MAS8091: MMath Project

Nathan Dixon
Supervisor: Professor Peter Jørgensen

2014/2015

Chapter 0

Abstract

The aim in this report is to present the necessary theory of modules in order to consider exact sequences. This involves motivating module theory through vector spaces, before considering homomorphisms of modules. One is then able to construct a 'Hom' functor which maps module homomorphisms to module homomorphisms. If

$$\begin{array}{ccc} A & & \\ \downarrow{\scriptstyle \varphi} & & \\ M & \xrightarrow{\mu} & N \end{array}$$

then there is an induced homomorphism

$$\mathrm{Hom}(A, M) \to \mathrm{Hom}(A, N).$$

This induced homomorphism can then be used, along with an exact sequence, to construct further exact sequences. In particular

$$0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0$$

induces

$$0 \to \mathrm{Hom}(A, X) \xrightarrow{f_*} \mathrm{Hom}(A, Y) \xrightarrow{g_*} \mathrm{Hom}(A, Z).$$

Contents

Chapter 1

Introduction

To begin this discussion the rudimentary ideas from vector theory will be recalled. These ideas will result in the consideration of the concepts of a ring and module, where the endeavour will be to construct a generalisation of such vector notions. From here the integers will be discussed, with particular emphasis on the properties underlying the set which leads to a *ring structure*. This report aims to introduce module theory in the sense of introducing the Hom functor for R–modules.

1.1 Vector Spaces

The motivation for module theory is the generalisation of vector spaces. In order to construct a framework for module theory it is important for one to first consider the mathematics behind vectors and vector spaces. It is entirely true that this report could have been constructed without any of this preliminary discussion, but the aim in doing so is to provide an insight in to the subsequent theory.
In the most basic sense one regards a **vector** as an element in a collection of objects which may be *added together* or *scaled*, in such a way that they adhere to certain conditions (or axioms). Under these rules, the collection is then the underlying **vector space**. Of course this is a somewhat minor consideration and must be formulated in a more rigorous routine. The information presented on vector spaces is inspired by Anton and Rorres. For further literature, the reader is referred to [**AR**].

Definition 1.1.1 (Vector Space and Vectors)**.** Consider an arbitrary (and non-empty) collection of objects V for which the following operations are defined

$$V \times V \to V; (\mathbf{v_1}, \mathbf{v_2}) \mapsto \mathbf{v_1} + \mathbf{v_2},$$
$$R \times V \to V; (r, \mathbf{v}) \mapsto r \cdot \mathbf{v} = r\mathbf{v}.$$

If the subsequent axioms are satisfied then we refer to V as a **vector space**, and elements from V as **vectors**.

Axioms (For a Vector Space)**.**

(I) For all $\mathbf{u}$ and $\mathbf{v}$ in V, then $\mathbf{u} + \mathbf{v} \in V$.

(II) For all $\mathbf{u}, \mathbf{v} \in V$ then $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.

(III) For all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ then $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$.

(IV) There is a zero vector, $\mathbf{0}$, in V for which $\mathbf{0} + \mathbf{u} = \mathbf{u} + \mathbf{0} = \mathbf{u}$ for any $\mathbf{u} \in V$.

(V) For each element $\mathbf{u} \in V$ there exists an element $-\mathbf{u}$ such that $\mathbf{u} + (-\mathbf{u}) = (-\mathbf{u}) + \mathbf{u} = \mathbf{0}$.

(VI) If r is any scalar, and $\mathbf{u}$ is an object of V, then $r\mathbf{u} \in V$.

(VII) For $1 \in R$ and $\mathbf{u} \in V$ then $1\mathbf{u} = \mathbf{u}$.

(VIII) For $r, s \in R$ and $\mathbf{u} \in V$ then $r(s\mathbf{u}) = (rs)\mathbf{u}$.

(IX) For $r, s \in R$ and $\mathbf{u} \in V$ then $(r+s)\mathbf{u} = r\mathbf{u} + s\mathbf{u}$.

(X) For all $r \in R$ and $\mathbf{u}, \mathbf{v} \in V$ then $r(\mathbf{u}+\mathbf{v}) = r\mathbf{u} + r\mathbf{v}$.

Remark 1.1.2. Note that in Definition 0.1.1, R typically represents the set of complex (or real) numbers.

Generalising the Notion of Vectors

Having seen the theory in the case of vectors and vector spaces, one may look to generalising this to the more abstract case. This will involve the notion of module theory, and will require an understanding of **rings, fields** and **modules.** From this point of view one can then begin to think of taking scalars from a generalised version of $\mathbb{C}$ (which is a ring) and further take 'vectors' from a module. Precisely how one views a ring can be seen by considering the integers - the canonical set with a ring structure.

Example 1.1.3 (The Integers)**.** The integers are one of the most recognisable sets in mathematics. There are two binary compositions defined on this set, referred to as plus and times (*or* addition and multiplication) respectively; $(+, \cdot)$. The first thing to note is that $\mathbb{Z}$ is **closed** under these operations. That is, for any two integers z_1, z_2 then $z_1 + z_2, z_1 \cdot z_2 \in \mathbb{Z}$. Furthermore, elements are **commutative over addition**; for $z_1, z_2 \in \mathbb{Z}$

$$z_1 + z_2 = z_2 + z_1.$$

Elements also satisfy **additive and multiplicative associativity**. In other words, the order of the parentheses are irrelevant in computations: for $z_1, z_2, z_3 \in \mathbb{Z}$

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$
$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3).$$

There are also **additive and multiplicative identities**, 0 and 1 respectively, such that for $z \in \mathbb{Z}$

$$z + 0 = 0 + z = z$$
$$1 \cdot z = z.$$

Of course there are also **additive inverses**. This means that for each $z \in \mathbb{Z}$ one can find an element $-z \in \mathbb{Z}$ such that

$$z + (-z) = 0 = (-z) + z.$$

One final property to discuss is the **left and right distributivity of multiplication over addition**. Quite simply, this means that for the elements $z_1, z_2, z_3 \in \mathbb{Z}$ then

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$$
$$(z_1 + z_2) \cdot z_3 = z_1 \cdot z_3 + z_2 \cdot z_3.$$

This is by no means an exhaustive list of properties of the integers. For example, $\mathbb{Z}$ is **commutative with respect to multiplication**. That is $z_1, z_2 \in \mathbb{Z}$ implies we have $z_1 \cdot z_2 = z_2 \cdot z_1$. In the interest of context, this report is concerned only with the aforementioned properties.

The discussed properties of $\mathbb{Z}$ cause it to have a **ring** structure. Precisely what this means shall be discussed in the next chapter.

Chapter 2

Rings and Modules

The material presented on rings and fields uses the literature of Ellis [**ELL**].

2.1 Rings

A ring is simply another mathematical object or structure subject to specific axioms. Intuitively, one may think of a ring as being a generalisation of a scalar set. That is, they can be regarded as sets with binary operations defined in a very natural way which somehow extend those defined on the integers.
In the basic sense a ring R, is an abelian group with extra multiplicative constraints. Note that this report will only consider a ring with an identity element. This is not consistent throughout the available literature. For example, Ellis [**ELL**], considers a ring in the same regard as this report without the inclusion of the identity element.

Definition 2.1.1 (Ring)**.** A set R is called a **ring** if it has two binary compositions

$$\begin{aligned}(+) : R \times R &\to R \\ (x, y) &\mapsto x + y, \\ (\cdot) : R \times R &\to R \\ (x, y) &\mapsto x \cdot y,\end{aligned}$$

and satisifies the following axioms for all x, y, z in R.

Axioms (For a Ring)**.**

(I) $x + y = y + x$,

(II) $(x + y) + z = x + (y + z)$,

(III) $0_R + x = x = x + 0_R$,

(IV) For all x there is an element $-x$ such that $x + (-x) = 0_R = (-x) + x$,

(V) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(VI) $1_R \cdot x = x = x \cdot 1_R$,

(VII) $x \cdot (y + z) = x \cdot y + x \cdot z$,

(VIII) $(y + z) \cdot x = y \cdot x + z \cdot x$.

Convention 2.1.2 (Multiplication)**.**

- It is typical to denote the additive and multiplicative identities of a ring by 0 and 1 respectively This is in analogy to $\mathbb{Z}$.

- In working with multiplication, one typically suppresses the $(\cdot)$ notation where no confusion may arise.
- It has already been stated (Example 0.1.3) that the integers are commutative. If a ring is to be called **commutative** then this will be with respect to multiplication.

2.1.1 Fields

Definition 2.1.3 (Field)**.** A ring R which has **mutliplicative inverses** for all non-zero elements is called a **skew field**. That is each $x \in R \setminus \{0\}$ satisfies

$$xx^{-1} = 1_R = x^{-1}x,$$

for some $x^{-1} \in R \setminus \{0\}$. This is the **inverse** of x. Furthermore R is called a field if it is a *commutative skew field*.

Example 2.1.4 (Fields)**.** The sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. It is well known that all non-zero elements of these sets are invertible. It is also understood that they are commutative.

2.2 Modules

It is now possible to generalise the notion of a vector field with that of a module. This is much the same as in the case of vectors with the major difference that scalar factors can be taken from any set with the ring structure. The bulk of the material presented on modules has been taken from the literature of Hilton and Stammbach [**HS**], with further explanation given on certain results and examples.

Definition 2.2.1 (R–module)**.** A set M is an R–module if there are two binary operations (addition and *scalar* multiplication)

$$\begin{aligned} M \times M &\to M \\ (m_1, m_2) &\mapsto m_1 + m_2, \\ R \times M &\to M \\ (r, m) &\mapsto r \cdot m = rm, \end{aligned}$$

defined on the set together with the element 0_M, subject to the axioms for a module. Note that R is a ring.

Axioms (For an R–Module)**.** For all $m, m_1, m_2, m_3 \in M$ and $r, s \in R$

(I) $m_1 + m_2 = m_2 + m_1$,

(II) $m_1 + (m_2 + m_3) = (m_1 + m_2) + m_3$,

(III) $m + 0_M = m = 0_M + m$,

(IV) For each m there is an element $-m$ such that $m + (-m) = 0_M = (-m) + m$,

(V) $1_R \cdot m = m$,

(VI) $r \cdot (s \cdot m) = (r \cdot s) \cdot m$,

(VII) $(r + s) \cdot m = r \cdot m + s \cdot m$,

(VIII) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.

Example 2.2.2 (R^n)**.** One of the most easily constructed modules is the set of $n \times 1$ column vectors, where entries are taken from a ring R. That is

$$M = R^n = \left\{ \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} \mid r_i \in R \right\},$$

is an R–module. It is necessary to define two binary operations for elements of this set. This can be achieved by taking addition and scalar multiplication componentwise, i.e.

(i) *Addition*

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} \underbrace{+}_{\text{in } M} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \stackrel{\text{def}}{=} \underbrace{\begin{pmatrix} r_1 + s_1 \\ r_2 + s_2 \\ \vdots \\ r_n + s_n \end{pmatrix}}_{\text{in } R}$$

(ii) *Scalar Multiplication*

$$r \cdot \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} r \cdot r_1 \\ r \cdot r_2 \\ \vdots \\ r \cdot r_n \end{pmatrix}$$

This defines a module almost vacuously - the entries are each from a ring, and consequently satisfy all module axioms.

The subsequent example indicates further rings (the details are omitted).

Example 2.2.3 (Rings)**.** The following are rings, as described.

- The set of $n \times n$ matrices with complex entries is a ring.

$$M_n(\mathbb{C}) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mid a_{ij} \in \mathbb{C}, \forall i, j \in \{1, \ldots, n\} \right\}.$$

  It is not difficult to check that this is a ring. In much the same way as R^n, it follows from the fact that entries come from $\mathbb{C}$ (which is a ring).

- The set of polynomials over the field $\mathbb{C}$. Note that $\mathbb{C}$ could be replaced with any field.

$$\mathbb{C}[X] = \{p(X) = p_0 + p_1 X + \cdots + p_m X^m \mid p_i \in \mathbb{C}, \forall i = 0, 1, \ldots, m\}.$$

- The set of remainders modulo n is a ring.

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

  Here, the binary operations are given by ordinary $(+, \cdot)$ modulo n.

Example 2.2.4 ($\mathbb{Z}_n$ as a Field)**.** It is entirely possible that $\mathbb{Z}_n$ is a **field**. If n is prime then all elements permit inverses and so one may say that $\mathbb{Z}_p$ is a field for any prime p. In particular,

- $\mathbb{Z}_4$ is a ring. The element $2 \in \mathbb{Z}_4$ is not invertible. If it was then it would be required that $2z = 1$. This cannot be true since any multiple will be even. Since there is (at least) one element which is not invertible then this cannot be a field.
- $\mathbb{Z}_2$ is a field. This is the set $\mathbb{Z}_2 = \{0, 1\}$. The only non-zero element 1, and this element is its own inverse. Whence all non-zero elements are invertible.

Proposition 2.2.5 (Abelian Groups as Modules)**.** *If $(M, +)$ is an abelian group it is possible to construct a binary operation*

$$\begin{aligned}(\cdot) : \mathbb{Z} \times M &\to M \\ (z, m) &\mapsto z \cdot m,\end{aligned}$$

such that M with $(+, \cdot)$ is a $\mathbb{Z}$–module.

Proof. Define $(\cdot)$ as follows:

$$z \cdot m = \begin{cases} \overbrace{m + m + \cdots + m}^{z \text{ times}} & \text{if } z > 0, \\ 0_M & \text{if } z = 0, \\ \underbrace{(-m) + (-m) + \cdots + (-m)}_{-z \text{ times}} & \text{if } z < 0. \end{cases}$$

One is required to check that this produces a $\mathbb{Z}$–module. It is clear that the axioms specific to $+$ are satisfied because $(M, +)$ is an abelian group. This means that one need only check the axioms specific to $(\cdot)$. It is obvious that

$$1_{\mathbb{Z}} \cdot m \stackrel{\text{def}}{=} m.$$

Next $r \cdot (s \cdot m) = (r \cdot s) \cdot m$. This is trivial if either $r = 0$ or $s = 0$. The remaining cases can be split into four:

- r is positive, s is positive;
- r is positive, s is negative;
- r is negative, s is positive;
- r is negative, s is negative.

In each of these cases then s is permitted to take any non-zero value. If we focus specifically on positive r and s.

$$\begin{aligned} r(sm) &\overset{\text{def}}{=} r \cdot \overbrace{(m + \cdots + m)}^{s \text{ times}} \\ &\overset{\text{def}}{=} \underbrace{\overbrace{[m + \cdots + m]}^{s \text{ times}} + \cdots + \overbrace{[m + \cdots + m]}^{s \text{ times}}}_{r \text{ times}} \\ &= \underbrace{m + \cdots + m}_{rs \text{ times}} \\ &\overset{\text{def}}{=} (rs)m. \end{aligned}$$

One can check the remaining cases in a similar way.
Now we check that $(r+s)m = rm + sm$. Again this has multiple possibilities. Consider $r+s$ to be negative only.

- r and s are both negative.
  When this is the case, the definitions of the binary operations result in $(r+s)m$ being $|r|+|s|$ copies of $(-m)$. This corresponds to the expression $rm + sm$.
- $r+s$ is negative, but (without loss of generality) $r > 0 > s$. Notably, this means $|s| > |r|$.
  Proceed by writing $s = -r - t = -(t+r)$.

$$\begin{aligned} (r+s)m = (-t)m &= \overbrace{(-m) + \cdots + (-m)}^{t \text{ times}} \\ &\equiv \underbrace{m + \cdots + m}_{r \text{ times}} + \underbrace{[(-m) + \cdots + (-m)]}_{r \text{ times}} + \underbrace{(-m) + \cdots + (-m)}_{t \text{ times}} \\ &\equiv \underbrace{m + \cdots + m}_{r \text{ times}} + \underbrace{(-m) + \cdots + (-m)}_{r+t=-s \text{ times}} \\ &= rm + sm. \end{aligned}$$

  The remaining cases are checked via the same methodology.

The final axiom requires $r(m_1 + m_2)$ to be equal to $rm_1 + rm_2$. If r is zero this is trivial. If it is non-zero then the result follows by repeating a similar process which showed $r(sm) = (rs)m$. □

Example 2.2.6. Let K be a $\mathbb{Z}_n$-module and $k \in K$ then

$$\underbrace{k + k + \cdots + k}_{n\text{-times}} = 0$$

Note that $k = 1_{\mathbb{Z}_n} \cdot k$. The distributive laws give

$$\begin{aligned} k + k + \cdots + k &= 1_{\mathbb{Z}_n} \cdot k + 1_{\mathbb{Z}_n} \cdot k + \cdots + 1_{\mathbb{Z}_n} \cdot k \\ &= (1_{\mathbb{Z}_n} + 1_{\mathbb{Z}_n} + \cdots + 1_{\mathbb{Z}_n}) \cdot k \\ &= 0_{\mathbb{Z}_n} \cdot k \\ &= 0 \in K. \end{aligned}$$

Proposition 2.2.7. *If M is any $R-$module and $m \in M$ then*

$$0_R \cdot m = 0_M.$$

Proof. Set $y = 0_R \cdot m$, then $y + y = (0_R + 0_R)m = 0_R m = y$. Composing from the right with $-y$ gives

$$\begin{aligned} y + y + (-y) &= y + (-y) \\ y + (y - y) &= 0_M \\ y + 0_M &= 0_M \\ y &= 0_M. \end{aligned}$$

That is $0_R \cdot m = 0_M$. □

Example 2.2.8 (Complex Modules)**.** Let M be a non-zero $\mathbb{C}-$module. One may view M as an $\mathbb{R}$, $\mathbb{Q}$ or $\mathbb{Z}$ module, but not as a $\mathbb{Z}_n-$module.
Firstly the only axioms which are specific to the ring $\mathbb{C}$ concern the binary composition

$$\begin{aligned} \mathbb{C} \times M &\to M, \\ (r, m) &\mapsto r \cdot m. \end{aligned}$$

This defines multiplication by a complex scalar. If one next notes that

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}, \tag{1}$$

then this property affords itself to a very natural binary composition. Let this be

$$\begin{aligned} R \times M &\to M \\ (s, m) &\mapsto s \cdot m, \end{aligned}$$

where R corresponds to any of the sets of numbers in (1). In particular one may view any element s (of R) as corresponding to the complex number $s + 0i$. The new scalar multiplication is simply taken to be that which is already defined for $s + 0i$.
This is not possible for $\mathbb{Z}_n$ because addition of complex numbers does not restrict to addition in $\mathbb{Z}_n$. Consider M as a $\mathbb{C}-$module, then

$$\begin{aligned} \underbrace{m + \cdots + m}_{n \text{ times}} &= \underbrace{1_{\mathbb{C}} m + \cdots + 1_{\mathbb{C}} m}_{n \text{ times}} \\ &= \underbrace{(1_{\mathbb{C}} + \cdots + 1_{\mathbb{C}})}_{n \text{ times}} m \\ &= nm. \end{aligned}$$

Furthermore $m = 1_{\mathbb{C}} m = (\frac{1}{n} n)m = \frac{1}{n}(nm)$. If this was to be regarded as an equation in $\mathbb{Z}_n$ then Example 1.2.6 tells us that $nm = 0_M$. This forces $M = 0$, since an arbitrary element $m \in M$ satisfies

$$m = \frac{1}{n}(nm) = \frac{1}{n} 0_M = 0_M.$$

This contradicts the fact that the module M is non-zero.

Example 2.2.9 (Vector Spaces)**.** If V is a complex vector space and $T : V \to V$ is a linear map, then T can be used to turn V into a $\mathbb{C}[X]$–module.
One can view V as a $\mathbb{C}[X]$–module if, for each $\tilde{X} \in \mathbb{C}[X]$ and $v \in V$, then $\tilde{X} \cdot v$ is defined and is an element of V.
The choice $X \cdot v \equiv T(v)$ achieves this. Begin by noting that

$$X^n \cdot v = \underbrace{(X \circ \cdots \circ X)}_{n \text{ times}}(v) = \underbrace{X(X \cdots (X(v)))}_{n \text{ times}}$$
$$= T(T(\cdots(T(v)))) \equiv T^{\circ n}(v).$$

Note that this choice of notation is clumsy. For this reason the notation $T^{\circ n} \equiv T_\circ^n$ shall be adopted. Multiplicative association gives $(\alpha_n X^n)v = \alpha_n(X^n v) = \alpha_n T_\circ^n(v)$. An element of $\mathbb{C}[X]$ will therefore take the form

$$Y = \sum_{n=0}^{N} \alpha_n X^n.$$

This means specifically that

$$Yv = \left(\sum_{n=0}^{N} \alpha_n X^n \right) v = \sum_{n=0}^{N} \alpha_n T_\circ^n(v).$$

It is clear that all of the additive operations are satisfied as V is a vector space.

- $1_{\mathbb{C}[X]} v = v$.
  Note $1_{\mathbb{C}[X]} \equiv X^0 = 1_{\mathbb{C}}$. This is a polynomial of degree 0. If one makes the definition that $T_\circ^0$ is identically equal to 1 then

  $$1_{\mathbb{C}[X]} v = X^0 v \stackrel{\text{def}}{=} T_\circ^0(v) \stackrel{\text{def}}{=} v.$$

- $r[X] \cdot (s[X] \cdot v) = (r[X] \cdot s[X]) \cdot v$.
  Begin with the following observation:
  If

  $$r[X] = \sum_{i=0}^{N} \alpha_i X^i \text{ and } s[X] = \sum_{i=0}^{M} \beta_i X^i.$$

  then it is enough to check that this works for single terms of the polynomials. This means that one need only consider

  $$\alpha_n X^n \in r[X] \text{ and } \beta_m X^m \in s[X]. \tag{2}$$

  Precisely what this means is: *if*

  $$(\alpha_n X^n)[\beta_m X^m v] = (\alpha_n X^n \beta_m X^m)v,$$

  then it is true for the whole polynomial (which is simply a sum of these terms!). Consider the action of these elements on v.

  $$\begin{aligned}(\alpha_n X^n) \cdot (\beta_m X^m v) &\stackrel{\text{def}}{=} (\alpha_n X^n) \cdot \beta_m (X^m v) \\ &= (\alpha_n X^n)\beta_m T_\circ^m(v) \\ &= \alpha_n \beta_m X^n \cdot T_\circ^m(v) \\ &= \alpha_n \beta_m T_\circ^n \left(T_\circ^m(v) \right) \\ &= \alpha_n \beta_m T_\circ^{m+n}(v). \end{aligned} \tag{3}$$

Under this choice, the following is also true.

$$\begin{aligned}(\alpha_n X^n \beta_m X^m)v &= \alpha_n \beta_m X^{n+m} v \\ &= \alpha_n \beta_m T_\circ^{n+m}(v). \end{aligned} \tag{4}$$

The fact that (3) and (4) agree shows that the axiom holds.

- $(r[X] + s[X]) \cdot v = r[X]v + s[X]v$.
  Proceeding with the notation in (2) then

$$(\alpha_n X^n + \beta_m X^m)v = (\alpha_n T_\circ^n + \beta_m T_\circ^m)(v) = \alpha_n T_\circ^n(v) + \beta_m T_\circ^m(v) = \alpha_n X^n v + \beta_m X^m v.$$

- $r[X](v_1 + v_2) = r[X]v_1 + r[X]v_2$.

$$\alpha_n X^n(v_1 + v_2) = \alpha_n T_\circ^n(v_1 + v_2) = \alpha_n T_\circ^n(v_1) + \alpha_n T_\circ^n(v_2) \overset{\text{def}}{=} \alpha_n X^n v_1 + \alpha_n X^n v_2.$$

This employs the definition of *linear* functions.

Example 2.2.10. If $n \geq 1$ is an integer, it is possible to define a $\mathbb{Z}$–module structure on

$$\mathbb{Z}^n = \left\{ \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \mid z_i \in \mathbb{Z} \right\}.$$

Denote by $(m)_i$ is the $i-th$ component of $m \in \mathbb{Z}^n$. Define the addition and scalar multiplication of elements in the usual way for matrices. In particular

$$\begin{aligned}(+) : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z}^n; (m_1 + m_2)_i &= (m_1)_i + (m_2)_i, \\ (\cdot) : \mathbb{Z} \times \mathbb{Z}^n \to \mathbb{Z}^n; (\alpha m)_i &= \alpha (m)_i.\end{aligned}$$

It takes little consideration to realise that all axioms are satisfied. Simply, they are satisfied because the problem reduces to checking the validity of the axioms over $\mathbb{Z}$, and it is understood that $\mathbb{Z}$ is a $\mathbb{Z}$–module. Additionally one has $(\mathbf{0})_i = 0$ for each i, and $(-m)_i = -(m)_i$.

Chapter 3

Module Homomorphisms

3.1 Homomorphisms

Definition 3.1.1 (Homomorphism)**.** Let A and B be R–modules. A homomorphism is a map

$$\alpha : A \to B,$$

such that for all $m, n \in R$ and $a_1, a_2 \in A$

$$\alpha(m \cdot a_1 + n \cdot a_2) = m \cdot \alpha(a_1) + n \cdot \alpha(a_2).$$

Definition 3.1.2 (Isomorphism)**.** An isomorphism (of modules) is a bijective homomorphism of modules.

Remark 3.1.3. Throughout this literature the focus will be on $\mathbb{Z}$–modules. If it is not explicitly stated we assume that the results are specific to $\mathbb{Z}$–modules, even when the result applies more generally.
In particular,

$$\alpha : A \to B,$$

means that for all $m, n \in \mathbb{Z}$, $a_1, a_2 \in A$ and $\mathbb{Z}$–modules A and B

$$\alpha(m \cdot a_1 + n \cdot a_2) = m \cdot \alpha(a_1) + n \cdot \alpha(a_2).$$

Example 3.1.4. Consider $\mathbb{Z}$ as a $\mathbb{Z}$–module and fix $y \in \mathbb{Z}$. The map

$$\begin{aligned} \mu : M &\to M \\ a &\mapsto y \cdot a \end{aligned}$$

defines a homomorphism. This is true if $\mu(na + mb) = n\mu(a) + m\mu(b)$. In this case each of the elements come from $\mathbb{Z}$, for this reason it is useful to make the subsequent distinctions. One regards the elements n and m as coming from a **ring**, whereas a and b are regarded as elements of the **module**.

$$\begin{aligned} \mu(na + mb) &\stackrel{\text{def}}{=} (na + mb)y \\ &= (na)y + (mb)y && \text{(distributivity of } \mathbb{Z}) \\ &= n(ay) + m(by) && \text{(associativity of } \cdot \text{ in } \mathbb{Z}) \\ &\stackrel{\text{def}}{=} n\mu(a) + m\mu(b). \end{aligned}$$

3.2 Submodules

Definition 3.2.1 (Submodule)**.** If A is an R–module and $K \subseteq A$, then K is a submodule of A if it is closed under addition and scalar multiplication. That is, for all $k_1, k_2 \in K$ and $n_1, n_2 \in R$ then

$$n_1 k_1 + n_2 k_2 \in K.$$

Example 3.2.2. Regarded as $\mathbb{Z}$–modules, $m\mathbb{Z}$ (for a fixed integer $m \geq 1$) is a submodule of $\mathbb{Z}$. This is true if $n_1k_1 + n_2k_2$ is an element of $m\mathbb{Z}$, where $n_i \in \mathbb{Z}$ and $k_i \in m\mathbb{Z}$.

$$\begin{aligned} n_1k_1 + n_2k_2 &\stackrel{\text{def}}{=} n_1(mz_1) + n_2(mz_2) \\ &= (n_1m)z_1 + (n_2m)z_2 && \text{(associativity of } \cdot) \\ &= (mn_1)z_1 + (mn_2)z_2 && \text{(commutativity of } \cdot) \\ &= (n_1z_1) + m(n_2z_2) && \text{(associativity of } \cdot) \\ &= (n_1z_1 + n_2z_2) && \text{(distributivity)} \\ &= \tilde{z}, && (\mathbb{Z} \text{ is closed}) \end{aligned}$$

where $\tilde{z}$ is some integer so $m\mathbb{Z} \subseteq \mathbb{Z}$ is a submodule.

Proposition 3.2.3 ($\mathbb{Z}$–modules)**.** *If M is any $\mathbb{Z}$–module and $x \in M$ a fixed element, then*

$$\mathbb{Z} \cdot x = \{z \cdot x \mid z \in \mathbb{Z}\}$$

is a submodule.

Proof. Recall that

$$\mathbb{Z} \cdot x = \{z \cdot x \mid z \in \mathbb{Z}\} = \{\dots, -2x, -x, 0x, 1x, 2x, \dots\}$$

can be a submodule only if $n_1k_1 + n_2k_2 \in \mathbb{Z} \cdot x$. Once again it is important to distinguish these elements. $n_i \in \mathbb{Z}$ (regarded as a ring), $k_i \in \mathbb{Z} \cdot x$ and $z_i \in \mathbb{Z}$ (taking into account the definition of $\mathbb{Z} \cdot m$).

$$\begin{aligned} n_1k_1 + n_2k_2 &\stackrel{\text{def}}{=} n_1(z_1x) + n_2(z_2x) \\ &= (n_1z_1)x + (n_2z_2)x && \text{(associativity)} \\ &= (n_1z_1 + n_2z_2)x && \text{(distributivity)} \\ &= \tilde{z}x \in \mathbb{Z} \cdot x. && (\mathbb{Z} \text{ is closed}) \end{aligned}$$

□

Proposition 3.2.4 (Submodules of $\mathbb{Z}_n$)**.** *Let $K \subseteq \mathbb{Z}_n$ be a non-zero submodule. Set*

$$k = \min(K \setminus \{0\}),$$

then $K = \mathbb{Z}k$.

Proof. First, by Proposition 2.2.3, $K = \mathbb{Z}k$ is a submodule.

- "$\supseteq$": $\mathbb{Z}k \subseteq K$.
  Take $k \in K$. Since K is a submodule it is closed under $(+, \cdot)$. In particular this says

  $$n \cdot k \in K$$

  for any integer n. Whence, any element of $\mathbb{Z}k$ is also an element of K.

- "$\subseteq$": $K \subseteq \mathbb{Z}k$.
  Take $x \in K$. If $x = 0$ then $x = 0 \cdot k$. If instead one has $x \neq 0$ then divide k into x with remainders. That is, calculate
  $$x = q \cdot k + r \; 0 \leq r < k,$$
  where q is some integer, and $x, k \in \mathbb{Z}_n$. If one rearranges this expression and takes the equation modulo n then
  $$r \pmod{n} = (x - qk) \pmod{n}.$$
  It is known that $r < k = \min(K \setminus \{0\})$. This then forces $r = 0$, or in other words $k|x$, which can be formulated as $x = qk$ for some integer q. Therefore any element of K is an element of $\mathbb{Z}k$.

□

Example 3.2.5 ($\mathbb{Z}_{12}$)**.** One can view $\mathbb{Z}_{12}$ as a $\mathbb{Z}$–module (see Proposition 1.2.5). For each $m \in \mathbb{Z}_{12}$ consider $\langle m \rangle$.

- $\langle 0 \rangle = \{0\}$,
- $\langle 1 \rangle = \mathbb{Z}_{12} = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$,
- $\langle 2 \rangle = \{0, 2, 4, 6, 8\} = \langle 10 \rangle$,
- $\langle 3 \rangle = \{0, 3, 6, 9\} = \langle 9 \rangle$,
- $\langle 4 \rangle = \{0, 4, 8\} = \langle 8 \rangle$,
- $\langle 6 \rangle = \{0, 6\}$.

Note that $0 \subset M$ is trivially a submodule of any module M. Furthermore in each of the above subsets, the non-zero minimum elements generate their respective subsets. Whence, via Proposition 2.2.4 they, together with 0, are the submodules of $\mathbb{Z}_{12}$.

3.3 The Quotient Module

It is possible to use submodules to construct further modules, called **quotient modules**.

Definition 3.3.1 (Quotient Module)**.** The quotient module A/K for some submodule $K \subseteq A$, is a collection of **cosets**. That is, a collection of sets of the form
$$a + K = \{a + k \mid k \in K\}.$$

Remark 3.3.2 (Cosets)**.** Recall that addition of cosets is given by
$$(a_1 + K) + (a_2 + K) = (a_1 + a_2) + K.$$
Similarly, scalar multiplication is given by
$$n \cdot (a + K) = (n \cdot a) + K \text{ for } n \in R.$$

Lemma 3.3.3. *For any submodule $N \subseteq M$*

$$m_1 + N = m_2 + N \Leftrightarrow m_1 - m_2 \in N.$$

Proof.
$\Leftarrow$:
"$\subseteq$": Assume that $m_1 - m_2 \in N$, and consider an element of $m_1 + N$, That is,

$$m_1 + n = m_2 + \underbrace{(m_1 - m_2) + n}_{\text{an element of } N} \in m_2 + N.$$

"$\supseteq$"
This is shown with the element as $m_1 - (m_1 - m_2)$.
$\Rightarrow$:
Assume now that $m_1 + N = m_2 + N$.
Consider $m_1 = m_1 + 0 \in m_1 + N = m_2 + N$. Consequently $m_1 = m_2 + n$ for some $n \in N$. Rearranging this expression gives

$$m_1 - m_2 = n \in N.$$

□

Proposition 3.3.4 (Quotient Modules)**.** *Consider $M/K = \{m_\lambda \mid \lambda \in \Lambda\}$, then*

$$\bigcup_{\lambda \in \Lambda} m_\lambda = M.$$

Proof. Consider any m in M. The coset $m + K$ contains the element m, so any m will be in some coset, this results in the union being M. □

Lemma 3.3.5. *Let $M \xrightarrow{\mu} N$ be a homomorphism of modules and define*

$$\begin{aligned} \theta : M/\ker\mu &\to \operatorname{Im}\mu \\ m + \ker\mu &\mapsto \mu(m). \end{aligned}$$

Then $\theta(m_1 + \ker\mu) = \theta(m_2 + \ker\mu)$ if and only if $m_1 = m_2$.

Proof.
$\Leftarrow$:
If $m_1 = m_2$ then $m_1 + \ker\mu = m_2 + \ker\mu$. By Lemma 2.3.3, $m_1 - m_2 \in \ker\mu$, so

$$\mu(m_1 - m_2) = 0_N.$$

Since μ is a homomorphism $\mu(m_1 - m_2) = 0_N$ is equivalent to $\mu(m_1) = \mu(m_2)$. In other words

$$\theta(m_1 + \ker\mu) = \mu(m_1) = \mu(m_2) = \theta(m_2 + \ker\mu).$$

$\Rightarrow$:
This is shown in a process which reverses the previous steps. □

Proposition 3.3.6 (Cosets)**.** *There are m elements of $\mathbb{Z}/m\mathbb{Z}$.*

Proof. The collection takes the form

$$\mathbb{Z}/m\mathbb{Z} = \{z + m\mathbb{Z} \mid z \in \mathbb{Z}\}.$$

where $z + m\mathbb{Z} = \{z + m\alpha \mid \alpha \in \mathbb{Z}\}$.
In particular the following are cosets of $\mathbb{Z}/m\mathbb{Z}$.

$$\begin{aligned}
0 + m\mathbb{Z} &= \{\dots, -2m, -m, 0, m, 2m, \dots\} \\
&= m\mathbb{Z}, \\
1 + m\mathbb{Z} &= \{\dots, -2m+1, -m+1, 1, m+1, 2m+1, \dots\}, \\
&\vdots \\
(m-2) + m\mathbb{Z} &= \{\dots, -2m+m-2, -m+m-2, m-2, m+m-2, \dots\} \\
&= \{-m-2, -2, m-2, 2m-2 \dots\}, \\
(m-1) + m\mathbb{Z} &= \{\dots, -2m+m-1, -m+m-1, m-1, \dots\} \\
&= \{-m-1, -1, m-1, \dots\}, \\
m + m\mathbb{Z} &= \{\dots, -2m+m, -m+m, m, m+m, 2m+m, \dots\} \\
&= \{\dots, -m, 0, m, 2m, 3m, \dots\} \\
&= m\mathbb{Z}, \\
&\vdots
\end{aligned}$$

Once the value of z reaches m the cosets simply repeat themselves. Hence

$$\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}. \tag{1}$$

Elements in (1) are pairwise different.
Consider $n + m\mathbb{Z} = l + m\mathbb{Z}$ for $n \neq l$ in $\{0, \dots, m-1\}$. If these cosets are to be equal then this forces

$$n + m\alpha_1 = l + m\beta_1$$

for some integers α_1 and β_1. This expression is equivalent to $n - l = m(\beta_1 - \alpha_1)$. In particular this says that m divides $n - l$. If one notes that $0 \leq n, l \leq m-1$, this yields $-(m-1) \leq n-1 \leq (m-1)$. The only integer in this range which is a multiple of m is 0. That is, $n - l = 0$ and so $n = l$. We can conclude $n + m\mathbb{Z} = l + m\mathbb{Z}$ only if $n = l$.
The cosets repeat themselves beyond $(m-1) + m\mathbb{Z}$.
This is an exercise in showing that

$$n + m\mathbb{Z} = (n + rm) + m\mathbb{Z},$$

where r is an integer and n an element of $\{0, \dots, m-1\}$. Consider

$$(n + rm) + m\mathbb{Z} = \{n + rm + mz \mid z \in \mathbb{Z}\} = \{n + m(r+z) \mid z \in \mathbb{Z}\} = \{n + m\tilde{z} \mid \tilde{z} \in \mathbb{Z}\}.$$

It is clear that this set has exactly the same elements as $n + m\mathbb{Z}$ does, from which it is clear that the two cosets coincide.
The union of the cosets is $\mathbb{Z}$.
Consider any $z \in \mathbb{Z}$. It is true that z is in the coset

$$(z \pmod m) + m\mathbb{Z}.$$

There are m elements of the quotient module.
It is obvious that the collection $\{m\mathbb{Z}, 1+m\mathbb{Z}, \dots, (m-1)+m\mathbb{Z}\}$ can be put in a one-to-one correspondence with the set $\{0, 1, \dots, m-1\}$. This means that the sets have the same cardinality, where the latter set has cardinality m. □

Example 3.3.7 (The Even Integers)**.** Consider $\mathbb{Z}$ as a $\mathbb{Z}$–module, with ordinary addition and scalar multiplication

a) $2\mathbb{Z}$ is a submodule of $\mathbb{Z}$.
Any elements of $2\mathbb{Z}$ have the form $2z_1$ and $2z_2$ for some integers z_1 and z_2. This means that the linear combination takes the form

$$n_1(2z_1) + n_2(2z_2) = 2(n_1z_1 + n_2z_2).$$

It is clear that this is also an element of $2\mathbb{Z}$. Note that the commutativity of the integers has been employed here.

b) The quotient module $\mathbb{Z}/2\mathbb{Z}$ is given by

$$\mathbb{Z}/2\mathbb{Z} = \{z + 2\mathbb{Z} \mid z \in \mathbb{Z}\}.$$

By Proposition 2.3.6 there are only two disjoint elements of this set. They are

$$\{0 + 2\mathbb{Z}\} = \{\dots, -4, -2, 0, 2, 4, \dots\} \text{ and } \{1 + 2\mathbb{Z}\} = \{\dots, -3, -1, 1, 3, \dots\}.$$

Or, in other words,

$$\mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}.$$

The group table is

$+$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$0+2\mathbb{Z}$	$0+2\mathbb{Z}$	$1+2\mathbb{Z}$
$1+2\mathbb{Z}$	$1+2\mathbb{Z}$	$0+2\mathbb{Z}$

Remark 3.3.8 (The Even Integers)**.** In the group theoretical sense, it is not difficult to see that $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$. Whence the quotient module $\mathbb{Z}/n\mathbb{Z}$ is analogous to how one finds $\mathbb{Z}_n$.

Lemma 3.3.9. *Let $M' \subseteq M$ be a submodule and*

$$M \xrightarrow{\mu} N$$

be a homomorphism. If also $\mu(M') = \{0\}$ (that is $M' \subseteq \ker \mu$), then there is a well-defined homomorphism

$$M/M' \to N$$
$$m + M' \mapsto \mu(m).$$

Proof. First of all μ is well-defined.
This means that the same cosets have the same image, or $m_1 + M' = m_2 + M'$ implies that $\varphi(m_1 + M') = \mu(m_2 + M')$. If $m_1 + M' = m_2 + M'$ then by Lemma 2.3.3

$$m_1 - m_2 \in M' \subseteq \ker \mu.$$

This is equivalent to $\mu(m_1 - m_2) = 0_N$. Since μ is a homomorphism this means that $\mu(m_1) = \mu(m_2)$. Hence the map is well-defined. Next one is required to show that

$$\varphi : M/M' \to N,$$

defines a homomorphism. If φ is a homomorphism (of R–modules) then has $\varphi(z_1m_1 + z_2m_2) = z_1\varphi(m_1) + z_2\varphi(m_2)$ for all $z_1, z_2 \in R$ and $m_1, m_2 \in M$. Note that here m_i is used to represent $m_i + M'$. Explicitly

$$\begin{aligned}
\varphi(z_1m_1 + z_2m_2) &= \varphi(z_1[m_1 + M'] + z_2[m_2 + M']) \\
&\overset{\text{def}}{=} \varphi([(z_1m_1) + M'] + [(z_2m_2) + M']) \\
&\overset{\text{def}}{=} \varphi([z_1m_1 + z_2m_2] + M') \\
&\overset{\text{def}}{=} \mu(z_1m_1 + z_2m_2) \\
&= z_1\mu(m_1) + z_2\mu(m_2) \\
&\overset{\text{def}}{=} z_1\varphi(m_1 + M') + z_2\varphi(m_2 + M').
\end{aligned}$$

Note that the operations defined for cosets, and the fact that μ is a homomorphism, have been employed here. □

3.4 The Cokernel

Definition 3.4.1 (Cokernel)**.** Let

$$\mu : M \to N$$

be a module homomorphism. The cokernel is the quotient module $M/\operatorname{Im}\mu$.

$$\operatorname{Coker}\mu = M/\operatorname{Im}\mu.$$

Remark 3.4.2. The kernel and the cokernel of a map satisfy the following properties.

$$\begin{aligned}
\ker\mu = \{m \in M \mid \mu(m) = 0_N\} \hookrightarrow M \text{ and} \\
\operatorname{Coker}\mu = N/\operatorname{Im}\mu \twoheadleftarrow N \\
n + \operatorname{Im}\mu \mapsfrom n.
\end{aligned}$$

Example 3.4.3 (The Cokernel)**.** Consider the following module homomorphisms.

(i)

$$\begin{aligned}
\mathbb{Z}_4 &\to \mathbb{Z}_2 \\
1 &\mapsto 1.
\end{aligned}$$

It is clear under this map that $0, 2 \mapsto 0$ and $1, 3 \mapsto 1$, whence $\ker\mu_a = \mathbb{Z}_2 = \operatorname{Im}\mu_a$, so

$$\operatorname{Coker}\mu_a = \mathbb{Z}_2/\mathbb{Z}_2 \cong 0.$$

(ii)

$$\begin{aligned}\mathbb{Z}_2 &\to \mathbb{Z}_4\\ 1 &\mapsto 2.\end{aligned}$$

Under this mapping $0 \mapsto 0$ and $1 \mapsto 2$. Thus $\ker \mu_b = \{0\}$ and $\operatorname{Im} \mu_b = \{0, 2\} \cong \mathbb{Z}_2$. This yields

$$\operatorname{Coker} \mu_b = \mathbb{Z}_4/\mathbb{Z}_2.$$

(iii)

$$\begin{aligned}\mathbb{Z}_8 &\to \mathbb{Z}_8\\ 1 &\mapsto 4.\end{aligned}$$

In particular it does the following

$$\begin{aligned}0, 2, 4, 6 &\mapsto 0,\\ 1, 3, 5, 7 &\mapsto 4.\end{aligned}$$

Thus $\ker \mu_c = \{0, 2, 4, 6\}$, $\operatorname{Im} \mu_c = \{0, 4\} \cong \mathbb{Z}_2$. This gives

$$\operatorname{Coker} \mu_c = \mathbb{Z}_8/\mathbb{Z}_2.$$

(iv)

$$\begin{aligned}\mathbb{Z} &\to \mathbb{Z}\\ 1 &\mapsto 2.\end{aligned}$$

In particular this means $\ker \mu_d = \{0\}$, and $\operatorname{Im} \mu_d = 2\mathbb{Z}$. This means that

$$\operatorname{Coker} \mu_d = \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2.$$

3.5 The Isomorphism Theorem

Here we present the first isomorphism theorem which, although is technically only one of three isomorphism theorems, shall be referred to as 'the isomorphism theorem' throughout this literature.

Theorem 3.5.1 (The Isomorphism Theorem)**.** *Let*

$$\mu : M \to N$$

be a homomorphism of $R-$modules. The kernel and image

$$\begin{aligned}\ker \mu &= \{m \in M \mid \mu(m) = 0_N\} \subseteq M\\ \operatorname{Im} \mu &= \{\mu(m) \mid m \in M\} \subseteq N.\end{aligned}$$

are submodules. Further there exists an isomorphism

$$\begin{aligned}M/\ker \mu &\xrightarrow[\theta]{\sim} \operatorname{Im} \mu\\ m + \ker \mu &\longmapsto \mu(m)\end{aligned}$$

Proof.

- The kernel is a submodule.
  Consider $k_1, k_2 \in \ker\mu$ and $n_1, n_2 \in R$. The kernel is a submodule if

  $$n_1k_1 + n_2k_2 \in \ker\mu.$$

  Elements of the kernel satisfy $\mu(k) = 0_N$, in particular one has

  $$\mu(n_1k_1 + n_2k_2) = n_1\mu(k_1) + n_2\mu(k_2) = (n_1 + n_2)0_N = 0_N.$$

  That is, the linear combination is in the kernel, and so the kernel is a submodule.

- The image is a submodule.
  Let k_1' and k_2' be elements of the image and consider $n_1, n_2 \in R$. If $k' \in \operatorname{Im}\mu$ this means that $k' = \mu(m)$ for some m in M. This results in

  $$n_1k_1' + n_2k_2' = n_1\mu(m_1) + n_2\mu(m_2) = \mu(n_1m_1 + n_2m_2).$$

  It is clear that this is an element of the image, and so the image being a submodule.

- θ defines a homomorphism.
  It is clear that θ is well-defined, and follows from Lemma 2.3.5. If θ is a homomorphism one requires that $\theta(n_1a_1 + n_2a_2) = n_1\theta(a_1) + n_2\theta(a_2)$, where $n_i \in R$, and $a_i \in M/\ker\mu$. If a_i is to be in $M/\ker\mu$ then this means $a_i = m_i + \ker\mu$ for some $m_i \in M$.

  $$\theta(n_1a_1+n_2a_2) = \theta(n_1(m_1+\ker\mu)+n_2(m_2+\ker\mu)) = \theta((n_1m_1+n_2m_2)+\ker\mu) = \mu(n_1m_1+n_2m_2),$$

  This follows from the operations of cosets and the definition of θ. Moreover, utilising the notion that μ is a homomorphism,

  $$\mu(n_1m_1 + n_2m_2) = n_1\mu(m_1) + n_2\mu(m_2) = n_1\theta(m_1 + \ker\mu) + n_2\theta(m_2 + \ker\mu).$$

  So this defines a homomorphism.

- θ is surjective. This is equivalent to saying $\theta(M/\ker\mu) = \operatorname{Im}\mu$.

  $$\theta(M/\ker\mu) = \{\theta(m + \ker\mu) \mid m \in M\} = \{\mu(m) \mid m \in M\}.$$

- θ is injective. This means $\theta(m_1 + \ker\mu) \neq \theta(m_2 + \ker\mu)$ whenever $m_1 \neq m_2$. By Lemma 2.3.5, $\theta(m_1 + \ker\mu) = \theta(m_2 + \ker\mu)$ if and only if $m_1 = m_2$. This tells us that the images can be equal if only the inputs are the same. Whence we have injectivity.

□

Example 3.5.2. Consider the following homomorphism of $\mathbb{Z}-$modules

$$\begin{aligned}\mu : \mathbb{Z} &\to \mathbb{Z}_m \\ x &\mapsto x \pmod m.\end{aligned}$$

The kernel and image are

$$\ker \mu = \mathbb{Z} \cdot m$$
$$\operatorname{Im} \mu = \mathbb{Z}_m.$$

By the isomorphism theorem, then

$$\mathbb{Z}/\mathbb{Z}m \xrightarrow[\theta]{\sim} \mathbb{Z}_m$$
$$y + \mathbb{Z}m \longmapsto \mu(y) = y \pmod{m},$$

is an isomorphism. This is also discussed in Remark 2.3.8.

Chapter 4

Sequences

Definition 4.0.3 (Sequence)**.** Let M^i be R–modules, and d^i be homomorphisms between them. If $d^i \circ d^{i-1} = 0$ for each i, then

$$\cdots \longrightarrow M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \longrightarrow \cdots$$

is called a **sequence**.

Definition 4.0.4 (Exact Sequence)**.** If

$$\cdots \longrightarrow M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \longrightarrow \cdots$$

is a sequence, it is said to be **exact at** M^i if $\operatorname{Im} d^{i-1} = \ker d^i$.
A sequence is called **exact**, if it is exact wherever it makes sense.

Definition 4.0.5 (Left and Right Exact Sequences)**.** A sequence is said to be **left exact** if it is an exact sequence of the form

$$0 \to A \to B \to C.$$

It is said to be a **right exact** sequence if it is exact and of the form

$$X \to Y \to Z \to 0.$$

4.1 Short Exact Sequences

Definition 4.1.1 (Short Exact Sequence)**.** A **short** exact sequence is an exact sequence of the form

$$0 \to K \to L \to M \to 0.$$

Remark 4.1.2. With this definition, the following is a short exact sequence

$$0 \to M' \xrightarrow{\mu'} M \xrightarrow{\mu} M'' \to 0.$$

Applying the isomorphism theorem to μ gives

$$\begin{aligned} M/\ker\mu &\xrightarrow{\sim} M'' \\ m + \ker\mu &\longmapsto \mu(m). \end{aligned}$$

Note that this is an exact sequence and so $\ker\mu = \operatorname{Im}\mu'$, or $M/\ker\mu = M/\operatorname{Im}\mu'$. Further, one could view the following map as an isomorphism

$$M' \xrightarrow{\sim} \operatorname{Im}\mu' \subseteq M.$$

It is vacuous that this defines a homomorphism (it is a mapping taken from an exact sequence), in addition it is injective (see Lemma 3.1.6). It is surjective by the definition of the image. In this sense one can construct the following short exact sequence

$$0 \to \operatorname{Im}\mu' \xrightarrow{\mu'} M \xrightarrow{\mu} M/\operatorname{Im}\mu' \to 0.$$

This means that a short exact sequence can be viewed as a mapping from a submodule, to the module, and then to the respective quotient module.

Lemma 4.1.3 (Injectivity)**.** *For any linear map $\mu : M' \to M$, then μ is injective* iff $\ker\mu = \{0 = e_{M'}\}$.

Proof.
$\Rightarrow$:
Assume that μ' is injective so that $\mu(m_1') = \mu(m_2') \Rightarrow m_1' = m_2'$. For any map $\mu(e_{M'}) = e_M$. This is obvious if one regards

$$\mu(m' - m') = \mu(e_{M'}) = e_M = \mu(m') - \mu(m').$$

Now

$$\ker\mu = \{m' \in M \mid \mu(m') = 0_M,$$

by injectivity this is possible for only one element. We already have $e_{M'} \in \ker\mu$, whence one has

$$\ker\mu = \{0\}.$$

$\Leftarrow$:
Assume that $\ker\mu = \{0\}$ and suppose that $\mu(m_1') = \mu(m_2')$. That is $\mu(m_1' - m_2') = 0$, or $m_1' = m_2'$. From which it follows that μ is injective. □

Remark 4.1.4 (Short Exact Sequence)**.** In a short exact sequence

$$0 \to K \to L \to M \to 0,$$

the first and last maps are fixed. In particular

$$\begin{aligned} 0 &\to K \\ 0 &\mapsto 0, \\ M &\to 0 \\ m &\mapsto 0. \end{aligned}$$

Example 4.1.5 (Short Exact Sequences)**.** The subsequent are short exact sequences. It is assumed without proof that the maps between the modules are indeed homomorphisms. Furthermore, the first and last map in the sequences are fixed.

a) With the maps indicated, τ is an exact sequence.

$$\tau = 0 \xrightarrow{0\longmapsto 0} \mathbb{Z} \xrightarrow{m\longmapsto 2m} \mathbb{Z} \xrightarrow{m\longmapsto m \bmod 2} \mathbb{Z}_2 \xrightarrow{m\longmapsto 0} 0.$$

(i) First $d^i \circ d^{i-1} = 0$.

$$(d^2 \circ d^1)(m) = d^2(d^1(0)) = d^2(0) = 0$$
$$(d^3 \circ d^2)(m) = d^3(2m) = 2m \bmod 2 = 0$$
$$(d^4 \circ d^3)(m) = d^4(m \bmod 2) = 0$$

(ii) Next $\operatorname{Im} d^i = \ker d^{i+1}$.

i	$\ker d^i$	$\operatorname{Im} d^i$
1	$\{0\}$	$\{0\}$
2	$\{0\}$	$2\mathbb{Z}$
3	$2\mathbb{Z}$	$\mathbb{Z}_2$
4	$\mathbb{Z}_2$	$\{0\}$

b) Again ξ (short) exact sequence.

$$\xi = 0 \xrightarrow{0 \longmapsto 0} \mathbb{Z}_2 \xrightarrow{m \longmapsto 2m} \mathbb{Z}_4 \xrightarrow{m \longmapsto m \bmod 2} \mathbb{Z}_2 \xrightarrow{m \longmapsto 0} 0.$$

(i) First $d^i \circ d^{i-1} = 0$.

$$(d^2 \circ d^1)(m) = d^2(d^1(0)) = d^2(0) = 0$$
$$(d^3 \circ d^2)(m) = d^3(2m) = 2m \bmod 2 = 0$$
$$(d^4 \circ d^3)(m) = d^4(m \bmod 2) = 0$$

(ii) Next $\operatorname{Im} d^i = \ker d^{i+1}$.

i	$\ker d^i$	$\operatorname{Im} d^i$
1	$\{0\}$	$\{0\}$
2	$\{0\}$	$\{0, 2\}$
3	$\{0, 2\}$	$\mathbb{Z}_2$
4	$\mathbb{Z}_2$	$\{0\}$

c) Finally ω is also an exact sequence.

$$\omega = 0 \to \mathbb{Z} \to \mathbb{Z}^2 \to \mathbb{Z} \to 0.$$

With maps defined by

$$\begin{aligned} d^1 : 0 &\to \mathbb{Z} \\ 0 &\mapsto 0 \\ d^2 : \mathbb{Z} &\to \mathbb{Z}^2 \\ m &\mapsto \begin{pmatrix} m \\ 0 \end{pmatrix} \\ d^3 : \mathbb{Z}^2 &\to \mathbb{Z} \\ \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} &\mapsto m_2 \\ d^4 : \mathbb{Z} &\to 0 \\ m &\mapsto 0 \end{aligned}$$

(i) First $d^i \circ d^{i-1} = 0$.

$$(d^2 \circ d^1)(m) = d^2(d^1(0)) = d^2(0) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
$$(d^3 \circ d^2)(m) = d^3(\begin{pmatrix} m \\ 0 \end{pmatrix}) = 0$$
$$(d^4 \circ d^3)(m) = d^4(m_2) = 0$$

(ii) Next $\operatorname{Im} d^i = \ker d^{i+1}$.

i	$\ker d^i$	$\operatorname{Im} d^i$
1	$\{0\}$	$\{0\}$
2	$\{0\}$	$\begin{pmatrix} m \\ 0 \end{pmatrix}$
3	$\begin{pmatrix} m \\ 0 \end{pmatrix}$	$\mathbb{Z}$
4	$\mathbb{Z}$	$\{0\}$

Lemma 4.1.6 (Short Exact Sequence)**.** *If*

$$0 \xrightarrow{\psi} M' \xrightarrow{\mu'} M \xrightarrow{\mu} M'' \xrightarrow{\psi'} 0$$

is short exact the μ' is injective, and μ is surjective.

Proof. First of all, μ' is injective if $\ker \mu' = 0$ (Lemma 3.1.3). In this exact sequence $\ker \mu' = \operatorname{Im} \psi = 0$.. Next consider what it means for μ to be surjective. Again, since this is an exact sequence, one has $\operatorname{Im} \mu = \ker \psi' = M''$. Clearly μ is surjective. □

Proposition 4.1.7. *Given a module homomorphism $M \xrightarrow{\mu} N$, there is an exact sequence*

$$0 \longrightarrow \ker \mu \longrightarrow M \xrightarrow{\mu} N \longrightarrow \operatorname{Coker} \mu \longrightarrow 0$$
$$k \longmapsto k \qquad n \longmapsto n + \operatorname{Im} \mu.$$

Proof. Let us consider first what this tells us given the map μ.

$$0 \xrightarrow[d^1]{} \ker \mu \xrightarrow[d^2]{} M \xrightarrow[d^3]{\mu} N \xrightarrow[d^4]{} \operatorname{Coker} \mu \xrightarrow[d^5]{} 0$$

$$0 \longmapsto 0, k \longmapsto k \longmapsto \mu(k) \longmapsto \mu(k) + \operatorname{Im} \mu \longmapsto 0.$$

Now, in an exact sequence, the following must be true

$$d^i \circ d^{i-1} = 0,$$
$$\ker d^i = \operatorname{Im} d^{i-1}.$$

Note that $\ker \mu \subseteq M$ and so we have

$$\ker \mu \hookrightarrow M,$$

where the inclusion map is

$$\imath : \ker \mu \to : k \mapsto k.$$

We can show that the composition rule for a sequence is satisfied.

$$\begin{aligned}
(d^2 \circ d^1)(0) = d^2(d^1(0)) = d^2(0 \in \ker \mu) = 0,\\
(d^3 \circ d^2)(k \in \ker \mu) = \mu(d^2(k \in \ker \mu)) = \mu(k \in \ker \mu) = 0,\\
(d^4 \circ d^3)(m \in M) = d^4(\mu(m \in M)) = d^4(\mu(m)) = \mu(m) + \operatorname{Im} \mu \cong 0,\\
(d^5 \circ d^4)(k \in \operatorname{Coker} \mu) = d^5(d^4(k)) \stackrel{\text{def}}{=} 0.
\end{aligned}$$

Check now that this is exact.

- $\operatorname{Im} d^1 = 0$ (trivially) and $\ker d^2 = 0$. The latter simply because the map is an inclusion (and hence only 0 maps to 0).
- $\operatorname{Im} d^2 = \ker \mu$ (again because we have used an inclusion map), and $\ker d^3 \stackrel{\text{def}}{=} \ker \mu$.
- $\operatorname{Im} d^3 \stackrel{\text{def}}{=} \operatorname{Im} \mu$ and $\ker d^4 = \{n \in N \mid n + \operatorname{Im} \mu \cong 0\} = \{n \in \operatorname{Im} \mu\} = \operatorname{Im} \mu$.
- $\operatorname{Im} d^4 \stackrel{\text{def}}{=} \operatorname{Coker} \mu$ and $\ker d^5 = \operatorname{Coker} \mu$ (which follows from the fact that the map sends the pre-image space to 0).

□

Chapter 5

Free Modules

Definition 5.0.8 (Free Module)**.** A **free module** is a module which has a basis.

Reminder 5.0.9 (Basis)**.** A **basis** is a linearly independent spanning set. That is, a set F for which the elements are linearly independent

$$\lambda_1 \mathbf{e_1} + \cdots + \lambda_n \mathbf{e_n} = 0 \Leftrightarrow \lambda_i = 0 \text{ for all } i,$$

and span the module (or other mathematical object); for each $f \in F$ then

$$f = \sum_{i=1}^{n} \lambda_i \mathbf{e_i}.$$

Example 5.0.10 (Basis for R^n)**.** In R^n the following is a *basis*:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

(i) **Linear Independence.**
For all $r_i \in R$, then $r_1 e_1 + \cdots + r_n e_n = 0$ if and only if each $r_i = 0$.

$$r_1 e_1 + \cdots + r_n e_n = r_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + r_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + r_n \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$$\stackrel{\text{def}}{=} \begin{pmatrix} r_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ r_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ r_n \end{pmatrix}$$

$$\stackrel{\text{def}}{=} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_n \end{pmatrix}.$$

Now clearly this can be equal to the zero vector only if each $r_i = 0$.

(ii) **Any element is a linear combination of these vectors.**
Consider an arbitrary vector in R^n and write it as

$$\begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_n \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} r_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ r_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ r_n \end{pmatrix}$$
$$= r_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + r_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + r_n \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Specifically $\mathbb{Z}^n$ is a free module, with basis

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Remark 5.0.11. By Example 4.0.10 $\mathbb{Z}^n$ is a free module. This is true in general for any module over a field.

Example 5.0.12 ($\mathbb{Z}_2$ has no Basis)**.** The $\mathbb{Z}$–module $\mathbb{Z}_2$ has no basis. It is the set $\{0, 1\}$ and cannot have either element as a basis element:

$$1 \cdot 0 = 0 \text{ and } 2 \cdot 1 = 0.$$

Then

$$\begin{array}{ccccccccc} 1 & \cdot & 0 & + & 2 & \cdot & 1 & = & 0. \\ \in & & \in & & \in & & \in & & \\ \mathbb{Z} & & \mathbb{Z}_2 & & \mathbb{Z} & & \mathbb{Z}_2 & & \end{array}$$

a contradiction of linear independence.

Proposition 5.0.13 (Uniqueness)**.** *Each element of a free $\mathbb{Z}$–module F, has a unique expression in terms of its basis elements.*

Proof. Consider $f \in F$ for which there are two different expressions. That is,

$$f = z_1 f_1 + \cdots + z_n f_n = \alpha_1 f_1 + \cdots + \alpha_n f_n.$$

F is a $\mathbb{Z}$–module so there are additive inverses such that

$$z_1 f_1 + \cdots + z_n f_n + (-\alpha_1) f_1 + \cdots + (-\alpha_n) f_n = 0.$$

Now this can be rearranged, applying the left distributivity of multiplication over addition, to look like

$$(z_1 - \alpha_1)f_1 + \cdots + (z_n - \alpha_n)f_n = 0.$$

Since the f_i are basis elements, then

$$z_i - \alpha_i = 0,$$

that is,

$$z_i = \alpha_i.$$

Hence the expressions are the same. □

Remark 5.0.14 (Free Module)**.** Consider a free $\mathbb{Z}$–module F with basis $\{f_1, \dots f_n\}$. Then

$$F = \left\{ \sum_{i=1}^{n} z_n f_n \mid z_i \in \mathbb{Z} \right\}.$$

Additionally knowing the element

$$z_1 f_1 + \cdots + z_n f_n,$$

is informative of what the respective f_i are. This is not true of modules in general.

Example 5.0.15 ($\mathbb{Z}_2$)**.** By Example 4.0.12, $\mathbb{Z}_2$ has no basis. In this $\mathbb{Z}$–module there is the non-unique expression

$$0 = 0 \cdot 1 = 2 \cdot 1.$$

Proposition 5.0.16. *Let M be any module with selected elements $m_1, \dots, m_n$. Note that repetitions are permitted. There is a homomorphism of modules*

$$\varphi : F \to M,$$

given by

$$\varphi(z_1 f_1 + \dots z_n f_n) = z_1 m_1 + \dots z_n m_n.$$

Proof. Ordinarily demonstrating that a mpa defines a homomorphism has been shown simply by demonstrating $\varphi(n_1 f_1 + n_2 f_2) = n_1 \varphi(f_1) + n_2 \varphi(f_2)$. This is somewhat more involved a calculation and so it will be more beneficial to consider the cases separately. First of all, note that an element f in F can be expressed as a linear combination and so

$$\begin{aligned}
\varphi(f + \tilde{f}) &= \varphi([z_1 f_1 + \cdots + z_n f_n] + [\tilde{z}_1 f_1 + \cdots + \tilde{z}_n f_n]) \\
&= \varphi([z_1 + \tilde{z}_1] f_1 + \cdots + [z_n \tilde{z}_n] f_n) \\
&= (z_1 + \tilde{z}_1) m_1 + \cdots + (z_n + \tilde{z}_n) m_n \\
&= (z_1 m_1 + \cdots + z_n m_n) + (\tilde{z}_1 m_1 + \cdots + \tilde{z}_n m_n) \\
&= \varphi(f) + \varphi(\tilde{f}).
\end{aligned}$$

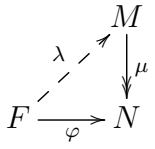
Also

$$\begin{aligned}
\varphi(zf) &= \varphi(z(z_1 f_1 + \cdots + z_n f_n)) \\
&= \varphi(z z_1 f_1 + \cdots + z z_n f_n) \\
&= z z_1 m_1 + \cdots + z z_n m_n \\
&= z(z_1 m_1 + \cdots + z_n m_n) \\
&= z\varphi(f).
\end{aligned}$$

That is, φ is a homomorphism. □

5.1 The Lifting Problem

Proposition 5.1.1. *If F is a free module and $M \twoheadrightarrow N$ is surjective, then the following lifting problem can always be solved.*



Note that

$$\begin{aligned} \lambda(f_i) &= m_i, \\ \mu(m_i) &= n_i, \text{ and} \\ \varphi(f_i) &= n_i = (\mu \circ \lambda)(f_i). \end{aligned}$$

Proposition 5.1.2.

$$G/N \cong 0 \Leftrightarrow N = G.$$

Proof.
$\Rightarrow$:
Assume that $G/N \cong 0$. The cosets of this quotient have the form

$$\{g + N \mid g \in G\}.$$

This means that for each $g \in G$ there can be only one coset produced, which can be possible if only $N = G$.
$\Leftarrow$:
Assume that $N = G$. Then the cosets take the form

$$\{g + G \mid g \in G\}.$$

It is clear that this simply produces G, that is $G/G = \{G\}$. This (one element set) is clearly isomorphic to $\{0\}$. □

Proposition 5.1.3 (Surjectivity of μ)**.** *In the lifting problem, μ is surjective if and only if* $\operatorname{Coker}\mu \cong 0$.

Proof.
$\Rightarrow$:
μ is surjective if everything in N is hit. That is $\operatorname{Im}\mu = N$. Thus

$$\operatorname{Coker}\mu = N/N \cong 0.$$

$\Leftarrow$:
Assume that $\operatorname{Coker}\mu \cong 0$. That is

$$N/\operatorname{Im}\mu \cong 0.$$

Proposition 4.1.2 says that $\operatorname{Im}\mu = N$, and hence μ is surjective. □

5.2 Free Presentation

Definition 5.2.1 (Free Presentation)**.** Take $m_i \in M$ such that they generate M, that is,

$$M = \{z_1 m_1 + \cdots + z_n m_n \mid z_i \in \mathbb{Z}\}.$$

The map

$$\begin{aligned} \varphi : F &\to M \\ f_i &\mapsto m_i, \end{aligned}$$

is surjective and there is a short exact sequence

$$0 \to \ker \varphi \hookrightarrow F \xrightarrow{\varphi} M \to 0.$$

This is known as a **free presentation**. We would say that φ approximates M by F.

Example 5.2.2 (Free Presentation of $\mathbb{Z}_3$)**.** In order to find a free presentation of $\mathbb{Z}_3$ one must solve the problem

$$0 \to \ker \varphi \hookrightarrow F \xrightarrow{\varphi} \mathbb{Z}_3 \to 0.$$

Consider the element $m_1 = 1 \in \mathbb{Z}_3$, and a basis $\{f_1\}$ for F. Let

$$\varphi(z_1 f_1) = z_1 m_1 = z_1.$$

It is clear to see that $\ker \varphi = 3F$, so, in this case one is left with

$$\begin{aligned} 0 \to \ker \varphi = 3F \hookrightarrow F &\to \mathbb{Z}_3 \to 0 \\ z \cdot f_1 &\mapsto z \cdot 1. \end{aligned}$$

As $\mathbb{Z}^n$ is free $\mathbb{Z}$ has basis: $\{1\}$. Whence the following is a free presentation of $\mathbb{Z}_3$.

$$\begin{aligned} 0 \to 3\mathbb{Z} \hookrightarrow \mathbb{Z} &\to \mathbb{Z}_3 \to 0 \\ 1 &\mapsto 1 \\ z &\mapsto z \cdot 1. \end{aligned}$$

Chapter 6

Functors

In the context of this report there are two important functors to consider. These are the 'Hom' functor and the 'Ext' functor. To this end it is beneficial to first consider what exactly a functor is. In order to define a functor, one needs to familiarise oneself with several important definitions. The subsequent formulation is based on the literature by Gelfand and Manin [**GM**].

Definition 6.0.3 (Class)**.** A **class** is a collection of mathematical objects.

Definition 6.0.4 (Category)**.** A **category** $\mathfrak{C}$ consists of

- a class $\mathrm{ob}(\mathfrak{C})$ of objects: $A, B, C, \dots$;
- a class $\hom(\mathfrak{C})$ of morphisms. Each morphism f has a unique source object A and target object B where $A, B \in \mathrm{ob}(\mathfrak{C})$. This is written as

  $$f : A \to B.$$

  This is a morphism from A to B, and can be denoted $\hom(A, B)$.
- For every triple $A, B, C \in \mathrm{ob}(\mathfrak{C})$ there is a binary operation

  $$\hom(A, B) \times \hom(B, C) \to \hom(A, C).$$

  This is a composition of morphisms. The composition of $f : A \to B$ and $g : B \to C$ is denoted $g \circ f$.

Such that the following axioms hold.

Axioms (Axioms for Categories)**.**

(i) Associativity: where it makes sense $h \circ (g \circ f) = (h \circ g) \circ f$;

(ii) Identity: For every object x there is an identity morphism

$$1_x : x \to x.$$

So that when it makes sense $f \circ 1_x = f$ and $1_x \circ g = g$.

Definition 6.0.5 (Functor)**.** Let $\mathfrak{C}$ and $\mathfrak{D}$ be categories. A functor F, is a mapping from $\mathfrak{C}$ to $\mathfrak{D}$, subject to the following axioms.

Axioms (Axioms for Functors)**.**

- F associates to each $X \in \mathfrak{C}$ an object $F(X) \in \mathfrak{D}$.
- F associates to each morphism $f : X \to Y \in \mathfrak{C}$, a morphism $F(f) : F(X) \to F(Y) \in \mathfrak{D}$ subject to

  (i) $F(id_X) = id_{F(X)}$ for each $X \in \mathfrak{C}$.

  (ii) $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $f : X \to Y$ and $g : Y \to Z$.

6.1 The Hom Functor

Definition 6.1.1 (Hom)**.** Let M and N be R–modules. **Hom** is defined as

$$\mathrm{Hom}(M,N) = \{f : M \to N \mid f \text{ is a homomorphism}\}.$$

On Hom addition of elements and multiplication (by elements of R) are defined as follows

$$\begin{aligned}(f+g)(m) &= f(m)+g(m)\\ (z\cdot f)(m) &= z\cdot(f(m)).\end{aligned}$$

Lemma 6.1.2 (Hom)**.** *The binary operations defined on* Hom *are closed. That is,* $f+g$ *and* $z\cdot f$ *are in* $\mathrm{Hom}(M,N)$.

Proof. This reduces to showing that $f+g$ and zf are homomorphisms.

a) $(f+g)(a_1+a_2) = (f+g)(a_1)+(f+g)(a_2)$ and $(f+g)(na) = n(f+g)(a)$.

(i)

$$\begin{aligned}(f+g)(a_1+a_2) &\overset{\text{def}}{=} f(a_1+a_2)+g(a_1+a_2)\\ &= f(a_1)+f(a_2)+g(a_1)+g(a_2)\ \ f,g \textbf{ are homomorphisms}\\ &= f(a_1)+g(a_1)+f(a_2)+g(a_2)\\ &\overset{\text{def}}{=} (f+g)(a_1)+(f+g)(a_2).\end{aligned}$$

(ii)

$$(f+g)(na) \overset{\text{def}}{=} f(na)+g(na) = nf(a)+ng(a) = n(f+g)(a).$$

Here we have employed the fact that f and g are homomorphisms.

b) $zf(a_1+a_2) = zf(a_1)+zf(a_2)$ and $zf(na) = nzf(a)$.

(i)

$$\begin{aligned}(zf)(a_1+a_2) &= zf(a_1+a_2)\\ &= zf(a_1)+zf(a_2)\\ &= (zf)(a_1)+(zf)(a_2).\end{aligned}$$

(ii)

$$(zf)(na) = zf(na) = nzf(a) = n(zf)(a).$$

Thus they are elements of Hom. □

Example 6.1.3 (Hom is a $\mathbb{Z}$–module)**.** $\mathrm{Hom}(M,N)$ with $(+,\cdot)$ is a $\mathbb{Z}$–module.

(i) Commutativity of Addition:

$$(f+g)(a) \overset{\text{def}}{=} f(a)+g(a) \equiv g(a)+f(a) \overset{\text{def}}{=} (g+f)(a).$$

It follows that we are able to do this as $f(a)$ and $g(a)$ are elements of the module N and so are commutative with respect to addition.

(ii) Associativity of Addition.
This is shown similarly.

(iii) The element 0.
This is simply the function

$$\begin{aligned} M &\to N \\ m &\mapsto 0_N. \end{aligned}$$

(iv) Additive Inverse.
This is given (for f) as $-f(m)$. This is clear by the subsequent expressions.

$$\begin{aligned} (f+g) = f(m) + g(m) = 0_N \\ \Rightarrow g(m) = -f(m). \end{aligned}$$

(v) $1_{\mathbb{Z}} \cdot f = f$.

$$(1_{\mathbb{Z}} f)(m) = 1_{\mathbb{Z}}(f(m)) = f(m).$$

The remaining conditions are checked by repeating a similar process.

Example 6.1.4 (Calculating Hom)**.** Compute $\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_3)$. The first thing to note is that this can consist only of maps which send $0 \mapsto 0$.
Consider a map which has $f(0) = a$ for some $a \in \mathbb{Z}_3$, then

$$\begin{aligned} f(0) &= a \\ f(0) = f(0+0) &= a + a = 2a \\ f(0) = f(0+0+0) &= a + a + a = 3a. \end{aligned}$$

This is possible if only $a = 0$.
Furthermore the maps are uniquely determined by what they do to the element 1. If one fixes 0, and chooses where to send 1, there are only two possible maps. Additionally there is the map which sends all elements to 0, denote this by o. That is

$$\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_3) = \{e, f, o\}.$$

Here e is the identity map

$$\begin{aligned} e : \mathbb{Z}_3 &\to \mathbb{Z}_3 \\ e(z) &\mapsto z, \end{aligned}$$

and f is the map given by

$$\begin{aligned} \mathbb{Z}_3 &\xrightarrow{f} \mathbb{Z}_3 \\ 0 &\mapsto 0 \\ 1 &\mapsto 2 \\ 2 &\mapsto 1. \end{aligned}$$

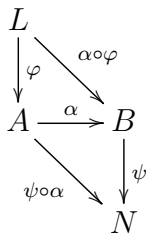
Definition 6.1.5 (α_*)**.** Let $\alpha : A \to B$ be a homomorphism of R–modules and L be a module. Let also $\varphi : L \to A$. It is possible to define a map

$$\begin{aligned} \alpha_* : \mathrm{Hom}(L, A) &\to \mathrm{Hom}(L, B) \\ \varphi &\mapsto \alpha_*(\varphi) = \alpha \circ \varphi. \end{aligned}$$

Definition 6.1.6 (α^*)**.** Let $\alpha : A \to B$ and $\psi : B \to N$ be homomorphisms of R–modules. It is possible to define a map

$$\begin{aligned} \alpha^* : \mathrm{Hom}(B, N) &\to \mathrm{Hom}(A, N) \\ \psi &\mapsto \alpha^*(\psi) = \psi \circ \alpha. \end{aligned}$$

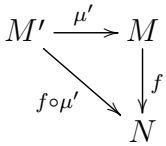
Remark 6.1.7. The definitions of α^* and α_* are more easily seen from the following diagram



Lemma 6.1.8. *Given a module homomorphism $M' \xrightarrow{\mu'} M$, and a module N, there is a module homomorphism*

$$\mathrm{Hom}(M', N) \leftarrow \mathrm{Hom}(M, N).$$

Proof. By Definition 5.1.6, μ'^* is a map between these modules. All that is required is to show μ'^* is a homomorphism. This particular problem has the following diagram.



Let f and g be elements of $\mathrm{Hom}(M, N)$ and n be a scalar (from the ring R).

$$\begin{aligned} \mu'^*(f+g) &= (f+g) \circ \mu' \\ &= (f+g)(\mu'(\cdot)) \\ &= f(\mu'(\cdot)) + g(\mu'(\cdot)) \\ &= f \circ \mu' + g \circ \mu' \\ &= \mu'^*(f) + \mu'^*(g). \end{aligned}$$

$$\begin{aligned} \mu'^*(nf) &= (nf) \circ \mu' \\ &= (nf)(\mu'(\cdot)) \\ &= nf(\mu'(\cdot)) \\ &= n(f \circ \mu') \\ &= n\mu'^*. \end{aligned}$$

Thus the map defines a homomorphism. □

Lemma 6.1.9. *Given a module homomorphism $M' \xrightarrow{\mu'} M$, and a module L, there is a module homomorphism*

$$\mathrm{Hom}(L, M') \to \mathrm{Hom}(L, M).$$

Proof. By Definition 5.1.5 μ'_* is a map between these modules. Following similarly to the proof of Lemma 5.1.8, this defines a homomorphism. □

Lemma 6.1.10. *If $f : M \to N$ and $g : L \to M$ are $R-$module homomorphisms, then*

$$f \circ g : L \to N,$$

is a homomorphism.

Proof. In order for this to define a homomorphism then two conditions must be satisfied.

- $(f \circ g)(l_1 + l_2) = (f \circ g)(l_1) + (f \circ g)(l_2)$ for l_i in L.

$$\begin{aligned}(f \circ g)(l_1 + l_2) &= f(g(l_1 + l_2)) \\ &= f(g(l_1) + g(l_2)) \\ &= f(g(l_1)) + f(g(l_2)) \\ &= (f \circ g)(l_1) + (f \circ g)(l_2).\end{aligned}$$

- $(f \circ g)(nl) = n(f \circ g)(l)$ for l in L and n in R.

$$\begin{aligned}(f \circ g)(nl) &= f(g(nl)) \\ &= f(ng(l)) \\ &= n(f(g(l))) \\ &= n(f \circ g)(l).\end{aligned}$$

This has employed the fact that f and g are homomorphism. □

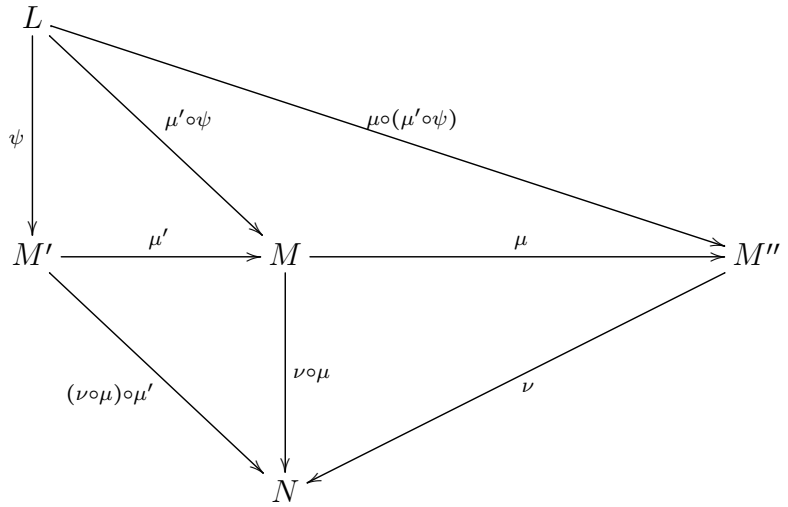
Lemma 6.1.11 (μ^* and μ_* are homomorphisms)**.** *The maps given by*

$$\begin{aligned}(\mu \circ \mu')_* &= \mu_* \circ \mu'_* \\ (\mu \circ \mu')^* &= \mu'^* \circ \mu^*. \end{aligned} \tag{1}$$

are homomorphisms.

Proof. In order to show this it will only be necessary to show that the maps are equal. The fact that they define homomorphisms will follow immediately from the fact that the upper and lower

star maps are homomorphisms and Lemma 5.1.10. Consider the following diagram



Note now that

$$(\mu \circ \mu')^* : \mathrm{Hom}(M', N) \longleftarrow \mathrm{Hom}(M'', N)$$
$$\nu \circ \mu \circ \mu' \longleftarrow\shortmid \nu,$$

and

$$(\mu \circ \mu')_* : \mathrm{Hom}(L, M') \longrightarrow \mathrm{Hom}(L, M'')$$
$$\psi \longmapsto \mu \circ \mu' \circ \psi.$$

It is not difficult to use this diagram to show that the maps, as described in (1) are the same. □

Theorem 6.1.12. *Let*

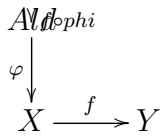
$$0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0$$

be an exact sequence. If A is a module then

$$0 \to \mathrm{Hom}(A, X) \xrightarrow{f_*} \mathrm{Hom}(A, Y) \xrightarrow{g_*} \mathrm{Hom}(A, Z),$$

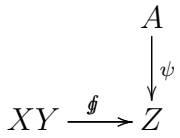
is exact.

Proof. If the induced sequence is to be exact then it suffices to show the following are satisfied. f_* is injective, and $\ker g_*$ is the same as $\mathrm{Im}\, f_*$.
f_* is injective. Consider the diagram



If we assume that $f \circ \varphi$ is zero and show that φ is identically zero, then we are done (the kernel will be zero). If $f \circ \varphi = 0$ and f is injective (it follows from the orginial short exact sequence) then this can happen only if $\varphi \equiv 0$.
$\ker g_* = \mathrm{Im}\, f_*$.
$\ker g_* \supseteq \mathrm{Im}\, f_*$: From the diagram it is clear that $f \circ \varphi \in \mathrm{Im}\, f_*$. We just had that $f \circ \varphi$ is zero and so

the map $g_*(f \circ \varphi) = g \circ f \circ \varphi$ will also be zero. That is, any element of the image is in the kernel.
$\ker g_* \subseteq \operatorname{Im} f_*$: Consider the diagram below.



We need that if $g \circ \psi \in \ker g_*$ then $g \circ \psi = 0$. Then ψ takes the form $f \circ \varphi$ where $\varphi : A \to X$. In particular, if $g \circ \psi = 0$ then the image of ψ is contained in $\ker g = \operatorname{Im} f$. Now f is injective so ψ gives rise to a unique map φ, such that $\psi = f \circ \varphi$. □

Chapter 7

Conclusion

The report set out with the aim of using vector spaces as a motivation for a new kind of theory, with the underlying sets called R–modules. It was necessary to familiarise the reader with the concepts that underpin rings, fields and modules before any endeavour could be made to present the final result.
It was then essential to present theory and results relevant to module homomorphisms in order to get to the end goal (exact sequences involving Hom). The isomorphism theorem and other properties of homomorphisms were used in the construction of short exact sequences. In particular one begins with a module and constructs a short exact sequence, regarded as taking a submodule to its underlying module and then taking this to the quotient module.
From there some interesting concepts related to free modules and free presentations were formalised. Free modules are particularly useful for projections, which are related to the induced exact sequence this report culminates in. See [**HS**].
This, along with the idea of the 'Ext' functor, offer potential further exploration.

Bibliography

[**AR**] H. Anton, C. Rorres, *Elementary Linear Algebra*, John Wiley & Sons, 1973.
[**ELL**] G. Ellis, *Rings and Fields*, OUP, 1992.
[**GM**] S.I. Gelfand, Yu.I. Manin, *Methods of Homological Algebra*, Springer, 1996.
[**HS**] P.J. Hilton, U. Stammbach, *A Course in Homological Algebra*, Springer, 1971.