Rice University

Department of Mathematics

Introduction to Module Theory

Author
Gabriel Gress

June 11, 2021

Chapter 0

Preamble

Introduction

Chapter 1

Introduction to Modules

1.1 Modules

An R-module M is an abelian group that comes equipped with a binary operation $\cdot$ that maps from $R \times M$ to M that is compatible with operations of both M and R. It is the natural generalization of vector spaces to rings, but with the key difference that we may not have multiplicative inverses for elements in our R-module.

Definition 1.1.1: Left R-module

Let R be a ring. A **left R-module** is a pair ${}_RM := (M, \cdot : R \times M \to M)$ where M is an abelian group, and $\cdot$ is a binary operation so that

$$\begin{aligned} \forall r, s \in R,\ \ m, n \in M &: \\ r \cdot (m + n) &= (r \cdot m) + (r \cdot n) \\ (r + s) \cdot m &= (r \cdot m) + (s \cdot m) \\ (rs) \cdot m &= r \cdot (s \cdot m) \end{aligned}$$

If R is unital, then we also require

$$1_R \cdot m = m.$$

The map is called the (left) **R-action map**.

Example 1.1.1: Free Module of Rank n

1. If R is a field F, then the R-module is an F-vector space.
2. Take $M = R^n := \{(t_1, \ldots, t_n) \mid t_i \in R\}$. Let the R-action map of ${}_RM$ be defined by

   $$\begin{aligned} R \times M &\to M \\ (r, (t_1, \ldots, t_n)) &\mapsto (rt_1, \ldots, rt_n). \end{aligned}$$

   One can check that this satisfies the necessary properties of a left R-action on $M = R^n$. This left R-module ${}_RR^n$ (which we will simply denote here on out by R^n) is called the **free left R-module of rank n**.

Example 1.1.2: $\mathbb{Z}$-Modules

An abelian group M can be made into a module ${}_{\mathbb{Z}}M$ over the integers in exactly one way. Consider the $\mathbb{Z}$-action map defined by

$$\begin{aligned} \mathbb{Z} \times M &\to M \\ (n, m) &\mapsto m + \ldots_n + m \end{aligned}$$

One can check that this indeed is a $\mathbb{Z}$-module over M.

Exercise 1.1.1

Prove that the $\mathbb{Z}$-action given above is the unique $\mathbb{Z}$-action for any $\mathbb{Z}$-module. Furthermore, show that ${}_{\mathbb{Z}}M$ is isomorphic to an abelian group.

Example 1.1.3: $F[x]$ Modules

Let $R = F[x]$ be a polynomial ring over a field F, and let V be a vector space over F with a linear operator $T \in \mathcal{L}(V)$. We can construct an $F[x]$-module on V via T (denoted ${}_{F[x]}V$)). To see this, let $p(x) \in F[x]$ be a polynomial given by

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

For each $v \in V$, we define the action of $p(x)$ on v by

$$\begin{aligned} p(x) \cdot v &= (a_n T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0)(v) \\ &= a_n T^n(v) + a_{n-1}T^{n-1}(v) + \ldots + a_1 T(v) + a_0 v \end{aligned}$$

Informally, we are defining an action of x on V by T, and then extending it onto $F[x]$ in a natural way.

Recall that $F \leq F[x]$ (as constant polynomials), and hence the action of F is exactly the same as constant polynomials, which correspond to the standard action of F on V. In other words, this action is an extension of the action of F onto a larger ring $F[x]$.

Because this action is dependent on the choice of T, this gives us many different $F[x]$-module structures on the same vector space V. One can check that $T = 0$ also yields us the standard action of F on V.

What is interesting to note is that the action of $F[x]$ via T encapsules *all* possible $F[x]$-modules– this holds because the action of $x \in F[x]$ on V is a linear transformation from V to V, and hence must correspond to some T which all actions $p(x)$ must adhere to.

One might ask what $F[x]$-submodules look like. We can see immediately that an $F[x]$-submodule ${}_{F[x]}W \leq {}_{F[x]}V$ must also be an F-submodule, and hence $W < V$ as a vector subspace. Furthermore, in order for it to be well-defined, W must be T-**invariant**, that is, $T(W) \subset W$. In fact this too is a bijection, so that all $F[x]$-submodules of V correspond to T-invariant subspaces of V.

This example shows that the ideal structure of $F[x]$ greatly restricts the module structure on V (and in fact can be used to derive its Jordan canonical form). In fact, the reasonings above can be applied to any PID R, and in the special case $R = \mathbb{Z}$ we can obtain the fundamental theorem of finitely generated abelian groups. In general, it is always interesting to see how the structure of a ring R will affect its modules.

1.2 Substructures of Modules

Definition 1.2.1: Submodule

Let R be a ring, let ${}_RM$ be a left R-module, and let $N \leq M$ be a subgroup of M. A R-**submodule of** ${}_RM$ is the R-module ${}_RN$ with the same R-action from ${}_RM$.

In other words, it is a subgroup with closure under the R-action.

Proposition 1.2.1: Submodule Criterion

Take a ring R with 1_R, and left R-module M. A subset N of M can be made into a R-submodule of M if and only if

- $N \neq \emptyset$ and
- $n + rn' \in N$ for all $r \in R$, $n, n' \in N$.

Proposition 1.2.2

Let M be an R-module, and let ${}_RN_i$ with $i \in I$ be R-submodules of M. Then

1. $\bigcap_{i \in I} {}_RN_i$ is an R-submodule of M
2. $\bigcup_{i \in I} {}_RN_i$ is not necessarily an R-submodule of ${}_RM$
3. If ${}_RN_1 \subset {}_RN_2 \subset {}_RN_3 \subset \ldots$ is an increasing chain of R-submodules of M, then $\bigcup_{i \in \mathbb{N}} {}_RN_i$ is an R-submodule of ${}_RM$
4. Let $N_1 + N_2 = \{n_1 + n_2 \mid n_1 \in N_1, n_2 \in N_2\}$ be the sum of N_1 and N_2. Then $N_1 + N_2$ can be made into an R-submodule of M.

Exercise 1.2.1

The submodules of the R-module ${}_RR$ are ${}_RI$ where $I \lhd R$ is an ideal.

1.3 R-module homomorphisms

Definition 1.3.1

Let R be a ring, and let ${}_RM$ and ${}_RN$ be R-modules. An R-**module homomorphism** is a group homomorphism

$$\varphi : M \to N \quad [\varphi(m + m') = \varphi(m) + \varphi(m')]$$

so that R-action is preserved. That is, for all $r \in R$, $m, m' \in M$, the group homomorphism satisfies:

$$[\varphi(rm) = r\varphi(m)]$$

for all $r \in R$, $m, m' \in M$.

The **kernel** of φ is

$$\mathrm{Ker}\varphi = \{m \in M \mid \varphi(m) = 0\},$$

and the **image** of φ is

$$\mathrm{Im}(\varphi) = \{\varphi(m) \mid m \in M\}.$$

The set of R-module homomorphisms from ${}_RM$ to ${}_RN$ is denoted by $\mathrm{Hom}_R(M, N)$. An R-**module isomorphism** is a bijective R-module homomorphism (trivial kernel and full range).

Example 1.3.1: $\mathbb{Z}$-submodules

Recall that any group homomorphism between abelian groups can be represented as a $\mathbb{Z}$-module homomorphism. Hence, if ${}_{\mathbb{Z}}N$ is a submodule of ${}_{\mathbb{Z}}M$, then $N \leq M$.

Exercise 1.3.1

If $\varphi \in \mathrm{Hom}_R(M, N)$ and $\psi \in \mathrm{Hom}_R(N, P)$ then $\psi \circ \varphi \in \mathrm{Hom}_R(M, P)$.

1.4 Quotient Modules and Isomorphism Theorems

Proposition 1.4.1: Modules of homomorphisms

Let R be a ring, and take R-modules ${}_RM$ and ${}_RN$.

1. If $\varphi, \psi \in \mathrm{Hom}_R(M, N)$, then define

$$(\varphi + \psi)(m) := \varphi(m) + \psi(m) \quad \forall m \in M$$
$$(r\varphi)(m) := r\varphi(m) \quad \forall r \in R, m \in M$$

   This gives $\mathrm{Hom}_R(M, N)$ the structure of an R-module, which we denote by ${}_R\mathrm{Hom}_R(M, N)$.

2. We denote $\mathrm{Hom}_R(M, M)$ by $\mathrm{End}_R(M)$. We get that $\mathrm{End}_R(M)$ is a ring with addition defined as above, and multiplication as defined in the exercise. We call this the **endomorphism ring of** M, and elements are **endomorphisms**.

There is a structure that combines being an R-module and a ring, which we call R-algebras.

Definition 1.4.1: R-algebra

Let R be a commutative ring with 1_R. A **(unital)** R-**algebra** is a unital ring A equipped with a unital ring homomorphism $f : R \to A$ such that the subring $f(R) \leq A$ is contained in the center $Z(A)$.

It is easy to see that A has a natural R-module structure given by $ra \mapsto f(r)a$. This is not the only module structure, but it is the most natural.

Example 1.4.1: Endomorphism

If R is commutative, then ${}_R\mathrm{End}_R(M)$ is an R-algebra via the action of function composition $r\varphi \mapsto r(\varphi(m))$.

The unital ring homomorphism from $R \to \mathrm{End}_R(M)$ is given by $r \mapsto r \cdot \mathrm{Id}$, where Id is the identity endomorphism. When R has an identity, this gives $\mathrm{End}_R(M)$ an R-algebra structure, as the image is clearly in the center of $\mathrm{End}_R(M)$.

Notice that it isn't necessarily injective, as $rm = 0$ is possible. If R is a field, however, it will be injective in which case the image is the **subring of scalar transformations**.

Definition 1.4.2: R-algebra homomorphism

If A, B are two R-algebras, an R-**algebra homomorphism** is a ring homomorphism $\varphi : A \to B$ such that, for all $r \in R$ and $a \in A$:

$$\varphi(r \cdot a) = r \cdot \varphi(a).$$

It follows that if A is an R-algebra, then it satisfies $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$ because $f(r)$ is in the center. If these conditions hold for a ring, then it defines an R-algebra– hence it can be considered an alternate definition.

Quotient Modules

Proposition 1.4.2

Take R as a ring, and ${}_RM$ an R-module with R-submodule ${}_RN$.

1. The quotient group M/N can be made into an R-module ${}_R(M/N)$ via

$$\begin{aligned} R \times M/N &\to M/N \\ (r, m + N) &\mapsto rm + N \quad \forall r \in R,\ m + N \in M/N \end{aligned}$$

2. The canonical projection map of groups

$$\begin{aligned} \pi : M &\to M/N \\ m &\mapsto m + N \quad \forall m \in M \end{aligned}$$

is a surjective R-module map, with $\mathrm{Ker}\pi = N$.

Theorem 1.4.1: Module Isomorphism Theorems

Let R be a ring, and ${}_RM, {}_RN$ to be R-modules.

(i). If $\varphi \in \mathrm{Hom}_R(M, N)$, then ${}_R\mathrm{Ker}\varphi$ is a R-submodule of M, and $M/\mathrm{Ker}\varphi \overset{R}{\cong} \varphi(M)$ as R-modules (by R-module isomorphism).

(ii). If ${}_RA, {}_RB$ are R-submodules of M, then $(A + B)/B \overset{R}{\cong} A/(A \cap B)$ as R-modules.

(iii). If ${}_RA, {}_RB$ are R-submodules of M and $A \subset B$, then

$$(M/A)/(B/A) \overset{R}{\cong} M/B$$

as R-modules.

(iv). Suppose ${}_RN$ is an R-submodule of ${}_RM$. Then there exists a bijection:

$$\{\text{submodules } {}_RA \text{ of } {}_RM \text{ containing } {}_RN\} \iff \{\text{submodules } {}_R(A/N) \text{ of } {}_R(M/N)\}.$$

Direct Products

Let R be a ring with 1_R.

Proposition 1.4.3

Let ${}_RM$ be an R-module, with ${}_RN_1, \dots, {}_RN_t$ as R-submodules. Then

(i). The sum of $\{N_i\}_{i=1}$ is

$$N_1 + \dots + N_t = \{n_1 + \dots + n_t \mid n_i \in N_i,\ i = 1, \dots, t\}$$

and forms an R-module.

(ii). The direct product of $\{N_i\}$ is

$$N_1 \times \dots \times N_t = \{(n_1, \dots, n_t) \mid n_i \in N_i,\ i = 1, \dots, t\}$$

and forms an R-module.

One can also define the direct product of R-modules (i.e. not just submodules).

Proposition 1.4.4

Let ${}_RN_1, \dots, {}_RN_t$ be R-submodules of an R-module ${}_RM$. Then the following are equivalent:

(i).

$$\begin{aligned} \varphi : N_1 \times \dots \times N_t &\to N_1 + \dots + N_t \\ (n_1, \dots, n_t) &\mapsto n_1 + \dots + n_t \end{aligned}$$

is an R-module isomorphism

(ii). $N_j \cap (N_1 + \dots + N_{j-1} + N_{j+1} + \dots N_t) = 0$ for all $j = 1, \dots, t$

(iii). Every $x \in N_1 + \dots + N_t$ can be written as $n_1 + \dots + n_t$ uniquely for some $n_i \in N_i$ for all $i = 1, \dots, t$

If the proposition holds, then

$$N_1 \times \dots \times N_t \overset{R}{\cong} N_1 + \dots + N_t$$

and we refer to the structure as the direct sum of R-modules.

Chapter 2

Generating Modules

2.1 Generating Sets

Definition 2.1.1

Take an R-module ${}_RM$ and a subset $X \subset M$.

1. The R-**submodule generated by** X is

$$RX = \{r_1x_1 + \ldots + r_mx_m \mid r_i \in R,\ x_i \in X,\ m \in \mathbb{Z} > 0\}.$$

   The set X is called the **generating set** of RX.

2. A R-submodule ${}_RN$ of ${}_RM$ is **finitely generated** if $N = RX$ for $|X| < \infty$ and **cyclic** if $N = RX$ for $|X| = 1$.

Free Modules

Definition 2.1.2: Linear independence by R-modules

We say that $X = \{x_1, \ldots, x_n\}$ is R-**linearly independent** if

$$r_1x_1 + \ldots + r_nx_n = 0 \implies r_i = 0 \quad \forall i = 1, \ldots, n$$

Definition 2.1.3

We say that an R-module ${}_RM$ is **free on the subset** X of M if

$$M = RX$$
$$X \text{ is } R\text{-linearly independent}$$

In this case, we call X the **basis** of ${}_RM$, and sometimes denote ${}_RM$ by $F_R(X)$.

If R is commutative, then we call $|X|$ the **rank** of ${}_RM$.

This illustrates a key difference between vector spaces and modules– vector spaces are always free, while modules need not be.

Example 2.1.1: Free and non-free modules

Most modules have no basis! A free $\mathbb{Z}$-module is also called a **free abelian group**; lattices in $\mathbb{R}^2$ are free abelian groups, while finite, non-zero abelian groups are not free.

Definition 2.1.4: R-Matrix

Let R be a ring. An R**-matrix** is a matrix whose entries are in R. An **invertible** R**-matrix** is an R-matrix that has an inverse that is also an R-matrix. The $n \times n$ invertible R-matrices form a group called the **general linear group over** R:

$$GL_n(R) = \{n \times n \text{ invertible } R\text{-matrices}\}.$$

The **determinant** of an R-matrix $A = (a_{ij})$ is defined in the usual way

$$\det(A) = \sum_p \pm a_{1,p1} \dots a_{n,pn}.$$

or the sum over all permutations of the indices and the sign being the sign of the permutation. Of course, all the usual properties of determinants hold for R-matrices.

Lemma 2.1.1

Le R be a non-zero ring. Then a square R-matrix A is invertible if and only if it has either a left inverse or a right inverse, and only if its determinant is a unit of the ring. Furthermore, an invertible R-matrix is square.

Proposition 2.1.1: Free modules and R-matrices

Let R be a non-zero ring. Then the matrix P of a change of basis in a free module is an invertible R-matrix. Furthermore, any two bases of the same free module over R have the same cardinality.

Every homomorphism f between two free modules is given by left multiplication by an R-matrix.

Theorem 2.1.1: Universal Property of Free Modules

For any set A there is a free R-module $F_R(A)$ on the set A and $F_R(A)$ satisfies the *universal property*: if ${}_RM$ is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F_R(A) \to M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$. In other words, the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "\text{inclusion}"] \arrow[dr, "\varphi"'] & F_R(A) \arrow[d, "\Phi"] \\
& M
\end{tikzcd}$$

Furthermore, if $A = \{a_1, \dots, a_n\}$, then

$$F_R(A) = Ra_1 \oplus Ra_2 \oplus \dots \oplus Ra_n \overset{R}{\cong} R^n$$

This corresponds to the notion of free groups from group theory.

Exercise 2.1.1

If F_R, F'_R are free modules on the same set A, there is a unique isomorphism between F_R and F'_R which is the identity map on A.

If ${}_RF$ is any free R-module with basis A, then ${}_RF \cong F_R(A)$.

If we have a free R-module with a basis A, the above statement says that we can define R-module homomorphisms from the free module into other R-modules by simply specifying how the homomorphism acts on elements of A.

The free module $F_{\mathbb{Z}}(A)$ is called the **free abelian group on** A. If A is finite, then we say it is of **rank** $|A|$ and is isomorphic to

$$\mathbb{Z} \oplus \ldots^{n} \oplus \mathbb{Z}.$$

2.2 Generators and Relations of Modules

Definition 2.2.1: Presentations

Let an $m \times n$ R-matrix denoted by A be a homomorphism of R-modules

$$R^n \overset{A}{\to} R^m.$$

We can denote its image by AR^n. We say that the quotient module $V = R^m/AR^n$ is **presented** by the matrix A. Any isomorphism $\sigma : R^m/AR^n \to V$ is a **presentation** of a module V, of which A is a **presentation matrix** for V if there is such an isomorphism.

We use the canonical map $\pi : R^m \to V = R^m/AR^n$ to interpret the quotient module as follows:

Proposition 2.2.1

V is generated by a set of elements $B = (v_1, \ldots, v_m)$, the images of the standard basis elements of R^m. Furthermore, if Y is a column vector in R^m, the element BY of V is zero if and only if Y is a linear combination of the columns of A, with coefficients in R, if and only if there exists a column vector X with entries in R such that $Y = AX$.

If a module V is generated by a set $B = (v_1, \ldots, v_m)$, we call any element $Y \in R^m$ such that $BY = 0$ a **relation vector**, or simply a **relation** among the generators. A set S of relations is a **complete set** if every relation is a linear combination of S with coefficients in the ring.

Proposition 2.2.2: Theoretical Method of Finding a Presentation

First, choose a set of generators $B = (v_1, \ldots, v_m)$ for V. These generators give a surjective homomorphism $R^m \to V$ that sends a column vector Y to the linear combination $BY = v_1 y_1 + \ldots + v_m y_m$. Denote the kernel of the map by W. It is the **module of relations**; its elements are the relation vectors.

Repeat this procedure, choosing a set of generators $C = (w_1, \ldots, w_m)$ for W, and define a surjective map $R^n \to W$ using them. Here the generators w_j are elements of R^m, and thus column vectors. Assemble the coordinate vectors A_j of w_j into a matrix with A_i as column i. Then multiplication by A defines

$$R^n \to^{A} R^m$$

which sends $e_j \mapsto A_j = w_j$, as it is the composition of $R^n \to W$ with the inclusion $W \subset R^m$. By construction W is its image and we denote it by AR^n. Because the map $R^m \to V$ is surjective, by the First Isomorphism Theorem, V is isomorphic to $R^m/W = R^m/AR^n$. Hence V is presented by the matrix A.

In short the presentation matrix A for a module V is determined by the set of generators for V, and the set of generators for the module of relations W. Assuming the set of generators does not form a basis, the number of generators will be equal to the number of rows of A.

Note that this relies on the assumption that V has finite generators. We must also assume that W has a finite set of generators, which is slightly more problematic.

Proposition 2.2.3: Rules for manipulating A without changing isomorphism class

Let A be an $m \times n$ presentation matrix for a module V. The following matrices A' present the same module V:

- $A' = Q^{-1}A$, $Q \in GL_m(R)$
- $A' = AP$ with $P \in GL_n(R)$
- A' is obtained by deleting a column of zeroes
- if the j-th column of A is e_i, then removing row i and column j preserves the presentation

2.3 Modules of Noetherian Rings

Proposition 2.3.1

The following conditions on an R-module V are equivalent:

- Every submodule of V is finitely generated
- There is no infinite strictly increasing chain $W_1 < W_2 < \dots$ of submodules of V.

We formalize this notion via Noetherian rings and modules.

Definition 2.3.1: Noetherian Modules

A left R-module ${}_RM$ is said to be a **Noetherian R-module** if it satisfies the ascending chain condition on submodules. That is, for any increasing chain of submodules of M

$$M_1 \subset M_2 \subset M_3 \subset \dots$$

there is a positive integer m such that, for all $k \geq m$, $M_k = M_m$.

A ring R is **Noetherian** if it is Noetherian as a left module over itself. That is, there are no infinite increasing chains of left ideals of R.

Corollary 2.3.1

If R is Noetherian then every ideal of R is finitely generated.

Theorem 2.3.1: Submodules of Noetherian

Let R be a ring and ${}_RM$ a left R-module. Then the following are equivalent:

- M is a Noetherian R-module
- Every nonempty set of submodules of M contains a maximal element under inclusion
- Every submodule of M is finitely generated

Notice that these conditions also imply that R is a Noetherian ring, and furthermore that every proper ideal of R is a maximal ideal.

Corollary 2.3.2

If R is a PID then every collection of ideals of R has a maximal element, and R is Noetherian.

Lemma 2.3.1

Let $\varphi : V \to V'$ be a homomorphism of R-modules.

- If V is finitely generated and φ is surjective, then V' is finitely generated.
- If the kernal and image of φ are finitely generated, then V is finitely generated.
- Let W be a submodule of an R-module V. If both W and $\overline{V} = V/W$ are finitely generated, then V is finitely generated. If V is finitely generated, so is $\overline{V}$.

Theorem 2.3.2: Hilbert Basis Theorem

Let R be a Noetherian ring. The polynomial ring $R[x]$ is Noetherian.

Proposition 2.3.2: Quotients of Noetherian

Let R be a Noetherian ring, and let I be an ideal of R. Any ring that is isomorphic to the quotient ring $\overline{R} = R/I$ is Noetherian.

Corollary 2.3.3

Let P be a polynomial ring in a finite number of variables over the integers/field. Any ring R that is isomorphic to the quotient ring P/I is Noetherian.

Lemma 2.3.2

Let R be a ring, let I be an ideal of the polynomial ring $R[x]$. The set A whose elements are the leading coefficients of the nonzero polynomials in I, together with the zero element of R, is an ideal of R, the **ideal of leading coefficients**.

2.4 Structure of Abelian Groups

Recall the fundamental theorem of finitely generated abelian groups.

Theorem 2.4.1: Structure Theorem for Abelian Groups

A finitely generated abelian group V is a direct sum of cyclic subgroups $C_{d_1}, \dots, C_{d_k}$ and a free abelian group L:

$$V = C_{d_1} \bigoplus \dots \bigoplus C_{d_k} \bigoplus L,$$

where the order d_i of C_{d_i} is greater than one, and $d_i \mid d_{i+1}$ for $i < k$.

Theorem 2.4.2: Structure Theorem (Alternate Form)

Every finite abelian group is a direct sum of cyclic groups of prime power orders.

Theorem 2.4.3: Uniqueness for Structure Theorem

Suppose that a finite abelian group V is a direct sum of cyclic groups of prime power orders $d_j = p_j^{r_k}$. The integers d_j are uniquely determined by the group V.

Analogues for Polynomial Rings and Linear Operators

Theorem 2.4.4

Let $R = F[t]$ be a polynomial ring in one variable over a field F and let A be an $m \times n$ R-matrix. There are products Q, P of elementary R-matrices such that

$$A' = Q^{-1}AP$$

is diagonal, each non-zero diagonal entry d_i of A' is a monic polynmial, and $d_1 \mid \ldots \mid d_k$.

Remark 2.4.1

Let M be a free cyclic R-module. Then there is a surjective homomorphism $\varphi : R \to M$ defined by $r \mapsto rv$, where v is the singular generating element in M. The kernel of φ is a submodule of R and hence an ideal $I \lhd R$. Therefore, M is isomorphic to the R-module R/I. When $R = F[t]$, the ideal I will be principal.

Theorem 2.4.5: Structure Theorem for Modules over Polynomial Rings

Let $R = F[t]$ be the ring of polynomials in one variable with coefficients in a field F. Let V be a finitely generated module over R. Then V is a direct sum of cyclic modules $C_1, C_2, \ldots, C_k$ and a free module L, where C_i is isomorphic to $R/(d_i)$, the elements $d_1, \ldots, d_k$ are monic polynomials of positive degree and satisfy both (but not simultaneously)

- $d_1 \mid d_2 \mid \ldots \mid d_k$
- Each d_i is a power of a monic irreducible polynomial

2.5 Tensor Products

The idea of a tensor product of modules M, N is to form another module in which we can take products mn of elements $m \in M$ and $n \in N$.

Definition 2.5.1: Ring Extension

Let $R \leq S$. If ${}_SN$ is a left S-module, then N can also construct a left R-module since the elements of R act on N by assumption.

More generally, if $f : R \to S$ is a ring homomorphism from R into S with $f(1_R) = 1_S$, then N can be considered as an R-module with $rn = f(r)n$ for $r \in R$ and $n \in N$. We consider S a **ring extension of** R and the resulting R-module is said to be obtained from N by **restriction of scalars** from S to R.

One might wonder if the reverse can be done– taking a ring R and attempting to extend the scalars to a larger ring. This cannot be done in general– for example, one can check that $\mathbb{Z}$ cannot be made into a $\mathbb{Q}$-module.

However, while $\mathbb{Z}$ cannot be made into a $\mathbb{Q}$-module, it is contained in a $\mathbb{Q}$-module (${}_{\mathbb{Q}}\mathbb{Q}$). That is, there is an embedding of the $\mathbb{Z}$-module ${}_{\mathbb{Z}}\mathbb{Z}$ into the $\mathbb{Q}$-module ${}_{\mathbb{Q}}\mathbb{Q}$. This isn't always the case however– to see this, consider the $\mathbb{Z}$-module ${}_{\mathbb{Z}}N$ where N is a finite abelian group. One can check that there are no nonzero homomorphisms into any $\mathbb{Q}$-module.

Our goal will be to construct a module which is the best candidate for which we can embed into.

Definition 2.5.2: Tensor Product of Modules

Let ${}_R N$ be a general R-module that we wish to embed into some S-module. First we will try and define a product of the form sn for $s \in S$, $n \in N$.

We start by considering the free $\mathbb{Z}$-module on the set $S \times N$. This is the collection of all finite commuting sums of elements of the form (s_i, n_i) with no relations imposed on sn. Our S-module structure requires that we must satisfy the relations

$$\begin{aligned} r_1 : &\quad (s_1 + s_2)n = s_1 n + s_2 n \\ r_2 : &\quad s(n_1 + n_2) = sn_1 + sn_2 \\ r_3 : &\quad (sr)n = s(rn) \end{aligned}$$

for $s_1, s_2, s \in S$, $r \in R$, and $n \in N$. We let $H \leq N$ be the subgroup given by $H := \langle r_1, r_2, r_3 \rangle$, that is, all elements of the form above, and consider N/H. We denote this quotient group by $S \otimes_R N$ and call it the **tensor module product of** S **and** N **over** R. We denote $s \otimes n$ the coset containing (s, n) in $S \otimes_R N$ and so we have

$$\begin{aligned} (s_1 + s_2) \otimes n &= s_1 \otimes n + s_2 \otimes n \\ s \otimes (n_1 + n_2) &= s \otimes n_1 + s \otimes n_2 \\ sr \otimes n &= s \otimes rn. \end{aligned}$$

The elements of $S \otimes_R N$ are called **tensors of modules** and can be written as finite sums of **simple tensors of modules** of the form $s \otimes n$ with $s \in S, n \in N$.

Now we give the tensor module product $S \otimes_R N$ an S-module action by

$$s \left(\sum_{\text{finite}} s_i \otimes n_i \right) = \sum_{\text{finite}} (ss_i) \otimes n_i.$$

We call this module ${}_S(S \otimes_R N)$ the S-**module obtained by extension of scalars from the** R**-module** N.

The natural map $\iota : N \to S \otimes_R N$ defined by $n \mapsto 1 \otimes n$. Because $1 \otimes rn = r(1 \otimes n)$, it follows that ι is an R-module homomorphism from N to $S \otimes_R N$. It is not injective in general, and so $S \otimes_R N$ need not contain an isomorphic copy of N.

Because the relatons imposed were the minimal relations necessary, one would expect that $S \otimes_R N$ is the best possible S-module for a module homomorphism.

Theorem 2.5.1: Universal Property for Tensor Modules

Let $R \leq S$, let ${}_R N$ be a left R-module and let $\iota : N \to S \otimes_R N$ be the R-module homomorphism defined by $\iota(n) = 1 \otimes n$. Suppose that ${}_S L$ is an arbitrary left S-module and $\varphi : N \to L$ is an R-module homomorphism from N to L. Then there is a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ such that $\varphi = \Phi \circ \iota$ and the diagram commutes:

$$\begin{tikzcd} N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & S \otimes_R N \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

Conversely, if $\Phi : S \otimes_R N \to L$ is an S-module homomorphism then $\varphi = \Phi \circ \iota$ is an R-module homomorphism from N to L.

Corollary 2.5.1

Let $\iota : N \to S \otimes_R N$ be the R-module homomorphism from the universal property of free modules. Then $N/\mathrm{Ker}\,\iota$ is the unique largest quotient of N that can be embedded in any S-module.

In particular, N can be embedded as an R-submodule of some left S-module if and only if ι is injective.

Example 2.5.1

General Tensor Product

Notice that forming $S \otimes_R N$ as an abelian group only required S_R to be a right R-module and ${}_RN$ a left R-module. We can construct an abelian group $M \otimes_R N$ for any right R-module M_R and any left R-module ${}_RN$.

The S-module structure on ${}_S(S \otimes_R N)$ required only a left S-module structure on ${}_SS$ and the compatibility relation

$$s'(^2) = (s's)r.$$

Definition 2.5.3: Tensor

Let ${}_RN$ be a left R-module and M_R a right R-module. We obtain an abelian group by quotient of the free $\mathbb{Z}$-module on $M \times N$ by the subgroup $H = \langle r_1, r_2, r_3 \rangle$, where

$$\begin{aligned} r_1 : &\quad (m_1 + m_2, n) = (m_1, n) + (m_2, n) \\ r_2 : &\quad (m, n_1 + n_2) = (m, n_1) + (m, n_2) \\ r_3 : &\quad (mr, n) = (m, rn) \end{aligned}$$

for $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$. We denote this by

$$M \otimes_R N := {}_{\mathbb{Z}}(M \times N)/\langle r_1, r_2, r_3 \rangle$$

and call it the **tensor product of** M **and** N **over** R. The elements of $M \otimes_R N$ are called **tensors**, and the coset $m \otimes n \in M \otimes_R N$ is called a **simple tensor**. Every tensor can be written (non-uniquely) as a finite sum of simple tensors.

Keep in mind that $m \otimes n$ are cosets and not elements directly– so caution must be used when defining maps on tensor products. That is, one needs to check that a map is well-defined on the entirety of a coset.

Furthermore, caution must be exercised when comparing tensor products. For example, if $M \leq M'$, we can have $m \otimes n = 0$ in $M' \otimes_R N$ but $m \otimes n \neq 0$ in $M \otimes_R N$. This essentially captures the notion that when more elements are included, the cosets will change. Hence there is no reason to expect $M \otimes_R N \leq M' \otimes_R N$.

Definition 2.5.4

Let M_R be a right R-module, ${}_RN$ a left R-module, and L an abelian group. A map $\varphi : M \times N \to L$ is called R-**balanced** or **middle linear with respect to** R if

$$\begin{aligned} \varphi(m_1 + m_2, n) &= \varphi(m_1, n) + \varphi(m_2, n) \\ \varphi(m, n_1 + n_2) &= \varphi(m, n_1) + \varphi(m, n_2) \\ \varphi(m, rn) &= \varphi(mr, n) \end{aligned}$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$.

We can define a map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$. This map is not a group homomorphism but it is in fact R-balanced.

Theorem 2.5.2: Universal Property of Tensor Products

Let R be a ring, M_R a right R-module, and ${}_RN$ a left R-module. Let $M \otimes_R N$ be the tensor product of M and N over R and let $\iota : M \times N \to M \otimes_R N$ be the R-balanced map defined by $\iota(m, n) = m \otimes n$. Then for any group homomorphism $\Phi : M \otimes_R N \to L$ to an abelian group L, the composite map

$$\varphi = \Phi \circ \iota$$

is an R-balanced map from $M \times N \to L$. Conversely, if L is an abelian group and $\varphi : M \times N \to L$ is any R-balanced map, then there is a unique group homomorphism $\Phi : M \otimes_R N \to L$ such that $\varphi = \Phi \circ \iota$.

In other words, there is a correspondence between φ and Φ by the commutative diagram:

$$\begin{tikzcd} M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

and this correspondence establishes a bijection between R-balanced maps and group homomorphisms, by the bijection between φ and Φ.

Corollary 2.5.2

Suppose D is an abelian group and $\iota' : M \times N \to D$ is an R-balanced map such that

- $D = \langle \mathrm{Im}(\iota') \rangle$
- every R-balanced map defined on $M \times N$ factors through ι'

Then there is an isomorphism $f : M \otimes_R N \cong D$ of abelian groups with $\iota' = f \circ \iota$

Now we'd like to give this abelian group a module structure. We simply need to impose a compatibility structure on M to obtain this.

Definition 2.5.5

Let R, S be rings. An abelian group M induces a (S, R)-**bimodule** if M forms a left S-module, a right R-module, and $s(mr) = (sm)r$ for all $s \in S, r \in R, m \in M$.

Example 2.5.2

Let R be a commutative ring. A left R-module ${}_RM$ can always be given the structure of a right R-module by simply defining $mr = rm$, and hence M becomes a (R, R)-bimodule. We call this the **standard** R-module structure on M.

Notice that if N has a left R-module structure and M a (S, R)-bimodule structure, then we have once again

$$s\left(\sum_{\text{finite}} m_i \otimes n_i\right) = \sum_{\text{finite}} (sm_i) \otimes n_i$$

and hence there is a well-defined action of S so that $M \otimes_R N$ can be considered a left S-module. It follows that for fixed s, $(m, n) \mapsto sm \otimes n$ is an R-balanced map, and hence there is a well-defined group homomorphism $\lambda_s : M \otimes_R N \to M \otimes_R N$ that satisfies $\lambda_s(m \otimes n) = sm \otimes n$.

A special case we might encounter is when M, N are left modules over a commutative ring R, and $S = R$. Then the standard R-module structure on M gives M the structure of an (R, R)-bimodule and hence $M \otimes_R N$ always has the structure of a left R-module.

Definition 2.5.6

Let R be a commutative ring and let M, N, L be left R-modules. The map $\varphi : M \times N \to L$ is called R-**bilinear** if it is R-linear in every factor:

$$\varphi(r_1m_1 + r_2m_2, n) = r_1\varphi(m_1, n) + r_2\varphi(m_2, n)$$
$$\varphi(m, r_1n_1 + r_2n_2) = r_1\varphi(m, n_1) + r_2\varphi(m, n_2)$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r_1, r_2 \in R$.

Corollary 2.5.3

Suppose R is a commutative ring, and M, N two left R-modules. Let $M \otimes_R N$ be the tensor product of M and N over R, where M is given the standard R-module structure. Then $M \otimes_R N$ is a left R-module with

$$r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn)$$

and the map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$ is an R-bilinear map. If L is any left R-module then there is a bijection between R-bilinear maps and R-module homomorphisms induced by the bijection between $\varphi : M \times N \to L$ and $\Phi : M \otimes_R N \to L$ via the commutative diagram:

$$\begin{tikzcd}
M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\Phi"] \\
 & L
\end{tikzcd}$$

Example 2.5.3

Theorem 2.5.3: Tensor Product of Homomorphisms

Let M, M' be right R-modules, let N, N' be left R-modules. Suppose $\varphi : M \to M'$ and $\psi : N \to N'$ are R-module homomorphisms. Then there is a unique group homomorphism denoted by $\varphi \otimes \psi$ given by

$$\varphi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$$
$$(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$$

for all $m \in M$ and $n \in N$.

If M, M' are (S, R)-bimodules for some ring S, and φ is also an S-module homomorphism, then $\varphi \otimes \psi$ is a homomorphism of left S-modules. Hence if R is commutative then $\varphi \otimes \psi$ is always an R-module homomorphism for the standard R-module structures.

Notice that the uniqueness conditions tells us that if $\lambda : M' \to M''$ and $\mu : N' \to N''$ are R-module homomorphisms, then

$$(\lambda \otimes u) \circ (\varphi \otimes \psi) = (\lambda \circ \varphi) \otimes (\mu \otimes \psi).$$

In fact, we can use this idea to extend the tensor product into an n-fold tensor product.

Theorem 2.5.4

Suppose M is a right R-module, N is an (R, T)-bimodule, and L is a left T-module. Then there is a unique isomorphism

$$(M \otimes_R N) \otimes_T L \cong M \otimes_R (N \otimes_T L)$$

of abelian groups such that

$$(m \otimes_R n) \otimes l \mapsto m \otimes_R (n \otimes_R l).$$

If M is an (S, R)-bimodule, then this is an isomorphism of S-modules.

Corollary 2.5.4

Let R be a commutative ring and M, N, L form left R-modules. Then

$$(M \otimes_R N) \otimes_R L \cong M \otimes_R (N \otimes_R L)$$

Of course, it will be useful to use the natural extension of a bilinear map.

Definition 2.5.7

Let R be a commutative ring and let $M_1, M_2, \ldots, M_n$ and L form R-modules with the standard R-module structures. A map $\varphi : M_1 \times \ldots \times M_n \to L$ is called n-**multilinear over** R if it is an R-module homomorphism in each component:

$$\varphi(m_1, \ldots, m_{i-1}, rm_i + r'm_i', m_{i+1}, \ldots, m_n) = r\varphi(m_1, \ldots, m_i, \ldots, m_n) + r'\varphi(m_1, \ldots, m_i', \ldots, m_n)$$

Hence we can define an n-fold tensor product by iterating the tensor product of pairs of modules.

Corollary 2.5.5

Let R be a commutative ring and let $M_1, \ldots, M_n, L$ be R-modules. Let $M_1 \otimes_R M_2 \otimes_R \ldots \otimes_R M_n$ be the sequence of tensor products of pairs of these modules and let

$$\begin{aligned} \iota : M_1 \times \ldots \times M_n &\to M_1 \otimes_R \ldots \otimes_R M_n \\ \iota(m_1, \ldots, m_n) &= m_1 \otimes_R \ldots \otimes_R m_n. \end{aligned}$$

Then for every R-module homomorphism $\Phi : M_1 \otimes_R \ldots \otimes_R M_n \to L$ the map $\varphi = \Phi \circ \iota$ is n-multilinear from $M_1 \times \ldots \times M_n \to L$.

If $\varphi : M_1 \times \ldots \times M_n \to L$ is an n-multilinear map then there is a unique R-module homomorphism $\Phi : M_1 \otimes_R \ldots \otimes_R M_n \to L$ such that $\varphi = \Phi \circ \iota$. This bijection induces a bijection between n-multilinear maps and R-module homomorphisms for which the following diagram commutes:

$$\begin{tikzcd} M \times \ldots \times M_n \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R \ldots \otimes_R M_n \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

We once again have a containment condition.

Theorem 2.5.5: Tensor Products of Direct Sums

Let M, M' be right R-modules and let N, N' be left R-modules. Then there are unique group isomorphisms

$$\begin{aligned}(M \oplus M') \otimes_R N &\cong (M \otimes_R N) \oplus (M' \otimes_R N)\\ M \otimes_R (N \oplus N') &\cong (M \otimes_R N) \oplus (M \otimes_R N')\\ (m, m') \otimes n &\mapsto (m \otimes n, m' \otimes n)\\ m \otimes (n, n') &\mapsto (m \otimes n, m \otimes n').\end{aligned}$$

If M, M' are also (S, R)-bimodules, then these are isomorphisms of left S-modules. In particular, if R is commutative, these are isomorphisms of R-modules.

Of course, this theorem extends inductively to any finite direct sum of R-modules (in fact any arbitrary direct sums). In essense, tensor products commute with direct sums.

Corollary 2.5.6

The module obtained from the free R-module $N \cong {}_RR^n$ by extension of scalars from R to S is the free S-module ${}_SS^n$:

$$S \otimes_R R^n \cong S^n$$

as left S-modules.

Corollary 2.5.7

Let R be a commutative ring and let $M \cong R^s$, $N \cong R^t$ form free R-modules with bases $m_1, \dots, m_s$ and $n_1, \dots, n_t$ respectively. Then $M \otimes_R N$ forms a free R-module of rank st with basis $m_i \otimes n_j$, $1 \le i \le s$ and $1 \le j \le t$, so that:

$$R^s \otimes_R R^t \cong R^{st}.$$

Remark 2.5.1

The tensor product of two free modules of arbitrary rank over a commutative ring is free.

Proposition 2.5.1

Suppose R is a commutative ring and M, N form left R-modules via the standard R-module structures. Then there is a unique R-module isomorphism

$$\begin{aligned}M \otimes_R N &\cong N \otimes_R M\\ m \otimes n &\mapsto n \otimes m\end{aligned}$$

One might think that if $M = N$, the above conditions are not necessary, but in fact it is not the case. Some tensors do have the property that $a \otimes b = b \otimes a$ for $a, b \in M$, which we refer to as symmetric tensors, to be studied later.

Proposition 2.5.2

Let R be a commutative ring and let A, B be R-algebras. Then the multiplication

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'$$

is well-defined and makes $A \otimes_R B$ into an R-algebra.

Example 2.5.4

2.6 Exact Sequences

Consider modules A, C. One question worth exploring is if there exists a module B such that $A/B \cong C$; that is, B is an extension of C by A. The tools we develop to understand this question are exact sequences. If A is isomorphic to a submodule of B, there is an injective homomorphism from A to B. And if C is isomorphic to the quotient, then there is a surjective homomorphism from B to C. This will give us a chain

$$A \to B \to C$$

where the homomorphisms are compatible with. We formalize this idea via exact sequences.

Definition 2.6.1: Exact Sequences

Let α, β be homomorphisms so that

$$X \to^{\alpha} Y \to^{\beta} Z.$$

If $\mathrm{Im}(\alpha) = \mathrm{Ker}(\beta)$, then we say the pair of homomorphisms are **exact**.

A sequence of homomorphisms

$$\ldots \to X_{n-1} \to X_n \to X_{n+1} \to \ldots$$

is said to be an **exact sequence** if it is exact at every X_n between a pair of homomorphisms.

Hence, our goal is to see whether we can form an exact sequence $A \to B \to C$. Our notions of injectivity and surjectivity correspond exactly to the notions of exactness.

Proposition 2.6.1

Let A, B, C form R-modules over some ring R. Then the sequence

$$0 \to A \to^{\psi} B$$

is exact at A if and only if ψ is injective. Likewise, the sequence

$$B \to^{\varphi} \to C \to 0$$

is exact at C if and only if φ is surjective.

Combining the two ideas, the sequence

$$0 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

is exact if and only if ψ is injective, φ is surjective, and $\mathrm{Im}(\psi) = \mathrm{Ker}(\varphi)$.

Definition 2.6.2

An exact sequence of the form

$$0 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

is called an **short exact sequence**.

Our goal then is to determine if two modules admit a short exact sequence, and if so, how many.

Notice that any exact sequence can be written as a succession of short exact sequences. For example, if

$$X \to^{\alpha} Y \to^{\beta} Z$$

is exact at Y, then equivalently

$$0 \to \alpha(X) \to Y \to Y/\mathrm{Ker}(\beta) \to 0$$

is a short exact sequence.

Example 2.6.1

For fixed A, C, there can be many extensions of C by A. Hence, we need to determine a notion of a homomorphism to distinguish exact sequences.

Definition 2.6.3: Homomorphism of Short Exact Sequences

Let

$$0 \to A \to B \to C \to 0$$
$$0 \to A' \to B' \to C' \to 0$$

be two short exact sequences of modules. A **homomorphism of short exact sequences** is a collection of module homomorphisms α, β, γ such that the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

This is an **isomorphism of short exact sequences** if α, β, γ are isomorphisms in which case the extensions B, B' are **isomorphic extensions**.

The two exact sequences are called **equivalent** if $A = A'$, $C = C'$, and there is an isomorphism between them where α, γ are identity. In this case B and B' are **equivalent extensions**.

Equivalency by extensions is stronger than just R-module isomorphisms between B and B'– it tells us tat there is an R-module isomorphism between B and B' that restricts to an isomorphism from A to A' and induces an isomorphism on the quotients by C and C'.

Example 2.6.2

Proposition 2.6.2: Short Five Lemma

Let α, β, γ be a homomorphism of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

- If α, γ are injective then so is β
- If α, γ are surjective then so is β
- If α, γ are isomorphisms then so is β

These results also hold for short exact sequences of groups.

Proof of Short Five Lemma. ■

There is always at least one extension of a module C by A given by $B = A \oplus C$.

Definition 2.6.4

Let R be a ring and let

$$0 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

be a short exact sequence of R-modules. We say the sequence is **split** if there is an R-module complement to $\psi(A)$ in B. If this holds, then $B = A \oplus C$ up to isomorphism by

$$B = \psi(A) \oplus C'$$

for some submodile C', where $\varphi(C') \cong C$.

We say B is a **split extension of** C **by** A.

This is really just the question of existence of a complement to $\psi(A)$ in B that is isomorphic by φ to C.

Proposition 2.6.3

The short exact sequence

$$0 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

of R-modules is split if and only if there is an R-module homomorphism $\mu : C \to B$ such that $\varphi \circ \mu \cong \mathrm{Id}_C$.

Any set map $\mu : C \to B$ such that $\varphi \circ \mu = \mathrm{Id}_C$ is called a **section** of φ. If μ is a homomorphism, then μ is called a **splitting homomorphism** for the sequence.

A section of φ is merely a choice of coset representative in B for $B/\mathrm{Ker}\varphi \cong C$. A section is a homomorphism if this set of coset representatives forms a submodule, in which case this submodule gives a complement to $\psi(A)$ in B.

Example 2.6.3

Proposition 2.6.4

Let

$$0 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

be a short exact sequence of modules. Then $B = \psi(A) \oplus C'$ for some submodule C' of B with $\varphi(C') \cong C$ if and only if there is a homomorphism $\lambda : B \to A$ such that $\lambda \circ \psi = \mathrm{Id}_A$.

For groups, this is a stronger notion. The existence of a splitting homomorphism on the left end of the sequence gives that the extension group is a direct product (instead of a semidirect product). Of course, in modules there is no distinction as the underlying groups are abelian.

Projective Modules

Let R be a ring and suppose that ${}_RM$ is an extension of N by L, so that

$$0 \to L \to^{\psi} M \to^{\varphi} N \to 0.$$

If another R-module has an R-module homomorphism into L or N, can it extend to a homomorphism to M?

We can see directly that if $f \in \mathrm{Hom}_R(D, L)$ then $f' = \psi \circ f$ is an R-module homomorphism from D to M:

$$\begin{aligned} \psi' : \mathrm{Hom}_R(D, L) &\to \mathrm{Hom}_R(D, M) \\ f &\mapsto f' = \psi \circ f. \end{aligned}$$

Proposition 2.6.5

Let D, L, and M form R-modules and let $\psi : L \to M$ be an R-module homomorphism. Then the map

$$\begin{aligned} \psi' : \mathrm{Hom}_R(D, L) &\to \mathrm{Hom}_R(D, M) \\ f &\mapsto f' = \psi \circ f \end{aligned}$$

is a homomorphism of abelian groups. If ψ is injective, then ψ' is injective. Hence, if

$$0 \to L \to^{\psi} M$$

is exact, then

$$0 \to \mathrm{Hom}_R(D, L) \to^{\psi'} \mathrm{Hom}_R(D, M)$$

is exact.

Unfortunately, if there is an R-module homomorphism $f : D \to N$, it isn't always the case that f **lifts** to an R-module homomorphism $f : D \to M$ by

$$\begin{aligned} \varphi' : \mathrm{Hom}_R(D, M) &\to \mathrm{Hom}_R(D, N) \\ F &\mapsto F' = \varphi \circ F \end{aligned}$$

This only holds if and only if f is in the image of φ'.

Example 2.6.4

Theorem 2.6.1

Let D, L, M, N form R-modules. If

$$0 \to L \to^{\psi} M \to^{\varphi} N \to 0$$

is exact, then

$$0 \to \mathrm{Hom}_R(D, L) \to^{\psi'} \mathrm{Hom}_R(D, M) \to^{\varphi'} \mathrm{Hom}_R(D, N)$$

is exact.

A homomorphism $f : D \to N$ lifts to a homomorphism $F : D \to M$ if and only if $f \in \mathrm{Hom}_R(D, N)$ is in the image of φ'. In general φ' is surjective if and only if every homomorphism from D to N lifts to a homomorphism from D to M, in which case the sequence above extends to a short exact sequence.

The sequence above is exact for all R-modules D if and only if

$$0 \to L \to^{\psi} M \to^{\varphi} N$$

is exact.

Hence, by the theorem, the sequence

$$0 \to \mathrm{Hom}_R(D, L) \to^{\psi'} \mathrm{Hom}_R(D, M) \to^{\varphi'} \mathrm{Hom}_R(D, N) \to 0$$

is in general not a short exact sequence, as φ' may not be surjective. In fact, this sequence is exact if and only if there is a bijection between homomorphisms $F : D \to M$ and $g : D \to L$, $f : D \to N$ where

$$F \mid_{\varphi(L)} = \psi'(g)$$
$$f = \varphi'(F).$$

Notice that if the original sequence is spit exact, then the sequence of homomorphisms is also split exact.

Proposition 2.6.6

Let D, L, N form R-modules. Then

$$\mathrm{Hom}_R(D, L \oplus N) \cong \mathrm{Hom}_R(D, L) \oplus \mathrm{Hom}_R(D, N)$$
$$\mathrm{Hom}_R(L \oplus N, D) \cong \mathrm{Hom}_R(L, D) \oplus \mathrm{Hom}_R(N, D)$$

Of course this extends by induction to any finite direct sum of R-modules. In other words, the group of module homomorphisms commute with dfinite direct sums in either variable.

Remark 2.6.1

For infinite direct sums, this does not always hold. If $L \oplus N$ is replaced by an arbitrary direct sum, and the direct sum on the right hand side is replaced by a direct product, then

$$\mathrm{Hom}_R(D, L \oplus \{N_i\}_{i \in I}) \cong \mathrm{Hom}_R(D, L) \otimes \{\mathrm{Hom}_R(D, N_i)\}_{i \in I}$$

holds. The second part must be translated into

$$\mathrm{Hom}_R(L \otimes \{N_i\}_{i \in I}, D) \cong \mathrm{Hom}_R(L, D) \otimes \{\mathrm{Hom}_R(N_i, D)\}_{i \in I}$$

Hence, a split short exact sequence of R-modules induces a split short exact sequence of abelian groups for every R-module D. In fact, the converse holds:

Exercise 2.6.1

Prove that if

$$0 \to \mathrm{Hom}_R(D, L) \to^{\psi'} \mathrm{Hom}_R(D, M) \to^{\varphi'} \mathrm{Hom}_R(D, N) \to 0$$

is exact for every R-module D, then

$$0 \to L \to^{\psi} M \to^{\varphi} N \to 0$$

is a split short exact sequence.

This implies that if the original homomorphism sequence is exact for every D, then it is in fact split exact for every D.

Proposition 2.6.7

Let P be an R-module. Then the following are equivalent:

- Let L, M, N form R-modules. If

  $$0 \to L \to^{\psi} M \to^{\varphi} N \to 0$$

  is a short exact sequence, then

  $$0 \to \mathrm{Hom}_R(P, L) \to^{\psi'} \mathrm{Hom}_R(P, M) \to^{\varphi'} \mathrm{Hom}_R(P, N) \to 0$$

  is a short exact sequence.
- Let M, N form R-modules. If

  $$M \to^{\varphi} N \to 0$$

  is exact, then every R-module homomorphism from P into N lifts to an R-module homomorphism into M, so the following diagram commutes:

  $$\begin{tikzcd} & P \arrow[dl, "\mu"'] \arrow[d, "\mathrm{Id}"] & \\ M \arrow[r, "\varphi"] & P \arrow[r] & 0 \end{tikzcd}$$

- If P is a quotient of the R-module M then P is isomorphic to a direct summand of P. That is, every short exact sequence

  $$0 \to L \to M \to P \to 0$$

  splits.
- P is a direct summand of a free R-module.

Definition 2.6.5: Projective Modules

An R-module ${}_RP$ is called **projective** if any module M that projects onto P has an isomorphic copy of P as a direct summand.

A projective module is merely one that satisfies any of the above equivalent conditions.

Corollary 2.6.1

Free modules are projective modules.

A finitely generated module is projective if and only if it is the direct summand of a finitely generated free module.

Every free module is a quotient of a projective module.

Example 2.6.5

Injective Modules

Of course we can also consider the reverse case– when do R-module homomorphisms from L or N to D exist?

We can see that an R-module map from N to D induces a map from M to D by composition by

$$\varphi' : \mathrm{Hom}_R(N, D) \to \mathrm{Hom}_R(M, D)$$
$$f \mapsto f' = f \circ \varphi$$

which is injective, and hence if the sequence

$$M \to^{\varphi} N \to 0$$

is exact, then

$$0 \to \mathrm{Hom}_R(N, D) \to^{\varphi'} \mathrm{Hom}_R(M, D)$$

is exact.

The reverse does not hold in general.

Example 2.6.6

Theorem 2.6.2

Let D, L, M, N form R-modules. If

$$0 \to L \to^{\psi} M \to^{\varphi} N \to 0$$

is exact, then

$$0 \to \mathrm{Hom}_R(N, D) \to^{\varphi'} \mathrm{Hom}_R(M, D) \to^{\psi'} \mathrm{Hom}_R(L, D)$$

is exact.

A homomorphism $f : L \to D$ lifts to a homomorphism $F : M \to D$ if and only if f is in the image of ψ'.

The sequence of homomorphisms is exact for all R-modules D if and only if

$$L \to^{\psi} M \to^{\varphi} N \to 0$$

is exact.

Hence the sequence

$$0 \to \mathrm{Hom}_R(N, D) \to^{\varphi'} \mathrm{Hom}_R(M, D) \to^{\psi'} \mathrm{Hom}_R(L, D) \to 0$$

is not a short exact sequence in general, as ψ' may not be surjective.

Of course, this sequence is exact if the original exact sequence is a split exact sequence (in which case the sequence of homomorphisms is a split exact sequence for every R-module D).

Exercise 2.6.2

If

$$0 \to \mathrm{Hom}_R(N, D) \to^{\varphi'} \mathrm{Hom}_R(M, D) \to^{\psi'} \mathrm{Hom}_R(L, D) \to 0$$

is exact for every R-module D, then

$$0 \to L \to^{\psi} M \to^{\varphi} N \to 0$$

is a split short exact sequence.

This implies that if the homomorphism sequence is exact for every D, then it is split exact for every D.

Proposition 2.6.8

Let Q be an R-module. Then the following are equivalent:

- Let L, M, N form R-modules. If

  $$0 \to L \to^{\psi} M \to^{\varphi} N \to 0$$

  is a short exact sequence, then

  $$0 \to \mathrm{Hom}_R(N, Q) \to^{\varphi'} \mathrm{Hom}_R(M, Q) \to^{\psi'} \mathrm{Hom}_R(L, Q) \to 0$$

  is also a short exact sequence.

- Let L, M form R-modules. If $0 \to L \to^{\psi} M$ is exact, then every R-module homomorphism from L to Q lifts to an R-module homomorphism of M into Q. That is, the following diagram commutes:

  $$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\psi"] \arrow[d, "f"'] & M \arrow[dl, "F"] \\ & Q & \end{tikzcd}$$

- If Q is a submodule of the R-module M, then Q is a direct summand of M. That is, every short exact sequence

  $$0 \to Q \to M \to N \to 0$$

  splits.

Definition 2.6.6: Injective Modules

An R-module ${}_RQ$ is called **injective** if for any module M that Q injects into, M has an isomorphic copy of Q as a direct summand.

Example 2.6.7

Unfortunately, there is not a nice equivalent to the direct summand of a free R-module condition from projective modules. Instead:

Proposition 2.6.9: Baer's Criterion

Let Q form an R-module. ${}_RQ$ is injective if and only if for every left ideal $I \triangleleft R$, any R-module homomorphism $g : I \to Q$ can be extended to an R-module homomorphism $G : R \to Q$.

If R is a PID, then Q is injective if and only if $rQ = Q$ for every nonzero $r \in R$. Hence, a $\mathbb{Z}$-module is injective if and only if it is divisible. When R is a PID, quotient modules of injective R-modules are injective.

Proof. ■

Corollary 2.6.2

Every $\mathbb{Z}$-module is a submodule of an injective $\mathbb{Z}$-module.

This can be useful to prove the more general statement:

Theorem 2.6.3

Let R be a ring and ${}_RM$ an R-module. Then M is contained in an injective R-module.

Flat Modules

Suppose D forms a right R-module. For every homomorphism $f : X \to Y$ of left R-modules, we obtain a homomorphism

$$1 \otimes f : D \otimes_R X \to D \otimes_R Y$$

of abelian groups. If D is also an (S, R)-bimodule, then $1 \otimes f$ is a homomorphism of left S-modules.

Theorem 2.6.4

Let D form a right R-module, and L, M, N form left R-modules. If

$$0 \to L \to^{\psi} M \to^{\varphi} N \to 0$$

is exact, then

$$D \otimes_R L^{1\otimes\psi} D \otimes_R M \to^{1\otimes\varphi} D \otimes_R N \to 0$$

is exact.

If D is an (S, R)-bimodule then the sequence of abelian groups is an exact sequence of left S-modules. Hence, if $S = R$ is commutative, then the sequence of abelian groups is an exact sequence of R-modules. The map $1 \otimes \varphi$ is not necessarily injective, so the sequence may not extend to a short exact sequence.

The sequence of abelian groups is exact for all right R-modules D if and only if

$$L \to^{\psi} M \to^{\varphi} N \to 0$$

is exact.

Proposition 2.6.10

Let A form a right R-module. Then the following are equivalent:

- Let L, M, N form left R-modules. If

  $$0 \to L \to^{\psi} M \to^{\varphi} N \to 0$$

  is a short exact sequence, then

  $$0 \to A \otimes_R L \to^{1\otimes\psi} A \otimes_R M \to^{1\otimes\varphi} A \otimes_R N \to 0$$

  is a short exact sequence.

- Let L, M be left R-modules, if

  $$0 \to L \to^{\psi} M$$

  is an exact sequence of left R-modules, then

  $$0 \to A \otimes_R L \to^{1\otimes\psi} A \otimes_R M$$

  is an exact sequence of abelian groups.

Definition 2.6.7

A right R-module ${}_RA$ is called **flat** if either of the above conditions hold.

Corollary 2.6.3

Free modules are flat. Moreover, projective modules are flat.

Example 2.6.8

Theorem 2.6.5

Let R, S be rings, left A form a right R-module, let B form an (R, S)-bimodule and let C form a right S-module. Then there is an isomorphism of abelian groups:

$$\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$$

If $R = S$ is commutative this is an isomorphism of R-modules with the standard R-module structures.

Corollary 2.6.4

If R is commutative then the tensor product of two projective R-modules is projective.

Chapter 3

Structure of Modules over Principal Ideal Domains

3.1 Fundamental Structure Theorems

Definition 3.1.1: Rank

Let R be an integral domain. The **rank** of an R-module ${}_R M$ is the maximum number of R-linearly independent elements of M.

In general, an R-module of finite rank may not have a basis– this only holds when the module is a free R-module.

Example 3.1.1

Proposition 3.1.1

Let R be an integral domain and let ${}_R M$ be a free R-module of rank $n < \infty$. Then any $n+1$ elements of M are R-linearly dependent:

$$\begin{aligned} \forall (y_1, y_2, \ldots, y_{n+1}) \in M^{n+1}\ \exists (r_1, r_2, \ldots, r_{n+1}) \neq (0, 0, \ldots, 0) \in \mathbb{R}^{n+1} &\text{ such that} \\ r_1 y_1 + r_2 y_2 + \ldots r_{n+1} y_{n+1} = 0&. \end{aligned}$$

In other words, the rank of a submodule of M is bounded by the rank of M.

Definition 3.1.2: Torsion Module

If R is an integral domain and ${}_R M$ an R-module, we define the **torsion module** to be the submodule of M given by

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

If $N \leq \mathrm{Tor}(M)$ is a submodule, then we say N is a **torsion submodule of** M.

If $\mathrm{Tor}(M) = 0$, then M is said to be **torsion free**.

Definition 3.1.3: Annihilator

For any submodule $N \leq M$ over a ring R, the **annihilator of** N is the ideal of R defined by

$$\mathrm{Ann}(N) = \{r \in R \mid rn = 0 \quad \forall n \in N\}.$$

If N is not a torsion submodule of M, then $\mathrm{Ann}(N) = 0$. If $N, L \leq M$ as submodules with $N \subset L$, then $\mathrm{Ann}(L) \subset \mathrm{Ann}(N)$.

Observe that if R is a PID and $N \subset L \subset M$ with $\mathrm{Ann}(N) = (a)$ and $\mathrm{Ann}(L) = (b)$, then $a \mid b$. Hence, the annihilator of any element $x \in M$ divides the annihilator of M.

Theorem 3.1.1

Let R be a Principal Ideal Domain, let ${}_RM$ be a free R-module of rank n, and let $N \leq M$ be a submodule. Then N is free with rank $m \leq n$, and there exists a basis $(y_1, y_2, \ldots, y_n) \in M^n$ so that

$$(a_1 y_1, a_2 y_2, \ldots, a_m y_m)$$

is a basis of N where $a_1, a_2, \ldots, a_m \in R$ are nonzero. Furthermore, they satisfy the divisibility relationship:

$$a_1 \mid a_2 \mid \ldots \mid a_m.$$

Proof. ■

Theorem 3.1.2: Fundamental Theorem of Invariant Factors

Let R be a PID and let ${}_RM$ be a finitely generated R-module.

- M is isomorphic to the direct sum of finitely many cyclic modules:

  $$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \ldots \oplus R/(a_m)$$

  for some $r \in \mathbb{N}$ and nonzero elements $a_1, a_2, \ldots, a_m$ of R which are nonunital and satisfy

  $$a_1 \mid a_2 \mid \ldots \mid a_m.$$

- M is torsion free if and only if M is free
- In the decomposition

  $$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \ldots \oplus R/(a_m)$$

  the torsion module is given by

  $$\mathrm{Tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \ldots \oplus R/(a_m)$$

  and hence M is a torsion module if and only if $r = 0$, in which case the annihilator of M is the ideal (a_m).

This decomposition is unique due to the divisibility condition.

Definition 3.1.4: Free Rank

The integer r in the decomposition of an R-module ${}_RM$ is called the **free rank** or **Betti number** of M and the elements $a_1, a_2, \ldots, a_m \in R$ are the **invariant factors** of M.

We can apply the Chinese Remainder Theorem here to decompose the cyclic modules into cyclic modules with simple annihilators.

Theorem 3.1.3: Fundamental Theorem of Elementary Divisors

Let R be a PID and let ${}_RM$ be a finitely generated R-module. Then

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha 2}) \oplus \ldots \oplus R/(p_t^{\alpha_t}$$

where $r \in \mathbb{N}$ and $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are positive powers of primes in R.

The prime powers $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are called the **elementary divisors**.

The elementary divisors of a module are unique.

Notice that the primes are not necessarily distinct. If we group together the distinct factors we can restate the theorem in a form that is also satisfied by infinitely generated modules.

Theorem 3.1.4: Primary Decomposition Theorem

LLet R be a PID and let ${}_RM$ be a nonzero torsion R-module with nonzero annihilator a. Suppose the factorization of a into distinct prime powers in R is

$$a = up_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$$

and let

$$N_i = \left\{x \in M \mid p_i^{\alpha_i}x = 0\right\}.$$

Then $N_i \leq M$ is a submodule with annihilator $p_i^{\alpha_i}$ and is the submodule of M of all elements annihilated by some power of p_i. Furthermore,

$$M = N_1 \oplus N_2 \oplus \dots \oplus N_n.$$

If M is finitely generated then each N_i is the direct sum of finitely many cyclic modules whose annihilators are divisors of $p_i^{\alpha_i}$.

We call the submodule N_i the p_i**-primary component of** M.

Notice that the elementary divisors of a finitely generated module M are the invariant factors of the primary components of $\mathrm{Tor}(M)$.

Lemma 3.1.1

Let R be a PID and let p be a prime in R. Let F denote the field $R/(p)$.

- If $M = R^r$, then $M/pM \cong F^r$.
- If $M = R/(a)$ with $a \in R$ nonzero, then if $p \mid a$

  $$M/pM \cong F$$

  Otherwise, $M/pM \cong 0$.
- If

  $$M = R/(a_1) \oplus R/(a_2) \oplus \dots \oplus R/(a_k)$$

  where $p \mid a_i$, then $M/pM \cong F^k$.

This is what gives us uniqueness. Tht is, two finitely generated R-modules are isomorphic if and only i they have the same free rank and lst of invariant factors (or elementary divisors).

Corollary 3.1.1

Let R be a PID and let M be a finitely generated R-module. The elementary divisors of M are the prime power factors of the invariant factors of M. Furthermore, the largest invariant factor of M is the product of the largest distinct prime powers among the elementary divisors of M.

In fact, the second largest invariant factor is the product of the largest of distinct prime powers among the remaining elementary divisors of M, and so on...

The Fundamental Theorem of Finitely Generated Abelian Groups follows directly from this by taking $R = \mathbb{Z}$.

3.2 Rational Canonical Form

Let V be a finite dimensional vector space over F with dimension n, and T a fixed linear transformation of V. Recall that we can view V as an $F[x]$-module where x acts on V as the linear transformation T.

Because V has finite dimension over F, it must be a torsion $F[x]$-module. Hence V is isomorphic as an $F[x]$-module to the direct sum of cyclic, torsion $F[x]$-modules.

When we decompose V into the invariant factor decomposition basis, we obtain the rational canonical form for the matrix for T. When we use the elementary divisor decomposition, we obtain the Jordan canonical form.

Definition 3.2.1: Minimal Polynomial

The **minimal polynomial of** T is the unique monic polynomial $m_T(x) \in F[x]$ that generates the ideal $\mathrm{Ann}(V)$ in $F[x]$.

Let A be a matrix. The **minimal polynomial of** T is the unique monic polynomial of smallest degree $m_A(x)$ that yields the zero matrix when evaluated at A.

The **rational canonical form** of the linear transformation T is the isomorphism

$$V \cong F[x]/(a_1(x)) \oplus F[x]/(a_2(x)) \oplus \ldots \oplus F[x]/(a_m(x))$$

where $a_1(x), a_2(x), \ldots, a_m(x)$ are polynomials in $F[x]$ of positive degree such that

$$a_1(x) \mid a_2(x) \mid \ldots \mid a_m(x)$$

Of course, the annihilator of V is the ideal $(a_m(x))$, and so we obtain:

Proposition 3.2.1

The minimal polynomial $m_T(x)$ is the largest invariant factor of V.

Observe that we can get a basis for the vector space $F[x]/(a(x))$ for a fixed

$$a(x) = x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0$$

by defining $\overline{x}^k = (x \pmod{a(x)})^k$. The basis is then $\left\{1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{k-1}\right\}$ which has an action under multiplication by x given by:

$$\begin{aligned} 1 &\mapsto \overline{x} \\ \overline{x} &\mapsto \overline{x}^2 \\ &\vdots \\ \overline{x}^{k-2} &\mapsto \overline{x}^{k-1} \\ \overline{x}^{k-1} &\mapsto \overline{x}^k = -b_0 - b_1\overline{x} - \ldots - b_{k-1}\overline{x}^{k-1} \end{aligned}$$

which follows because

$$\overline{x}^k + b_{k-1}\overline{x}^{k-1} + \ldots + b_1\overline{x} + b_0 = 0$$

This gives us a matrix for multiplication by x:

Definition 3.2.2: Companion Matrix

Let $a(x) = x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0$ be a monic polynomial in $F[x]$. The **companion matrix** of $a(x)$ is the $k \times k$ matrix representing the matrix for multiplication by x, and is of the form

$$\begin{pmatrix} 0 & 0 & \ldots & \ldots & -b_0 \\ 1 & 0 & \ldots & \ldots & -b_1 \\ 0 & 1 & \ldots & \ldots & -b_2 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & -b_{k-1} \end{pmatrix}$$

We denote the companion matrix of $a(x)$ by $\mathcal{C}_{a(x)}$.

Now we will apply this to each of the cyclic modules in the rational canonical form of V. Let $\mathcal{B}_i$ be the set of basis elements for each cyclic factor $F[x]/(a_i(x))$. The linear transformation T acts on $\mathcal{B}_i$ by the companion matrix for $a_i(x)$, and hence the union $\mathcal{B} = \cup_i \mathcal{B}_i$ and the matrix of the transformation on V is the direct sum of the companion matrices.

Definition 3.2.3: Rational Canonical Form

A matrix is said to be in **rational canonical form** if it is the direct sum of companion matrices for monic polynomials $a_1(x), \ldots, a_m(x)$ with

$$a_1(x) \mid a_2(x) \mid \ldots \mid a_m(x).$$

The matrix is then of the form

$$\begin{pmatrix} \mathcal{C}_{a_1(x)} & & & \\ & \mathcal{C}_{a_2(x)} & & \\ & & \ddots & \\ & & & \mathcal{C}_{a_m(x)} \end{pmatrix}.$$

The polynomials are called the **invariant factors** of the matrix, and the matrix is said to be a **block diagonal matrix** with the blocks being the companion matrices for $a_i(x)$.

A **rational canonical form** for a linear transformation T is a matrix representing T in rational canonical form.

One can check that every linear transformation T has a rational canonical form that is unique.

Theorem 3.2.1: Rational Canonical Form for Linear Transformation

Let V be a finite dimensional vector space over the field F and let T be a linear transformation of V. Thne there is a basis for V and the matrix of T is in rational canonical form with respect to this basis. Furthermore, the rational canonical form for T is unique.

We will see that this exists for every T, but Jordan canonical form may not.

For linear transformations S and T, the following are equivalent:

- S and T are similar linear transformations
- The $F[x]$-modules obtained from V via S, T are isomorphic
- S and T have the same rational canonical form

Of course, any matrix can be translated into a rational canonical form, as each matrix corresponds to a linear transformation. The **invariant factors** of an $n \times n$ matrix over a field F are the invariant factors of its rational canonical form.

Lemma 3.2.1

Let $a(x) \in F[x]$ be any monic polynomial. The characteristic polynomial of the companion matrix of $a(x)$ is $a(x)$, and if M is given by

$$M = \begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k \end{pmatrix}$$

then the characteristic polynomial of M is the product of the characteristic polynomials of $A_1, A_2, \dots, A_k$.

Theorem 3.2.2: Cayley-Hamilton Theorem

Let A be an $n \times n$ matrix over the field F. The minimal polynomial of A divides the characteristic polynomial of A.

In fact, the characteristic polynomial of A divides some power of the minimal polynomial of A.

Theorem 3.2.3

Let A be an $n \times n$ matrix over the field F. The $n \times n$ matrix $xI - A$ can be put into the diagonal form

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & a_1(x) & & \\ & & & & \ddots & \\ & & & & & a_m(x) \end{pmatrix}$$

with monic nonzero elements

$$a_1(x) \mid a_2(x) \mid \dots \mid a_m(x).$$

via the operations

- interchanging two rows or columns
- adding a multiple of one row or column to another
- multiplying any column or row by a unit in $F[x]$

The elements $a_1(x), \dots, a_m(x)$ are the invariant factors of A.

Invariant Factor Decomposition Algorithm

Converting an $n \times n$ Matrix to Rational Canonical Form

3.3 Jordan Canonical Form

Of course, we can create a similar representation of elementary divisors, which we will refer to as the Jordan canonical form. Unlike invariant factors however, we have to make an additional assumption– the field F contains all the eigenvalues of the linear transformation T. This is equivalent to assuming all plynomials factor completely into linear factors.

It follows that V is a direct sum of finitely many cyclic $F[x]$-modules of the form $F[x]/(x-\lambda)^k$.

We will choose as our basis

$$\left\{(\overline{x}-\lambda)^{k-1}, (\overline{x}-\lambda)^{k-2}, \dots, \overline{x}-\lambda, 1\right\}$$

in the quotient $F[x]/(x-\lambda)^k$. Then the linear transformation of multiplication by x acts as follows:

$$\begin{aligned}(\overline{x}-\lambda)^{k-1} &\mapsto \lambda(\overline{x}-\lambda)^{k-1}+(\overline{x}-\lambda)^k = \lambda(\overline{x}-\lambda)^{k-1}\\ (\overline{x}-\lambda)^{k-2} &\mapsto \lambda(\overline{x}-\lambda)^{k-2}+(\overline{x}-\lambda)^{k-1}\\ &\vdots\\ \overline{x}-\lambda &\mapsto \lambda(\overline{x}-\lambda)+(\overline{x}-\lambda)^2\\ 1 &\mapsto \overline{x}\end{aligned}$$

This linear map has a corresponding matrix, of course.

Definition 3.3.1: Jordan Blocks

The $k\times k$ **elementary Jordan matrix with eigenvalue** λ is the $k\times k$ matrix corresponding to the linear transformation of multiplication by x on the Jordan canonical basis:

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

We refer to a matrix of this form as a **Jordan block**.

We can apply this to each of the cyclic factors of V in its elementary divisor decomposition to obtain a basis for V, with respect to which the matrix for T has a special form.

Definition 3.3.2: Jordan Canonical Form

A matrix is in **Jordan canonical form** if it is of the form

$$\begin{pmatrix}J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_t\end{pmatrix}$$

where J_i are Jordan blocks.

The linear transformation T is in Jordan canonical form with respect to the elementary divisor basis.

Theorem 3.3.1

Let V be a finite dimensional vector space over F and T a linear transformation of V. If F contains all the eigenvalues of T, then there is a basis for V with respect to which the matrix for T is in Jordan canonical form. Furthermore, this matrix is unique up to permutation.

Corollary 3.3.1

If a matrix A is similar to a diagonal matrix D, then D is the Jordan canonical form. Hence, two diagonal matrices are similar if and only if their diagonal entries are the same up to permutation.

Corollary 3.3.2

If A is an $n\times n$ matrix with entries from F, and F contains all the eigenvalues of A, then A is similar to a diagonal matrix over F if and only if the minimal polynomial of A has no repeated roots.

Example 3.3.1

Changing from one canonical field to another

Elementary Divisor Decomposition Algorithm

Converting an $n \times n$ matrix to Jordan canonical form

Chapter 4

Group Representation Theory

4.1 Ties to Group Representation Theory

If, when taking an R-module M, we may work over a field K and modify $M = V$ to be a K-vector space by $K \times V \to V$. This then gives us that an R-module over V is a pair V with $R \times V \to V$.

Definition 4.1.1: Group Module

Let G be a group. We say that a K-vector space V is a G-**module** if it comes equipped with a G-action map

$$G \times V \to V \quad (g, v) \mapsto g * v := gv$$

compatible with operations of G and V :

(a). $e_G v = v$

(b). $(gh)v = g(hv)$

(c). $g(v + w) = gv + gw$

(d). $g(\lambda v) = \lambda(gv)$

for all $g, h \in G$, $v \in V$, $\lambda \in K$.

If one is given a G-module V, then there is a natural group homomorphism

$$\begin{aligned} \rho : G &\to \mathrm{End}_K(V) \\ g &\mapsto [\rho g : V \to V,\ v \mapsto g * v := gv] \end{aligned}$$

The image of ρ is inside of $GL(V)$.

Definition 4.1.2

A K-**linear representation of a group** G is a K-vector space V equipped with a group homomorphism $\rho : G \to GL(V)$.

Definition 4.1.3

Given a representation of a group G, $(V : \rho)$, its **degree** is $\mathrm{dim}V$.

Note that when $\mathrm{dim}_K V = n$, we get that

$$GL(V) \cong GL_n(K)$$

as groups.

Representations of G of degree n over a field K are congruent to group homomorphisms $\rho : G \to GL_n(K)$.

Definition 4.1.4

For any group G, the **trivial representation of** G **over** K is $(V = K, \rho : G \to GL_1(K) = K^\times)$ given by $g \mapsto 1_K$ for all $g \in G$.

Definition 4.1.5

Let $\rho : G \to GL(V)$ and $\rho' : G \to GL(V')$ be two representatives of a group G. We say that p and p' are **equivalent** or isomorphic if there exists an invertible linear transformation

$$\tau : V \to V'$$

so that τ **intertwines** with action of G :

$$\tau(\rho g(v)) = \rho' g(\tau(v)) \quad \forall g \in G, v \in V$$

Remark 4.1.1

$\rho : G \to GL_n(K)$ and $\rho' : G \to GL_{n'}(K)$ are equivalent if and only if $n = n'$ and $\exists T \in GL_n(K)$ such that $T\rho(g)T^{-1} = \rho'(g)$ for all $g \in G$.

This notion will be captured more clearly later with homomorphism/isomorphisms.

4.2 Subrepresentations and Irreducibility

Let K be a field and G a group. Recall that if $\dim_K V = n$, we can identify the group $GL(V)$ with $GL_n(K)$, the group of invertible K-linear operators on V under composition.

Definition 4.2.1: Subrepresentations

Let $\rho : G \to GL(V)$ be a representation of G. Suppose that W is a subspace of V which is G-invariant. That is, for all $w \in W$, $g \in G$, it holds that $\rho_g(w) \in W$. Then W becomes a representation of G and we say that

$$(W, \rho w : G \to GL(W))$$
$$g \mapsto [\rho_g \mid W : W \to W \quad w \mapsto \rho_g(w)]$$

is a **subrepresentation** of (V, ρ).

Definition 4.2.2

The **direct sum** of two representations of G, (V', ρ'_V) and (V'', ρ''_V) is the representation of G given by:

$$(V := V' \bigoplus V'', \rho_{V' \bigoplus V''} : G \to GL(V))$$
$$g \mapsto \left[\rho_g : V \to V \quad v = v' + v'' \mapsto \rho'_g(v') + \rho''_g(v'')\right]$$

If we fix a basis for both V' and V'', then their union is a basis of $V = V' \bigoplus V''$.

Definition 4.2.3: Irreducible

A representation is called **irreducible** if it contains no proper subrepresentations– otherwise it is called **reducible**. A representation is called **completely reducible** if it decomposes as a direct sum of irreducible subrepresentations.

Irreducible representations will turn out to be the building blocks of group representation theory. This is complemented by Mascinke's Theorem, which will state that every $\mathbb{C}$-linear representation of a finite group G of finite degree is completely reducible.

4.3 Complete Reducibility

Recall that the **characteristic** of a field K is the smallest positive integer p such that $p1_K = 0$. If p exists, then it is prime; else we say K has characteristic 0.

Theorem 4.3.1

Let (V, ρ) be a representation of a finite group G of finite degree n over a field K of characteristic p with $p \not| |G|$. If W is a subrepresentation of (V, ρ), then there exists another subrepresentation W' of V so that

$$V \cong W \bigoplus W'$$

as K-vector spaces. We refer to W' as the **complement** of the subrepresentation W of (V, ρ).

Corollary 4.3.1: Maschke's Theorem

Let V be a representation of a finite group G of finite degree over a field of characteristic p with $p \not| |G|$. Then V is completely reducible.

This can be proven by induction on $\dim V$. Note that this fails for infinite groups.

4.4 G-homomorphisms

Let K be a field and G be a group. We are going to look at a structure of interest: we define K-linear representations of G as a K-vector space V equipped with a group homomorphism

$$\rho : G \to GL(V)$$
$$g \mapsto [\rho g : V \to V]$$

Definition 4.4.1: G-homomorphism

Let (V', ρ') and (V'', ρ'') be representations of G over K. A G-**homomorphism from** (V', ρ') **to** $V'', \rho'')$ is a K linear map $\varphi : V' \to V''$ which intertwines with the action of G :

$$\varphi(\rho' g(v')) = \rho'' g(\varphi(v')) \quad \forall g \in G, v' \in V'$$

We denote the collection of G-homomorphisms from (V', ρ') to (V'', ρ'') by $\mathrm{Hom}_G(V', V'')$, and $\mathrm{End}_G(V') := \mathrm{Hom}_G(V', V')$. Finally, a G-**isomorphism** is an invertible G-homomorphism.

This is really just a change in basis.

Proposition 4.4.1

If $\varphi \in \mathrm{Hom}_G(V, W)$, then $\varphi^{-1} \in \mathrm{Hom}_G(W, V)$.

Proposition 4.4.2

Take $\varphi \in \mathrm{Hom}_G(V, W)$. Then

(a). $\mathrm{Ker}\varphi$ is a subrepresentation of V, and

(b). $\mathrm{Im}\varphi$ is a subrepresentation of W.

For the rest of the section, we take $K = \mathbb{C}$.

Lemma 4.4.1: Schur's Lemma

Let (V, ρ) be an irreducible representation of G. If $\varphi \in \mathrm{End}_G(V)$, then φ is a scalar multiple of $\mathrm{Id}V$:

$$\exists \lambda \in \mathbb{C}\ s.t.\ \varphi(v) = \lambda v \quad \forall v \in V$$

This result has many applications.

Theorem 4.4.1

All nonzero complex irreducible representations of an abelian group G have degree 1.

Using these tools, we now can complete a few problems.

Exercise 4.4.1

Given a finite abelian group G, describe its irreducible representations, up to equivalence. Illustrate this for the Klein-four group $G = C_2 \times C_2$.

Moreover, one can apply Schur's lemma to complete the following problem:

Exercise 4.4.2

Let V and W be irreducible representations of G, and take $\varphi \in \mathrm{Hom}_G(V, W)$. Show that

(a). If $V \ncong W$, then φ is the zero map.

(b). If $V \cong W$ and $\varphi \neq 0$, then φ is a G-isomorphism.

4.5 Character Theory

Character theory will serve as a very convenient bookkeeping tool for representations of G when G is finite. We still keep $K = \mathbb{C}$.

Definition 4.5.1

Let (V, ρ) be a $\mathbb{C}$-representation of G of finite degree n. Choose any basis of V and express ρ_g as a matrix in $GL_n(\mathbb{C})$, for all $g \in G$. The **character of** (V, ρ), denoted X_V is the function

$$\begin{aligned} X_V &: G \to \mathbb{C} \\ g &\mapsto \mathrm{Tr}(\rho g) \end{aligned}$$

We say that X_V is **irreducible** if (V, ρ) is irreducible.

It turns out that characters detect irreducibility. Let X_V, ψ_W be given. We define a scalar by

$$\langle X_V, \psi_W \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{X_V(g)} \psi_W(g).$$

Proposition 4.5.1

Let V be a representation of G. Then

$$V \text{ is irreducible} \iff \langle X_V, X_V \rangle = 1.$$

Of course, we need to be sure that our construction of characters is well-defined. It turns out that they capture the properties of our representation well and are unique.

Proposition 4.5.2

1. The definition of X_V is independent of choice of basis of V
2. If $V \cong W$, then $X_V = X_W$
3. If $g, h \in G$ are conjugate, then $X_V(g) = X_V(h)$

Definition 4.5.2

The **character table** of G is defined as

$$\begin{bmatrix} X_{V_1}(g_1) & X_{V_1}(g_2) & \dots & X_{V_1}(g_k) \\ \vdots & & & \vdots \\ X_{V_\ell}(g_1) & X_{V_\ell}(g_2) & \dots & X_{V_\ell}(g_k) \end{bmatrix}$$

The number of irreducible characters of G is the same as the number of conjugacy classes of elements of G. Furthermore, the character table is a square matrix with entries in $\mathbb{C}$ when the rows are indexed by irreducible representations of G and the columns are indexed by conjugacy classes representations of elements of G.

In this case, $(X_{V_i}(g_j))$ is an invertible matrix.

Proposition 4.5.3

Let (V, ρ) be a representation of G, and take $g \in G$. Then

1. $X_V(e) = \dim(V)$
2. $X_V(g)$ is a sum of roots of unity
3. $X_{V \oplus W}(g) = X_V(g) + X_W(g)$
4. $X_V(g^{-1}) = \overline{X_V(g)}$
5. $\overline{X_V}$ is a character of G

Let $X_1, \dots, X_r$ be irreducible characters of a finite group G. Define

$$\langle X_i, X_j \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{X_i(g)} X_j(g)$$

Theorem 4.5.1

1. $\langle X_i, X_j \rangle = \delta_{ij}$
2. $$\sum_{i=1}^{r} \overline{X_i(x)} X_i(y) = \begin{cases} |C_G(x)| & x, y \text{ conjugate in } G \\ 0 & \text{otherwise} \end{cases}$$

Here, $C_G(x)$ is the centralizer of $x \in G$, that is, $C_G(x) = \mathrm{Stab}_x(G) = \{g \in G \mid gxg^{-1} = x\}$.

Theorem 4.5.2

If V, W are irreducible representations of G, then

$$\begin{aligned}\langle X_V, X_V\rangle &= 1\\ \langle X_V, X_W\rangle &= 0 \text{ when } V \ncong W\end{aligned}$$

This shows us that characters completely determine representations, and forthermore characters completely determine irreducibility.