure theorem is to the study of linear operators on finite dimensional vector spaces. This application comes from the fact that if T is a linear operator on V, then V can be considered as a $k[X]-$ module via T (which you have already seen). In fact, historically the structure theorem for arbitrary PID's was motivated by the theory of abelian groups and the theory of linear operators on finite dimensional vector spaces over a field. Both these theories existed independent of each other (cf. Artin). What is being done at present is to put these two theories together under one roof. In the case of abelian groups, the structure of both finite abelian groups (torsion $\mathbb{Z} - modules$) and finitely generated infinite abelian groups, play important role; for instance, in Number Theory. As far as the applications to linear operators is concerned, it is the structure of the torsion modules that is important. However this does not mean that the general theory is useless. It is important both in Number Theory and Algebra. In fact it lays foundation for *Linear Algebra over Commutative rings*. Since PID's are a small subclass of the family of all Commutative rings, it is natural to question whether such a theory can be extended to a wider class of rings; for instance, for polynomial rings $\mathbb{Z}[X], k[X, Y]$ etc.. As you have seen (exercise 4(c)) PID's are the best commutative rings for which the statements like sub module of a free module is free, of smaller rank etc. hold.

Let us first review a bit of linear algebra over a field.

4.1 Review of Linear operators on finite dimensional vector spaces

Let V be a finite dimensional vector space over k and T be a linear operator on V. Then the simplest thing that a the linear operator can do to a vector v is to map $v \mapsto v$; that is to fix the vector v. (If $v = 0, T(v) = v$ for all T.) If $v \neq 0$, the next best that it can do is to fix the line spanned by v. That is to say, $T(v) = \alpha v$, where α is a scalar. Suppose that there exists a basis $B := \{v_1, v_2, \cdots, v_n\}$ of V and scalars $\alpha_i, 1 \leq i \leq n$ such that $T(v_i) = \alpha_i v_i$ for every $1 \leq i \leq n$. Then the matrix of T, with respect to the basis B is the diagonal matrix $\text{Diag}[\alpha_1, \alpha_2, \cdots, \alpha_n]$. Thus $T = T_1 \oplus T_2 \oplus \cdots \oplus T_n$, where each T_i is a linear operator on a one dimensional subspace of V. But this is not always true. However, we can try to decompose T as the direct sum of linear operators on smaller dimensional subspaces. We shall now show how this can be done using the structure theorem. As pointed out earlier, this can be done independently, without the use of structure theorem. In the language of matrices, one may express this fact as follows. If $A \in M(n, k)$, we say A is digonalizable if A is similar to $\text{Diag}[\alpha_1, \alpha_2, \cdots, \alpha_n]$. That is to say, there exists an invertible matrix $P \in Gl(n, k)$ such that $PAP^{-1} = \text{Diag}[\alpha_1, \alpha_2, \cdots, \alpha_n]$. Clearly P denotes the matrix of change of basis. But it is not true that every matrix $A \in M(n, k)$ is similar to a diagonal matrix. (The student is advised give an example of such a matrix over say $\mathbb{R}$ or $\mathbb{C}$.) Let V be a vector space of dimension n over k and T be a linear operator on V. Then $k[T]$ is a sub ring of $\text{End}_k V$. Fixing a basis of V, we get an isomorphism $\text{End}_{\ k} V \cong M(n, k)$, by the correspondence $T \mapsto A := A(T)$, where A denotes the matrix of T with respect to the given basis. We shall often consider these two rings as one and the same. A linear operator commutes with the scalars. Therefore although $M(n, k)$ is a non commutative ring, $k[T]$ is a commutative ring with identity. Also V is a finitely generated module over $k[T]$. Let $\phi : k[X] \to \text{End}_k V$ be the ring homomorphism given by $X \mapsto T$. Then $k[X]/\ker \phi \cong k[T]$. In view of exercise (5.1, (3)), V is a module over $k[X]$. We had given an explicit description of this scalar multiplication in exercise (5.1, (7)). Note that the two descriptions give the same module structure on V. The ring $k[T]$ is a homomorphic image of the polynomial ring $k[X]$. Once again, we remark that in view of exercise 5.1, (3), V may be regarded as a $k[X]$-module or $k[T]$-module. (Loosely speaking, the two structures are one and the same.) However, the ring $k[X]$ is a PID whereas $k[T]$ may not even be an integral domain. It may have zero divisors. So considering V as a module over $k[X]$ has an advantage. The structure theorem can be used to study the module V. More over, from this we can derive useful information about the operator T. Let us begin by recalling some terminology from linear

algebra.

Exercise 4.1 *Let $\phi : k[X] \to k[T]$ be the homomorphism defined above. If T is a non zero operator, prove the following:*

(a) $\ker \phi$ *is generated by a nonconstant polynomial.*

(b) There exists a unique monic polynomial $f(X) \in k[X]$ such that

(i) $f(T) = 0$ and

(ii) if $g(X)$ is any polynomial, such that $g(T) = 0$, then $f(X)$ divides $g(X)$.

Definition 4.2 *The polynomial $f(X)$ as guaranteed by the above exercise is called the minimal polynomial of T (respectively A). The polynomial* $\det(XI - T)$ *(respectively* $\det(XI - A)$*is called the characteristic polynomial of T(respectively A).*

Theorem 4.3 *(Cayley-Hamilton Theorem) Every square matrix $A \in M(n, k)$ satisfies its characteristic polynomial:*

$$\det(XI - A) = 0.$$

Proof: The students might have seen several proofs of this theorem. We are going to prove it using invariant factors of the $k[X]-$module V, via the linear operator $T := T_A$. Let $\{v_1, v_2, \cdots, v_n\}$ be a basis of V as a vector space over k. Then $\{v_1, v_2, \cdots, v_n\}$ is a set of generators for V as a $k[X]$-module. Let $\{e_1, e_2, \cdots, e_n\}$ be the standard basis of the free $k[X]$ module $k[X]^n$. Then, we have an onto homomorphism $\phi : k[X]^n \to V$ given by $\phi(e_i) = v_i$ of $k[X]$- modules. We claim that the elements

$$f_i = Xe_i - \sum_{j=1}^{n} a_{ij}e_i$$

is a basis of $\ker \phi$.

Proof of the claim: By the definition of the matrix of T, with respect to the given basis, we know that $T(v_i) = \sum_{j=1}^{n} a_{ij}T(v_j)$. So,

$$\phi(f_i) = \phi(Xe_i) - \sum_{j=1}^{n} a_{ij}\phi(e_j) = X\phi(e_i) - \sum_{j=1}^{n} a_{ij}v_j = Xv_i - \sum_{j=1}^{n} a_{ij}v_j = T(v_i) - \sum_{j=1}^{n} a_{ij}v_j = 0.$$

Thus $f_i \in \ker \phi$. Next, we prove that the set $\{f_i : 1 \leq i \leq n\}$ generates $\ker \phi$. Let $z \in \ker \phi$. Then $z = \sum_{i=1}^{n} b_i(X)e_i$, where $b_i(X) \in k[X]$. But $Xe_i = f_i + \sum_{j=1}^{n} a_{ij}e_j$. Therefore $z = \sum_{i=1}^{n} b_i(X)e_i = \sum_{i=1}^{n} g_i(X)f_i + \sum_{i=1}^{n} c_ie_i$, where $c_i \in k$. But then $\phi(z) = 0$. This implies $\sum_{i=1}^{n} c_iv_i = 0$. Since v_i are linearly independent over k, it follows that $c_i = 0$ for all i. Hence z is a $k[X]$-linear combination of f_i's. So it remains to prove that f_i's are linearly independent over $k[X]$. Let $\sum_{i=1}^{n} b_i(X)f_i = 0$. Then,

$$\sum_{i=1}^{n} b_i(X)Xe_i = \sum_{i,j=1}^{n} b_i(X)a_{ij}e_j.$$

Since $\{e_1, e_2, \cdots, e_n\}$ is linearly independent over $k[X]$, we must have

$$b_i(X)X = \sum_{j=1}^{n} b_j(X)a_{ij}.$$

If some $b_i(X) \neq 0$, then let $b_r(X)$ be one of maximal degree amongst all non zero $b_i(X)$. Clearly $b_r(X)X = \sum_{j=1}^{n} b_j(X)a_{rj}$ is not possible. Therefore $b_i(X) = 0 \ \forall \ i$. Now by the structure theorem, there exists a basis

$\{u_1, u_2, \cdots, u_n\}$ of $k[X]^n$ and elements $g_i \in k[X]$, for $1 \leq i \leq n$ such that $\{g_1u_1, g_2u_2, \cdots, g_nu_n\}$ is a basis of $\ker \phi$, and $g_i | g_{i+1}$. (Note that $\ker \phi$ has rank n.) Suppose that $g_r(X)$ is a non unit, then the invariant factors of the $k[X]$-module V are $d_i(X) : n \geq i \geq r$ and $V \cong \oplus_{i=1}^{s} k[X]/\langle d_i(X) \rangle$ where $d_i(X) = g_{r+i-1}, s+r-1 = n$. Thus, if

$$D = \text{ diag}[1, 1, \cdots, d_1(X), d_2(X), \cdots d_s(X)],$$

we have $D = P(XI - A)Q^{-1}$ for some invertible matrix P, Q over $k[X]$. But a square matrix over $k[X]$ is invertible if and only if its determinant is a non zero scalar; i.e., an element of $k - \{0\}$. (You must prove it). Thus $\det(XI - A) = d_1(X)d_2(X) \cdots d_s(X)$. But then $f(X) := \det(XI - A)$ annihilates V. That is to say $f(T)$ (equivalently $f(A)$) is the zero operator on V. In other words, A is a root of its characteristic polynomial. This completes the proof of Cayley-Hamilton theorem.

4.2 Canonical forms: Rational and Jordan

We shall now discuss how the structure theorem can be applied to certain problems on linear operators and (hence to square matrices, since fixing a basis of V allows us to identify linear operators bijectively with square matrices of a fixed size). In fact the problem is to determine the similarity class of matrices. That is, to find a simple enough matrix in each similarity class, called a canonical form. Over an arbitrary field, the best that can be done is the so called rational canonical form, which we discuss in subsecion 3.3, below. If the field k is algebraically closed, we can do better. This is the content of subsection 3.4 below.

4.3 Rational canonical form

Suppose that T is a linear operator and V is a cyclic operator on V. Then there exists a vector $v \in V$ such that $\{v, T(v), T^2(v), \cdots, T^{n-1}(v)\}$ is a $k-$basis of V. This means, V as a $k[X]-$ module is cyclic and the minimal polynomial of T is equal to the characteristic polynomial of T. Let $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ be the characteristic polynomial of T. The matrix of T with respect to the above basis can be easily written down.

$$\begin{bmatrix} 0 & 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & 0 & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 0 & 1 & -a_{n-1} \end{bmatrix}.$$

Such a matrix is called the rational canonical form of the operator T. If T is not cyclic, we can decompose T as $T = T_1 \oplus T_2 \oplus \cdots \oplus T_s$, with T_i cyclic. Since T_i is cyclic, we can write down the rational canonical form of T_i for all $1 \leq i \leq s$. Thus the matrix of T with respect to a suitable basis (what is the basis ?) is of the form $\text{Diag}[B_1, B_2, \cdots, B_s]$, where each B_i is a block matrix in the rational canonical form. This is the best that one can do, if k is not algebraically closed.

4.4 Jordan canonical form

Suppose that the field k is algebraically closed or that all the eigen values of the linear operator T belong to k. Then, we can apply the primary decomposition of V as a $k[X]-$module via T, to obtain a nicer form of the matrix of T.

By the elementary divisor theorem (2.20), we know that the $k[X]-$module V decomposes uniquely as a direct sum of primary cyclic submodules. That is, $V \cong \oplus_{j=1}^{m} V_{p_j}$ where $V_{p_j} \cong \oplus_{i=1}^{r_j} k[X]/(p_j^{n_i})$, p_j are distinct prime factors of the characteristic polynomial of T. Therefore if we can write the matrix of the linear operator restricted to $W_{ij} \cong k[X]/(p_j^{n_i})$, we get a matrix representation for T. If k is algebraically

closed, each $p_j = X - \alpha_j$ for some $\alpha_j \in k$. So we have to write the matrix of a linear operator T on $W = k[X]/((X-\alpha)^r)$. Let $w \in W$ be the image of $1 \in k[X]/((X-\alpha)^r)$. Then of course, W is cyclic and we can write the rational canonical form. But we want to do better. We shall write the matrix of T with respect to a different $k-$basis of W. Let $w = w_0, (X-\alpha)(w_0) = w_1, (X-\alpha)(w_i) = w_{i+1}, 1 \leq i \leq r-2$. Clearly, $\{w_i : 0 \leq i \leq (r-1)\}$ is a $k-$ basis of W. The matrix of T with respect to this basis, is

$$\begin{bmatrix} \alpha & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & \alpha & 0 & \cdot & \cdot & 0 \\ 0 & 1 & \alpha & 0 & \cdot & 0 \\ \vdots & 0 & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & 0 & 1 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 1 & \alpha \end{bmatrix}.$$

5 Exercises

In these exercises, R denotes a commutative ring with identity, k denotes a field, V denotes a finite dimensional vector space over k, and M denotes a module over R, unless otherwise stated.

5.1 Exercises I

1.

(a) If $\mathfrak{a}$ is an ideal of R such that $R/\mathfrak{a}$ is free $R-$module, then prove that $\mathfrak{a} = \{0\}$.

(b) If every module over R is free, prove that R is either the zero ring or a field.

2.

(a) Let $\mathfrak{a}$ be an ideal of R. Prove that $\mathfrak{a}$ is free as an R-module if and only if $\mathfrak{a}$ is a principal ideal generated by an element which is not a zero divisor in R.

(c) Suppose that for every finitely generated free module M over R of rank n, every submodule N of M is free of rank $\leq n$, prove that R is necessarily a PID.

3. Let $\mathfrak{a}$ be an ideal of R and M be an $R-$module, such that $\mathfrak{a}M = \{0\}$. Prove that M is an $R/\mathfrak{a}-$module in a natural way.

4. Prove or disprove: $\mathbb{Z}/n\mathbb{Z}$ (with the usual addition) is a module over $\mathbb{Q}$.

5. Prove or disprove: $k[X]/(f(X))$ is a module over $k(X)$.

6. Prove that $(\mathbb{Q}_+, *)$ is a free $\mathbb{Z}$-module and find a basis for this module. Also, prove that $(\mathbb{Q}^*, *)$ as a $\mathbb{Z}$-module is $\cong \mathbb{Z}/2\mathbb{Z} \oplus M$ where M is free with a countable basis.

7. Let V be a vector space of dimension n over k. Let $T \in \mathrm{End}_k(V)$. Prove that V is a module over $k[X]$ with scalar multiplication given by $f(X).v = f(T)(v)$ for all $v \in V$. Is V free as a module over $k[X]$?

8.

(a) Prove or disprove: $\mathbb{Q}/\mathbb{Z}$ is a free $\mathbb{Z}-$module.

(b) Is $k(X)/k[X]$ is a free $k[X]$-module? (Here, $k(X)$ is considered as a $k[X]$-module via the inclusion map $k[X] \hookrightarrow k(X)$.)

9. What is the dimension of the vector space $k[X]/\left((X-\alpha)^r\right)$ over k? Is it free as a $k[X]$ module? What about the $k[X]/\left(f(X)\right)$, where $f(X)$ is a non constant polynomial over k?

10. Prove that every (finitely generated) R-module is the quotient of a (respectively finitely generated) free module.

5.2 Exercises II

1. Discuss whether the following abelian groups can be written as the direct sum of two proper sub groups:

$$\mathbb{Z}/p^n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z},$$

where $m = p^2q^3r^4$, p, q, r being distinct primes.

2. Determine the following modules:

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^2,\mathbb{Z}), \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^2,\mathbb{Z}^2), \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}/n\mathbb{Z}), \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},\mathbb{Z}/n\mathbb{Z}),$$

where $m, n \in \mathbb{N}$.

3. Find a base for the submodule N of $\mathbb{Z}^3$ generated by $v_1 = (1, 0, -1),\ v_2 = (2, -3, 1),\ v_3 = (0, 3, 1),\ v_4 = (3, 1, 5)$.

4. If $M_1, M_2, \cdots, M_r$ are R-modules and N_i are submodules of M_i for $1 \leq i \leq r$, prove that

$$\frac{\oplus_{i=1}^r M_i}{\oplus_{i=1}^r N_i} \cong \oplus_{i=1}^r \frac{M_i}{N_i}.$$

5. If R is a PID, and M, N are finitely generated free R-modules of rank m, n respectively, prove that $M \oplus N$ is finitely generated free R-module of rank $m + n$.

6. Let R be a PID. Prove that a vector $v = (a_1, a_2, \cdots, a_n)$ can be completed to a basis of R^n if and only if the gcd of $(a_1, a_2, \cdots, a_n)$ is (1).

7.

(a) Find the Smith normal form of the following integral matrices:

$$\begin{bmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{bmatrix}, \quad \begin{bmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{bmatrix}.$$

(b) Find the Smith normal form of the following matrices over $k[x]$.

$$\begin{bmatrix} X+1 & 2 & -6 \\ 1 & X & -3 \\ 1 & 1 & X-4 \end{bmatrix}, \quad \begin{bmatrix} X-17 & 8 & 12 & -14 \\ -46 & X+22 & 35 & -41 \\ 2 & -1 & X-4 & 4 \\ -4 & 2 & 2 & X-3 \end{bmatrix}.$$

8. Verify that the elementary row and column operations on a matrix correspond to left and right multiplication by elementary matrices.

9. Let R be a Euclidean domain. Prove that every element of $GL_n(R)$ is a product of elementary matrices.

10. *If R is a PID, prove that every element of $GL_n(R)$ is a product of elementary matrices and matrices of the following type: $[a_{ij}]_{1 \leq i,j \leq n}$, with $a_{ii} = 1$ for all $i \geq 3$, $a_{ij} = 0$ for $i \neq j, \geq 3$ and the two by two matrix $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ is invertible.

5.3 Exercises III

1. Let R be an integral domain and k be the field of fractions of R. Let M be a finitely generated R-module. Let V be the vector space over k obtained from M, by extension of scalars. Prove that the rank of M is equal to the dimension of the vector space V over k.

2. If R is a PID, and M, N are finitely generated R-modules of rank m, n respectively, prove that $M \oplus N$ is finitely generated R-module of rank $m + n$. Describe the torsion submodule of $M \oplus N$.

3. Let M be a torsion free module over a PID. Is it true that M is free? Justify.

4. *Let R be a PID, $a \in R$ and $M = R/(a)$. Let p be a prime of R dividing a and n be the highest power of p dividing a. Prove that
$$p^{k-1}M/p^kM \cong R/(p),$$
if $k \leq n$ and
$$p^{k-1}M/p^kM \cong \{0\},$$
if $k > n$.

5. Determine the number of non isomorphic abelian groups of order $55,1000,360,400$. What do you think is the number of non isomorphic abelian groups of order n, if $n = \prod_{i=1}^{r} p_i^{n_i}, n_i \geq 1$?

6. Recall the following definition.

Definition 5.1 *(exponent of a group) Let G be a group. The exponent of G is defined to be the smallest natural number n such that $a^n = e$ for all $a \in G$, if it exists. (Clearly the exponent of a finite group is defined.)*

(a) Find the exponents of the following abelian groups:
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

(b) Using the structure theorem, prove that, if G is a finite abelian group, then there exists an element $a \in G$ such that $o(a) =$ exponent of G.

(c) Prove that a finite abelian group is cyclic if and only if the exponent of G is equal to $o(G)$.

7. Prove that a finite sub group of the multiplicative group of any field is cyclic. (Hint: Observe that a polynomial of degree n over a field has at most n roots and use exercise 6.)

8. Let $R = \mathbb{Q}[X]$. Find a base for the submodule N of R^3 generated by $v_1 = (2X-1, X, X^2+3), v_2 = (X, X, X^2), v_3 = (X+1, 2X, 2X^2-3)$.

9. Let T be the linear operator on $V = \mathbb{C}^2$ whose matrix is $\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$. Is the corresponding $\mathbb{C}[X]$-module cyclic?

10. Let $R = k[X,Y]$ be a polynomial ring in two variables over k. Give an example of a module over R, which is finitely generated torsion free, but not free. Do the same for $R = \mathbb{Z}[X]$.

5.4 Exercises IV

1. Let T be a linear operator on V. Prove that the following statements are equivalent:

(a) $k[T]$ is an integral domain.

(b) $k[T]$ is a field.

(c) The minimal polynomial of T is irreducible over k.

2. Let V be finite dimensional vector space over k and T be a linear operator on V. Prove that V as a $k[X]-$module via T is cyclic if and only if the minimal polynomial of T is equal to the characteristic polynomial of T.

3. Diagonalization of matrices: Prove that $A \in M_n(\overline{k})$ is diagonalizable (i.e., similar to a diagonal matrix) if and only the minimal polynomial of A has no repeated roots.
4. Find all possible Jordan forms of a matrix A whose characteristic polynomial is $(X+2)^2(X-5)^3$.
5. Prove or disprove: Two matrices over $\overline{k}$ are equivalent if and only if they have the same Jordan canonical form.
6. Prove or disprove: Two matrices over k are similar if and only if they have the same rational canonical form.
7. Find all possible Jordan forms of 8×8 matrices over $\mathbb{R}$ whose minimal polynomial is $X^2(X-1)^3$.
8. If N is a $k \times k$ nilpotent matrix such that $N^k = 0$ but $N^{k-1} \neq 0$, prove that N is similar to its transpose.
9. Prove or disprove: An $n \times n$ matrix over $\mathbb{C}$ is similar to its transpose.
10. If $f(X) \in k[X]$ is a non constant polynomial, prove that there exists a linear transformation with $f(X)$ as its minimal polynomial (respectively characteristic polynomial).
11. Let $M = M_1 \oplus M_2$ and $N = N_1 \oplus N_2$ be modules over R. Prove that every homomorphism $\phi : M \to N$ can be represented by a matrix $\begin{bmatrix} \sigma_{11} & \sigma_{12} \\ \sigma_{21} & \sigma_{22} \end{bmatrix}$ and conversely, where $\sigma_{ji} : M_i \to N_j$. If M, N are finitely generated free modules over a PID, how do you interpret this matrix with respect to given bases of M_i, N_i? Generalize it to a finite direct sum of modules.
12. Prove that all $n \times n$ matrices with characteristic polynomial $f(X) \in k[X]$ are similar if and only if $f(X)$ has no repeated factors in its factorization in $k[X]$.
13. Prove that two 2×2 matrices over k are similar if and only if they have the same minimal polynomial.
14. Prove that two 3×3 matrices over k are similar if and only if they have the same characteristic and minimal polynomials.
15. Prove or disprove: two 4×4 matrices over k are similar if and only if they have the same characteristic and minimal polynomials.
16. Let $f(X) = \prod_{i=1}^{r} p_i(X)^{n_i}$, where $n_i \geq 1$ and $p_i(X)$ are distinct primes in $k[X], r \geq 1$. For $m \in \mathbb{N}$, let $P(m)$ denote the number of partitions of m. Prove that the number of matrices up to similarity, with characteristic polynomial $f(X)$, is equal to $\prod_{i=1}^{r} P(n_i)$.

5.5 Exercises V: Miscellaneous

This set consists of Miscellaneous exercises.

1. Define the annihilator of an R-module as follows:

$$\text{ann}(M) := \{x \in R : xM = \{0\}\}.$$

   Prove that $\text{ann}(M)$ is an ideal in R. What is the annihilator of the $\mathbb{Z}$- module $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$?
2. Prove that a power series ring $k[[X]]$ in one variable over k is a Euclidean domain.
3. Prove that the following subrings of $\mathbb{C}$ are Euclidean domains.

$$\mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[e^{2\pi i/3}].$$

   Give more examples as home study.

4. **Prove that the subring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ of $\mathbb{C}$ is a PID but not a Euclidean domain. (Leave it as home study with some reference.)
5. *Let A be an $m \times n$ integral matrix. Consider the linear map $T : \mathbb{Z}^n \to \mathbb{Z}^m$ given by left multiplication by A. Prove the following:

(a) T is injective if and only if the rank of A is n.

(b) T is surjective if and only if the gcd of the determinants of the $m \times m$ minors of A is 1.

6. Prove that every invertible matrix over $\mathbb{Z}$ is a product of elementary matrices. Is the corresponding result true for matrices over $k[X]$? What about an arbitrary PID?
7.

(a) Let $R \subset S$ be commutative rings. Suppose that S is finitely generated as an $R-$module. Let $x \in S$. Show that multiplication by x can be represented by a square matrix over R.

(b) *Prove the Cayley-Hamilton Theorem: Let $A \in M_n(R)$. If $f(X) = \det(XI - A)$, then $f(A) = 0$.

8. Let $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ be the $\mathbb{Z}-$linear map given by left multiplication by $A \in M_n(\mathbb{Z})$. Prove that the image of ϕ is of finite index in $\mathbb{Z}^n$ if and only if $\det A \neq 0$ and in that case the index is equal to $|\det A|$.
9. Show that every $n \times n$ complex matrix A is similar to a matrix of the form $D + N$ where D is diagonal and N is nilpotent and $DN = ND$.
10. *Let R be a PID. Define the rank of a free module over R (not necessarily finitely generated). Prove that every submodule N of a free module M is free and rank $N \leq$ rank M (Use transfinite induction or Zorn's lemma).
11. **Definition 5.2** *A complex number α is called an algebraic integer, if there exists a monic polynomial $f(X) \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.*

(a) Prove that $\alpha \in \mathbb{C}$ is algebraic if and only if $\mathbb{Z}[\alpha]$ is a finitely generated abelian group.

(b) Let $A \subset B \subset C$ be commutative rings. If C is finitely generated as a $B-$module and B is finitely generated as an $A-$module, then prove that C is finitely generated as an $A-$module.

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

12. *Show that the following (concepts) are equivalent:

(a) V is an R-module, where $R = \mathbb{Z}[\sqrt{-1}]$

(b) V is an abelian group with an endomorphism ϕ such that $\phi \circ \phi = -I$, where I denotes the identity endomorphism of V.

13. *Let $k = \mathbb{F}_p$. Describe the primes p for which the additive group $(k, +)$ has the structure of a $\mathbb{Z}[\sqrt{-1}]$-module.
14. *Classify finitely generated modules over $\mathbb{C}[\epsilon]$ where $\epsilon^2 = 0$.
15. Let V be a complex vector space of dimension 5 and T be a linear operator whose characteristic polynomial is $(X - \alpha)^5$. Suppose that the rank of the operator $T - \alpha I$ is 2. What are the possible Jordan forms for T?
16. *Let $L|K$ be a field extension. Let $A \in M_n(K)$. Prove or disprove :

(a) The minimal polynomial of A over L is the same as the minimal polynomial of A over K.

(b) The characteristic polynomial of A over L is the same as the characteristic polynomial of A over K.

17. *Prove that two matrices $A, B \in M_n(k)$ are similar if and only if $XI - A$ and $XI - B$ have the same invariant factors as elements of $M_n(k[X])$.
18. *Prove that every ring with identity is a subring of the endomorphism ring of an abelian group.

19. *Let M be an ideal in $\mathbb{Z}[X]$. Prove that M is not a direct sum of cyclic $\mathbb{Z}[X]$-modules.
20. *Let $R = \mathbb{Z}[\sqrt{-1}]$. Let N be the submodule of R^3 generated by $\{(1,3,6),(2+3i,-3i,12-18i),(2-3i,6+9i,-18i)\}$. Determine the structure of R^3/N as an $R-$module. Show that R^3/N is finite of order 352512.
21. **Let $A \in M(n,k)$. Let $f(X) = \det(XI - A)$ be the characteristic polynomial of A and $m(X)$ be the minimal polynomial of A. Let $\Delta_{n-1}(X)$ denote the monic gcd of the $(n-1)\times(n-1)$ minors of $XI - A$. Prove that $m(X) = f(X)/\Delta_{n-1}(X)$.
22. * (Modules over non commutative rings) The following exercise provides an example of a noncommutative ring R for which $R^n \cong R^m$ for all $m, n \in \mathbb{N}$. Let V be an infinite dimensional vector space over $\mathbb{R}$ with a countable basis, $\{v_1, v_2, \cdots, v_n, \cdots\}$. Let $R = \mathrm{End}_{\mathbb{R}} V$. Let T, T' be defined by $T(v_{2n}) = v_n, T(v_{2n-1}) = 0, T'(v_{2n}) = 0, T'(v_{2n-1}) = v_n$ for all n. Prove that $\{T, T'\}$ is a basis of R as a left vector space over itself. Thus $R \cong R^2$. Prove that $R^n \cong R^m$ for any $m, n \in \mathbb{N}$.
23. * (Simultaneous diagonalization) Prove that $A, B \in M(n,\mathbb{C})$ are simultaneously diagonalizable (i.e., there exists an invertible matrix $P \in M(n,\mathbb{C})$ such that both PAP^{-1} and PBP^{-1} are diagonal) if and only if $AB = BA$.
24. Let G be a finite abelian group, which is the direct sum of cyclic groups of order $n_i, 1 \le i \le s$ where $n_i | n_j$ for $i \le j$. Show that the number of endomorphisms of G is

$$N = \prod_{j=1}^{s} n_j^{2s-2j+1}.$$

25. Prove that a linear transformation T on a finite dimensional vector space over a field is cyclic if and only if the ring of linear transformations commuting with T is a commutative ring.
26. Prove that $Sl(2,\mathbb{Z})$ is generated by the following two matrices:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

27. Let $R = \mathbb{Z}[\sqrt{-5}]$ and M be the module presented by the matrix $\begin{bmatrix} 2 \\ 1+\sqrt{-5} \end{bmatrix}$.

(i) Prove that the residue of A has rank one for every prime ideal $\mathfrak{p}$ of R.

(ii) Prove that V is not free. (Note: R is not a PID).

28. Let R be any commutative ring with identity and M be a free module over R. Let e be a basis vector and $f \in M$ is any vector. If $r \in R$ is such that $rf = e$, prove that r is a unit in R.
29. Prove that the group of units of $\mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if n is the power of an odd prime or $n = 2, 4$. (You need some number theory for this). Find the structure of the group of units of $\mathbb{Z}/n\mathbb{Z}$.
30. Show that the following matrices in $M(p,\mathbb{F}_p)$ are similar.

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \cdots & \cdots & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \cdots & 0 & 0 & 1 & 1 \\ 0 & 0 & \cdots & \cdots & 1 \end{bmatrix}$$

31. Show that any matrix $A \in M(n, \mathbb{R})$ is similar to a matrix consisting of blocks which have one of the following forms:

$$\begin{bmatrix} r & 1 & 0 & \cdots & 0 \\ 0 & r & 1 & \cdots & 0 \\ \cdots & \cdots & \ddots & \ddots & \cdots \\ 0 & \cdots & \cdots & r & 1 \\ 0 & \cdots & \cdots & 0 & r \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ -b & a & 0 & 1 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & -b & a & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & 1 & 1 & 0 \\ 0 & \cdots & \cdots & \cdots & -b & a & 0 & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & 0 & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & -b & a \end{bmatrix},$$

32. Let V be a finite dimensional vector space over k. Then the group $Gl(n, k)$ acts on $M(n, k)$ by conjugation. Define

$$\chi : M(n, k) \to k[X],$$

by $\chi(A) = \det(XI - A)$. Then the following are true:

(i) χ induces a map which we denote by χ itself, on the quotient set (conjugacy classes):

$$\chi : M(n, k)/Gl(n, k) \to k[X].$$

(ii) χ is surjective.

(iii) χ is a finite map.

(iii) Let for $m \in \mathbb{N}$, $p(m)$ denote the number of partitions of m. If $\det(XI - A) = \prod_{i=1}^{s} p_i(X)^{n_i}$, with $n_i \in \mathbb{N}$, then $|\chi^{-1}(A)| = \prod_{i=1}^{s} p(n_i)$.

6

References

[ART] M. Artin, Algebra.

[BOU] N. Bourbaki, Algebra II.

[D-F] D. S. Dummit and R. M. Foote, Abstract Algebra.

[JA1] N. Jacobson, Basic Algebra, Volume I.

[LAN] S. Lang, Algebra.

[COH] P. M. Cohn, *On the structure of Gl_2 of a ring*, IHES, vol. 66, 1966.