Atiyah-MacDonald: Modules

James Pagan

January 2024

Contents

1 Modules

1.1 Definition

An **R-module** over a commutative ring R is an abelian group M (with operation written additively) endowed with a mapping $\mu : R \times M \to M$ (written multiplicatively) such that the following axioms are satisfied for all $x, y \in M$ and $a, b \in R$:

1. $1x = x$;
2. $(ab)x = a(bx)$;
3. $a(x + y) = ax + ay$;
4. $(a + b)x = ax + bx$.

1.2 Examples of Modules

- If R is a ring, $R[x]$ is a module.
- All ideals $\mathfrak{a} \subseteq R$ are R-modules using the same additive and multiplicative operations as R — in particular R itself is an R-module.
- If R is a field, R-modules are R-vector spaces. In fact, the axioms above are identical to the vector axioms, defined over commutative rings instead of fields.
- Abelian groups G are precisely the modules over $\mathbb{Z}$.

1.3 R-Module Homomorphisms

A map $f : M \to N$ between two R-modules M and N is an **R-module homomorphism** (or is **R-linear**) if for all $a \in R$ and $x, y \in M$,

$$f(x + y) = f(x) + f(y)$$
$$f(ax) = af(x).$$

Thus, an R-module homomorphism f is a homomorphism of abelian groups that commutes with the action of each $a \in R$. If R is a field, an R-module homomorphism is a linear map. A bijective R-homomorphism is called an R-isomorphism.

The set $\mathrm{Hom}_R(M,N)$ denotes the set of all R-module homomorphisms from M to N, and is a module if we define the following operations for $a \in R$ and $f, g \in \mathrm{Hom}_R(M,N)$:

$$(f+g)(x) = f(x) + g(x)$$
$$(af)(x) = af(x).$$

We denote $\mathrm{Hom}_R(M,N)$ by $\mathrm{Hom}(M,N)$ if the ring R is unambiguous.

Theorem 1. $\mathrm{Hom}_R(R,M) \cong M$

Proof. The mapping $\phi : \mathrm{Hom}_R(R,M) \to M$ defined by $\phi(f) = f(1)$ is a homomorphism, as verified by a routine computation: for all $f, g \in \mathrm{Hom}_R(M,N)$ and $a \in R$,

$$\phi(f+g) = (f+g)(1) = f(1) + g(1) = \phi(f) + \phi(g)$$
$$\phi(af) = (af)(1) = af(1) = a\phi(f),$$

so ϕ is an R-homomorphism. This mapping is injective, since each f is uniquely determined by $f(1)$. It is also surjective; for each $m \in M$, set define a homomorphism by $h(1) = m$. Thus ϕ is the desired isomorphism. □

Homomorphisms $u : M' \to M$ and $v : N \to N''$ induce mappings $\bar{u} : \mathrm{Hom}(M,N) \to \mathrm{Hom}(M',N)$ and $\bar{v} : \mathrm{Hom}(M,N) \to \mathrm{Hom}(M,N'')$ defined for $f \in \mathrm{Hom}(M,N)$ as follows

$$\bar{u}(f) = f \circ u \qquad \text{and} \qquad \bar{v}(f) = v \circ f.$$

I do not know why such a manipulation is noteworthy. The formulas above are quite easy to memorize if the time ever comes to invoke them.

1.4 Submodules

A **submodule** M' of M is an abelian subgroup of M closed under multiplication by elements of the commutative ring R.

Lemma 1. $\mathfrak{a}$ *is an ideal of* R *if and only if it is an* R*-submodule of* R*.*

Proof. The proof evolves from a fundamental observation:

$$R\mathfrak{a} = \mathfrak{a} \iff \text{scalar multiplication in the } R\text{-module } \mathfrak{a} \text{ is closed.}$$

The rest of the multiplicative module conditions follow from the ring axioms. □

The following proof outlines the construction of **quotient modules**:

Theorem 2. *The abelian quotient group $M \,/\, M'$ is an R-module under the opreation $a(x + M') = ax + M'$.*

Proof. We must perform four rather routine calculations: for all $x, y \in M$ and $a, b \in R$,

1. **Identity**: $1(x + M') = 1x + M' = x + M'$.
2. **Compatability**: $a(b(x + M')) = a(bx + M') = abx + M' = (ab)(x + M')$.
3. **Left Distributivity**: $(a + b)(x + M') = (a + b)x + M' = (ax + bx) + M' = (ax + M') + (bx + M') = a(x + M') + b(x + M')$.
4. **Right Distriutivity**: $a((x+M')+(y+M')) = a((x+y)+M') = a(x+y)+M' = (ax + M') + (ay + M') = a(x + M') + a(y + M)'$.

Therefore, M/M' is an R-module. Also, this operation is naturally well-defined. □

R-module homomorphisms $f : M \to N$ induce three notable submodules:

1. **Kernel**: $\operatorname{Ker} f = \{x \in M \mid f(x) = 0\}$, a submodule of M.
2. **Image**: $\operatorname{Im} f = \{f(x) \mid x \in M\}$, a submodule of N.
3. **Cokernel**: $\operatorname{Coker} f = N \,/\, \operatorname{Im} f$, a quotient of N.

The cokernel is perhaps an unfamiliar face. Such a quotient is not possible for rings or groups; images of homomorphisms need not be ideals of R nor normal subgroups of G.

Theorem 3 (First Isomorphism Theorem)**.** $N \,/\, \operatorname{Ker} f \cong \operatorname{Im} f$.

Proof. Let $K = \operatorname{Ker} f$, and define an R-morphism $g : M \,/\, N \to \operatorname{Im} f$ by $g(x+K) = f(x)$. We have for arbitrary $x, y \in N$ and $a \in R$ that

$$g(x + y + K) = f(x + y) = f(x) + f(y) = g(x + K) + g(y + K).$$
$$g(ax + K) = f(ax) = af(x) = ag(x + K).$$

Hence g is a homomorphism. For injectivity, suppose that $g(x + K) = g(y + K)$ — that is, $f(x) = f(y)$. Then

$$f(y - x) = f(y) - f(x) = 1,$$

so $y - x \in K$. Thus $x + K = y + K$. Surjectivity is quite clear. We conclude that g is the desired isomorhism. □

Let $f : M \to N$ be an R-module homomorphism. Here are two special cases of the prior theorem:

1. If f is a monomorphism, them $M \cong \operatorname{Im} f$.
2. If f is an epimorphism, then $M \,/\, \operatorname{Ker} f \cong N$.

For a submodule $N' \subseteq \operatorname{Im} f$, I call $M' = \{x \in M \mid f(a) \in N'\}$ the **contraction module**.

Theorem 4 (Correspondence Theorem)**.** *Submodules of G which contain* $\operatorname{Ker} f$ *correspond one-to-one with submodules of* $\operatorname{Im} f$*.*

Proof. For each submodule $N' \subseteq \operatorname{Im} f$ consider the contraction module $M' = \{x \mid f(x) \in N'\}$. Since this is an Abelian subgroup, we need only check for multiplicative closure: for all $x \in M'$ and $a \in R$, we have

$$f(ax) = af(x) \in N' \implies ax \in N'.$$

Hence M' is a submodule. It is clear that $\operatorname{Ker} f \subseteq M'$, so the First Isomorphism Theorem yields that

$$N' \,/\, \operatorname{Ker} f \cong M'.$$

Thus this construction is injective. It is surjective, since for each $\operatorname{Ker} \subseteq N' \subseteq N$, the subgroup N' is contracted by $f(N')$. The correspondence is now established. □

The Second Isomorphism Theorem utilizes the definitioins of Section 2.1:

Theorem 5 (Second Isomorphism Theorem)**.** *If $M_1, M_2 \subseteq M$ are submodules, then* $(M_1 + M_2) \,/\, M_1 \cong M_2 \,/\, (M_1 \cap M_2)$*.*

Proof. Define a mapping $f : M_2 \to (M_1 + M_2) \,/\, M_1$ by $\phi(m_2) = m_2 + M_1$. Clearly ϕ is well-defined; it is an R-module homomorphism, since $x_1, x_2 \in M_2$ and $a \in R$ implies

$$\begin{aligned} f(x_1 + x_2) \;&=\; x_1 + x_2 + x_1 \;=\; (x_1 N)(x_2 N) \;=\; f(x_1) f(x_2) \\ f(ax_1) \;&=\; ax_1 + x_1 \;=\; a(x_1 + x_1) \;=\; af(x_1). \end{aligned}$$

f is surjective, since for all $x_1 + M_1 \in (M_1 + M_2) \,/\, M_2$, we have $f(x_1) = x_1 + X_1$. The kernel of f is all $x \in M_1$ — namely, $M_1 \cap M_2$. We conclude by the First Isomorphism Theorem that

$$(M_1 + M_2) \,/\, M_1 \quad = \quad M_2 \,/\, (M_1 \cap M_2),$$

which completes the proof. □

Theorem 6 (Third Isomorphism Theorem)**.** *If $L \lhd M$ and $L \subseteq N \lhd M$, then $M \,/\, N = (M \,/\, L) \,/\, (N \,/\, L)$.*

Proof. Let $\phi : M \to M \,/\, L$ be the canonical epimorphism. Define $\psi : M \to \phi(M) \,/\, \phi(N)$ by the rule $\psi(a) = \phi(a)\phi(M)$. It is clear that ψ is well-defined and surjective; it is an R-module homomorphism since

$$\psi(ab) \;=\; \phi(ab)\phi(N) \;=\; \big(\phi(a)\phi(M)\big)\,\big(\phi(b)\phi(M)\big) \;=\; \psi(a)\psi(b).$$

The kernel of ϕ is all $a \in N$. The First Isomorphism Theorem yields that

$$M \,/\, N \quad\cong\quad \phi(M) \,/\, \phi(M).$$

Since the kernel of ϕ is L, we have that $\phi(M) \cong M \,/\, L$ and $\phi(N) \cong N \,/\, L$; substituting yields the desired $M \,/\, N = (M \,/\, L) \,/\, (N \,/\, L)$. □

2 Operations on Submodules

2.1 Sums, Intersections, Products

Let M be an R-module with submodules $M_1, \ldots, M_n$. We can consider two crucial operations on these submodules:

1. **Sum**: The sum $M_1 + \cdots + M_n$ is the set of all sums $m_1 + \cdots + m_n$, where $m_i \in M_i$ ($i \in \{1, \ldots, n\}$). It is the smallest submodule of M that contains all $M_1, \ldots, M_n$.
2. **Intersecrtion**: The intersection $M_1 \cap \cdots \cap M_n$ is the largest submodule of M that is contained inside each $M_1, \ldots, M_n$.

For an ideal $\mathfrak{a}$ of R and an R-module M, we define the **product** $\mathfrak{a}M$ as all finite sums $a_1x_1 + \cdots + a_nx_n$ for $a_i \in \mathfrak{a}$ and $x_i \in M$ for each $i \in \{1, \ldots, n\}$. It is a submodule of M.

2.2 The Annihilator

If N and P are R-submodules of M, we define $(N : P)$ to be the set of all $a \in R$ such that $aP \subseteq N$.

Theorem 7. *$(N : P)$ is an ideal of R.*

Proof. If $a, b \in (N : P)$, then $aP, bP \subseteq N$; we must have that $aP + bP \subseteq N$. Observe that $(N : P)$ is nonempty, as $0P = (0) \subseteq N$; and clearly if $aP \in N$, then $-aP \in N$ as N is an abelian group. $(N : P)$ satifies the multiplicative condition too. □

The **annihilator** of a module M is $(0 : M)$, the ideal of all a such that $aM = 0$, and is denoted $\operatorname{Ann} M$. If $\mathfrak{a} \subseteq \operatorname{Ann} M$, we may regard M as an $R/\mathfrak{a}$-module. In particular, observe that if $\bar{a} \in R/\mathfrak{a}$, then $a_1, a_2 \in \bar{a}$ implies $a_1 x = a_2 x$ — so $\bar{a}$ is well-defined.

An R-module is **faithful** if $\operatorname{Ann} M = 0$. The annihalator of R may change depending on the ring — if $\operatorname{Ann} M = \mathfrak{a}$, then M is faithful as an $R/\mathfrak{a}$ module.

Theorem 8. *If M_1 and M_2 are submodules of M, then* $\operatorname{Ann}(M_1 + M_2) = \operatorname{Ann} M_1 \cap \operatorname{Ann} M_2$

Proof. If $r \in \operatorname{Ann} M_1 \cap \operatorname{Ann} M_2$, then for all $x_1 + x_2 \in M_1 + M_2$, r annihalates x_1 and x_2, so $r(x_1 + x_2) = 0$. Thus $r \in \operatorname{Ann}(M_1 + M_2)$.

Now, suppose $r \notin \operatorname{Ann} M_1 \cap \operatorname{Ann} M_2$. Then r must fail to annnihilate an element in either M_1 or M_2 (or both) — without loss of generality, let there exist $x_1 \in M_1$ such that $rx_1 \neq 0$.

Then as $rx_1 \in M_1 + M_2$, we find that $r \notin \operatorname{Ann}(M_1 + M_2)$. By contraposition, we find that if $r \in \operatorname{Ann}(M_1 + M_2)$, then $r \in \operatorname{Ann} M_1 \cap \operatorname{Ann} M_2$. This completes the proof. □

2.3 Direct Sum and Product

If M and N are R-modules, their **direct sum** $M \oplus N$ is the set of all pairs (x, y) (with $x \in M$ and $y \in N$) endowed with the natural operations:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$r(x, y) = (rx, ry)$$

More generally, for a family of R-modules $(M_j)_{j \in J}$, we define their **direct sum** $\bigoplus_{j \in J} M_j$ as the families $(x_j)_{j \in J}$ such that $x_j \in M_j$ for all $j \in J$, with the restriction that only finitely many x_j are nonzero.

If we allow infinitely many x_j to be nonzero, we attain the family's **direct product** $\prod_{j \in J} M_j$. Direct sums and direct products are equivalent if J is finite, but not otherwise.

2.4 Direct Sums on Rings

Suppose that a commutative ring R is a direct product $R = R_1 \times \cdots \times R_n$. Then R has n ideals of the form

$$\mathfrak{a}_j = (0, \ldots, 0, r_j, 0, \ldots, 0),$$

where $a_i \in R_i$ for each $i \in \{1, \ldots, n\}$. Viewing this relation in terms of modules,

$$R \cong \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$$

by the isomorphism $f(r_1, \ldots, r_n) = ((r_1, 0, \ldots), \ldots, (\ldots, 0, r_n))$.

Similarly, suppose R is a commutative ring with ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, and

$$R = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n.$$

Then define $\mathfrak{b}_i = \bigoplus_{j \neq i} \mathfrak{a}_j$ for each $i \in \{1, \ldots, n\}$. We find that

$$R \cong (R \,/\, \mathfrak{b}_1) \times \cdots \times (R \,/\, \mathfrak{b}_n)$$

by the isomorphism $f(a_1, \ldots, a_n) = (a_1 + \mathfrak{b}_1, \ldots, a_n + \mathfrak{b}_n)$. We conclude that direct sums of ideals and direct products of subrings are dual notions. This is a critical strength of modules: it treats ideals and rings on equal footing, resulting in clarity and simplicity.

3 Finitely Generated Modules

3.1 Definition

An R-module M is said to be **finitely generated** if there exist a set of **generators** $x_1, \ldots, x_n$ such that $M = Rx_1 + \cdots + Rx_n$, where Rx_i denotes the set $\{rx_i \mid r \in R\}$ $(i \in \{1, \ldots, n\})$. In the following theorem, we denote $R \oplus \cdots \oplus R$ by R^n.

Theorem 9. *M is a finitely-generated R-module if and only if M is isomorphic to a quotient of R^n.*

Proof. Suppose M is a finitely-generated R-module. Let $x_1, \ldots, x_n \in M$ generate M, and define $f : R^n \to M$ by $f(r_1, \ldots, r_n) = r_1x_1 + \cdots + r_nx_n$. Then if $(r_1, \ldots, r_n), (s_1, \ldots, s_n) \in R^n$,

$$\begin{aligned} f(r_1 + s_1, \ldots, r_n + s_n) &= (r_1 + s_1)x_1 + \cdots (r_n + s_n) \\ &= (r_1x_1 + \cdots + r_nx_n) + (s_1x_1 + \cdots + s_1x_1) \\ &= f(r_1, \ldots, r_n) + f(s_1, \ldots, s_n), \end{aligned}$$

and if $s \in R$,

$$f(sr_1, \ldots, sr_n) = sr_1x_1 + \cdots + sr_nx_n = sf(r_1, \ldots, r_n).$$

Thus f is an R-module homomorphism; its surjectivity follows from the generation of M by $x_1, \ldots, x_n$. Then if we set $\operatorname{Ker} f = \mathfrak{a}$, the First Isomorphism Theorem yields that

$$R^n \,/\, \mathfrak{a} \cong M.$$

Now, suppose that $R^n \,/\, \mathfrak{a} \cong M$ for some submodule $\mathfrak{r}$ of R^n by the mapping f. The canonical epimorphism $g : R^n \to R^n \,/\, \mathfrak{r}$ defined by $g(r_1, \ldots r_n) = (r_1, \ldots, r_n) + \mathfrak{r}$ is surjective, so $f \circ g : R^n \to M$ is a surjective R-module homomorhism.

Denote $x_i = (f \circ g)(0, \ldots, 0, 1, 0, \ldots 0)$ for $i \in \{1, \ldots, n\}$. Then for all $x \in M$, there exist $r_1, \ldots, r_n$ such that

$$\begin{aligned} x &= (f \circ g)(r_1, \ldots, r_n) \\ &= (f \circ g)(r_1, 0, \ldots, 0) + \cdots + (f \circ g)(0, \ldots, 0, r_n) \\ &= r_1(f \circ g)(1, 0, \ldots, 0) + \cdots + r_n(f \circ g)(0, \ldots, 0, 1) \\ &= r_1x_1 + \cdots r_nx_n. \end{aligned}$$

We conclude that $x_1, \ldots, x_n$ generate M. □

The following proof is a transcription from Atiyah-MacDonald:

Theorem 10. *Let M be a finitely-generated R-module, let $\mathfrak{a}$ be an ideal of R, and let $f : M \to M$ be an R-module endomorphism of M such that $f(M) \subset \mathfrak{r}M$. Then ϕ satisfies an equation of the form*

$$f^n + r_{n-1}f^{n-1} + \cdots + r_0f^0 = 0,$$

where the r_i are in $\mathfrak{a}$.

Proof. Let $x_1, \ldots, x_n$ generate M. Then each $f(x_i) \in \mathfrak{a}M$, so we may define $r_{ij} \in \mathfrak{r}$ for $i, j \in \{1, \ldots, n\}$ by $f(x_i) = \sum_{j=1}^n r_{ij}x_j$. This equation may be equivalently written for each $i \in \{1, \ldots, n\}$ as

$$\sum_{j=1}^{n} (\delta_{ij}f - a_{ij}f^0)x_j = 0,$$

where δ_{ij} is the Kronecker delta. By multiplying the left by the adjoint of the matrix $\delta_{ij}f - a_{ij}f^0$, it follows that $\det\big(\delta_{ij}f - a_{ij}f^0\big)$ annihilates each x_{ij} — hence, it is the zero endomorphism of M. Expanding out the determinant yields an equation of the required form. □

Corollary 1. *Let M be a finitely-generated R-module and let $\mathfrak{a}$ be an ideal of R such that $\mathfrak{r}M = M$. Then there exists $r \in (1 + \mathfrak{r})$ such that $rM = 0$.*

Proof. Consider Theorem 7 under the identity transformation — namely f^0 for some nonzero endomorphism f. Then there exist $r_{n-1}, \ldots, r_0 \in \mathfrak{a}$ such that

$$\begin{aligned} 0 &= f^n + r_{n-1}f^{n-1} + \cdots + r_0 f^0 \\ &= f^0 + r_{n-1}f^0 + \cdots + r_0 f^0 \\ &= (1 + r_{n-1} + \cdots + r_0)f^0. \end{aligned}$$

Setting $r = 1 + r_{n-1} + \cdots + r_0$ yields that rf^0 is the zero endomorphism, so $rf^0(x) = rx = 0$ for each $x \in M$. We conclude that $rM = 0$. □

A **free R-module** M is a module such that $M \cong \bigoplus_{j \in J} M_j$, where $M_j \cong R$ for each $j \in J$. A finitely generated module M is therefore free if M is isomorphic to R^n itself, in which case M has a "basis".

3.2 Relation to the Jacobson Radical

The following lemma is called **Nakayama's Lemma** and has two proofs:

Lemma 2 (Nakayama's Lemma)**.** *Let M be a finitely generated R-module and $\mathfrak{a}$ an ideal of R contained in the Jacobson radical $\mathfrak{J}$ of R. Then $\mathfrak{r}M = M$ implies $M = 0$.*

Proof. By Corollary 1, there exists $r \in 1 + j$ for $j \in \mathfrak{a}$ such that $rM = 0$. By the properties of the Jacobson radical, $1 + j$ (and thus r) is a unit. Hence,

$$M = (r^{-1}r)M = r^{-1}(rM) = r^{-1}(0) = 0,$$

as desired. □

Proof. Suppose for contradiction that $\mathfrak{a}M = M$ and $M \neq 0$; let $x_1, \ldots, x_n$ be a set of generators of M of shortest length. Then $x_n \in \mathfrak{r}M$, so x_n satisfies an equation of the form

$$x_n = r_1 x_1 + \cdots + r_n x_n$$

for $r_1, \ldots, r_n \in \mathfrak{a}$. None of these are 1, since the Jacobson Radical is the intersection of maximal ideals, of which none contain 1. We can therefore eliminate x_n;

$$(1 - r_n)x_n = r_1 x_1 + \cdots + r_{n-1}x_{n-1}.$$

Since r_n is in the Jacobson radical, $(1 - r_n)$ is a unit. We may therefore multiply this equation by the inverse of $(1 - r_n)$ to express x_n as a linear combination of $x_1, \ldots, x_{n-1}$.

Then $x_1, \ldots, x_{n-1}$ generate M. This contradicts the minimality of the length of $x_1, \ldots, x_n$; we conclude that if $\mathfrak{a}M = M$, then $M = 0$. □

Corollary 2. *Let M be a finitely-generated R-module, N a submodule of M, and $\mathfrak{a}$ an ideal of R contained in the Jacobson radical $\mathfrak{R}$ of R. Then $M = IM + N$ implies $M = N$.*

Proof. Suppose $M = \mathfrak{a}M + N$. Realize that for *all* ideals $\mathfrak{r}$ of R,

$$\mathfrak{a}(M \,/\, N) = (\mathfrak{r}M) \,/\, N = (\mathfrak{r}M + N) \,/\, N.$$

Therefore, $\mathfrak{a}(M \,/\, N) = M \,/\, N$. By Nakayama's Lemma, $M \,/\, N = 0$, so $M = N$. □

3.3 Relation to Local Rings

Consider a finitely-generated module M over a local ring R with maximal ideal $\mathfrak{m}$.

Theorem 11. *The elements of the R-module $M \,/\, \mathfrak{m}M$ and the $(R \,/\, \mathfrak{m})$-module M are identical.*

Proof. It is relatively simple to verify that the function $f : M \,/\, \mathfrak{m}M \to M$ defined by

$$f(r_1x_1 + \cdots + r_nx_n + \mathfrak{m}M) = (r_1 + \mathfrak{m})x_1 + \cdots + (r_n + \mathfrak{m})x_n$$

is bijective. It further satisfies $f(x + y) = f(x) + f(y)$ — and $f(rx) = sf(x)$, where s is the image of r under the canonical epimorphism $\phi : R \to R \,/\, \mathfrak{m}$. □

This realization arises naturally, as $\mathfrak{m}$ annihalates the quotient module $M \,/\, \mathfrak{m}M$. Since $R \,/\, \mathfrak{m}$ is a field, $M \,/\, \mathfrak{m}M$ is actually a vector space.

Theorem 12. *Let M be a module over a local ring. Then $x_1, \ldots, x_n \in M$ generate M if and only if the images of $x_1, \ldots, x_n$ span the the vector space $M \,/\, \mathfrak{m}M$.*

Proof. Let $f : M \to M \,/\, \mathfrak{m}M$ be the canonical epimorphism. Then

$$\begin{aligned} x_1, \ldots, x_n \text{ generate } M &\iff x_1, \ldots, x_n \text{ generate } M \,/\, \mathfrak{m}M \\ &\iff x_1, \ldots, x_n \text{ are a basis of } M \,/\, \mathfrak{m}M \text{ over } R \,/\, \mathfrak{m}. \end{aligned}$$

The ommitted details are relatively simple to verify. □

4 Exact Sequences

4.1 Definition

A sequence of R-modules and R-homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots \tag{1}$$

is **exact** at M_i if $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$. The sequence is **exact** if it is exact at each M_i. Such sequences induce a wealth of identities relating the modules and their images, kernels, and cokernels. Three examples of exact sequences are as follows:

$$\begin{aligned}
0 \to M' \xrightarrow{f} M \text{ is exact} &\iff f \text{ is injective, so } M' \cong \operatorname{Im} f \\
M \xrightarrow{g} M'' \to 0 \text{ is exact} &\iff g \text{ is surjective, so } M \,/\, \operatorname{Ker} g \cong M'. \\
0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \text{ is exact} &\iff f \text{ is injective, } g \text{ is surjective, and} \\
&\qquad \operatorname{Coker} f = M \,/\, \operatorname{Ker} g \cong M'.
\end{aligned}$$

An exact sequence of this third type is called a **short exact sequence**. Any long exact sequence, like that in equation (1), can be broken into numerous short exact sequences:

$$0 \longrightarrow \operatorname{Coker} f_{i-1} \xrightarrow{f_i'} M_i \xrightarrow{f_{i+1}} \operatorname{Im} f_{i+1} \longrightarrow 0,$$

where f_i' is defined as $f_i'(x + \operatorname{Ker} f_i) = f_i(x)$. To save time, we will often write that $0 \to N_i \to M_i \to N_{i+1} \to 0$ for some modules N_i and N_{i+1} instead.

4.2 Exact Sequences of Homomorphisms

Theorem 13. *The sequence*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{2}$$

of R-modules and R-module homomorphisms is exact if and only if for all R-modules N, the sequence

$$0 \longrightarrow \operatorname{Hom}(M'', N) \xrightarrow{\bar{v}} \operatorname{Hom}(M, N) \xrightarrow{\bar{u}} \operatorname{Hom}(M', N) \tag{3}$$

is exact, where $\bar{u}$ and $\bar{v}$ are as in Section 1.3.

Proof. The exactness of (2) is equivalent to $\operatorname{Im} u = \operatorname{Ker} v$ and the surjectivity of v, while the exactness of (3) is equivalent to the injectivity of $\bar{v}$ and $\operatorname{Im} \bar{v} = \operatorname{Ker} \bar{u}$.

Claim 1. *v is surjective if and only if $\bar{v}$ is injective.*

Proof. Suppose that v is surjective, and suppose $f \in \operatorname{Ker} \bar{v}$ for any N. Then f is in $\operatorname{Hom}(M, M'')$ and

$$\bar{v}(f) = f \circ v = 0.$$

Since v is surjective, f must map the entirety of M to zero; thus $f = 0$, and $\bar{v}$ is injective.

Now, suppose that v is not surjective. Then set $N = M'' / \operatorname{Im} v$ and let $f \in \operatorname{Hom}(M'', N)$ be the canonical epimorphism; both are nonzero. Then

$$\bar{v}(f)(M) = (f \circ v)(M) = f(\operatorname{Im} v) = 0.$$

Then f is a nonzero element of $\operatorname{Ker} \bar{v}$, so $\bar{v}$ is not surjective.

The second claimed biconditional relation requires proof of the following claim.

Claim 2. $\operatorname{Im} u = \operatorname{Ker} v$ *for surjective v implies that* $\operatorname{Im} \bar{v} = \operatorname{Ker} \bar{u}$.

Proof. Suppose $\operatorname{Im} u = \operatorname{Ker} v$, so $v \circ u = 0$. Let $f \in \operatorname{Im} \bar{v}$; then there exists g such that $\bar{v}(g) = g \circ v = f$. We conclude that

$$\bar{u}(f) = f \circ u = g \circ v \circ u = g \circ 0 = 0,$$

so $f \in \operatorname{Ker} \bar{u}$. Now, suppose $f \in \operatorname{Ker} \bar{u}$, so $\bar{u}(f) = f \circ u = 0$. Since v is surjective, $m'' \in M''$ implies the existence of $m \in M$ such that $v(m) = m''$. Then define $g \in \operatorname{Hom}(M'', N)$ such that $g(m'') = f(m)$; it is relatively easy to demonstrate that g is well-defined and a homomorphism. Thus, $f = g(u) = \bar{u}(g)$, so $f \in \operatorname{Im} \bar{v}$, so $\operatorname{Im} \bar{v} = \operatorname{Ker} \bar{u}$.

If we suppose $\operatorname{Im} \bar{v} = \operatorname{Ker} \bar{u}$, then $\bar{u} \circ \bar{v} = 0$ — that is, $v \circ u \circ f = 0$ for all $f \in \operatorname{Hom}(M'', N)$. This is equivalent to $\operatorname{Im} u = \operatorname{Ker} v$ in the start of Claim 2, with some added work to demonstrate that $\operatorname{Im} u \supseteq \operatorname{Ker} v$. □

Really, the natural language for these proofs is Homosexual Algebra and Abelian categories. Thus we will state the lemmas from this chapter without proof.

The following theorem is asserted without proof, because I value my sanity.

Theorem 14. *The sequence*

$$0 \longrightarrow N' \xrightarrow{u} N \xrightarrow{v} N''$$

of R-modules and R-module homomorphisms is exact if and only if for all R-modules N, the sequence

$$0 \longrightarrow \mathrm{Hom}(M, N') \xrightarrow{\bar{u}} \mathrm{Hom}(M, N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N'')$$

is exact, where $\bar{u}$ and $\bar{v}$ are as in Section 1.3.

The following theorem is called the Snake Lemma, a special case of exact homology sequences in Homosexual Algebra:

Theorem 15 (Snake Lemma)**.** *Suppose that*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0 \end{array}$$

is a commutative diagram of R-modules and homomorphisms, with the rows exact. Then there exists an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(f') & \xrightarrow{\bar{u}} & \mathrm{Ker}(f) & \xrightarrow{\bar{v}} & \mathrm{Ker}(f'') & & \\ & & & & & \searrow^{d} & & & \\ & & & & \mathrm{Coker}(f') & \xrightarrow{\bar{u}'} & \mathrm{Coker}(f) & \xrightarrow{\bar{v}'} & \mathrm{Coker}(f'') \longrightarrow 0 \end{array}$$

in which $\bar{u}$ and $\bar{v}$ are restrictions of u and v, and in which $\bar{u}'$ and $\bar{v}'$ induced by u' and v'. The ***boundary homomorphism*** *d is defined in Atiyah-MacDonald page 23.*

We encourage the reader to adopt these results on faith. Homosexual Algebra is a complex subject of math that deserves its own set of notes.