A Course in Module Theory

Amber Habib
Stat Math Unit
Indian Statistical Institute
Bangalore Centre
Bangalore 560059
habib@isibang.ac.in, a_habib@yahoo.com

S. Kumaresan
Department of Mathematics
University of Mumbai
Mumbai 400098
kumaresa@math.mu.ac.in

Contents

In these notes, the difference between an example and an exercise is somewhat superficial. Even in an example, the student should take care to fill in the details. Further exercises and material are in the attached Problem Set, hereafter referred to as [P].

1 Basic Notions

Topics: definition, examples, submodule, quotient, direct sum and product, homomorphism, isomorphism theorems, internal direct sum.

Definition and Examples

The notion of module generalizes that of vector space. So we start by recalling the definition of a vector space.

Definition 1. A *vector space over a field* $\mathbb{F}$ is a set V with a binary operation $+ : V \times V \to V$ called *addition* as well as a map $\mathbb{F} \times V \to V$ called *scalar multiplication* and denoted $(\alpha, x) \longmapsto \alpha \cdot x$ or αx, such that

1. $x + y = y + x \quad \forall\, x, y \in V$
2. $x + (y + z) = (x + y) + z \quad \forall\, x, y, z \in V$
3. $\exists\, 0 \in V$ such that $x + 0 = x \quad \forall\, x \in V$
4. Given $x \in V$, $\exists\, y \in V$ such that $x + y = 0$ (And y is called $-x$)
5. $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y \quad \forall\, \alpha \in \mathbb{F}, \quad \forall\, x, y \in V.$
6. $(\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x) \quad \forall\, \alpha, \beta \in \mathbb{F}, \quad \forall\, x \in V$
7. $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x \quad \forall\, \alpha, \beta \in \mathbb{F}, \quad \forall\, x \in V$
8. $1 \cdot x = x$

Conditions (1) to (8) are called "the axioms for a vector space". Observe that axioms (1) to (4) exactly establish that $(V, +)$ is an abelian group with identity 0.

Example 2. Some familiar vector spaces:

1. A field over a subfield (e.g. $\mathbb{C}$ over $\mathbb{R}$).
2. $\mathbb{F}^n$ over $\mathbb{F}$, $\mathbb{F}$ is any field.
3. $M_{n\times m}(\mathbb{F}) = \{n \times m$ matrices with entries from $\mathbb{F}\}$ over $\mathbb{F}$, with componentwise operations.
4. $L(V) =$ linear maps from a vector space into itself.
5. $X =$ any non-empty set, $\mathbb{F} =$ any field. Then $V = \{f : X \to \mathbb{F}\}$ is a vector field over $\mathbb{F}$.

Example 3. The following are *not* vector spaces:

1. $GL_n(\mathbb{F})$ = invertible $n \times n$ matrices with entries from a field $\mathbb{F}$. (not closed under addition)

2. $\mathbb{R}$ over $\mathbb{C}$. (not closed under scalar multiplication)

3. $\mathbb{Z}$ over $\mathbb{Z}_p$, p prime. (axioms aren't consistent)

4. $\mathbb{Z}^n$ over $\mathbb{Z}$. ($\mathbb{Z}$ is not a field)

Of these non-examples the last is in a sense closest to being a vector space. For it is closed under $+$ and $\cdot$, and all the eight axioms hold. The only lack is that $\mathbb{Z}$ is a ring but not a field. The question this raises is : How essential is it to work over a field? For the axioms make sense over any ring (with 1)!

Definition 4. Let $(M, +)$ be an abelian group. We say it is a *module over a ring* R, or an R-*module*, if there is a map $R \times M \to M$ called *scalar multiplication* and denoted $(\alpha, x) \longmapsto \alpha \cdot x$ such that

1. $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y \quad \forall\, \alpha \in R,\, x, y \in M.$

2. $\alpha \cdot (\beta \cdot x) = (\alpha\beta) \cdot x \quad \forall\, \alpha, \beta \in R,\, x \in M.$

3. $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x \quad \forall\, \alpha, \beta \in R,\, x \in M.$

4. $1 \cdot x = x \quad \forall\, x \in M.$

Remark. It is implicit above that R has a multiplicative identity 1. We will work with such rings alone. We further assume $0 \neq 1$ in R, i.e. R is not the zero ring. Note that we put the scalars on the left. So what we have defined is more precisely called a *left* R-*module*.

Example 5. Some rings:

1. Fields

2. $\mathbb{Z}$

3. $\mathbb{Z}_n$, $n \in \mathbb{N}$

4. $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$

5. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

6. $\mathbb{F}[X]$ = polynomials with coefficients from a field $\mathbb{F}$ and indeterminate X.

7. $M_{n \times n}(\mathbb{F})$

8. $L(V)$, V is a vector space over $\mathbb{F}$, under pointwise addition and composition.

9. Fix $A \in L(V)$. Then $\mathbb{F}[A]$ is a ring (a subring of $L(V)$).

10. $X \neq \emptyset$, R = any ring. Consider $\{f : X \to R\}$.

11. $G =$ finite group, $R =$ any ring. Consider $R[G] = \{f : G \to R\}$ with

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (f*g)(x) &= \sum_{y \in G} f(xy^{-1})g(y). \end{aligned}$$

$R[G]$ is called the **group ring** of G.

Ex. 6. Check that $R[G]$ is a ring. Find its multiplicative identity. When is this ring abelian?

Example 7. We introduce the most imortant examples of modules. Whenever new concepts are introduced, the reader should investigate/explore them in these examples.

1. Any vector space over a field $\mathbb{F}$ is an R-module with $R = \mathbb{F}$.
2. A ring over a subring, under left multiplication.
3. Abelian groups are $\mathbb{Z}$-modules. We have to define scalar multiplication. The obvious choice is:

$$n \cdot x = \begin{cases} 0 & n = 0 \\ \underbrace{x + \cdots + x}_{n \text{ times}} & n > 0 \\ \underbrace{-x \cdots - x}_{-n \text{ times}} & n < 0 \end{cases}$$

   Ex. Check that the axioms for a $\mathbb{Z}$-module hold in this example.

4. Let $V =$ a vector space over a field $\mathbb{F}$, and fix $A \in L(V)$. Consider the polynomial ring $\mathbb{F}(X)$. We make $(V, +)$ into an $\mathbb{F}(X)$-module by defining $p \cdot v = p(A)(v)$ for $p \in \mathbb{F}[A]$.

   Ex. Check that the axioms for a module hold in this example.

   We shall call V as $\mathbb{F}[X]$-module via A. This is *one of the most important examples* of this course. It will link the understanding of modules with linear algebra.

Ex. 8. Is it possible to make $\mathbb{Z}$ into a $\mathbb{Z}_n$-module?

Main Philosophical Question: How much of the theory of vector spaces can be recovered for modules?

We start with a simple example that illustrates how elementary results for vector spaces need not be available for modules.

Example 9. Let $M = \mathbb{Z}_n$ viewed as a $\mathbb{Z}$-module. Consider any non-zero $x \in M$. Then we have $n \cdot x = 0$ even though n is a non-zero scalar. Thus we do not have any non-empty linearly independent subsets of M. In particular, $\{1\}$ is a spanning set but not a basis.

In the example we have used the usual definitions from vector spaces of "span" and "basis". We will look at these more closely later.

Submodules and Quotient Modules

Definition 10. An *R-submodule* M' of an R-module M is a subgroup of M (with respect to $+$) which is closed under scalar multiplication with R. It is then an R-module in its own right.

Ex. 11. If $M' \subset M$ is closed under addition and scalar multiplication, it is a submodule of M.

Example 12. Some submodules:

1. Vector subspaces.
2. If M is an R-module then $\{0\}$ and M are obviously submodules.
3. Let R be a ring, viewed as a module over itself under left multiplication. Then the R-submodules are the left ideals of R.
4. $G =$ an abelian group viewed as a $\mathbb{Z}$-module. Then the $\mathbb{Z}$-submodules of G are all its subgroups.

Ex. 13. Find the $\mathbb{Z}$-submodules of $\mathbb{Z}$ and $\mathbb{Z}_n$.

Ex. 14. Let V be a vector space over $\mathbb{F}$, viewed as an $\mathbb{F}[X]$-module via $A \in L(V)$. Identify the $\mathbb{F}[X]$-submodules of V.

Ex. 15. Consider $\mathbb{R}^2$ as an $\mathbb{R}[X]$-module via A, where A is given by the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Find the $\mathbb{R}[X]$-submodules of $\mathbb{R}^2$.

Definition 16. Let M be an R-module and $X \subset M$. By the submodule *generated* or *spanned* by X we mean the smallest submodule of M that contains X. We denote it by $\langle X \rangle$ or RX.

Ex. 17. Show that

$$\begin{aligned} \langle X \rangle &= \left\{ \sum_{i=1}^{n} \alpha_i \cdot x_i \mid \alpha_i \in R, x_i \in X, n \in \mathbb{N} \right\} \\ &= \bigcap \left\{ M' \mid M' \text{ is a submodule of } M \text{ that contains } X \right\}. \end{aligned}$$

Definition 18. Let M' be a submodule of an R-module M. Then the quotient group M/M' becomes an R-module with the scalar multiplication

$$\alpha \cdot (x + M') = (\alpha \cdot x) + M'.$$

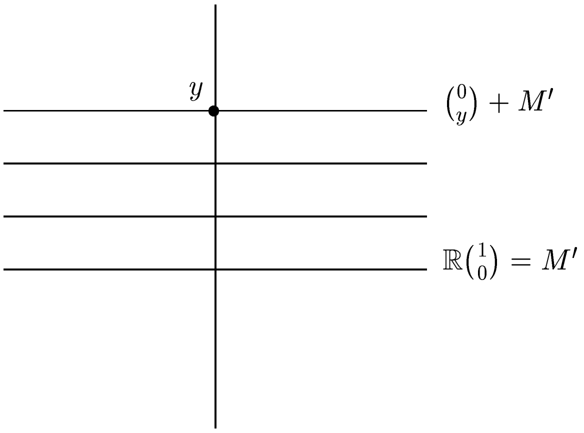
Ex. 19. Check that M/M' satisfies the axioms for an R-module.

Example 20. Some quotient modules:

1. If V' is a vector subspace of V, then V/V' is called the *quotient vector space.*

2. If $G =$ abelian group, the quotient $\mathbb{Z}$-submodules of G are just all its quotient groups.

3. Consider again $M = \mathbb{R}^2$ as an $\mathbb{R}[X]$-module via A, where $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then the only non-trivial submodule is $M' = \mathbb{R}\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. The quotient submodule M/M' consists of all the horizontal lines.



The action of A on any horizontal line is:

$$
\begin{aligned}
A \cdot \begin{pmatrix} 0 \\ y \end{pmatrix} + M' &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ y \end{pmatrix} + M' = \begin{pmatrix} y \\ y \end{pmatrix} + M' \\
&= \begin{pmatrix} 0 \\ y \end{pmatrix} + M'
\end{aligned}
$$

Thus for every coset $[m]$ we have $A \cdot [m] = [m]$. So M/M' can be viewed as $\mathbb{R}$ with the $\mathbb{R}[X]$-action given by

$$p \cdot x = p(1)x, \qquad p \in \mathbb{R}[X].$$

Direct Product and Sum

Definition 21. Let $(M_i)_{i \in I}$ be a collection of R-modules, for a fixed ring R. Consider the cartesian product $\prod_{i \in I} M_i$. It becomes an R-module under the componentwise operations.

Definition 22. Let $(M_i)_{i \in I}$ be a collection of R-modules, for a fixed ring R. Then each M_i sits inside $\prod_{i \in I} M_i$ in an obvious way as the tuples $(x_j)_{j \in I}$ where $x_j = 0 \; \forall \; j \neq i$. By $\bigoplus_{i \in I} M_i$ we mean the submodule of $\prod_i M_i$ generated by all the M_i's.

Ex. 23. Show $\bigoplus_{i\in I} M_i = \left\{ (x_i) \in \prod_i M_i \;\middle|\; \begin{array}{l}\text{all but finitely}\\ \text{many } x_i \text{ are zero}\end{array} \right\}$.

Consequently, the direct sum and product are equal exactly when the index set is finite.

Notation. If I has finite size n, we write $M_1 \times M_2 \times \ldots \times M_n$ or $M_1 \bigoplus M_2 \bigoplus \ldots \bigoplus M_n$ for the direct product or sum. If each $M_i = M$ we denote the result by M^n.

Homomorphisms

We give the analog of "linear map" for modules.

Definition 24. Let R be a ring and M, N be R-modules. A map $\phi : M \to N$ is a *homomorphism of R-modules* or an *R-homomorphism* if it preserves the module structure:

1. $\phi(x) + \phi(y) = \phi(x + y)\ \forall x, y \in M$
2. $\alpha \cdot \phi(x) = \phi(\alpha \cdot x)\ \forall x \in M,\ \forall \alpha \in R$

An immediate consequence is that $\phi(0) = 0$.

Notation. $\operatorname{Hom}_R(M, N)$ = All R-homomorphisms from M into N.
$\operatorname{End}_R(M) = \operatorname{Hom}_R(M, M)$. The members of $\operatorname{End}_R(M)$ are called *endomorphisms.*

Ex. 25. $\operatorname{End}_R(M)$ is a ring and M is an $\operatorname{End}_R(M)$-module.

Example 26.
1. $0 \in \operatorname{Hom}_R(M, N)$, $I \in \operatorname{End}_R(M)$.
2. If $\alpha \in R$ then $\alpha I \in \operatorname{End}_R(M)$ if and only if α commutes with every element of R.
3. If N is a submodule of M, then $I|_N \in \operatorname{Hom}_R(N, M)$.
4. If N is a submodule of M, then the canonical projection $p : M \to M/N$ is an R-homomorphism.
5. Linear maps among vector spaces.
6. Group homomorphisms among abelian groups.

Ex. 27. List the members of $\operatorname{End}_{\mathbb{Z}}(\mathbb{Z})$ and $\operatorname{End}_{\mathbb{Z}}(\mathbb{Z}_n)$.

Ex. 28. Let V be a vector space over $\mathbb{F}$, viewed as $\mathbb{F}[X]$-module via $A \in L(V)$. Characterize the members of $\operatorname{End}_{\mathbb{F}[X]}(V)$.

Ex. 29. Apply the above to $V = \mathbb{R}^2$, $\mathbb{F} = \mathbb{R}$, and $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Ex. 30. The above shows $\mathbb{F}[A] \subset \text{End}_{\mathbb{F}[X]}(V)$. When will we have equality : always, never, sometimes ?

This raises the following problem in linear algebra : Given matrices A and B such that $AB = BA$, is it necessary that B is a polynomial in A? When is it necessary? We will return to this issue later.

Isomorphism Theorems

Definition 31. An R-homomorphism is an *isomorphism* if it is a bijection.

Ex. 32. If $\phi \in \text{Hom}_R(M, N)$ is an isomorphism then ϕ^{-1} is an isomorphism.

Notation. If there is an isomorphism $\phi : M \to N$ of R-modules we say M, N are *isomorphic* and we write $M \simeq N$.

Definition 33. Let $\phi \in \text{Hom}_R(M, N)$. Then we write

Kernel $= \ker\phi = \{x \in M : \phi(x) = 0\}$

Image $= \text{im}\phi = \{\phi(\text{x}) : \text{x} \in \text{M}\}$

Ex. 34. The spaces $\ker\phi, \text{im}\phi$ are submodules of M, N respectively.

Ex. 35. An R-homomorphism ϕ is one-one if and only if $\ker\phi = \{0\}$.

The following results are obvious adaptations of the corresponding statements in group theory. Their standard proofs are left to the student.

Theorem 36 (Mapping Theorem). *Let $\phi \in \text{End}_R(M, N)$. Let M' be a submodule of M such that $M' \subseteq \ker\phi$. Then there is a unique R-homomorphism $\tilde{\phi} : M/M' \to N$ such that $\tilde{\phi} \circ p = \phi$ (here $p : M \to M/M'$ is the canonical projection).*

Theorem 37 (First Isomorphism Theorem). *Let M, N be R-modules and $\phi : M \to N$ an R-homomorphism. Then $M/\ker\phi \simeq \text{im}\,\phi$.*

Corollary 38. $(M_1 \bigoplus M_2)/M_1 \simeq M_2$.

Theorem 39 (Second Isomorphism Theorem). *Let M_1, M_2 be submodules of M. Then*

$$M_1/(M_1 \cap M_2) \simeq (M_1 + M_2)/M_2.$$

Theorem 40 (Third Isomorphism Theorem). *If N' is a submodule of M containing N, then*

$$(M/N)/(N'/N) \simeq M/N'.$$

Theorem 41 (Fourth Isomorphism Theorem). *Let N be a submodule of M. There is a bijection :*

$$\{\textit{submodules of } M \textit{ containing } N\} \leftrightarrow \{\textit{submodules of } M/N\}$$

$$A \mapsto A/N$$

Internal Direct Sum

Let M be an R-module and $(M_i)_{i \in I}$ a collection of its submodules. By $\sum\limits_i M_i$ we denote the submodule generated by $\bigcup\limits_i M_i$, i.e. the set of finite linear combinations

$$\sum_i \alpha_i \cdot x_i \qquad (\alpha_i \in R, x_i \in M_i).$$

Considering each M_i as an R-module in its own right we also get the direct sum $\bigoplus\limits_i M_i$. There is an obvious surjective R-homomorphism

$$\begin{aligned} \pi : \bigoplus_i M_i &\to \sum_i M_i \\ (x_i) &\longmapsto \sum_i x_i \end{aligned}$$

If π is injective, we call $\sum\limits_i M_i$ an *internal direct sum* and call the (M_i) *independent*.

Ex. 42. The collection (M_i) is independent if and only if

$$\sum x_i = 0, x_i \in M_i \Rightarrow x_i = 0 \ \forall i.$$

Ex. 43. Let M_i be submodules of M, $i = 1, \ldots, n$. Then M is the internal direct sum of the M_i if and only if every $x \in M$ can be uniquely written as $x = x_1 + \cdots + x_n$ with $x_i \in M_i$.

Ex. 44. Let M_1, M_2 be submodules of M. They are independent if and only if $M_1 \cap M_2 = \{0\}$. What is the condition for *three* submodules being independent?

2 Classes of Modules

Topics: modules which are simple, semisimple, free, finitely generated, over commutative rings, or Noetherian; generators and relations.

We start considering particular *types* of modules, i.e. we put natural restrictions on M or R and consider the consequences. The following facts often aid insight :

1. The $\mathbb{Z}$-submodules of $\mathbb{Z}$ are $m\mathbb{Z}$ $(m \in \mathbb{Z})$.
2. The $\mathbb{Z}$-submodules of $\mathbb{Z}_n$ are isomorphic copies of $\mathbb{Z}_k$, and exist for each $k|n$.

Simple and Semisimple Modules

Definition 45. A module M is *simple* if $\{0\}$ and M are its only submodules.

One hope would be to analyze a given module by breaking it down to a direct sum of simple modules.

Example 46. 1. A vector space is simple if and only if it is one dimensional.

2. The only simple abelian groups are $\mathbb{Z}_p$, where p is prime.

3. Let V = vector space over $\mathbb{F}$, fix $A \in L(V)$, consider V as an $\mathbb{F}[X]$-module via A. Then V is simple if it has no A-invariant subspaces except $\{0\}$ and V.

   Example $V = \mathbb{R}^2$, $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

   Ex. $V = \mathbb{C}^n$, $A \in L(V)$. Then V is simple $\Leftrightarrow n = 1$.

Ex. 47. Let $\phi \in \operatorname{Hom}_R(M, N)$ and suppose M, N are simple. What can we say about $\ker \phi$ and $\operatorname{im} \phi$?

Theorem 48 (Schur's Lemma). *If M is a simple R-module then* $\operatorname{End}_R(M)$ *is a division ring (every non-zero element has an inverse).*

Definition 49. A module M is called *semisimple* if it is a finite direct sum of simple modules.

Ex. 50. When is a vector space semisimple?

Ex. 51. $\mathbb{Z}$ is *not* semisimple.

Ex. 52. $\mathbb{Z}_n$ is semisimple if and only if n = product of distinct primes. ($\mathbb{Z}_n = \mathbb{Z}_r \bigoplus \mathbb{Z}_s$ if and only if $rs = n$ and $(r, s) = 1$.)

Ex. 53. V = finite dimensional vector space over $\mathbb{C}$, $A \in L(V)$. Then V is a semisimple $\mathbb{C}[A]$-module if and only if A is diagonalizable.

Ex. 54. Let M be a semisimple module. Then every submodule of M has a complementary submodule : If M' is a submodule of M then there is another submodule M'' of M such that $M = M' \bigoplus M''$.

Question: Can we expect the converse to the exercise ?

Possible hurdle: If we go through an inductive process of successive decompositions into smaller submodules, why should the process terminate? We won't go further into this topic.

Free Modules

One key property of vector spaces is the presence of bases.

Definition 55. Let M be an R-module and $X = \{x_1, \dots, x_n\} \subset M$. We say X is *linearly dependent* if there are scalars $\alpha_1, \dots, \alpha_i \in R$, not all zero, such that $\alpha_1 x_1 + \cdots + \alpha_n x_n = 0$. Else we say X is *linearly independent*.

Definition 56. A subset X of an R-module M is *linearly independent* if it has no finite linearly dependent subsets, i.e.,

$$\sum_{i=1}^{n} \alpha_i \cdot x_i = 0,\ \alpha_i \in R, x_i \in X \quad \Rightarrow \quad \alpha_i = 0\ \forall i.$$

Definition 57. $X \subset M$ *spans* or *generates* M if $\langle X \rangle = M$.

Definition 58. $X \subset M$ is a *basis* if it spans M and is linearly independent.

Example 59. $\mathbb{Z}_n$ has no basis (although $\{1\}$ is a spanning subset).

Definition 60. M is a *free* R-module if it has a basis.

Theorem 61. *Let M be an R-module. Then M is free if and only if $M \simeq \bigoplus_{i \in I} R$ for some index set I.*

Proof. Let $\{e_i : i \in I\}$ be the standard basis of $\bigoplus_{i \in I} R$:

$$e_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

($\Rightarrow$) Let $\{f_i\}_{i \in I}$ be a basis of M. Define $\phi : M \to \bigoplus_{i \in I} R$ by $\phi(f_i) = e_i$.

($\Leftarrow$) Suppose $\phi : M \to \bigoplus_{i \in I} R$ is an R-isomorphism. Define $f_i = \phi^{-1}(e_i)$.

$\square$

Theorem 62. *Every R-module is isomorphic to a quotient of a free R-module.*

Proof. Let $X = \{x_i : i \in I\}$ be a generating set for M (e.g. $X = M$). Define a map $\bigoplus_{i \in I} R \to M$ by $(\alpha_i)_{i \in I} \longmapsto \sum_i \alpha_i \cdot x_i$. $\square$

Ex. 63. Is every R-module isomorphic to a submodule of a free R-module?

Note that :

$$\begin{array}{lcll} \text{simple} & \Rightarrow & \text{semisimple} & \multirow{2}{*}{} \\ \text{semisimple} & \not\Rightarrow & \text{simple} & \end{array} \Big\} \text{ trivially}$$

$$\begin{array}{lcll} \text{simple} & \not\Rightarrow & \text{free} & (\mathbb{Z}_p,\ p \text{ prime}) \\ \text{free} & \not\Rightarrow & \text{semisimple} & (\mathbb{Z}) \end{array}$$

Warning. A general free module is still not as nice as a vector space:

1. A linearly independent set may not extend to a basis: $M = \mathbb{Z}$, $X = \{2\}$.
2. A spanning set need not contain a basis: $M = \mathbb{Z}$, $X = \{2, 3\}$.

Finitely Generated Modules

For vector spaces, a natural restriction is to restrict to the case of finite basis.

Definition 64. A module M is *finitely generated* (FG for short) if it has a finite subset X such that $\langle X \rangle = M$.

Ex. 65. Every FG module is a quotient of a FG free module.

Theorem 66. *M is a finitely generated free R-module if and only if*

$$M \simeq R^n = \underbrace{R \oplus \cdots \oplus R}_{n}$$

for some finite n.

Proof. ($\Leftarrow$) Obviously the standard basis is a finite generating set.

($\Rightarrow$) We have to show M has a finite basis. We do know it has a finite generating subset $(f_i)_{i=1}^n$ and a basis $(e_\alpha)_{\alpha \in I}$. Then each f_i is expanded in a finite sum

$$f_i = \sum r_{\alpha i} \cdot e_{\alpha_i}.$$

The e_{α_i} that show up in these equations are linearly independent, span M, and finitely many. Hence they form a finite basis of M. □

Definition 67. If M is a FG free R-module, we define $\mathrm{Rank}_R(M)$ = smallest size of its bases.

Natural Question: Is every basis of a FG free module of the same size? An equivalent question is whether $\mathrm{Rank}_R(R^n) = n$ always. What is obvious is that $\mathrm{Rank}_R(R^n) \le n$.

Counter-Example. Consider $V = \mathbb{R}^\infty = \bigoplus_{i=1}^{\infty} \mathbb{R}$ as a vector space over $\mathbb{R}$. Let $E = L(V)$. We can view the ring E as $\infty \times \infty$ matrices in which each column has finitely many non-zero entries. Then composition in E corresponds to matrix multiplication. Let $E^1 = E$ as an E-module.

Let $\{v_n\}$ = standard basis of $\mathbb{R}^\infty$. Define $T, T' \in E$ by:

$$T \;:\; \begin{cases} v_{2n} & \longmapsto \; v_n \\ v_{2n-1} & \longmapsto \; 0 \end{cases}$$

$$T' \;:\; \begin{cases} v_{2n} & \longmapsto \; 0 \\ v_{2n-1} & \longmapsto \; v_n \end{cases}$$

These maps are represented by the following matrices:

$$[T] = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}, \qquad [T'] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Consider any linear combination in E^1 involving T, T':

$$\begin{aligned} [AT + BT'] &= [A][T] + [B][T'] \\ &= \begin{bmatrix} 0 & a_{11} & 0 & a_{12} & \cdots \\ 0 & a_{21} & 0 & a_{22} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix} + \begin{bmatrix} b_{11} & 0 & b_{12} & 0 & \cdots \\ b_{21} & 0 & b_{22} & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}. \end{aligned}$$

So it is clear that T, T' are a basis for E. Hence $E^1 \simeq E^2 \simeq E^3 \simeq \ldots$ Thus all the E^n $(n \in \mathbb{N})$ are isomorphic, and their common rank is one!

Why is theory for general R^n so different from the familiar one for $\mathbb{R}^n$ or $\mathbb{C}^n$? One problem is that for a non-commutative R there are the following technical hurdles.

1. Left multiplication by a scalar or a matrix is not a linear map.
2. Determinant is not available.

Both hurdles vanish when R is commutative.

Modules Over Commutative Rings

Example 68. Suppose R is a commutative ring, viewed as a module over itself, and $\alpha \neq \beta$ are non-zero members of R. Then $\{\alpha, \beta\}$ is linearly dependent : $\alpha \cdot \beta - \beta \cdot \alpha = 0$, hence every basis has size one. (A counter example like the previous one for $\text{Rank}_R(R^n) = n$ can't be constructed).

Let us consider the notion of determinant. Fix a commutative ring R.

Definition 69. $M_n(R) = n \times n$ matrices with entries from R.

Definition 70. A function $\det : M_n(R) \to R$ is called *determinant* if

1. det is linear in each column.
2. If A has two equal columns then $\det A = 0$
3. $\det I = 1$.

Lemma 71. *1.* det *is alternating in the columns. If we switch two columns,* det *changes by a* -1 *factor.*

2. det *is given by the following formula:*

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma 1,1} a_{\sigma 2,2} \cdots a_{\sigma n,n}$$

(In particular, det *exists !)*

3. $\det(AB) = \det A \cdot \det B$

4. $A \in M_n(R)$ *is invertible if and only if* $\det A$ *is a unit in* R. A^{-1} *is then given as usual by* $A^{-1} = (\det A)^{-1} \operatorname{Adj}(A)$, *where* $\operatorname{Adj}(A)$ *is the transpose of the cofactor matrix of* A.

Proof. The standard proofs from linear algebra require only a commutative ring! □

Ex. 72. $A \in M_n(\mathbb{Z})$ has an inverse in $M_n(\mathbb{Z})$ if and only if $\det A = \pm 1$.

Theorem 73. *Let* R *be a commutative ring, and* $m \in \mathbb{N}$. *Then* $\operatorname{Rank}_R(R^m) = m$.

Proof. If R^m has a basis with size $n < m$, we get an isomorphism $\phi : R^m \to R^n$, given by an $n \times m$ matrix A. While $\phi^{-1} : R^n \to R^m$ is given by an $m \times n$ matrix B. Then we have $BA = I_{m \times m}$ and $AB = I_{n \times n}$. Increase A, B to $m \times m$ matrices :

$$A_1 = \begin{bmatrix} A \\ 0 \end{bmatrix}, \qquad B_1 = \begin{bmatrix} B & 0 \end{bmatrix}.$$

Then $B_1 A_1 = BA = I_m$ is invertible. But $\det(B_1 A_1) = \det B_1 \cdot \det A_1 = 0!$.
Similarly, we can rule out $n < m$. □

Ex. 74. Let M be a free FG module over a commutative ring R. Then every basis of M has the same size.

So it would be natural to impose the following restriction: R is commutative. On the one hand this is a very strong restriction. On the other, it is not strong enough.

Example 75. Consider the commutative ring $R = \mathbb{R}[x_1, x_2, x_3, \dots]$ with infinitely many indeterminates. Then the ideal $\langle x_1, x_2, \dots \rangle$ is not finitely generated as an R-module. Thus a FG free module over a commutative ring may have a submodule which is not finitely generated !

This motivates the following discussion.

Noetherian Modules

Let R be an arbitrary ring, possibly non-commutative.

Definition 76. An R-module M is *Noetherian* if every submodule is finitely generated.

Theorem 77. *An R-module M is Noetherian if and only if every ascending chain of submodules terminates (Thus if M_i are submodules of M such that $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ then $\exists\, N \in \mathbb{N}$ such that $M_N = M_{N+1} = M_{N+2} = \dots$).*

Proof. ($\Rightarrow$) Consider an ascending chain of submodules (M_i). Define $M' = \bigcup_i M_i$. Let $X = \{x_1, \dots, x_n\}$ be a finite generating subset of M'. Then $\exists\, N$ such that $X \subset M_N$, and hence $M_N = M_{N+1} = \cdots = M'$.

($\Leftarrow$) Conversely, let M' be a submodule of M. Let $0 \neq x_1 \in M'$. If $\langle x_1 \rangle \neq M'$, $\exists\, x_2 \in M' \setminus \langle x_1 \rangle$. Proceeding inductively we get a sequence (x_i) in M' such that

$$\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \langle x_1, x_2, x_3 \rangle \cdots$$

This ascending chain terminates at $N \Rightarrow M' = \langle x_1, \dots, x_N \rangle$. $\square$

Example 78. Some Noetherian modules:

1. Every finite module, e.g. $\mathbb{Z}_n$ as $\mathbb{Z}$-module.
2. $\mathbb{Z}$ as $\mathbb{Z}$-module.

Definition 79. A ring R is *Noetherian* if it is Noetherian as an R-module under left multiplication (i.e. every left ideal is finitely generated).

Example 80. Every PID (Principal Ideal Domain) is a Noetherian ring.

Ex. 81. Let M be a Noetherian module and M' a submodule of M. Then M' and M/M' are Noetherian.

Theorem 82. *Let M be a module and M' a submodule. Then M is Noetherian $\Leftrightarrow$ M' and M/M' are Noetherian.*

Proof. ($\Rightarrow$) Previous exercise. ($\Leftarrow$) Let (M_i) be an ascending chain of submodules of M. Let p be the projection map $M \to M/M'$. Then

(a) $p(M_i)$ is an ascending chain in M/M'.

(b) $M' \cap M_i$ is an ascending chain in M'.

Hence $\exists\, N$ such that $p(M_N) = p(M_{N+1}) = \dots$ and $M' \cap M_N = M' \cap M_{N+1} = \dots$

Now let $r \geq N$ and $x \in M_r$. $\exists\, y \in M_N$ such that $p(x) = p(y)$, i.e., $x - y \in M'$. In fact we have $x - y \in M' \cap M_r = M' \cap M_N \Rightarrow x \in M_N$. Hence $M_N = M_{N+1} = \dots = M_r = \dots$. $\square$

Ex. 83. Try to prove the above theorem from the original definition of a Noetherian module.

Ex. 84. 1. $M_1, \ldots, M_n$ are Noetherian R-modules $\Rightarrow M_1 \bigoplus \ldots \bigoplus M_n$ is Noetherian.

2. M is FG R-module and R is Noetherian $\Rightarrow M$ is Noetherian.

In particular, every finitely generated module over a PID is Noetherian. We will make a special study of such modules.

Generators and Relations

Let M be a FG R-module over a Noetherian ring R. Then we have an onto homomorphism $f : R^m \longrightarrow M$, so that $M \simeq R^n / \ker f$. Now $\ker f$ is itself finitely generated and hence we also have an onto homomorphism $g : R^m \longrightarrow \ker f$. By composing with inclusion we get a homomorphism $\phi : \mathbb{R}^m \to R^n$ such that

$$M \simeq R^n / \ker f = R^n / \operatorname{im} \phi = \mathrm{R}^\mathrm{n} / \phi \mathrm{R}^\mathrm{m}.$$

If R is commutative, then ϕ is left multiplication by an $n \times n$ matrix A, which is called a *presentation matrix* of M. It represents the linear relations which exist among the chosen generators of M.

Example 85. Suppose M is a $\mathbb{Z}$-module with generators (v_1, v_2, v_3) that satisfy the linear relations:

$$\begin{aligned} 3v_1 + 2v_2 + v_3 &= 0 \\ 8v_1 + 4v_2 + 2v_3 &= 0 \\ 7v_1 + 6v_2 + 2v_3 &= 0 \\ 9v_1 + 6v_2 + v_3 &= 0 \end{aligned}$$

Then we first get a map $f : \mathbb{Z}^3 \to M$ with kernel $\langle (3,2,1), (8,4,2), (7,6,2), (9,6,1) \rangle$. The kernel has 4 generators, hence is given by a map $g : \mathbb{Z}^4 \to \ker f$, in fact by the matrix

$$A = \begin{pmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{pmatrix}.$$

Theorem 86. *Let A be an $n \times m$ presentation matrix for a Noetherian module M over a commutative ring R. The following A' represent the same module M (upto isomorphism of course).*

1. *$A' = PAQ, P_{n\times n}, Q_{m\times m}$ are invertible.*
2. *A' obtained by deleting a column of zeros from A.*
3. *The j^{th} column of A is e_i, and A' is obtained by deleting the j^{th} column and i^{th} row of A.*

Proof. Exercise! Try to interpret the changes in terms of the generators and relations. $\square$

Ex. 87. Show the $\mathbb{Z}$-module of the previous example is isomorphic to $\mathbb{Z}_4$.

Ex. 88. We know $\mathbb{Z}_2 \bigoplus \mathbb{Z}_3 \simeq \mathbb{Z}_6$. Find how to move the presentation matrix $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$ to $\begin{bmatrix} 6 \end{bmatrix}$. Similarly move $\begin{bmatrix} 6 & 0 \\ 0 & 16 \end{bmatrix}$ (over $\mathbb{Z}$) to $\begin{bmatrix} 2 & 0 \\ 0 & 48 \end{bmatrix}$. (Using the "moves" of Theorem 86.)

Ex. 89. Find a general procedure for transforming $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ (over $\mathbb{Z}$) to $\begin{bmatrix} HCF(a,b) & 0 \\ 0 & LCM(a,b) \end{bmatrix}$, using the moves of Theorem 86.

Exercises from [Artin]:

1. Suppose R is a commutative ring and M is a Noetherian R-module. Let A be a presentation matrix of M via generators $(v_1, \ldots, v_m)$. Let $(w_1, \ldots, w_m)$ be another set of elements of M. A presentation matrix of M with the generating set $(v_1, \ldots, v_n; w_1, \ldots, w_m)$ is
$$\left[\begin{array}{c|c} P & -P \\ \hline 0 & I \end{array}\right],$$
where P is given by $w_i = \sum_j p_{ij} v_j$.

2. In the above situation suppose the (w_i) are also a generating set with presentation matrix B. Then we get a matrix Q defined by $v_i = \sum_j q_{ij} w_j$. Another presentation matrix of M with generators $(v_1, \ldots, v_n; w_1, \ldots, w_m)$ is
$$T = \left[\begin{array}{c|c|c|c} A & -P & I & 0 \\ \hline 0 & I & -Q & B \end{array}\right]$$
Show T reduces to both A and B by the moves of Theorem 86.

3. Any two presentation matrices of the same M can be transformed into each other via the moves of Theorem 86 and their inverses.

3 Modules Over PIDs

Topics: finitely generated module over a PID, Smith Normal Form, invariant factors, elementary divisors.

We quickly recall the basic facts about PIDs.

Definition 90. A ring R is an *integral domain* if

1. It is commutative.

2. It has no "zero divisors" : $\alpha\beta = 0 \Rightarrow \alpha = 0$ or $\beta = 0$.

Ex. 91. Give some examples which are integral domains and some which are not.

Definition 92. A ring R is *principal* if every left ideal has a singleton generating set. ("Every left ideal is principal".)

Ex. 93. Give some examples.

Definition 94. A *principal ideal domain* (PID) is a ring which is principal and an integral domain.

Ex. 95. The generator of an ideal in a PID is unique upto units.

Example 96. 1. Fields.

2. $\mathbb{F}[X]$, where $\mathbb{F}$ is a field.

3. $\mathbb{Z}$

There are two aspects of PIDs which will be essential for us. First we recall that for $a, b \in R$ we say $a|b$ ("a divides b") if $\exists\ c \in R$ such that $b = ac$. Also, a *unit* in R is an element with a multiplicative inverse.

Let R be a PID.

Existence of HCF (or GCD).

Let $a, b \in R$ and consider the ideal $\langle a, b \rangle$. Then it is generated by some member d : $\langle\, d\,\rangle = \langle a, b \rangle$. This means

(1) $d = \alpha a + \beta b$ (for some $\alpha, \beta \in R$)

(2) $d|a$ and $d|b$

From (1) and (2) it follows that if $x|a$ and $x|b$ then $x|d$. Thus we can call d a Highest Common Factor (HCF) or Greatest Common Denominator (GCD) of a, b. We use the notation $d = (a, b)$.

Ex. 97. Is d uniquely determined by a, b?

Ex. 98. Show that HCF exists for any $a_1, \ldots, a_n \in R$ and is a linear combination of them.

Ex. 99. Show the Least Common Multiple (LCM) exists (define it first!) and find a formula for it.

Notion of Length.

Definition 100. An element of R is *irreducible* (or an *atom*) if it is a non-unit that can't be written as the product of two non-units.

Recall: Every PID is a UFD : Every non-unit in a PID can be expressed as a product of some atoms, and the factors are unique upto rearrangement and multiplication by units.

Thus every member of a PID has a *length* defined to be the number of atoms in its factorization. The length of a unit is zero.

Finitely Generated Modules Over PIDs

Theorem 101. *If R is a PID then every submodule of $R^n (n \in \mathbb{N})$ is free, with rank $\leq n$.*

Proof. (It helps to draw a picture for subspaces of $\mathbb{R}^2$ or $\mathbb{R}^3$ and to see how the proof is proceeding there.) We proceed by induction on n. The truth of the assertion for $n = 1$ is immediate. Now let M be a submodule of R^n, $n > 1$. We write

$p_i : R^n \to R$ (projection onto i-th coordinate)

$e_i : M \to R$ ($e_i = p_i|M$)

If $e_1 = 0$ then $M \subseteq \ker p_1 = R^{n-1}$, so we are done. Therefore suppose $e_1 \neq 0$. Then $e_1(M)$ is an ideal of R, and hence $e_1(M) = \langle \alpha \rangle$ for some $0 \neq \alpha \in R$. Choose $x \in M$ such that $e_1(x) = \alpha$.

Exercise. $M = Rx \bigoplus \ker e_1$.

Exercise. Rx is free with basis $\{x\}$.

Now, by induction hypothesis, $\ker e_1 \subset R^{n-1}$ is free with rank $\leq n - 1$. Hence M is free with rank $\leq n$. ☐

Note. A *proper* submodule of R^n may have rank n.

Corollary 102. *Every finitely generated module over a PID R is isomorphic to R^n/R^m for some $m \leq n$.*

Corollary 103. *Let M be a finitely generated module over a PID R, with n generators. Then every submodule of M can be generated by $\leq n$ elements.*

Proof. Apply third isomorphism theorem to $R^n/R^m \simeq M$. ☐

Smith Normal Form

Here we try to carry out as much as possible of Gauss elimination to put a matrix in echelon form. The unavailability of division in general is compensated for by the existence of HCF.

Let us consider an $m \times n$ matrix A with entries from a PID R.

Ex. 104. Show that by multiplication with an invertible matrix from the left, we can perform the following row operations on A :

(1) Switching two rows.

(2) Adding a multiple of one row to another.

(3) Multiplying a row by a unit in R.

Ex. 105. What is missing here, compared to the row operations available for Gaussian elimination over $\mathbb{R}$ or $\mathbb{C}$?

We also have the following operation, which is not needed for Gaussian elimination over a field (and here compensates for the lack referred to in the above exercise).

(4) Alter two rows such that the first elements are replaced by their HCF and O respectively.

Ex. 106. Find the matrix which accomplishes the row operation (4).

Similarly, we can perform the corresponding column operations by multiplying with invertible matrices from the right. We use the same numbers (1) to (4) to identify them.

Ex. 107. Reduce the following matrix (over $\mathbb{Z}$) as much as you can :

$$\begin{bmatrix} 6 & 12 & 8 \\ 9 & 10 & 1 \\ 5 & 0 & 1 \end{bmatrix}$$

Theorem 108. *Let A be an $m \times n$ matrix with entries in a PID R. Then there are invertible $m \times m$ and $n \times n$ matrices P, Q with entries in R such that*

$$PAQ = \begin{bmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

with $d_i | d_{i+1}$ $(1 \leq i \leq r-1)$. *This is called the* Smith Normal Form *or* PAQ Reduction.

Proof. If $A = 0$ there is nothing to be done. Suppose $A \neq 0$. By switching rows and columns we can arrange $a_{11} \neq 0$.

Now if a_{11} divides a_{12} we can use a column operation of type (2) to convert a_{12} to 0. If not we use an operation (4) to replace a_{11} by the HCF (a_{11}, a_{12}) and a_{12} by 0. In this case the length of a_{11} decreases by at least 1. We repeat the process with the new a_{11} and with a_{13}, etc. Finally, we have replaced a_{11} by a factor of it, and all the other a_{1i} have become 0.

Now we attack the first column, using row operations, and proceed in the same way. If we can do it without using (4), we will not alter the first row and will achieve a form

$$\left[\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right] \tag{$*$}$$

If we do use (4) the length of a_{11} will strictly decrease. Now we attack the first row once more. Proceeding in this way, each time reducing the length of a_{11} we must finally reach the form $(*)$. In the "worst" case, a_{11} finally becomes a unit.

Having reduced $(*)$ we apply the process to A' and by induction reach a diagonal form

$$\begin{bmatrix} a_{11} & & & & & \\ & \ddots & & & & \\ & & a_{rr} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}.$$

Now suppose $a_{11} \not| a_{22}$. Observe that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{22} \\ 0 & a_{22} \end{pmatrix} \xrightarrow{(4)} \begin{pmatrix} a'_{11} & 0 \\ 0 & a'_{22} \end{pmatrix}$$

where $a'_{11} = HCF(a_{11}, a_{22})$ has strictly lesser length than a_{11}. Repeat till a_{11} divides a_{22}.

Now we do the process with each a_{ii}. So that finally a_{11} divides each a_{ii}. Then we do this for a_{22} and so on. □

A question that arises is whether the Smith Normal Form is unique. We defer this issue to the next section.

Invariant Factors Decomposition

Let M be a FG R-module, where R is a PID. Then M is Noetherian, and so it is given by a presentation matrix $A_{n\times m} : M \simeq R^n/AR^m$. Additionally we know that $m \leq n$, and that A can be reduced to diagonal form. Putting all this together we get :

Theorem 109. *Let M be a FG R-module, where R is a PID. Then there is an isomorphism of R-modules:*

$$M \simeq R^s \bigoplus \frac{R}{a_1 R} \bigoplus \cdots \bigoplus \frac{R}{a_r R}$$

where the scalars $a_1, \ldots, a_r$ are non-units satisfying $a_i | a_{i+1} (1 \leq i < r)$. Moreover M uniquely determines the numbers r and s, while the a_i are determined upto units.

Proof. We know M has some $n \times m$ presentation matrix A such that $M \simeq R^n / AR^m$. We know that applying the moves of Theorem 86 doesn't change the isomorphism class of M. By Smith Normal Form we can therefore assume that A is a diagonal matrix of the form

$$A = \begin{bmatrix} a_1 & & & & & \\ & \ddots & & & & \\ & & a_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$$

where the a_i are non-units such that $a_i | a_{i+1} (1 \leq i < r)$ and there are s zero rows.

The statement $M \simeq R^s \bigoplus R/a_1 R \bigoplus \ldots \bigoplus R/a_r R$ immediately follows. Uniqueness is the content of [P, Theorem 131]. $\square$

Notation. The scalars $a_1, \ldots, a_r$ are called the *invariant factors* of M. The number s is called the *rank* of M.

Ex. 110. As noted in Corollary 102, a FG module M over a PID is of the form R^n / R^m. Conclude that $n - m$ is independent of the particular presentation of M, and equals its rank as defined above.

Definition 111. Let M be an R-module. We say $x \in M$ is a *torsion element* if $\alpha \cdot x = 0$ for some non-zero $\alpha \in R$. We set $\mathrm{Tor}\,(M) =$ set of torsion elements of M.

Ex. 112. $\mathrm{Tor}\,(M)$ is a submodule of M.

Definition 113. M is a *torsion module* if $M = \mathrm{Tor}\,(M)$. M is *torsion free* if $\mathrm{Tor}\,(M) = \{0\}$.

Ex. 114. In the IF decomposition of an R-module M,

$$\mathrm{Tor}\,(M) \simeq \frac{R}{a_1 R} \bigoplus \cdots \bigoplus \frac{R}{a_n R}.$$

Ex. 115. A FG module M over a PID is free if and only if it is torsion free.

Corollary 116 (Structure Theorem for FG Abelian Groups). *Every finitely generated abelian group is isomorphic to*

$$\mathbb{Z}^s \bigoplus \mathbb{Z}_{a_1} \bigoplus \cdots \bigoplus \mathbb{Z}_{a_r}$$

where $a_i | a_{i+1}$ $(1 \leq i < r)$, and the a_i are uniquely determined by the group.

Elementary Divisors Decomposition

Motivating Example: Suppose one of the terms in the invariant factor decomposition of an abelian group is $\mathbb{Z}_6$. Then we can decompose it further into $\mathbb{Z}_2 \bigoplus \mathbb{Z}_3$. Thus the invariant factor decomposition doesn't give the *smallest* pieces of a module. In this section we see how to methodically get to these smallest pieces.

Ex. 117. Let $n = p_1^{n_1} \dots p_e^{n_3}$ be a decomposition into prime factors. Then

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{n_1}} \bigoplus \dots \bigoplus \mathbb{Z}_{p_e^{n_e}}.$$

So we can further decompose each $\mathbb{Z}_{a_i}$ into prime power factors. Let's try to do this methodically, and in general.

Recall: An element p in a ring R is called **prime** if it is a non-unit and $p|ab \Rightarrow p|a$ or $p|b$. Two primes are **distinct** if they are not unit multiples of each other.

Ex. 118. If R is a PID, then $p \in R$ is prime if and only if it is an atom.

Again, fix a ring R which is a PID.

Definition 119. An R-module M is called *p-primary* if p is a prime in R such that every $x \in M$ satisfies $p^n \cdot x = 0$ for some n.

Definition 120. An R-module M is *primary* if it is p-primary for some prime p.

Example 121. R/p^nR is p-primary.

Theorem 122. *Let M be a torsion module over a PID R. Then*

$$M = \bigoplus M_p$$

where each M_p is a maximal p-primary submodule of M. If M is FG then the direct sum is finite.

Proof. First define $M_p = \{x \in M : p^n \cdot x = 0 \text{ for some } n\}$ for each prime $p \in R$.

Ex. M_p is a maximal p-primary submodule of M.

We check that the M_p's span M. If $x \in M$ then $g_1 \cdots g_\ell \cdot x = 0$ where $g_i = p_i^{n_i}$ and the p_i are distinct primes. Define

$$\begin{aligned} t_1 &= g_2 g_3 \cdots g_\ell \\ t_2 &= g_1 g_3 g_4 \cdots g_\ell \\ &\cdots \\ t_\ell &= g_1 g_2 \cdots g_{\ell-1} \end{aligned}$$

Then the HCF of the t_i is 1 and hence there exist $s_1, \dots, s_\ell$ such that $\sum_{i=1}^{\ell} s_i t_i = 1$. Then

$$x = \sum_i (s_i t_i) x = \sum_i x_i \quad \text{where } x_i = s_i t_i \cdot x.$$

Ex. $x_i \in M_{p_i}$.

Now we check that the M_p are independent. Let $x_i \in M_{p_i}$ such that $\sum_{i=1}^{\ell} x_i = 0$. Let $n_i \in \mathbb{N}$ be smallest such that $p_i^{n_i} \cdot x_i = 0$. Define $\beta = p_1^{n_1 - 1} p_2^{n_2} \cdots p_\ell^{n_\ell}$. Then $0 = \beta \cdot \sum_i x_i = \beta \cdot x_1$. But $(\beta, p_1^{n_1}) = p_1^{n_1 - 1} \Rightarrow \exists\, s, t \in R$ such that $s\beta + t p_1^{n_1} = p_1^{n_1 - 1}$. Hence

$$p_1^{n_1 - 1} \cdot x_1 = (s\beta + t p_1^{n_1}) \cdot x_1 = 0.$$

Therefore $x_1 = 0$. Similarly, each $x_i = 0$.

Finally, suppose that M is FG. If $x_1, \dots, x_n$ are generators of M, there exist $\alpha_1, \dots, \alpha_n \in R$ such that $\alpha_i \cdot x_i = 0\ \forall i$. Define $\beta = \alpha_1 \cdots \alpha_n$. Then β annihilates M. Now if $M_p \neq 0$, $\exists\ x \neq 0$ in M_p such that $px = 0$. If $(p, \beta) = 1$ then $sp + t\beta = 1$ for some s, t. But $(sp + t\beta) \cdot x = 0$. Hence we must have $p|\beta$. So there are only finitely many choices of p that give $M_p \neq 0$. ☐

Definition 123. A module is *cyclic* if it is generated by a single element.

The invariant factor decomposition shows that a FG module over a PID is a direct sum of cyclic submodules. By the above result we can proceed to decompose the cyclic torsion submodules into their primary constituents.

Ex. 124. Fix a PID R. Let M be an R-module.

a M is cyclic and free $\Rightarrow M \simeq R^1$.

b M is cyclic and torsion $\Rightarrow M \simeq R/\alpha R$.

c M is cyclic and p-primary $\Rightarrow M \simeq R/p^n R$ for some n.

d M is cyclic $\Rightarrow$ every quotient of M is cyclic.

e The primary constituents of $R/\alpha R$ are of the form $R/p^n R$ with $p|\alpha$.

Applying these considerations to the invariant factor decomposition, we get the *elementary divisors decomposition*:

Theorem 125. *Let M be a FG module over a PID R. Then*

$$M \simeq R^s \bigoplus_{i,j} \frac{R}{p_i^{\alpha_{ij}} R} \qquad (ED)$$

where $s = \mathrm{Rank}(M)$, the p_i are distinct primes in R, and $0 < \alpha_{i1} \leq \alpha_{i2} \leq \cdots$. Moreover the numbers $p_i^{\alpha_{ij}}$ are uniquely determined by M (upto unit factors) and are called its elementary divisors.

Proof. Only the uniqueness remains to be established. We again refer the reader to the Problem Set [P, Theorem 131]. ☐

Corollary 126. *Every finitely generated abelian group has a decomposition* $\mathbb{Z}^s \bigoplus_{i,j} \mathbb{Z}_{p_i}^{\alpha_{ij}}$ *where the* p_i *are distinct primes,* $0 < \alpha_{i1} \leq \alpha_{i2} \leq \cdots$, *and the* $p_i^{\alpha_{ij}}$ *are uniquely determined by the group.*

Definition 127. Let $x \in M$ be a torsion element. Then the *order* of x is the generator of the ideal $\{r \in R : r \cdot x = 0\}$.

Definition 128. M is *bounded* if $\exists 0 \neq \alpha \in R$ such that $\alpha \cdot M = 0$. The generator of $\{r \in R : r \cdot M = 0\}$ is then called the *bound* of M.

Theorem 129. *A FG module* M *over a PID is bounded if and only if it is a torsion module. Then* M *has an element whose order is the bound of* M.

Proof. The first part is trivial. Now consider the invariant factors decomposition

$$M \simeq \frac{R}{a_1 R} \oplus \cdots \oplus \frac{R}{a_n R}$$

with $a_i | a_{i+1}$. Then the bound of M is a_n. ☐

Theorem 130. *Let* M *be a module over a PID, and* $M = M_1 \bigoplus \ldots \oplus M_r$. *Then* M *is bounded if and only if each* M_i *is bounded. The bound of* M *is the LCM of the bounds of the* M_i.

[Remark : LCM of a, b is ab/HCF]

Proof. Exercise! ☐

4 Jordan and Rational Canonical Forms

We now come full circle – we will apply the general theory we have developed to obtain information about linear maps on vector spaces. Let V be an n-dimensional vector space over a field $\mathbb{F}$. Fix an $A \in L(V)$. Then V becomes a $\mathbb{F}[X]$-module :

$$g \cdot v = g(A)(v), \qquad\qquad g \in \mathbb{F}[X], \; v \in V.$$

Since $\mathbb{F}[X]$ is a PID and V is finitely generated we can apply the results of the previous section.

Ex. 131. Linear polynomials $X - \lambda$ are prime in $\mathbb{F}[X]$.

Consider the members $I, A, A^2, \ldots, A^{n^2}$ of $L(V)$. Since $L(V)$ is a vector space of dimension n^2, they satisfy a linear relation $a_0 I + a_1 A + \ldots + a_{n^2} A^{n^2} = 0$. Define $g \in \mathbb{F}[X]$ by $g(X) = a_0 + a_1 X + \ldots + a_{n^2} X^{n^2}$. Then $g(A) = 0$.

Ex. 132. $I_A = \{p \in \mathbb{F}[X] : p(A) = 0\}$ is a non-zero ideal in $\mathbb{F}[X]$.

Ex. 133. The ideal I_A has a unique monic (coefficient of highest degree term is 1) generator m_A.

Definition 134. We call m_A the *minimal polynomial* of A. Its identifying properties are : m_A is monic, $m_A(A) = 0$, $p \in I_A \Rightarrow m_A | p$.

Ex. 135. $B = PAP^{-1} \Rightarrow m_B = m_A$.

Ex. 136. λ is an eigenvalue of $A \Leftrightarrow (X - \lambda) | m_A$.

Ex. 137. m_A is the bound of V (over $\mathbb{F}[X]$).

Ex. 138. Find the minimal polynomials of the linear maps given by the following matrices (over $\mathbb{R}$):

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Theorem 139. *A is diagonalizable if and only if m_A consists of distinct linear factors.*

Proof. ($\Rightarrow$) Suppose that A can be diagonalized and the distinct diagonal entries are $d_1, \ldots, d_r$. We directly check that $\mu(X) = (X - d_1)\ldots(X - d_r)$ satisfies $\mu(A) = 0$. So we must have $m_A = \mu$.

($\Leftarrow$) Let $m_A = p_1 \ldots p_r$ where $p_i = x - \lambda_i$ are distinct linear factors. Since m_A is the bound of V, we have a decomposition into primary components, (Theorem 122) :

$$V = V_1 \oplus \ldots \oplus V_\ell$$

where V_i is annihilated by the prime factor $X - \lambda_i$. Hence $A|_{V_i} = \lambda_i I$ and the result follows. $\square$

To apply the elementary division decomposition, we have to investigate cyclic modules.

Definition 140. We call A *cyclic* if V is a cyclic $\mathbb{F}[X]$-module via A.

Assume A is cyclic, and let v be a generator of V over $\mathbb{F}[X]$. Define $v_i = A^{i-1}v$ ($i = 1, 2, \ldots$). Then $\exists\, r$ such that $v_1, \ldots, v_r$ are linearly independent but $v_{r+1} = a_1 v_1 + \ldots + a_r v_r$.

Ex. 141. $\mathbb{F}[X] \cdot v = \langle v_1, \ldots, v_r \rangle_{\mathbb{F}}$

Hence we must have $r = n$ and $v, AV, \ldots A^{n-1}v$ as a basis of V. In this basis, we find

$$[A] = \begin{bmatrix} 0 & \cdots & \cdots & 0 & a_1 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-1} \\ 0 & \cdots & 0 & 1 & a_n \end{bmatrix}$$

Ex. 142. $m_A(X) = X^n - a_1 - a_2X - \ldots - a_nX^{n-1}$.

The matrix $[A]$ is called the *companion matrix* of m_A, and we denote it by C_A. It is defined by the above formula for any monic polynomial.

Theorem 143. *A is cyclic if and only if* $\deg m_A = n$.

Proof. ($\Rightarrow$) Done.

($\Leftarrow$) Since m_A is the bound of V, $\exists\, v \in V$ with order m_A (Theorem 129). Then $v, Av, \ldots, A^{n-1}v$ are linearly independent. Hence v generates V. □

Frobenius or Rational Canonical Form

Since V is a torsion module over $\mathbb{F}[X]$, in fact bounded by m_A, we get an invariant factor decomposition

$$V = V_1 \oplus \cdots \oplus V_r$$

where each V_i is cyclic with bound $\mu_i \in \mathbb{F}[X]$, and $\mu_i | \mu_{i+1}$.

Ex. 144. $\mu_i = m_{A|_{V_i}}$, $\mu_r = m_A$.

Ex. 145. Consider $XI - A$ as a member of $M_n(\mathbb{F}[X])$. Then the μ_i are its invariant factors (as in Smith Normal Form).

Since $A|_{V_i}$ is cyclic it is given by the companion matrix of μ_i. Hence we have

Theorem 146 (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*

$$\begin{pmatrix} C_{\mu_1} & & & \\ & C_{\mu_2} & & \\ & & \ddots & \\ & & & C_{\mu_r} \end{pmatrix} \tag{1}$$

where $\mu_1 \mid \cdots \mid \mu_r$ are monic polynomials, and the C_{μ_i} are their companion matrices.

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 ν_j of degree at least one with the divisibility property $\nu_1 \mid \cdots \mid \nu_s$, then $r = s$ and $\nu_i = \mu_i$ for $1 \le i \le r$. □

Definition 147. The matrix in Eq. 1 is called the *rational canonical form* of T.

Jordan Canonical Form

Example 148. Suppose $m_A(X) = (X - \lambda)^n$, with $n = \dim V$. Then V is a cyclic $\mathbb{F}[X]$-module via A. Let v be a generator of V. The vectors $v, (A-\lambda)v, \dots, (A-\lambda)^{n-1}v$ are linearly independent, hence a basis. In this basis, we get

$$[A] = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{bmatrix}, \quad \text{a "Jordan Block".}$$

Now we try out the elementary divisors decomposition for a general A. This requires the use of the prime members of $\mathbb{F}[X]$. So we assume that $\mathbb{F} = \mathbb{C}$ (or that $\mathbb{F}$ is algebraically closed): then the primes in $\mathbb{F}[X]$ are exactly the linear polynomials $X - \lambda$ ($\lambda \in \mathbb{F}$). This simplifies life! (Note, however, that the results will remain true if we assume only that $\mathbb{F}[X]$ contains all the eigenvalues of A.)

Applying the elementary divisors decomposition and noting that V is a torsion module over $\mathbb{F}[X]$, we get:

$$V = \bigoplus_{i=1}^{\ell} \left(\bigoplus_{j=1}^{n_i} V_{ij} \right)$$

where V_{ij} is cyclic and has bound $(X-\lambda_i)^{\alpha_{ij}}$, the λ_i ($1 \le i \le l$) are all distinct, and $0 < \alpha_{i1} \le \alpha_{i2} \ldots \le \alpha_{in_i}$. The first implication of this is that A can be expressed as a block diagonal matrix

$$\begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_\ell \end{bmatrix}$$

where B_i is a square matrix representing $A|_{\bigoplus_j V_{ij}}$. On V_{ij}, A has minimal polynomial $(X-\lambda_i)^{\alpha_{ij}}$. It follows that $A|_{V_{ij}}$ can be made into a Jordan block:

$$A|_{V_{ij}} = J_{ij} = \begin{bmatrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}_{\alpha_{ij} \times \alpha_{ij}}$$

Hence

$$B_i = \begin{bmatrix} J_{i1} & & O \\ & \ddots & \\ O & & J_{in_i} \end{bmatrix}.$$

The net result is the *Jordan Canonical Form* of A.

Ex. 149. Set $m_i = \alpha_{i,n_i} = \max\{\alpha_{ij}\}$. Then $m_A(X) = (X - \lambda_1)^{m_1} \cdots (X - \lambda_\ell)^{m_\ell}$.

Thus we have obtained:

Theorem 150 (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.* □

Calculating the Jordan Canonical Form.

The general theory has given us the existence of Jordan Canonical Form. Now the theory is fairly prescriptive and says what calculations need to be undertaken. The following small example should give a sufficient idea of the process. Consider the following matrix as an operator on $\mathbb{R}^3$:

$$A = \begin{bmatrix} 4 & 2 & -4 \\ 2 & 3 & -3 \\ 3 & 2 & -3 \end{bmatrix}.$$

The first task is to find the eigenvalues of A. Now $\det(XI - A) = 0$ gives $(X-2)(X-1)^2 = 0$. So the Jordan blocks will come from powers of $X - 2$ and $X - 1$.

$$\begin{aligned}
A - 2I &= \begin{bmatrix} 2 & 2 & -4 \\ 2 & 1 & -3 \\ 3 & 2 & -5 \end{bmatrix} \quad \text{has kernel } \langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rangle, \\
A - I &= \begin{bmatrix} 3 & 2 & -4 \\ 2 & 2 & -3 \\ 3 & 2 & -4 \end{bmatrix} \quad \text{has kernel } \langle \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} \rangle, \\
(A - I)^2 &= \begin{bmatrix} 1 & 2 & -2 \\ 1 & 2 & -2 \\ 1 & 2 & -2 \end{bmatrix} \quad \text{has kernel } \langle \begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} \rangle;
\end{aligned}$$

the vector $\begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix}$ being chosen in order that $(A - I)\begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$.

Give $\mathbb{R}^3$ the basis $\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix} \right\}$. Then $[A]_{\mathcal{B}} = \left[\begin{array}{c|cc} 2 & 0 & 0 \\ \hline 0 & 1 & 1 \\ 0 & 0 & 1 \end{array}\right]$.

A Curiosity. Note that the characteristic polynomial c_A of A has been missing from our discussion – we never needed it (except to calculate the eigenvalues in the last example). Now the Jordan Canonical Form shows that m_A divides c_A and hence we have proven the Cayley-Hamilton Theorem : $c_A(A) = 0$.

P Problem Set

In this Problem Set, the main notes are referred to as [M].

Basic Definitions and Examples

> **Topics:** Definitions of modules, submodules, direct sums of modules and submodules, quotient 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. We also assume that $0 \neq 1$!

Definition 1. By an R-module, we shall always mean a left R-module and we always write rx for $r \cdot x$.

Ex. 2. Let M be an additive abelian group. Show that there is only one way of making M a $\mathbb{Z}$-module.

Ex. 3. How will you define a right R-module?

Ex. 4. 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. 5. 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. 6. 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. 7. 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.

Definition 8. Recall that if T is a linear operator on a vector space V then we make V an $\mathbb{F}[X]$-module by $p \cdot v = p(T)(v)$, and call it as $\mathbb{F}[X]$-module via T.

Ex. 9. 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. 10. Keep the notation of Ex. 9. 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. 11. 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. 12. 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. 13. 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. 14. 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. 15. 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. 16. 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. 17. Show that the intersection of any nonempty collection of submodules is again a submodule.

Ex. 18. 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. 19. How do you define $A + B$ if A and B are subsets of a module?

Ex. 20. 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. 21. Let M be generated by x_j, $1 \leq j \leq n$. Show that $M = \{r_1 x_1 + \cdots + r_n x_n : r_j \in R\}$.

Definition 22. An R-module M is 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 $1 \leq j \leq k$. [M, Ex. 43]

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

Ex. 23. 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. 24. 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 $M = \mathbb{R}^2$!

Module Maps

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

Definition 25. Let M and N be two modules over the same ring R. An R-module homomorphism between them will also be called an R-map.

Ex. 26. Let V and W be vector spaces over $\mathbb{F}$. When is a map $f \colon V \to W$ a module homomorphism?

Ex. 27. Let V_i $(i = 1, 2)$ 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. 28. 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. 29. Give an example of a map from one R-module into another which is a group homomorphism but not an R-map.

Ex. 30. 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. 31. 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.

Ex. 32. Let R be commutative. Show that $\mathrm{Hom}_R(R, M) \simeq M$ as R-modules.

Ex. 33. 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. 34. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}) \simeq \mathbb{Q}$ as rings.

Ex. 35. With the notation of Ex. 24, show that $L_2 \simeq M_2$.

Ex. 36. 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. 37. 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. 38 (Chinese Remainder Theorem). If I is any ideal of R, recall the definition of the submodule IM (Ex. 15).

(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

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

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 $i \neq j$. 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.

Finitely Generated Modules

> **Topics:** Annihilator of submodules and ideals, torsion elements and torsion modules, finitely generated modules and cyclic modules.
> Simple and indecomposable modules.

Definition 39. 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. 40. Keep the notation of Def. 8. Is V finitely generated? (Ex. 59 elaborates on this!)

Ex. 41. 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. 42. Show that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.

Ex. 43. An R-module M is cyclic iff $M = Rx$ for some $x \in M$.

Ex. 44. Keep the notation of Def. 8.

(a) Let $T = I$, the identity. When is V cyclic $\mathbb{F}[X]$-module via T?

(b) Let T be the shift operator (Ex. 9). Prove that V is cyclic.

Ex. 45. Which of the modules in Ex. 11 are cyclic?

Ex. 46. Let R be the ring of all functions $f : \mathbb{R} \to \mathbb{R}$. 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. 47. 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 48. 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. 49. Let M be an abelian group considered as a $\mathbb{Z}$-module. What are the torsion elements?

Ex. 50. 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. 51. 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. 52. Show that if R has zero divisors then every nonzero R-module has torsion elements.

Ex. 53. 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. 54. 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. 55. 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. 56. 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. 57. 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. 58. Let R be an integral domain. Prove that $\operatorname{Ann}_R M \neq (0)$ for any finitely generated R-module M.

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

Ex. 59. Consider a vector space V over $\mathbb{F}$ as an $\mathbb{F}[X]$-module via $T \in \operatorname{End}_{\mathbb{F}}(V)$. Show that V is FG and torsion $\mathbb{F}[X]$-module with $\operatorname{Ann}_{\mathbb{F}[X]} V = (p[X])$ 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. 60. 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. 16.

Ex. 61. Let R be a commutative ring and M be a cyclic R-module. The *order ideal* of M is defined to be $\operatorname{Ann}_R(x)$ for any generator of M. Show that this is well-defined.

Ex. 62. 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 $\operatorname{Ann}_R(e_j)$.

Contrast this with Ex. 61

Ex. 63. 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. 64. 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. 65. Determine all simple $\mathbb{Z}$-modules.

Ex. 66. Let R be a ring with identity. Show that R is a simple R-module iff R is a division ring.

Ex. 67. 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. 68. 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. 69. Is $\mathbb{Q}$ an indecomposable $\mathbb{Z}$-module?

Ex. 70. 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 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \simeq A_n$ 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. 71. Exhibit all $\mathbb{Z}$-maps from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/12\mathbb{Z}$.

Ex. 72. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/(m,n)\mathbb{Z}$.

Ex. 73. Let $f\colon M \to N$ be an R-module homomorphism. Show that $f(\mathrm{Tor}\,(M)) \subset \mathrm{Tor}\,(N)$.

Ex. 74. 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. 75. An R-module is cyclic iff $M \simeq R/I$ for some left ideal I in R.

Ex. 76. 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. 77. 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. 78. 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. 79. 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. 80. 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. 81 (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. 80).

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

Ex. 82. Understand the last exercise (Ex. 81) when M is finite abelian group.

Free Modules

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

Definition 83. 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 84. *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. 4.) 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. 85. Prove [M, Theorem 73 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.

Ex. 86. 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. 87. Show that every principal left ideal in an integral domain with 1 is free as a left R-module.

Ex. 88. Prove that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module. Can you generalize this? *Hint:* Field of fractions.

Ex. 89. Show that every ideal of $\mathbb{Z}$ is free as a $\mathbb{Z}$-module.

Ex. 90. Prove that every principal left ideal in an integral domain R with 1 is a free R-module.

Ex. 91. 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. 92. 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. 91

Ex. 93. What is the analogue of Ex. 91 in the case of an onto map f?

Ex. 94. 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. 95. 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 a PID. *Hint:* Ex. 94.

Ex. 96. Let R be a PID. Assume that M is FG torsion free R-module. Show that M is free.

Ex. 97. 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. 98 (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. 99. 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. 100. 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. 101. Let $M := \oplus_{n\in\mathbb{N}} R$ be the direct sum of countably infinite number of copies 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.

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. 112 (e) or Proposition 122, page 42) 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 102. 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. 103. 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. 104. 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. 105. 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. 106. 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 107. Let $\varphi\colon R^n \to M$ be a surjective R-map. By [M, Ex. 84], $\ker\varphi$ 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

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

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. 108. 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. 109. 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. 110. 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. 111. 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. 112. 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. 113. 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. 114. 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. 115. 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, $(1+x)^2(x+3)$.

Structure Theorem over a PID

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

For the rest of this section, we shall assume that R is a PID unless specified otherwise. Recall this means R is Noetherian and every FG R-module is Noetherian.

Definition 116. 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. 117. Let M be a FG free R-module and let N be a submodule of M. For any $f \in \operatorname{Hom}_R(M,R)$, the image $f(N)$ is an ideal in R so that $f(N) = (a_f)$. Let $\Sigma := \{(a_f) \mid f \in \operatorname{Hom}_R(M,R)\}$. 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 $x_1, \dots, x_n$ of M. Let $\pi_i \in \operatorname{Hom}_R(M,R)$ 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 122.

Ex. 118. Keep the notation of Ex. 117. Show that a_1 divides $f(y)$ for any $f \in \operatorname{Hom}_R(M,R)$. *Hint:* Let $(d) = (a_1, y)$. Then $d = ra_1 + sf(y)$. Consider $\psi := r\varphi + sf$. Observe that $\psi(y) = d$.

Ex. 119. 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. 120. With the notation of the last exercise, prove the following:
(a) $M = Ry_1 \oplus \ker\varphi$,
(b) $N = Ra_1y_1 \oplus (N \cap \ker\varphi)$.

Conclude that y_1 can be taken as one element of a basis of M and that a_1y_1 can be taken as one element in a basis of N.

Ex. 121. With the notation of Ex. 117, 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 proof of [M, Thm. 101].

Proposition 122. *Let R be a PID. Let M be a FG free R-module and let N be a submodule of M. Then there exists a basis $y_1, y_2, \dots, y_n$ of M and nonzero elements $a_i \in R$ such that*
(i) *$a_1y_1, \dots, a_my_m$ 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. 121) and Ex. 120 to $\ker\varphi$ to conclude that $\ker\varphi$ is free of rank $n-1$. ☐

Ex. 123. What does the last proposition say in the context of vector spaces?

Theorem 124 (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 $x_1, \dots, x_n$ 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. 121 and Prop. 122 to the pair R^n and $\ker\pi$. ☐

Remark 125. 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 126 (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. 127. Let R be a PID. Let M be an R-module. Then M is free iff it is torsion free.

Ex. 128. With the notation of the Structure Theorem (Thm. 124), 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. 129. 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 130. *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

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

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

Theorem 131. *[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. 129 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 130.

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. 132. 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. 133. 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. 134. 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. 135. Let M be a torsion module over a PID. Show that M is simple iff M is cyclic with prime exponent.

Ex. 136. Let M be a torsion module over a PID. Show that M is indecomposable iff M is cyclic with prime power exponent.

Applications

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

Ex. 137. Find the number of abelian groups of order p^n (p, a prime).

Ex. 138. Find the number of abelian groups of order $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Ex. 139. Find all abelian groups of order 60.

Ex. 140. For what values of $n \in \mathbb{N}$, is it true that the only abelian groups of order n are cyclic?

Ex. 141. 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. 142. 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.

Rational Canonical Form

Definition 143. 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. 144. 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. 145. Let A and B be two $n \times n$-matrices over the field $\mathbb{F}$. Assume that $\mathbb{F}$ is a subfield of a field $\mathbb{K}$.
(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. 146. The characteristic polynomial of the companion matrix 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. 147. 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. 146).

Ex. 148. 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. 115! 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. 149. Prove that two non-scalar 2×2 matrices over a field $\mathbb{F}$ are similar iff they have the same characteristic polynomial.

Ex. 150. Prove that two 3×3 matrices are similar iff they have the same characteristic and same minimal polynomials.

Ex. 151. Find two 4×4 matrices over $\mathbb{C}$ which have the same characteristic and minimal polynomials but are not similar.

Ex. 152. Describe the 2×2 matrices over $\mathbb{C}$ whose similarity classes contain only one element. Generalize your answer.

Jordan Canonical Form

Ex. 153. If a matrix A is similar to a diagonal matrix D, then D is the Jordan canonical form of A. Consequently, two diagonal matrices are similar iff they have the same diagonal entries up to permutation.

Ex. 154. 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. 155. Use Ex. 154 to find the JCF of $\begin{pmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix}$.

References

[1] M. Artin, *Algebra*, Prentice-Hall, 3rd Indian Reprint, 1996.

[2] P.M. Cohn, *Algebra, Volume 1*, Wiley, 2nd Edition, 1982.

The first two were our main references for this course. Other sources are:

[3] S.D. Adhikari, An Introduction to Commutative Algebra and Number Theory, Narosa, 1999.

[4] P.B.Bhattacharya, S.K. Jain and S.R. Nagpaul, *Basic Abstract Algebra*, Cambridge University Press, 2nd Edition, 1995.

[5] D.S. Dummit and R.M. Foote, *Abstract Algebra*, John-Wiley, 2nd Edition, 1999.

[6] N.S. Gopalakrishnan, *University Algebra*, New Age, 2nd Edition, 1986

[7] B. Hartley and T.O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman and Hall, 1970.

[8] C. Musili, *Introduction to Rings and Modules*, Narosa, 1992.