A Problem Course in Module Theory

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

1 Basic Definitions and Examples

Topics: Definitions of modules, submodules, direct sums of modules and submodules, quotient modules.

Annihilator of submodules and ideals, torsion elements and torsion modules, finitely generated modules and cyclic modules.

Simple and indecomposable modules.

Two most important examples: Abelian groups as $\mathbb{Z}$-modules and a vector space V over $\mathbb{F}$ as an $\mathbb{F}[X]$-module via a linear map $T\colon V \to V$.

Let R be a ring with identity 1. All rings will be assumed to have the multiplicative identity 1. A left R-module generalizes the concept of a vector space over a field.

Definition 1. A *left R-module* M is an abelian group M together with a map $f\colon R\times M \to M$ given by $(r, x) \mapsto r \cdot x$ satisfying the following conditions:
(i) $1 \cdot x = x$ for all $x \in M$
(ii) $r \cdot (x + y) = r \cdot x + r \cdot y$ for $r \in R$ and $x, y \in M$.
(iii) $(r + s) \cdot x = r \cdot x + s \cdot x$ for $r, s \in R$ and $x \in M$.
(iv) $r \cdot (s \cdot x) = (r \cdot s) \cdot x$ for $r, s \in R$ and $x \in M$.

By an R-module, we shall always mean a left R-module and we always write rx for $r \cdot x$.

The first four exercises introduce the most important examples of modules. Whenever new concepts are introduced, the reader should investigate/explore them in these examples.

Ex. 2. Any vector space V over a field $\mathbb{F}$ is an R-module where $R = \mathbb{F}$.

Ex. 3. The ring R can be considered as a left R-module over itself in a natural way.

Ex. 4. Let M be an additive abelian group. Show that there is only one way of making M a $\mathbb{Z}$-module.

Ex. 5. Let V be a vector space over a field $\mathbb{F}$. Let $T\colon V \to V$ be a linear transformation. Let $\mathbb{F}[X]$ be the ring of polynomials over $\mathbb{F}$. Show that V can be made into an $\mathbb{F}[X]$-module by the action

$$(p, v) \mapsto p(T)(v),$$

where $p(T) = \sum_{k=0}^{n} c_k T^k$ if $p(X) := \sum_{k=0}^{n} c_k X^k$.

We shall call V as $\mathbb{F}[X]$-module via T.

This example is *one of the most important examples* of this course.

Ex. 6. How will you define a right R-module?

Ex. 7. Any left ideal of R is an R-module in a canonical way.

Ex. 8. Let S be a nonempty set and R a ring with identity. Let F be the set of all maps $f\colon S \to R$ such that $f(s) = 0$ for all but finitely many $s \in S$. Define a natural R-module structure on F.

Ex. 9. Let R and A be rings with identity. Let $f\colon A \to R$ be a ring homomorphism which preserves the identity. Let M be an R-module. Show that M can be regarded as an A-module in a canonical way.

Ex. 10. If M is a finite abelian group then it is a $\mathbb{Z}$-module in a natural way. Can this structure be extended so that M becomes a $\mathbb{Q}$-module?

Ex. 11. Let A be an abelian group. Let $R := \operatorname{End} A$ be the set of all endomorphisms (i.e. group homomorphisms of A to itself). Show that R can be made into a ring with identity in a natural way and that A is an R-module in a canonical way.

Ex. 12. Assume that $rx = 0$ for some $r \in R$ and nonzero x in an R-module M. Prove that r does not have a left inverse in R.

Ex. 13. Let M and N be two left R-modules. Define an R-module structure (in a natural way) on $M \times N$. Generalize this to finite products.

A particular case is R^n of the R-module R.

Ex. 14. How will you define a submodule of an R-module M?

Definition 15. Let M be an R-module. A subset $N \subseteq M$ is called a *submodule* of M if N is a subgroup of the abelian group M with the property that $rx \in N$ for all $r \in R$ and $x \in N$.

Ex. 16. Let G be an abelian group considered as a $\mathbb{Z}$-module. What are the submodules?

Ex. 17. Let the notation be as in Ex. 5. Characterize the $\mathbb{F}[X]$-submodules of V.

Ex. 18. Let $T\colon \mathbb{F}^n \to \mathbb{F}^n$ be the *shift operator*:

$$T(x_1, x_2, \ldots, x_n) := (x_2, x_3, \ldots, x_n, 0).$$

Let e_i denote the standard i-th basic vector.
(a) Find $T^k(e_i)$.
(b) If $m < n$, find $(a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0)(e_n)$.
(c) If $m \geq n$, find $(a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0)(e_n)$.

Ex. 19. Keep the notation of Ex. 18. Let $W_k := \{x \in \mathbb{F}^n : x_j = 0 \text{ for } j > k\}$. Show that these are the only $\mathbb{F}[X]$-submodules of V.

Ex. 20. Let $\mathbb{F} = \mathbb{R}$ and $V = \mathbb{R}^2$. Find the $\mathbb{F}[X]$-submodules of V via T where
(a) T is the rotation clockwise about the origin by $\pi/2$.
(b) T is the projection onto the x-axis.
(c) T is the rotation by π.

Ex. 21. Consider a two dimensional vector space V over a field $\mathbb{F}$. Let v_1, v_2 be a basis of V. Let

$$T\colon av_1 + bv_2 \mapsto bv_1 + av_2.$$

Consider V as $\mathbb{F}[X]$-module via T. What are the submodules of V? (The characteristic of $\mathbb{F}$ may matter in your investigations.)

Ex. 22. Let R be a commutative ring with identity. Let M be an R-module. For $r \in R$, let

$$rM := \{rx : x \in M\} \quad \text{and} \quad M_r := \{x \in M : rx = 0\}.$$

Show that rM and M_r are R-submodules.

Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$ with $n = rs$ where r and s are relatively prime. Relate rM and M_s.

Ex. 23. Let $M := R^n$. Let I_j be left ideal for $1 \leq j \leq n$. Prove that the following are submodules of M:
(a) $\{(x_1, x_2, \ldots, x_n) \mid x_j \in I_j\}$.
(b) $\{(x_1, x_2, \ldots, x_n) \mid x_i \in R \text{ and } x_1 + x_2 + \cdots + x_n = 0\}$.

Ex. 24. Let I be a left ideal of R and let M be an R-module. Define

$$IM := \{\sum_{\text{finite}} r_i x_i \mid r_i \in I, x_i \in M\}$$

to be the collection of all finite sums of elements of the form rx where $r \in I$ and $x \in M$. Prove that IM is a submodule of M.

Ex. 25. Let $N_1 \subset N_2 \subset N_3 \cdots$ be an ascending chain of submodules of M. Show that $\cup N_k$ is a submodule of M.

Ex. 26. Show that the intersection of any nonempty collection of submodules is again a submodule.

Ex. 27. Let S be a subset of an R-modules M. What do you mean by the term "the smallest submodule containing S"? This submodule is called the *submodule generated by S*.

What do you mean by a *finitely generated* module?

Ex. 28. If N_i, $1 \leq i \leq k$ is a collection of submodules of an R-module M, then the smallest submodule N containing each of the N_i's is given by $N = N_1 + \cdots + N_k$.

Ex. 29. How do you define $A + B$ if A and B are subsets of a module?

Ex. 30. Let L_j, $j = 1, 2$ be submodules of M. Then the submodule generated by $S = L_1 \cup L_2$ is $L_1 + L_2$.

Ex. 31. Let M be generated by x_j, $1 \leq j \leq n$. Show that $M = \{r_1x_1 + \cdots + r_nx_n : r_j \in R\}$.

Definition 32. An R-module M is said to be an (internal) *direct sum* of submodules N_j, $1 \leq j \leq k$ if every $x \in M$ can be written *uniquely* as $x = x_1 + \cdots + x_k$ where $x_j \in M_j$ for $1 \leq j \leq k$.

In such a case, we write $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$.

Ex. 33. An R-module $M = M_1 \oplus \cdots \oplus M_k$ iff
(i) $M = M_1 + \cdots + M_k$ and
(ii) $M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} \cdots + M_k) = (0)$ for $1 \leq i \leq n$.

Ex. 34. Let $M = L_1 \oplus L_2$ and $M = M_1 \oplus M_2$ be two internal direct sums. Assume that $L_1 = M_1$. Prove or disprove that $L_2 = M_2$. *Hint:* You may look at $M = \mathbb{R}^2$!

Ex. 35 (Quotient Module)**.** Let N be a submodule of an R-module M. Let M/N denote the cosets $\{x + N : x \in M\}$ of the subgroup N in the group M. Since M is abelian, there is a natural abelian group structure on M/N. Define an R-module structure on M/N. The resulting module is called the *quotient module* of M by N. It is, of course, denoted by M/N.

Definition 36. We say that an R module M is*finitely generated* (in short FG) if there exists a finite subset S of M such that the submodule generated by S is M.

A module M is said to be *cyclic* if it is generated by a single element.

Ex. 37. Keep the notation of Ex. 5. Is V finitely generated? (Ex. 56 elaborates on this!)

Ex. 38. Let V be a vector space over $\mathbb{F}$. Consider V as an $\mathbb{F}[X]$-module via the identity map of V. When is it cyclic?

Ex. 39. Show that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.

Ex. 40. An R-module M is cyclic iff $M = Rx$ for some $x \in M$.

Ex. 41. Keep the notation of Ex. 5.
(a) Let $T = I$, the identity. When is V cyclic $\mathbb{F}[X]$-module via T?
(b) Let T be the shift operator (Ex. 18). Prove that V is cyclic.

Ex. 42. Which of the modules in Ex. 20 are cyclic?

Ex. 43. Let R be the ring of all functions $f\colon \mathbb{R} \to \mathbb{R}$. Consider $M = R$ as an R-module over itself. Then M is a cyclic R-module.

Let N be the submodule of all functions which vanish outside some finite interval. (The interval may depend on the function.) Then N is not finitely generated.

Ex. 44. Let N be a submodule of an R-module M. Assume that both N and M/N are finitely generated. Show that M is finitely generated.

Definition 45. An element x of an R-module M is called a *torsion element* if $rx = 0$ for some nonzero $r \in R$. The set of all torsion elements is denoted by

$$\mathrm{Tor}\,(M) := \{x \in M \mid rx = 0 \text{ for some nonzero } r \in R\}.$$

An R-module is called a *torsion module* if $M = \mathrm{Tor}\,(M)$, i.e., if for each $x \in M$, there exists a nonzero $r \in R$ such that $rx = 0$.

An element is said to be *torsion-free* if it is not a torsion element. A module M is *torsion-free* if all its nonzero elements are torsion-free.

Ex. 46. Let M be an abelian group considered as a $\mathbb{Z}$-module. What are the torsion elements?

Ex. 47. Prove that if R is an integral domain, then $\mathrm{Tor}\,(M)$ is a submodule of M. It is called the *torsion submodule* of M.

Show that the quotient module $M/\mathrm{Tor}\,(M)$ is torsion-free.

Ex. 48. Give an example of a ring R and an R-module such that $\mathrm{Tor}\,(M)$ is not a submodule of M. *Hint:* Consider the torsion elements in the R-module R.

Ex. 49. Show that if R has zero divisors then every nonzero R-module has torsion elements.

Ex. 50. Prove that any finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group which is a torsion $\mathbb{Z}$-module.

Ex. 51. Let M be an R-module and N a submodule. Let $\mathrm{Ann}_R N := \{r \in R : ry = 0 \text{ for all } y \in N\}$. Show that $\mathrm{Ann}_R N$ is an ideal in $\mathbb{R}$. The ideal $\mathrm{Ann}_R N$ is called the *annihilator* of N in R.

Ex. 52. Let M be an R-module. Let $\mathrm{Ann}_R M$ denote the annihilator of M in R. Show that there exists a natural $R/\mathrm{Ann}_R M$-module structure on M. What is the annihilator of M in $R/\mathrm{Ann}_R M$?

Ex. 53. Let I be a **right** ideal of R. Let M be an R-module. The *annihilator* of I in M is defined to be $\{x \in M \mid ax = 0 \text{ for all } a \in I\}$. Prove that the annihilator of I in M is a submodule.

Ex. 54. Let M be the $\mathbb{Z}$-module $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.
(a) Find the annihilator of M in $\mathbb{Z}$.
(b) Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a product of cyclic groups.

Ex. 55. Let R be an integral domain. Prove that $\mathrm{Ann}_R M \neq (0)$ for any finitely generated R-module M.

Give an example of a torsion R-module whose annihilator is the zero ideal.

Ex. 56. Consider a vector space V over $\mathbb{F}$ as an $\mathbb{F}[X]$-module via $T \in \mathrm{End}_{\mathbb{F}}(V)$. Show that V is FG and torsion $\mathbb{F}[X]$-module with $\mathrm{Ann}_{\mathbb{F}[X]} V = (p[X])$ where p is the minimal polynomial of T. (Recall that the minimal polynomial of T is by definition the monic polynomial p of least degree such that $p(T) = 0$.)

Ex. 57. Let I be an ideal in R. Let N denote the set of all elements x of M such that $I^k x = 0$ for some $k \in \mathbb{N}$ which may depend on x. Show that N is a submodule of M. *Hint:* Ex. 25.

Ex. 58. Let R be a commutative ring and M be a cyclic R-module. The *order ideal* of M is defined to be $\mathrm{Ann}_R(x)$ for any generator of M. Show that this is well-defined.

Ex. 59. Let $R := M(n, \mathbb{F})$ be the ring of $n \times n$-matrices with entries in the field $\mathbb{F}$. Then $M := \mathbb{F}^n$ is a cyclic R-module. In fact, $M = Re_1 = Re_2$. Find $\mathrm{Ann}_R(e_j)$.

Contrast this with Ex. 58

Ex. 60. Prove that $\mathbb{Q}/\mathbb{Z}$ is a torsion group which has only one subgroup of order n for each n and that this subgroup is cyclic.

Ex. 61. An R-module is said to be *simple* or *irreducible* if the only submodules are 0 and M.

Show that an R-module is simple iff M is generated by every nonzero element of M.

Ex. 62. Determine all simple $\mathbb{Z}$-modules.

Ex. 63. Let R be a ring with identity. Show that R is a simple R-module iff R is a division ring.

Ex. 64. An R-module M is said be *indecomposable* if it cannot be written as the direct sum of nonzero submodules.

Show that $M := \mathbb{Z}/(p^n)$, where p is a prime and $n \geq 1$, is indecomposable.

Ex. 65. Let $V = \mathbb{R}^2$ and $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Consider V as an $\mathbb{R}[X]$-module. Show that V is not simple but indecomposable.

Ex. 66. Is $\mathbb{Q}$ an indecomposable $\mathbb{Z}$-module?

2 Module Maps

Topics: R-module homomorphisms or simply R-maps, Isomorphism theorems and Chinese Remainder Theorem.

Ex. 67. Let M and N be two left R-modules. How will you define a homomorphism $f\colon M \to N$?

Definition 68. Let M and N be two modules over the same ring R. We say that a map $f\colon M \to N$ is an (R-module) *homomorphism* (or simply an R-map) if f is a group homomorphism with the additional property that $f(rx) = rf(x)$ for $r \in R$ and $x \in M$.

Ex. 69. Let $f\colon M \to N$ be an R-map. Define the kernel and the image of f. Show that they are submodules of ....

Ex. 70. What are the $\mathbb{Z}$-module homomorphisms?

Ex. 71. Let V and W be vector spaces over $\mathbb{F}$. When is a map $f\colon V \to W$ a module homomorphism?

Ex. 72. Keep the notation of Ex. 5. When is a map $A\colon V \to V$ an R-map?

Ex. 73. Let V_i be considered as $\mathbb{F}[X]$-modules via the linear maps T_i. Show that $V_1 \simeq V_2$ iff $T_1 = \varphi^{-1} \circ T_2\varphi$ for some vector space isomorphism $\varphi\colon V_1 \to V_2$.

Ex. 74. Let R be a commutative ring with 1. Prove that a map $f\colon R \times R \to R$ is an R-map iff there exist $a, b \in R$ such that $f(x, y) = ax + by$ for all $(x, y) \in R \times R$.

Ex. 75. Give an example of a map from one R-module into another which is a group homomorphism but not an R-map.

Ex. 76. Let $M = R$ considered as an R-module. Show that R-modules homomorphisms of M need not be ring homomorphisms and ring homomorphisms need not be module homomorphisms. *Hint:* Consider $\varphi\colon p(X) \mapsto p(X^2)$ for one of the parts.

Ex. 77. Let R be the ring $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. We may think of R as an R-module or as a $\mathbb{Z}$-module.

(i) Show that the map $f\colon a + b\sqrt{2} \mapsto a + b$ is a $\mathbb{Z}$-map.

(ii) The map f in (i) is not an R-map.

(iii) f is not a ring homomorphism.

Theorem 78 (Isomorphism Theorems)**.**

(1) **(First Isomorphism Theorem).** *Let M, N be R-modules and let $f\colon M \to N$ be an R-map. Then* $\ker f$ *is a submodule of M and we have $M/\ker f \simeq f(M)$.*

(2) **(Second Isomorphism Theorem).** *Let A and B be submodules of M. Then $(A + B)/B \simeq A/(A \cap B)$.*

(3) **(Third Isomorphism Theorem).** *Let M be an R-module and let A and B be submodules of M with $A \subset B$. Then $(M/A)/(B/A) \simeq M/B$.*

(4) **(Fourth Isomorphism Theorem).** *Let N be a submodule of the R-module M. Then there is a bijection between the submodules of M which contain N and the submodules of M/N. The correspondence is given by $A \leftrightarrow A/N$.*

Furthermore, this correspondence is a lattice isomorphism between the lattice of submodules of M/N and the lattice of submodules of M that contain N.

Proof. The proofs are similar to those of the corresponding results for groups. Begin the proofs by invoking the corresponding results for groups and then prove that the resulting group homomorphisms are, in fact, R-module homomorphisms. Details are left to you. □

Ex. 79. Let A be any $\mathbb{Z}$-module. Let $a \in A$ and $n \in \mathbb{N}$. Prove that the map $\varphi_a\colon \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi([k]) = ka$ is a well-defined $\mathbb{Z}$-map iff $na = 0$.

Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \simeq A_n$ where $A_n = \{a \in A \mid na = 0\}$. Conclude that A_n is the annihilator in A of the ideal $n\mathbb{Z}$.

Ex. 80. Exhibit all $\mathbb{Z}$-maps from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/12\mathbb{Z}$.

Ex. 81. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/(m, n)\mathbb{Z}$.

Ex. 82. Let $f\colon M \to N$ be an R-module homomorphism. Show that $f(\mathrm{Tor}\,(M)) \subset \mathrm{Tor}\,(N)$.

Ex. 83. Let R be commutative. Show that $\mathrm{Hom}_R(R, M) \simeq M$ as R-modules.

Ex. 84. Let R be a commutative ring with identity. Let M_n denote the R-module of all polynomials over R of degree at most n. Show that $M_{n-1} \simeq M_n/R$. *Hint:* Derivation map.

Ex. 85. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}) \simeq \mathbb{Q}$ as rings.

Ex. 86. With the notation of Ex. 34, show that $L_2 \simeq M_2$.

Ex. 87. Let M be an R-module and $x \in M$ be such that if $rx = 0$ then $r = 0$. Show that $Rx \simeq R$ as R-modules.

Ex. 88. Let A and B be submodules of an R-module M. Construct a short exact sequence

$$0 \to A \cap B \to A \times B \to A + B \to 0.$$

Ex. 89. Assume that R is commutative. Show that an R-module is simple iff M is isomorphic as an R-modules to R/I where I is a maximal ideal of R.

Ex. 90. Let M and N be R-modules. If M is simple, then any nonzero R-module map $f\colon M \to N$ is one-one.

What will be analogous result if N is simple?

What can you say about the ring $\mathrm{End}_R M$ if M is simple?

Ex. 91 (Schur's Lemma)**.** Let M and N be simple R-modules. Then an R-homomorphism from M to N is either the zero map or an isomorphism. As a consequence, deduce that $\mathrm{End}_R(M)$, the set of all R-maps from M to itself, is a division ring if M is simple.

Ex. 92. An R-module is cyclic iff $M \simeq R/I$ for some left ideal I in R.

Ex. 93. Let $M = Rx$ be a cyclic R-module. Show that $M \simeq R/\mathrm{Ann}_R\{x\}$.

Use this to prove the following: If R is a PID and $x \in R$ is such that $\mathrm{Ann}_R x = p^k R$ for some prime $p \in R$, then the only submodules of M are of the form $M' = p^r R$ for some $0 \le r \le k$.

Ex. 94. If M is generated by n elements, then any quotient of M can be generated by at most n elements. Hence conclude that the quotient of a cyclic module is cyclic.

Ex. 95. Let R be a commutative ring with 1 and let $M = Rx$ be a cyclic R-module. Prove that R is isomorphic to the quotient module $R/\mathrm{Ann}_R M$. Hence conclude that two cyclic modules are isomorphic iff they have the same annihilator.

Ex. 96. Let N be a FG submodule of an R-module M. Assume that the quotient M/N is also FG as an R-module. Prove that M is FG R-module.

Ex. 97 (Chinese Remainder Theorem)**.** If I is any ideal of R, recall the definition of the submodule IM (Ex. 24).

(a) Let A_j, $1 \le j \le k$, be ideals in R. Prove that the map $\varphi\colon M \to (M/A_1M) \times \cdots \times (M/A_kM)$ defined by

$$\varphi(x) := (x + A_1M, \ldots, x + A_kM)$$

is an R-map with kernel $A_1M \cap \cdots \cap A_kM$.

(b) Assume further that A_j are comaximal, i.e., $A_i + A_j = R$ for all $i \ne j$. Prove that

$$M/(A_1 \cdots A_k)M \simeq (M/A_1M) \times \cdots \times (M/A_kM).$$

Hint: Recall the proof of CRT in the context of rings.

Ex. 98. Let R be a PID and M be a torsion R-module with $\mathrm{Ann}_R M = (c)$. Assume that $c = ab$ in R with $(a, b) = 1$. Show that $M = M_a \oplus M_b$ where $M_r := \{x \in M : rx = 0\}$ for $r \in R$.

Ex. 99 (Primary Decomposition)**.** Let R be a PID. Let M be an R-module annihilated by a nonzero proper ideal (a). Let $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the unique factorization of a into distinct prime powers in R. Let M_i be annihilator of $(p_j^{\alpha_j})$ in M. Thus, $M_i := \{x \in M : p_j^{\alpha_j} x = 0\}$. Prove that

$$M = M_1 \oplus \cdots \oplus M_k.$$

Hint: Use the last exercise (Ex. 98).

M_i is called the *p_i-primary component* of M.

Ex. 100. Understand the last exercise (Ex. 99) when M is finite abelian group.

3 Free Modules

Topics: Linear independence, basis; Free modules and free rank of a free module over commutative rings.

Ex. 101. When do you say a finite subset of an R-module is linearly dependent?

Definition 102. A finite subset $S = \{x_j : 1 \le j \le n\}$ is said to be *linearly dependent* if there exist elements $r_i \in R$, not all zero, such that $r_1 x_1 + \cdots + r_n x_n = 0$. Otherwise S is said to be *linearly independent*.

Ex. 103. $x_1, \ldots, x_n$ are linearly independent iff whenever $\sum_i r_i x_i = 0$ then each of $r_i = 0$.

Definition 104. An R-module F is said to be *free* on the subset $S \subset F$ if for every element $x \in F$ there exist unique nonzero elements $r_1, r_2, \ldots, r_n \in R$ and unique $x_1, \ldots, x_n \in S$ such that $x = r_1 x_1 + \cdots + r_n x_n$ for some $n \in \mathbb{Z}_+$.

In this case, we say that S is a *basis* or *a set of free generators* of F.

Theorem 105. *For any set S there is a free R-module $F(S)$ on the set S.*

The module $F(S)$ satisfies the following universal property*: if M is an R-module and $\varphi\colon S \to M$ is any (set theoretic) map, there exists a unique R-map $\Phi\colon F(A) \to M$ such that $\Phi(x) = \varphi(x)$ for all $x \in S$.*

Proof. Let $F(S) = (0)$ if $S = \emptyset$. If $S \neq \emptyset$, let $F(S)$ stand for the set of all functions $f\colon S \to R$ such that $f(s) = 0$ except for finitely many $s \in S$. (Compare Ex. 8.) For $s \in S$, let $f_s \in F(S)$ be defined by $f_s(s) = 1$ and $f_s(t) = 0$ for $t \in S$ and $t \neq s$. Any $f \in F(S)$ can be written formally as $r_1 s_1 + \cdots + r_n s_n$ where $r_i \neq 0$ for each i.

Given φ as in the theorem, define $\Phi(\sum_{i=1}^n r_i s_i) = \sum_i r_i \varphi(s_i)$. □

Ex. 106. Let M be a free R-module with a basis $\{x_i : 1 \le i \le n\}$. Then show that $M \simeq R^n$.

Ex. 107. Let M be a free module over a commutative ring R. Then all bases of M have the same number of elements. *Hint:* Enough to show that if $\varphi\colon R^m \to R^n$ is an R-isomorphism, then $m = n$. Let $\psi := \varphi^{-1}$. Let $\{e_i : 1 \le i \le m\}$ (resp. $\{f_j : 1 \le j \le n\}$) be a basis of R^m (resp. R^n). Write $\varphi(e_i) = \sum_{j=1}^n a_{ji} f_j$ and $\psi(f_j) = \sum_{i=1}^m b_{kj} e_k$. Observe that $AB = I_n$ and $BA = I_m$ using an obvious notation.

Ex. 108. Solve the last exercise using the following observation. Let I be a maximal ideal of R. Then $V := M/IM$ is a vector space over the field R/I.

Definition 109. In view of Ex. 107 or Ex. 108, we define the (free) *rank* of a free module over a commutative ring to be the number of elements in a basis.

Ex. 110. Let R be a commutative ring with identity. Let $e \in R$ be such that $e^2 = e$ and $e \neq 0, 1$. Show that Re cannot be a free R-module.

Ex. 111. A set of generators of a free R-module need not contain a basis. *Hint:* Consider the abelian group $\mathbb{Z}$ with the generating set $\{2, 3\}$.

Ex. 112. Show that every principal left ideal in an integral domain with 1 is free as a left R-module.

Ex. 113. Prove that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module. Can you generalize this? *Hint:* Field of fractions.

Ex. 114. Show that every ideal of $\mathbb{Z}$ is free as a $\mathbb{Z}$-module.

Ex. 115. Prove that every principal left ideal in an integral domain R with 1 is a free R-module.

Ex. 116. Let $f \in \operatorname{End}_R(M)$. Show that if f is one-one, then f is not a left zero divisor in the ring $\operatorname{End}_R(M)$.

Prove the converse if M is free. *Hint:* If $\{x_i\}$ is a basis of M and $\{y_i\}$ arbitrary nonzero elements of $\ker f$, consider $g(x_i) = y_i$.

Ex. 117. Let $p \in \mathbb{N}$ be a prime. Let

$$Q_p := \{x \in \mathbb{Q} : (\exists k \in \mathbb{Z}) \text{ and } (\exists n \in \mathbb{N}) \text{ such that } x = k/p^n\}.$$

Show that $\mathbb{Q}_p/\mathbb{Z}$ is not free as $\mathbb{Z}$-module. *Hint:* Last exercise Ex. 116

Ex. 118. What is the analogue of Ex. 116 in the case of an onto map f?

Ex. 119. Let R be a commutative ring with 1. Let I be an ideal of R. Prove that every linearly independent subset of the R-module I has at most one element. *Hint:* $xy - yx = 0$!

Deduce that if I is finitely generated, but not principal, then I has no basis.

Ex. 120. Let R be a commutative ring with 1 with the property that every ideal of R is free as an R-module. Show that R is PID. *Hint:* Ex. 119.

Ex. 121. Let R be a PID and let M be a FG free R-module with a basis containing n elements. Assume that N is a submodule of M. Then show that N is free and that there exists a basis whose number of elements is at most n. *Hint:* Induction on n. Assume $M = R^n$ and consider $\pi\colon N \to R$ given by $\pi(x_1, \ldots, x_n) = x_1$. Then $\pi(N) = Ra = (a)$. Show that $M = (a) \oplus \ker \pi$. Observe that $\ker \pi \subset R^{n-1} \subset R^n$.

Ex. 122. Let R be a PID. Assume that M is FG torsion free R-module. Show that M is free.

Ex. 123. Let M be FG module over a PID R. Show that M can be expressed as $M = F \oplus \mathrm{Tor}\,(M)$ where F is a free R-module. *Hint:* Consider $N = M/\mathrm{Tor}\,(M)$. Then N is torsion free.

Ex. 124 (Splitting Property of Free Submodules)**.** Let M be an R-module. Let F be a FG free R-module. Let $f\colon M \to F$ be a surjective R-map. Then M has a submodule $G \simeq F$ such that $M = G \oplus \ker(f)$.

Ex. 125. Let $\mathbb{F}$ be a field of p elements. Let V be an n-dimensional vector space over $\mathbb{F}$. Prove the following:

(a) V has p^n elements.

(b) V has $p^n - 1$ linearly independent singleton sets.

(c) The number of linearly independent subsets of V consisting of m elements, $(1 \leq m \leq n)$, is

$$\frac{1}{m!}\prod_{k=0}^{m-1}(p^n - p^k).$$

Hint: Induction.

Determine the number of bases of V.

Ex. 126. Show that every FG (finitely generated) R-module is the homomorphic image of a free R-module.

Ex. 127. Give an example to show that a submodule of a free module need not be free. *Hint:* Consider $R := \mathbb{Z} \times \mathbb{Z}$ as a module over itself.

Ex. 128. Let $M := \oplus_{n\in\mathbb{N}} R$ be the direct sum of countably infinite number of a ring R with 1. We may regard M as the set of functions $f\colon \mathbb{N} \to R$ with the property that $f(k) = 0$ except for finitely many k.

(a) Show that if we define $f_i(k) = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{otherwise} \end{cases}$, then $\{f_i : i \in \mathbb{N}\}$ is a basis of M considered as an R-module.

(b) Consider $S := \mathrm{End}\,(M)$, the ring of **group** homomorphisms. If we consider S as a module over itself, then $\{\mathrm{id}\}$ is a basis for this module. Consider $\varphi, \psi \in S$ defined by

$$\varphi(f_i) = \begin{cases} f_n & \text{if } i = 2n; \\ 0 & \text{if } i = 2n+1, \end{cases}$$

and

$$\psi(f_i) = \begin{cases} 0 & \text{if } i = 2n; \\ f_n & \text{if } i = 2n+1. \end{cases}$$

Show that $\{\varphi, \psi\}$ is also a basis of S as an S-module.

4 Structure Theorem over a Euclidean Domain

Topics: The Structure theorem in the matrix form in an algorithmic fashion. Smith Normal Form. Concrete examples.

The following set of exercises outline a proof of a major step (Ex. 139 (e) or Proposition 153, page 15) towards the structure theorem for FG modules over a Euclidean ring. Till further notice, let us assume that R is Euclidean and let M be an R-module.

Definition 129. Let A and B be two matrices over R of the same size. We say that B is *equivalent* to A over R if there exist invertible matrices X and Y (over R)of appropriate sizes so that $B = XAY$.

Ex. 130. When are two 1×1 matrices equivalent?

Give two matrices over $\mathbb{Z}$ which are not equivalent over $\mathbb{Z}$ but are equivalent over $\mathbb{Q}$.

Ex. 131. Let R be a PID and let A be an $n \times n$ matrix over R. Show that R is invertible iff A is equivalent to the $n \times n$ identity matrix.

Ex. 132. Let R be a Euclidean domain. Show that the set of all $n \times n$ elementary matrices over R generate the group of all $n \times n$ invertible matrices over $\mathbb{R}$.

What is the corresponding result when R is a PID?

Ex. 133. Prove that M is finitely generated iff there is a surjective R-map $\varphi\colon R^n \to M$. (This is true for any ring.)

Definition 134. Let $\varphi\colon R^n \to M$ be a surjective R-map. By Ex. 146, $\ker\varphi$ is FG. If $x_1, \ldots, x_n$ is a basis of R^n and if $y_1, \ldots, y_m$ generate $\ker\varphi$, then we can write

$$y_i = a_{i1}x_1 + \cdots + a_{in}x_n, \text{ for } 1 \leq i \leq n,$$

where the coefficients $a_{ij} \in R$. The matrix $A = (a_{ij})$ is called the *relations matrix* corresponding to the choices of $\{x_i\}$ and $\{y_j\}$.

Ex. 135. This is essentially an observation.

Keep the notation of the definition. The homomorphism and hence the module structure of M is completely determined by the choice of generators for R^n and the relations matrix A.

The next few exercises tell us how the relations matrix changes if we effect "elementary operations" either on the basis $\{x_i\}$ of R^n or on the set of generators of $\ker\varphi$.

Ex. 136. Show that interchanging x_i and x_j in the basis of R^n interchanges the i-th and j-th columns of the relations matrix A.

Ex. 137. Show that, for any $a \in R$, replacing the element x_j by $x_j - ax_i$, $(i \neq j)$ in the basis of R^n gives another basis of R^n.

Show also that the new relations matrix is the same as the original one except that the new i-th column is the old one plus a-times the old j-th column.

Ex. 138. Show that interchanging the basic elements y_i and y_j interchanges the corresponding rows of the relations matrix.

Show that, for any $a \in R$ and $i \neq j$, replacing the element y_j by $y_j - ay_i$ gives another set of generators for $\ker\varphi$. How are the relations matrices 'related?'

Ex. 139. By the last few exercises, we may perform elementary row and column operations on a given matrix by choosing different generators for R^n and $\ker\varphi$. If all relation matrices are zero, then $\ker\varphi = (0)$ and $M \simeq R^n$. Otherwise, let a_1 be the (nonzero) g.c.d. of all the entries of a fixed relations matrix.

(a) Prove that by elementary row and column operations we may assume that a_1 occurs in (1,1)-th place and that a_1 divides all the entries a_{ij}, $1 \le i \le m$ and $1 \le j \le n$.

(b) Prove that there is a relations matrix of the form

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

where a_1 divides all the entries.

(c) Let a_2 be the g.c.d. of all the entries except a_1 in the relations matrix in (b). Prove that there is a relations matrix of the form

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

where a_1 divides a_2 and a_2 divides all other entries of the matrix.

(d) Prove that there is a relations matrix of the form $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ where D is a diagonal matrix with nonzero entries $a_1, a_2, \dots, a_k$, $k \le n$, satisfying $a_1 \mid a_2 \mid \cdots \mid a_k$.

(e) Conclude that

$$M \simeq R^{n-k} \oplus R/(a_1) \oplus \cdots \oplus R/(a_k).$$

(f) If n is not the minimal number of generators required for M some of the initial a_i will be units so that the corresponding direct summands will be zero modules. If we remove these irrelevant factors we have produced the *invariant factors* (a_i), $1 \le i \le k$, of the module M.

Ex. 140. Observe that the steps in the last exercise have proved the following. If A is an $m \times n$ matrix over a Euclidean domain R , by elementary row and column operations, we may bring it to a diagonal matrix of the form $(a_1, a_2, \dots, a_r, 0, \dots, 0)$ where $a_1 \mid a_2 \mid \cdots \mid a_r$ in R.

This is known as the *Smith normal form* of A. Its uniqueness will be seen by different means in a later section.

Ex. 141. Obtain the Smith normal form of the following matrices over $\mathbb{Z}$.

(i) $\begin{pmatrix} 0 & 2 & -1 \\ -3 & 8 & 3 \\ 2 & -4 & -1 \end{pmatrix}$ Ans: (1,1,10).

(ii) $\begin{pmatrix} 5 & 9 & 5 \\ 2 & 4 & 2 \\ 1 & 1 & -3 \end{pmatrix}$ Ans. (1,2,4).

Ex. 142. Find the invariant factors and the Smith normal form of the matrix

$$\begin{pmatrix} -x-3 & 2 & 0 \\ 1 & -x & 1 \\ 1 & -3 & -x-2 \end{pmatrix}$$

over $\mathbb{Q}[X]$. Ans. 1,1 $(1+x)^2(x+3)$.

5 Structure Theorem over a PID

Topics: Structure theorem in invariant factor and elementary divisor forms. Uniqueness.

Definition 143. An R-module is said to satisfy the *ascending chain condition* on submodules (or said to be *Noetherian*) if given any ascending chain $M_1 \subseteq M_2 \subseteq \cdots$ of submodules of M, then there exists $N \in \mathbb{N}$ such that $M_n = M_N$ for all $n \geq N$.

A ring R is said to be *left Noetherian* if it is Noetherian when considered as a left module over itself.

Ex. 144. Show that any PID is Noetherian.

Ex. 145. Let R be a ring and M be an R-module. Then the following are equivalent:
(a) M is Noetherian.
(b) Every nonempty collection of submodules of M contains a maximal element under inclusion.
(c) Every submodule of M is finitely generated.

Ex. 146. Prove that if R is a Noetherian ring, then R^n is a Noetherian R-module. *Hint:* If M is a submodule of R^n, then the set of first coordinates of M is a submodule of R and hence is f.g. Let $m_1, \ldots, m_k$ be elements of M whose first coordinates generate the submodule of R. Show that any element of M can be written as an R-linear combination of m_j's and an element of M whose first coordinate is zero. Prove that $M \cap R^{n-1}$ is a submodule of R^{n-1}, the set of elements of R^n whose first coordinate is zero. Use induction on n.

For the rest of this section, we shall assume that R is a PID unless specified otherwise.

Definition 147. Let M be an R-module over an integral domain. The *rank* of M is the maximum number of R-linear independent elements of M.

Ex. 148. Let M be a FG free R-module and let N be a submodule of M. For any $f \in \mathrm{Hom}_R(M, R)$, the image $f(N)$ is an ideal in R so that $f(N) = (a_f)$. Let $\Sigma := \{(a_f) \mid f \in \mathrm{Hom}_R(M, R)\}$. Show that this nonempty collection of ideals in R has a maximal element, say (a_φ) and that $a_\varphi \neq 0$. *Hint:* Choose a basis $x_1, \ldots, x_n$ of M. Let $\pi_i \in \mathrm{Hom}_R(M, R)$ be the natural projections. Observe that there exists i such that $\pi_i(N) \neq 0$.

We denote a_φ by a_1 in the sequel. Let $y \in N$ be such that $\varphi(y) = a_1$. We keep the notation of this till Proposition 153.

Ex. 149. Keep the notation of Ex. 148. Show that a_1 divides $f(y)$ for any $f \in \mathrm{Hom}_R(M, R)$. *Hint:* Let $(d) = (a_1, y)$. Then $d = ra_1 + sf(y)$. Consider $\psi := r\varphi + sf$. Observe that $\psi(y) = d$.

Ex. 150. Apply the last exercise to π_i to conclude that a_1 divides $\pi_i(y)$ for all i so that $\pi_i(y) = a_1 b_i$ for some $b_i \in R$. Define

$$y_1 := \sum_i b_i x_i.$$

Show that $\varphi(y_1) = 1$.

Ex. 151. With the notation of the last exercise, prove the following:
(a) $M = Ry_1 \oplus \ker \varphi$,
(b) $N = Ra_1 y_1 \oplus (N \cap \ker \varphi)$.

Conclude that y_1 can be taken as one element of a basis of M and that $a_1 y_1$ can be taken as one element in a basis of N.

Ex. 152. With the notation of Ex. 148, show that N is a free submodule of rank m with $m \leq n$. *Hint:* Proof by induction on the rank m of N.

Compare this with the hint in Ex. 121.

Proposition 153. *Let R be a PID. Let M be a free FG R-module and let N be a submodule of M. Then there exists a basis $y_1, y_2, \ldots, y_n$ of M and nonzero elements $a_i \in R$ such that*
(i) *$a_1 y_1, \ldots, a_m y_m$ is a basis of N and*
(ii) *$a_1 \mid a_2 \mid \cdots \mid a_m$.*

Proof. Prove it by induction on n, the rank of M. Apply the last exercise (Ex. 152) and Ex. 151 to $\ker \varphi$ to conclude that $\ker \varphi$ is free of rank $n - 1$. □

Ex. 154. What does the last proposition say in the context of vector spaces?

Theorem 155 (Structure Theorem - Invariant Factor Form)**.** *Let R be a PID and let M be a FG R-module. Then M is isomorphic to the direct sum of finitely many cyclic R-modules. More precisely, we have*

$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

for some integers $r \geq 0$ and nonzero and nonunit elements $a_i \in R$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$.

Proof. Let $x_1, \ldots, x_n$ be a *minimal* set of generators of M. Let R^n be the free module with a basis b_j, $1 \leq j \leq n$. Let $\pi \colon R^n \to M$ be the R-map defined by $\pi(b_i) = x_i$. We have $R^n / \ker \pi \simeq M$. Apply Ex. 152 and Prop. 153 to the pair R^n and $\ker \pi$. □

Remark 156. The elements a_j, $1 \leq j \leq m$, which are unique up to units are called the *invariant factors* of M. (We are yet to show that these invariant factors are 'unique'!)

Theorem 157 (Structure Theorem - Elementary Divisor Form)**.** *Let R be a PID and let M be a FG R-module. Then M is the direct sum of a finite number of cyclic modules whose annihilators are either (0) or generated by powers of prime elements of R. That is,*

$$M \simeq R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k})$$

where $r \geq 0$ and $\alpha_j > 0$ are integers and p_j's are (not necessarily distinct) primes in R.

Proof. If $a = up_1^{\alpha_1} \cdots p_k \alpha_k$ is the prime factorization of $a \in R$, it follows from Chinese Remainder Theorem that

$$R/(a) \simeq R/(p_1^{\alpha_1}) \oplus \cdots R/(p_k^{\alpha_k}),$$

as (rings as well as) R-modules. Use this in conjunction with the Structure Theorem. □

Ex. 158. Let R be a PID. Let M be an R-module. Then M is free iff it is torsion free.

Ex. 159. With the notation of the Structure Theorem (Thm. 155), show that

$$\mathrm{Tor}\,(M) \simeq R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

What is $\mathrm{Ann}_R(M)$?

Ex. 160. Let R be a PID and let p be a prime in R. Let F be the field $F := R/(p)$. Then
(a) If $M \simeq R^r$, then $M/pM \simeq F^r$.
(b) Let $M = R/(a)$ where a is a nonzero element. Then

$$M/pM \simeq \begin{cases} F & \text{if } p \text{ divides } a \text{ in } R \\ 0 & \text{if } p \text{ does not divide } a \text{ in } R. \end{cases}$$

(c) Let $M = R/(a_1) \oplus \cdots \oplus R/(a_k)$ where each a_i is divisible by p. Then $M/pM \simeq F^k$.

Lemma 161. *Let M_j be two R-modules such that $Ann_R(M_j) = (p^{\alpha_j}$, $j = 1, 2$. Assume that $M_1 \simeq M_2$. Then they have the same elementary divisors.*

Proof. Induction on the power of p in $\mathrm{Ann}_R(M_1)$. If the elementary divisors of M_1 are given by

$$\underbrace{p, \ldots, p}_{m \text{ times}}, p^{\alpha_1}, \ldots, p^{\alpha_k},$$

where $\alpha_j \geq 2$, then look at the elementary divisors of pM_1. □

Theorem 162 (Structure Theorem - Uniqueness)**.** *Let R be a PID.*
(a) *Two FG R-modules M_1 and M_2 are isomorphic iff they have the same free rank and the same list of invariant factors.*
(b) *Two FG R-modules M_1 and M_2 are isomorphic iff they have the same free rank and the same list of elementary divisors.*

Proof. Let r_j be the free rank of M_j. Observe that

$$R^{r_1} \simeq M_1/\mathrm{Tor}\,(M_1) \simeq M_2/\mathrm{Tor}\,(M)_2 \simeq R^{r_2}.$$

Use (a) of Ex. 160 to deduce that $r_1 = r_2$.

So, we may assume that the modules are torsion modules. To show that they have the same elementary divisors, it suffices to show that for any fixed prime p, the elementary divisors which are powers of p are the same for both M_1 and M_2. This is reduced to the case of Lemma 161.

To show that they have the same invariant factors, using the divisibility properties of these factors, the elementary divisors are obtained by taking the prime power factors of these invariant factors. □

Ex. 163. Let M be a FG module over a PID R. The elementary divisors of M are prime powers of the invariant factors of M

Ex. 164. Let $R = \mathbb{Z}[X]$. Show that the ideal $I = (2, X)$ cannot be written as a direct sum of cyclic $\mathbb{Z}[X]$-modules.

Ex. 165. Let R be a PID. Let $M = Rx$ be a cyclic R-module of prime power exponent, say p^n. Show that the only submodules of M are

$$\{0\} = M_n \subset M_{n-1} \subset \cdots \subset M_1 \subset M_0 = M,$$

where $M_k := p^k M$.

Ex. 166. Let M be a torsion module over a PID. Show that M is simple iff M is cyclic with prime exponent.

Ex. 167. Let M be a torsion module over a PID. Show that M is indecomposable iff M is cyclic with prime power exponent.

6 Applications

Topics: (i) Structure theorem for FG abelian groups; (ii) Rational canonical forms and (iii) Jordan canonical forms.

6.1 Finitely Generated Abelian Groups

The following result is immediate form the Structure Theorem when we take $R = \mathbb{Z}$.

Theorem 168 (Structure Theorem for FG Abelian Groups)**.** *If G is a finitely generated abelian group, then*

$$G \simeq \mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(q_1)} \oplus \cdots \oplus \frac{\mathbb{Z}}{(q_k)}, \quad q_1 \mid \cdots \mid q_k.$$

Furthermore this decomposition is unique. □

Ex. 169. Find the number of abelian groups of order p^n (p, a prime).

Ex. 170. Find the number of abelian groups of order $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Ex. 171. Find all abelian groups of order 60.

Ex. 172. For what values of $n \in \mathbb{N}$, is it true that the only abelian groups of order n are cyclic?

Ex. 173. Let G be a finite abelian group which is not cyclic. Show that G contains a subgroup isomorphic to $\mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$ for some prime p.

Ex. 174. Show that the abelian group generated by
(i) x_1 andx_2 with the relations $2x - 1 = 0$ and $3x_2 = 0$is isomorphic to $\mathbb{Z}/(6)$.
(ii) x_1 andx_2 with the relation $x_1 + x_2 = 0$ is isomorphic to $\mathbb{Z}$.
(iii) x_1, x_2 and x_3 with the relations

$$\begin{aligned} 5x_1 + 9x_2 + 5x_3 &= 0 \\ 2x_1 + 4x_2 + 2x_3 &= 0 \\ x_1 + x_2 - x_3 &= 0 \end{aligned}$$

is isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(4)$.
Hint: What is the relations matrix in each case? Bring it to the Smith normal form.

6.2 Rational Canonical Form

We keep the notation of Ex. 5. By Ex. 56, we know that V is a FG torsion $\mathbb{F}[X]$-module. If we apply the Structure Theorem in invariant factor form (Theorem155) to this module, we get the so-called rational canonical form of T.

Definition 175. The unique monic polynomial which generates the ideal $\mathrm{Ann}_{\mathbb{F}[X]}(V)$ is called the minimal polynomial of T. We shall denote it by $m_T(X)$.

Ex. 176. Show that $\deg(m_T(X)) \leq n^2$ where $n := \dim V$. (In fact, the degree of the minimal polynomial of T is at most $\dim V$.)

Ex. 177. We have

$$V \simeq \frac{\mathbb{F}[X]}{(a_1(X))} \oplus \cdots \oplus \frac{\mathbb{F}[X]}{(a_m(X))} \tag{1}$$

as $\mathbb{F}[X]$-modules where $a_j(X)$ are monic polynomials of degree at least one and are such that $a_1(X) \mid \cdots \mid a_m(X)$. These polynomials $a_j(X)$ are the invariant factors of V and are unique.
Hint: Straight forward application of Theorem 155.

Ex. 178. The minimal polynomial $m_T(X)$ is the largest invariant factor of V and all invariant factors divide $m_T(X)$. *Hint:* This follows from 3) of Theorem 155.

To arrive at the canonical form of T, we need to choose a basis for each of the summands on the right side of Eq. 1. We look at the simplest case.

Proposition 179. *Let $V \simeq \mathbb{F}[X]/(a(X))$. Then there exists a basis of V with respect to which the matrix of T is given by*

$$\begin{pmatrix} 0 & 0 & \dots & \dots & \dots & -b_0 \\ 1 & 0 & \dots & \dots & \dots & -b_1 \\ 0 & 1 & \dots & \dots & \dots & -b_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 1 & -b_{k-1} \end{pmatrix}, \tag{2}$$

where $a(X) = X^k + b_{k-1}X^{k-1} + \cdots + b_1X + b_0$.

Proof. We use the natural basis of $\mathbb{F}[X]/(a(X))$. T's action on V is same as X's action on the right side. Now X maps the basic element $\overline{X}^j$ to $\overline{X}^{j+1}$ for $0 \leq j \leq k-2$ and $\overline{X}^{k-1}$ is mapped to $\overline{X}^k$ which is $-b_0 - b_1\overline{X} - \cdots - b_{k-1}\overline{X}^{k-1}$. The result follows from this observation. □

Definition 180. The matrix in Eq. 2 is called the *companion matrix* of the monic polynomial a and will be denoted by C_a.

Theorem 181 (Rational Canonical Form)**.** *Let V be a finite dimensional vector space over a field $\mathbb{F}$ and let $T\colon V \to V$ be a linear map. Then there exists a basis of V with respect to which the matrix T looks like*

$$\begin{pmatrix} C_{a_1} & & & \\ & C_{a_2} & & \\ & & \ddots & \\ & & & C_{a_m} \end{pmatrix} \tag{3}$$

where $a_1 \mid \cdots \mid a_m$ are monic polynomials.

Furthermore, this matrix is "unique". In other words, if there exists a basis of V with respect to which the matrix of T is a block diagonal matrix whose diagonal blocks are the companion matrices of monic polynomials b_j of degree at least one with the divisibility property $b_1 \mid \cdots \mid b_k$, then $m = k$ and $b_i = a_i$ for $1 \leq i \leq m$. □

Definition 182. The matrix in Eq. 3 is called the *rational canonical form* of T.

Definition 183. Two linear transformations $S, T\colon V \to V$ are said to be *similar* if there exists a linear isomorphism $\varphi\colon V \to V$ such that $\varphi^{-1} \circ S \circ \varphi = T$.

Ex. 184. Let $S, T\colon V \to V$ be linear transformations. Then the following are equivalent:
(i) S and T are similar.
(ii) The $\mathbb{F}[X]$-module V via S is isomorphic to the $\mathbb{F}[X]$-module V via T.
(iii) S and T have the same rational canonical form.

Ex. 185. Let A and B be two $n \times n$-matrices over the field $\mathbb{F}$. Assume that $\mathbb{F}$ is a subfield of a filed $\mathbb{K}$.

(i) The rational canonical form of A is the same whether computed over $\mathbb{F}$ or over $\mathbb{K}$. The minimal and characteristic polynomials and invariant factors of A are the same whether A is considered as a matrix over $\mathbb{F}$ or over $\mathbb{K}$.

(ii) The matrices A and B are similar over $\mathbb{K}$ iff they are similar over $\mathbb{F}$.

Ex. 186. The characteristic polynomial of C_a of a monic polynomial $a(X) \in \mathbb{F}[X]$ is $a(X)$.

What can you say of a matrix which is in "rational canonical form"?

Ex. 187. Let A be an $n \times n$ matrix over $\mathbb{F}$.

(i) The characteristic polynomial of A is the product of invariant factors of A.

(ii) The minimal polynomial of A divides the characteristic polynomial of A.

(iii) The characteristic polynomial of A divides some power of the minimal polynomial of A. In particular, these polynomials have the same roots not counting the multiplicities. *Hint:* Last exercise (Ex. 186).

Ex. 188. Find the rational canonical forms of the following matrices over $\mathbb{Q}$:

(i) $\begin{pmatrix} -3 & 2 & 0 \\ 1 & 0 & 1 \\ 1 & -3 & 1 \end{pmatrix}$. *Hint:* Some work is already done in Ex. 142! Ans. $\begin{pmatrix} 0 & 0 & -3 \\ 1 & 0 & -7 \\ 0 & 1 & -5 \end{pmatrix}$.

(ii) $A = \begin{pmatrix} 2 & -2 & 14 \\ 0 & 3 & -7 \\ 0 & 0 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -4 & 85 \\ 1 & 4 & -30 \\ 0 & 0 & 3 \end{pmatrix}$, $C = \begin{pmatrix} 2 & 2 & 1 \\ 0 & 2 & -1 \\ 0 & 0 & 3 \end{pmatrix}$. Are they similar?

Hint: A shorter way would be to compute the characteristic polynomials and the possible minimal polynomials. Verify directly which of them are minimal polynomials of the matrices under question.

Ex. 189. Prove that two non-scalar 2×2 matrices over a field $\mathbb{F}$ are similar iff they have the same characteristic polynomial.

Ex. 190. Prove that two 3×3 matrices are similar iff they have the same characteristic and same minimal polynomials.

Ex. 191. Find two 4×4 matrices over $\mathbb{C}$ which have the same characteristic and minimal polynomials but are not similar.

Ex. 192. Describe the 2×2 matrices over $\mathbb{C}$ whose similarity classes contain only one element. Generalize your answer.

6.3 Jordan Canonical Form

We keep the notation of Ex. 5. By Ex. 56, we know that V is a FG torsion $\mathbb{F}[X]$-module. If we apply the Structure Theorem in elementary divisor form (Theorem 157) to this module, we get the so-called Jordan canonical form of T with an additional assumption that $\mathbb{F}$ contains all the roots of the characteristic polynomial of T.

Hypothesis: To make our life easy, we shall assume that $\mathbb{F}$ is algebraically closed. Note, however, that the results will remain true if we assume that the characteristic polynomial of T factors into linear factors in $\mathbb{F}[X]$.

Ex. 193. The elementary divisors of V are powers $(X - \lambda)^k$ of linear polynomials. *Hint:* Ex. 163.

Ex. 194. V is the direct sum of finitely many cyclic $\mathbb{F}[X]$-modules of the form $\frac{\mathbb{F}[X]}{(X-\lambda)^k}$.

Ex. 195. Let V be a cyclic $\mathbb{F}[X]$-module isomorphic to $\mathbb{F}[X]/(X - \lambda)^k$. Then we can choose a basis for V so that T has a matrix of the form

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \ddots & & \\ & & \ddots & 1 & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \tag{4}$$

where the blank entries are zero. *Hint:* See how X acts on the basis (?)

$$(\overline{X} - \lambda)^{k-1}, (\overline{X} - \lambda)^{k-2}, \ldots, (\overline{X} - \lambda), 1.$$

Definition 196. A matrix of the form in Eq. 4 is known as a *Jordan block* of size k with eigen value λ.

Theorem 197 (Jordan Canonical Form)**.**
Let V be a finite dimensional vector space over a field $\mathbb{F}$. Let $T\colon V \to V$ be a linear map. Assume that $\mathbb{F}$ contains all the eigenvalues of T.

(i) *There exists a basis of V with respect to which the matrix of T is a block diagonal matrix whose diagonal blocks are the Jordan blocks for the elementary divisors of T.*

(ii) *The above form is unique up to permutations of the Jordan blocks.* □

Ex. 198. If a matrix A is similar to a diagonal matrix D, then D is th Jordan canonical form of A. Consequently, two diagonal matrices are similar iff they have the same diagonal entries up to permutation.

Ex. 199. Let A be a matrix over $\mathbb{F}$. Assume that $\mathbb{F}$ contains all the eigenvalues of A. Then A is similar to a diagonal matrix iff the minimal polynomial $m_A(X)$ of A has no repeated roots.

Ex. 200. Prove that for 3×3 complex matrices the knowledge of the characteristic and minimal polynomials determine the JCF.

Using this, write down all possible JCF's for 3×3 matrices over $\mathbb{C}$.

Ex. 201. Use Ex. 200 to find the JCF of $\begin{pmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix}$.