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. $\square$

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:

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

The rest of the multiplicative module conditions follow from the ring axioms. $\square$

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. $\qquad\square$

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 a mapping $g : M \,/\, N \to \operatorname{Im} f$ 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. $\qquad\square$

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. $\qquad\square$

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

$$f(x_1 + x_2) = x_1 + x_2 + x_1 = (x_1 N)(x_2 N) = f(x_1)f(x_2)$$
$$f(ax_1) = ax_1 + x_1 = a(x_1 + x_1) = af(x_1).$$

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. $\qquad\square$

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 $M \,/\, N = (M \,/\, L) \,/\, (N \,/\, L)$. $\qquad\square$

The following theorem is intimately related to the Third Isomorphism Theroem. Suppose that $L \subseteq N \subseteq M$ are R-modules and $f : M \to L$, $g : M \to N$, and $f' : N \to L$ are epimorphisms such that $f = f' \circ g$.

Theorem 7. *Given any two of f, g, and g', the third epimorphism exists and is unique.*

Proof. The case where one is given g and f' is quite clear.

1. **Reconstructing g**: Suppose $f : M \to L$ and $f' : N \to L$ are given. Define the function $g : M \to N$ such that

$$g(n + L) = f(n).$$

$\qquad\square$

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 $a_1 x_1 + \cdots + a_n x_n$ 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 8. $(N : P)$ *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. $\qquad\square$

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 9. *If $M_1, M_2 \subseteq M$ are submodules, then $\operatorname{Ann}(M_1 + M_2) = \operatorname{Ann} M_1 \cap \operatorname{Ann} M_2$.*

Proof. Suppose $a \in \operatorname{Ann} M_1 \cap \operatorname{Ann} M_2$. Then a annihalates all $x_1 + x_2 \in M_1 + M_2$, so $a \in \operatorname{Ann}(M_1 + M_2)$.

Suppose $a \notin \operatorname{Ann} M_1 \cap \operatorname{Ann} M_2$. Then a 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 $ax_1 \neq 0$. Then as $ax_1 \in M_1 + M_2$, we find that $a \notin \operatorname{Ann}(M_1 + M_2)$. This completes the proof. $\quad\square$

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:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$a(x, y) = (ax, ay)$$

More generally, for a family of R-modules (M_α), we define their **direct sum** $\bigoplus_\alpha M_\alpha$ as the families (x_α) such that $x_\alpha \in M_\alpha$ for each α with the restriction that only finitely many x_α are nonzero.

If we allow infinitely many x_α to be nonzero, we attain the family's **direct product** $\prod_\alpha M_\alpha$. Direct sums and direct products are equivalent if there are finitely many α, but not otherwise.

2.4 Direct Sums on Rings

Direct products of rings and direct sums of ideals are equivalent notions:

1. Suppose that $R = R_1 \times \cdots \times R_n$. Then R has n ideals of the form $(\delta_{n,m})$ for each $m \in \{1, \ldots, n\}$. Viewing this relation in terms of modules,

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

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

2. Suppose that $R = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$, where $\mathfrak{a}_i \subseteq R$ are ideals. Defining $\mathfrak{b}_i = \bigoplus_{j \neq i} \mathfrak{a}_j$ for each i, we find that
$$R \cong (R / \mathfrak{b}_1) \times \cdots \times (R / \mathfrak{b}_n)$$
   by $f(a_1, \ldots, a_n) = (a_1 + \mathfrak{b}_1, \ldots, a_n + \mathfrak{b}_n)$. Each $\mathfrak{a}_i$ is a ring isomorphic to $R / \mathfrak{b}_i$.

This illustrates how one may define a direct sum of ideals.

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 $M = Rx_1 + \cdots + Rx_n$. The R-module $R \oplus \cdots \oplus R$ is denoted by R^n.

Theorem 10. *M is finitely-generated by n elements if and only if M is isomorphic to a quotient of R^n.*

Proof. Suppose M is finitely-generated by $x_1, \ldots, x_n$. Define a mapping $f : R^n \to M$ by $f(a_1, \ldots, a_n) = a_1 x_1 + \cdots + a_n x_n$. Then for all $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in R^n$, we have

$$
\begin{aligned}
f(a_1 + b_1, \ldots, a_n + b_n) &= (a_1 + b_1)x_1 + \cdots + (a_n + b_n)x_n \\
&= (a_1 x_1 + \cdots + a_n x_n) + (b_1 x_1 + \cdots + b_n x_n) \\
&= f(a_1, \ldots, a_n) + f(s_1, \ldots, s_n),
\end{aligned}
$$

and for all $(a_1, \ldots, a_n) \in R^n$ and $b \in R$, we have

$$f(ba_1, \ldots, ba_n) = ba_1 x_1 + \cdots + ba_n x_n = b f(a_1, \ldots, a_n).$$

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

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

Suppose that $R^n / \mathfrak{a} \cong M$ by an isomorphism f. Two definitions are in order:

1. Let $g : R^n \to R^n / \mathfrak{a}$ be the canonical epimorphism. Then the composition $f \circ g$ is a surjective R-module homomorphism.

2. For each $(\delta_{mi}) \in R^n$, Let $x_i = (f \circ g)(\delta_{mi})$ across each $i \in \{1, \ldots, n\}$. We claim that the x_i generate M.

From the surjectivity of $f \circ g$, all $x \in M$, there exists $r = (r_1, \ldots, r_n) \in R^n$ such that $(f \circ g)(r) = x$. Therefore

$$
\begin{aligned}
x &= (f \circ g)(r_1, \ldots, r_n) \\
&= (f \circ g)(r_1 \delta_{m1}) + \cdots + (f \circ g)(r_n \phi_{mn}) \\
&= r_1 (f \circ g)(\delta_{m1}) + \cdots + r_n (f \circ g)(\delta_{mn}) \\
&= r_1 x_1 + \cdots r_n x_n.
\end{aligned}
$$

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

The following proof is a transcription from Atiyah-MacDonald:

Theorem 11. *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 $f(M) \subset \mathfrak{a}M$. Then f satisfies an equation of the form*

$$f^n + a_{n-1} f^{n-1} + \cdots + a_0 f^0 = 0,$$

where each a_i lies 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 $a_{ij} \in \mathfrak{a}$ for $i, j \in \{1, \ldots, n\}$ by $f(x_i) = \sum_{j=1}^{n} a_{ij} x_j$. This equation may be equivalently written for each $i \in \{1, \ldots, n\}$ as

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

By multiplying the left by the adjoint of the matrix $\delta_{ij} f - a_{ij} f^0$, it follows that the determinant of $\delta_{ij} f - a_{ij} f^0$ annihilates each x_{ij} — hence it is the zero endomorphism. Expanding out the determinant yields an equation of the required form. $\qquad\square$

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

Proof. Consider Theorem 7 under the identity transformation f. Then there exist $a_{n-1}, \ldots, a_0 \in \mathfrak{a}$ such that

$$
\begin{aligned}
0 &= f^n + a_{n-1}f^{n-1} + \cdots + a_0 f^0 \\
&= f + a_{n-1}f + \cdots + a_0 f \\
&= (1 + a_{n-1} + \cdots + a_0)f.
\end{aligned}
$$

Setting $a = 1 + a_{n-1} + \cdots + a_0$ yields that af is the zero endomorphism, so $af(x) = ax = 0$ for each $x \in M$. We conclude that $a \in \operatorname{Ann} M$. $\qquad\square$

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.

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 $\mathfrak{a}M = M$ implies $M = 0$.*

Proof. By Corollary 1, there exists $a \in (1 + \mathfrak{J})$ such that $a \in \operatorname{Ann} M$. By the properties of the Jacobson radical, a is a unit. Hence,

$$
M = (a^{-1}a)M = a^{-1}(aM) = a^{-1}(0) = 0,
$$

which completes the proof. $\qquad\square$

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 $x_n \in \mathfrak{a}M$, so x_n satisfies an equation of the form

$$
x_n = a_1 x_1 + \cdots + a_n x_n
$$

for $a_1, \ldots, a_n \in \mathfrak{a}$. Since none of these scalars are 1, we have

$$
(1 - a_n)x_n = a_1 x_1 + \cdots + a_{n-1}x_{n-1}.
$$

Since $a_n \in \mathfrak{J}$, the element $(1 - a_n)$ is a unit. Thus $x_1, \ldots, x_{n-1}$ generate M, which yields the desired contradiction. $\qquad\square$

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

Proof. Suppose that $M = \mathfrak{a}M + N$. Then

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

Thus applying Nakayama's Lemma to $M \,/\, N$, we have $M \,/\, N = 0$; hence $M = N$. □

3.3 Relation to Local Rings

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

Theorem 12. *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

$$f(a_1 x_1 + \cdots + a_n x_n + \mathfrak{m}M) = (a_1 + \mathfrak{m})x_1 + \cdots + (a_n + \mathfrak{m})x_n$$

is bijective. It further satisfies $f(x+y) = f(x) + f(y)$ and $f(ax) = bf(x)$, where b is the image of a 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 13. *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

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

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 $\mathrm{Im}\, f_i = \mathrm{Ker}\, f_{i+1}$. 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:

$$0 \to M' \xrightarrow{f} M \text{ is exact} \iff f \text{ is injective, so } M' \cong \mathrm{Im}\, f$$

$$M \xrightarrow{g} M'' \to 0 \text{ is exact} \iff g \text{ is surjective, so } M\,/\,\mathrm{Ker}\, g \cong M'.$$

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \text{ is exact} \iff f \text{ is injective, } g \text{ is surjective, and}$$
$$\mathrm{Coker}\, f = M\,/\,\mathrm{Ker}\, g \cong M'.$$

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:

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

where f_i' is defined as $f_i'(x + \mathrm{Ker}\, f_i) = f_i(x)$. 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

Theorem 14. *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

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

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 $\operatorname{Im} u \supseteq \operatorname{Ker} v$. $\qquad\square$

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 15. *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 16 (Snake Lemma)**.** *Suppose that*

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

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

$$0 \longrightarrow \mathrm{Ker}(f') \xrightarrow{\bar{u}} \mathrm{Ker}(f) \xrightarrow{\bar{v}} \mathrm{Ker}(f'')$$

$$\xrightarrow{d}$$

$$\mathrm{Coker}(f') \xrightarrow{\bar{u}'} \mathrm{Coker}(f) \xrightarrow{\bar{v}'} \mathrm{Coker}(f'') \longrightarrow 0$$

*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.

Theorem 17. *Let $0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$ be an exact sequence of R modules in which all the modules M_i and the kernels of all the homomorphisms belong to C. Then for any additive function ϕ on C, we have*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

16

5   Tensor Products of Modules

Let M, N, P be R-modules. A mapping $f : M \times N \to P$ is **R-bilinear** if each component is R-linear: for each $x \in M$, the mapping $y \mapsto f(x, y)$ is R-linear, and if for each $y \in M$, the mapping $x \mapsto f(x, y)$ is R-linear.

Our goal is to construct a module T such that the R-bilinear mappings $M \times N \to P$ are in natural one-to-one correspondence with the R-linear mappings $T \to P$ for all P. This module is called the **tensor product** of M and N.

Theorem 18. *Let N, N be R-modules. Then there exists a pair (T, g) consisting of an R-module T and an R-bilinear mapping $g : M \times N \to T$ with the following property:*

For all R-modules P and R-bilinear mappings $f : M \times N \to P$, there exists a unique R-linear mapping $f' : T \to P$ such that $f = f' \circ g$.

Moreover, if (T, g) and (T, g') are two pairs with this property, there exists an isomorphism $j : T \to T'$ such that $j \circ g = g'$.

Proof. The key is to take a special quotient of $M \times N$.

1. **Existence**: Let C denote $R^{(M \times N)}$: the formal combination of elements of $M \times N$ with coefficents in R. Let D be the submodule *generated* by all elements of the form:

$$(x + x', y) - (x, y) - (x', y)$$
$$(x, y + y') - (x, y) - (x, y')$$
$$(ax, y) - a(x, y)$$
$$(x, ay) - a(x, y).$$

Let $T = C / D$, and denote the image of (x, y) in the quotient by $x \otimes y$. The quotient of the above ensures the desired properties of the tensor product:

$$(x + x') \otimes y = x \otimes y + x' \otimes y$$
$$x \otimes (y + y') = x \otimes y + x \otimes y'$$
$$a(x \otimes y) = (ax) \otimes y = x \otimes (ay).$$

Equivalently, the mapping $g : M \times N \to T$ defined by $g(x, y) = x \otimes y$ is R-bilinear. Now, suppose $f : M \times N \to P$ is R-bilinear; this extends by linearity to a mapping $\bar{f} : C \to P$. Since $\bar{f}$ is R-bilinear, it annihilates each generator of D — so by

17

extension, the entirety of D. The Third Isomorphism Theorem thus guarantees the existence of a unique mapping $\bar{f}' : \mathrm{Ker}\,\bar{f} \to D$ such that

$$f = f' \circ g.$$

2. **Uniqueness**:

$\square$